Tenable Security Center Version 6.5.x API Guide

Last Revised: November 25, 2024

Table of Contents

Tenable Security Center API: Changelog

-

Version 6.5.x

Tenable Security Center 6.5.x API includes updates for the following endpoints:

For SC / SCI node:

- WAS Scanner:
  - Added /wasScanner::GET endpoint
  - Added /wasScanner/{id}::GET endpoint
  - Added /wasScanner/{id}::PATCH endpoint
  - Added /wasScanner/{id}::DELETE endpoint
- Sensor Proxy:
  - Added /sensor-proxy::GET endpoint
  - Added /sensor-proxy/{id}::GET endpoint
  - Added /sensor-proxy/{id}::PATCH endpoint
  - Added /sensor-proxy/{id}::DELETE endpoint
  - Added /sensor-proxy/search::POST endpoint
- Scan Zone:

  Added type as returning field.
- System:
  - Added postgresConnStatus, postgresConnectionType, postgresDsn, VulnerabilityIntelligenceEnabled to /system endpoint.
  - Added postgresConnStatusto /system/diagnostics endpoint.

Version 6.4.5

Tenable Security Center 6.4.5 API includes updates for the following endpoints:

For Tenable Enclave Security:

- TES User Permissions:

  Added new /tes/userPermissions endpoint.

- TES Admin Roles:

  Added new /tes/role/admin endpoint.

- System:

  Added new /tes/system/debug endpoint.

- Role:

  Added new /tes/role and /tes/role/{id} endpoints.

- Group:

  Added new /tes/group endpoint.

- User:

  Added new /tes/user endpoint.

- Current Organization:

  Added new /tes/currentOrganization endpoint

- Configuration:

  Added new /tes/config/license/register endpoint.

Version 6.4.x

Tenable Security Center 6.4.x API includes updates for the following endpoints:

For SC / SCI node:

- Hosts:

  Modified /hosts::GET

  - Added systemType as returning field.

  Modified /hosts/search::POST

  - Added systemType as a searchable field.

- Role:

  Updated the documentation to include the missing permissions as fields for request and in the responseModified /policy::GET

Version 6.3.x

Tenable Security Center 6.3.x API includes updates for the following endpoints:

For SC / SCI node:

- Accept Risk Rule:

  Modified /acceptRiskRule::POST

  Added the allowed entries for the hostType field for each repository type:

  - Universal: All Available Devices, Asset, Host IDs.
  - Agent: All Available Devices, Asset, Agent IDs.
  - IPv4: All Available Devices, Asset, IPs.
  - IPv6: All Available Devices, Asset, IPs.

  Modified /acceptRiskRule::GET

  - Implemented pagination support that returns a limited number of results instead of all results when the **paginated=true** parameter is included in the request. This functionality is accompanied by support for parameters such as **startOffset**, **endOffset**, **sortField**, and **sortDirection**.

- Recast Risk Rule:

  Modified /recastRiskRule::GET

  Added the allowed entries for the hostType field for each repository type:

  - Universal: All Available Devices, Asset, Host IDs.
  - Agent: All Available Devices, Asset, Agent IDs.

- IPv4: All Available Devices, Asset, IPs.
- IPv6: All Available Devices, Asset, IPs.

Modified /recastRiskRule::GET

- Implemented pagination support that returns a limited number of results instead of all results when the **paginated=true** parameter is included in the request. This functionality is accompanied by support for parameters such as **startOffset**, **endOffset**, **sortField**, and **sortDirection**.

- Report:

  Modified /report::GET

  - Implemented pagination support that returns a limited number of results instead of all results when the **paginated=true** parameter is included in the request. This feature is accompanied by support for parameters like **startOffset**, **endOffset**, **sortField**, and **sortDirection**. Furthermore, filtration parameters such as **name**, **owner**, **status**, **startTime**, and **endTime** are now also supported.

- Scan Policy:

  Modified /policy::GET

  - Implemented pagination support, which returns a limited number of results when the paginated=true parameter is included in the request. The supported parameters include **startOffset**, **endOffset**, **sortField**, and **sortDirection**. Additionally, support has been added for filtration parameters such as **name**, **owner**, **policyTemplate**, **groupID**, and **tags**.

- User:

  Modified /user::GET

  - Implemented pagination support that returns a limited number of results when the paginated=true parameter is included in the request. This feature is accompanied by

support for parameters like **startOffset**, **endOffset**, **sortField**, and **sortDirection**. Additionally, support has been added for the following filtration parameters: **firstname**, **lastname**, **username**, **lastLoginTimeFrame**, **lastLoginStartTime**, **lastLoginEndTime**, **locked**, **groupID**, **authType**, **roleID**, **title**, **email**, **address**, **state**, **country**, **phone**, **fax**, and **name**.

Version 6.2.x

Tenable Security Center 6.2.x API includes updates for the following endpoints:

For SC / SCI node:

- Group:

  Modified /group::GET and /group/::GET

  - The response fields list is now modified to match the FE behavior and to follow the objectives of roles and permissions.

- Hosts:

  Modified /hosts/search::POST.

  - Added an example of the new **sourceType** filter to the example request payload. The endpoint now allows users to filter on source type. (e.g., Nessus Scan, Agent Scan, Web App Scan, NNM, LCE)
  - Added an example of the new **hostid** filter to the example request payload. The endpoint now allows users to filter on host UUIDs.

- Repository:

  Added **/repository/{repID}/attachment/{attachmentID}::GET**.

  - Added a new API to get an attachment for the attachment ID and repository ID or UUID provided. The downloaded file is returned.

- Role:

  Modified /role::GET and /role/::GET

  - The response fields list is now modified to match the FE behavior and to follow the objectives of roles and permissions.

- Scan:

Modified /scan::GET, /scan/::GET, /scan::POST, and /scan/::PATCH

- Added new field **inactivityTimeout**. Allows user to customize the timeout to wait before switching scanner (or mark as partial if no more scanners) if the scanner response is not obtained due to a scan involving a long running plugin. Allowed values are 1 to 120 hrs. Default value is 12hrs.

- Scanner:

  Modified **/scanner::GET**, **/scanner/::GET**, and **/scanner::POST**.

  - Added support for the new field **wasCapable** that identifies if a scanner is WAS capable or not. The /scanner::POST endpoint allows **wasCapable** to be set to **true** or **false**. The /scanner::GET and /scanner/::GET endpoints return the value of the **wasCapable** field.

- Scan Policy:

  Modified /policy::GET, /policy/::GET, /policy::POST, /policy//copy::POST, and /policy//share::POST

  - Added support for the new field **isWas** that identifies a policy template as a WAS policy template. The value is returned in the response payload from the listed endpoints as part of the **policyTemplate** object.

- Scan Policy Template:

  Modified /policyTemplate::GET and /policyTemplate/::GET.

  - Added support for the new field **isWas** that identifies a policy template as a WAS policy template. Valid values are **true** or **false**.

- Scan Result:

  Added **/scanResult/{resultID}/attachment/{attachmentID}::GET**.

  - Added a new API to get an attachment for the attachment ID and scan result ID provided. The downloaded file is returned.

- Software Update:

Added /softwareUpdate::GET.

- Added a new API to get the list of Software Updates for the current version of Security Center.

Added /softwareUpdate::PATCH.

- Added a new API that for a provided list of Software Update IDs sets to status to be ready to install. Use this to stage Software Updates for installation. The Software Updates are installed during the next system restart.

- System:

  Modified **/system/logs::POST**.

  - Added a new field **scrollModel** to the request payload that can have the values **virtual** or **paged** with **virtual** being the default. **virtual** is the scroll model used in the old UI where **paged** is the model used in the updated UI.

  Added **/system/logs/modules::GET**.

  - This endpoint returns a collection of all of the module names that can be found in the system log.

- Ticket:

  Modified /ticket/{id}::PATCH.

  - When the status of a ticket is changed to **closed**, all queries associated with the ticket are deleted.

- User:

  Modified /user::GET and /user/::GET

  - The response fields list is now modified to match the FE behavior and to follow the objectives of roles and permissions.

- WAS Scan:

Added new WAS Scan endpoints /wasScan::GET, /wasScan/::GET, /wasScan::POST, /wasScan/::PATCH, /wasScan/::DELETE, /wasScan//copy::POST, and /wasScan//launch::POST.

- Respectively these endpoints allow users to get all WAS Scans, get an individual WAS Scan, add a WAS Scan, edit a WAS Scan, delete a WAS Scan, copy a WAS Scan, and launch a WAS Scan. There is a new field **urlList** for providing a single URL target (e.g. “http://example.com“).

Version 6.1.x

Tenable Security Center 6.1.x API includes updates for the following endpoints:

For SC / SCI node:

- Bulk:

  Modified **/bulk::POST**.

  - Added a new bulk action, /hosts/acr::PATCH.

- Lumin:

  Modified **/lumin/repositories::PATCH**.

  - Removed the note that only IPv4 and Agent repositories are supported. Now IPv4, IPv6, Agent, and Universal repositories are supported.

- System:

  Modified **/system::GET**.

  - Added "riskRuleCommentsEnabled" to the response.

- Scan Policy:

  Modified **/policy::POST**.

  - Added "state" parameter for each family for the POST request.
  - Added "state" and "type" to each family in the POST response.

  Modified **/policy/uuid::GET and /policy/id::GET**.

  - Added "state" and "type" for each family in the response.

- User:

  Modified **/user::GET**.

- Added a note that as an admin user if the orgID field provided, the fields parameters are not supported, and added an Example Response for that case.

Modified **/user/::GET**.

- Added Request User Parameters for using the orgID field as an admin user.

Version 6.0.x

Tenable Security Center 6.0.x API includes updates for the following endpoints:

For Director:

- Director Scan Result:

  Modified **/mgmt/scanResult::GET**.

  - Returns the "type" and "dataFormat" fields in the "repository" field.

For SC / SCI node:

- Current User:

  Modified **/currentUser::GET**.

  - Added the following field parameters related to the Password Expiration feature: passwordExpires, passwordExpiration, passwordExpirationOverride, passwordSetDate.
  - Fields returned related to the new Password Expiration feature: passwordExpires, passwordExpiration, passwordExpirationOverride, passwordSetDate.

- Device Information:

  Modified **/deviceInfo::GET**.

  - Can accept a "hostUUID" field in place of the other, available fields.

- Organization:

  Modified **/organization::GET**.

  - Added the following field parameters related to the Password Expiration feature: passwordExpires, passwordExpiration.

- Fields returned related to the new Password Expiration feature: passwordExpires, passwordExpiration.

Modified **/organization::POST**.

- Added the following field parameters related to the Password Expiration feature: passwordExpires, passwordExpiration.
- Fields returned related to the new Password Expiration feature: passwordExpires, passwordExpiration.

Modified **/organization::PATCH**.

- Added the following field parameters related to the Password Expiration feature: passwordExpires, passwordExpiration.
- Fields returned related to the new Password Expiration feature: passwordExpires, passwordExpiration.

- Organization Security Manager:

  Modified **/organization/{orgID}/securityManager::GET, /organization/{orgUUID}/securityManager::GET**.

  - Added the following field parameters related to the Password Expiration feature: passwordExpires, passwordExpiration, passwordExpirationOverride, passwordSetDate.
  - Fields returned related to the new Password Expiration feature: passwordExpires, passwordExpiration, passwordExpirationOverride, passwordSetDate.

  Modified **/organization/{orgID}/securityManager::POST, /organization/{orgUUID}/securityManager::POST**.

  - Added the following field parameters related to the new Password Expiration feature: passwordExpires, passwordExpiration, passwordExpirationOverride.

- Fields returned related to the new Password Expiration feature: passwordExpires, passwordExpiration, passwordExpirationOverride, passwordSetDate.

Modified **/organization/{orgID}/securityManager::PATCH, /organization/{orgUUID}/securityManager::PATCH**.

- Added the following field parameters related to the new Password Expiration feature: passwordExpires, passwordExpiration, passwordExpirationOverride.
- Fields returned related to the new Password Expiration feature: passwordExpires, passwordExpiration, passwordExpirationOverride, passwordSetDate.

- Repository:

  Modified **/repository/assetIntersections::GET**.

  - Can accept a "hostUUID" field in place of the other, available fields.

  Modified **/repository/deviceInfo::GET**.

  - Can accept a "hostUUID" field in place of the other, available fields.

- Scan

  Modified **/scan::GET**.

  - Returns a "dataFormat" field in the "repository" field.

  Modified **/scan::POST**.

  - Returns a "dataFormat" field in the "repository" field.

  Modified **/scan::PATCH**.

  - Returns a "dataFormat" field in the "repository" field.

  Modified **/scan/copy::POST**.

  - Returns a "dataFormat" field in the "repository" field.

- Scan Result

Modified **/scanResult::GET**.

- Returns a "dataFormat" field "repository" field.

Modified **/scanResult/pause::POST**.

- Returns a "dataFormat" field in the "repository" field.

Modified **/scanResult/resume::POST**.

- Returns a "dataFormat" field "repository" field.

Modified **/scan/stop::POST**.

- Returns a "dataFormat" field in the "repository" field.

- System

  Added **/system/fips::GET**.

  - Returns status of FIPS in Tenable.sc.

  Added **/system/fips::POST**.

  - Updates the status of FIPS in Tenable.sc.

- User

  Modified **/user::GET**.

  - Added the following field parameters related to the Password Expiration feature: passwordExpires, passwordExpiration, passwordExpirationOverride, passwordSetDate.
  - Fields returned related to the new Password Expiration feature: passwordExpires, passwordExpiration, passwordExpirationOverride, passwordSetDate.

  Modified **/user::POST**.

  - Added the following field parameters related to the new Password Expiration feature: passwordExpires, passwordExpiration, passwordExpirationOverride.

- Fields returned related to the new Password Expiration feature: passwordExpires, passwordExpiration, passwordExpirationOverride, passwordSetDate.

Modified **/user::PATCH**.

- Added the following field parameters related to the new Password Expiration feature: passwordExpires, passwordExpiration, passwordExpirationOverride.
- Fields returned related to the new Password Expiration feature: passwordExpires, passwordExpiration, passwordExpirationOverride, passwordSetDate.

Version 5.23.x

Tenable.sc 5.23.x API includes updates for the following endpoints:

- Hosts
  - Added **/hosts/download::POST** endpoint for exporting Host Assets.
- Vulnerability Routing Rule
  - Added **/vulnRoutingRule::POST** endpoint for creating a Vuln Routing Rule. Added **/vulRoutingRule::GET** for getting all Vuln Routing Rules or an individual Vuln Routing Rule by **id**. Added **/vulnRoutingRule::PATCH** for editing a Vuln Routing Rule by id. Added **/vulnRoutingRule::DELETE** for deleting a Vuln Routing Rule by **id**.
- Vulnerability Routing Summary
  - Added **/vulnRoutingSummary::GET** endpoint for getting the list of Users with explicitly routed Vulns. Added **/vulnRoutingSummary/{userID}::GET** endpoint for getting the Vuln Routing Rules details for the User associated with the provided **userID**.

Version 5.22.x

Tenable.sc 5.22.x API includes updates for the following endpoints:

- Publishing Site
    - The ability to use a configured proxy for a publishing site was added. A checkbox was added to the Publishing Site configuration page to enable and disable the use of a proxy. The useProxy field was added to GET, POST, and PATCH requests.
- Hosts
    - Added **aes** as a valid field for the /hosts::GET endpoint (used to retrieve a list of hosts). This returns the Asset Exposure Score in the response.
- System
    - The "version" parameter for the /system::GET endpoint will only show if the user is authenticated.
- Scanner
    - Added "statusMessage" as a valid field for /scanner::GET and /scanner/{id}::GET. This returns an additional message based on the current status (Mostly will be used if a scanner is in an error state).
    - Added "apiKeys" as an option for authType. This allows users to add scanners to Tenable.sc using API Keys as its main authentication.

Version 5.21.x

Tenable.sc 5.21.x API includes updates for the following endpoints:

- Director Repository
  - Added a new Director endpoint /mgmt/repository::GET for getting all repositories or getting repositories by id, uuid, or SCI ID.
- Director User
  - Added a new Director endpoint /mgmt/user::GET for getting all users or getting users by id, uuid, organization ID, or SCI ID.
- Director Scan Policy
  - Added a new Director endpoint /mgmt/policy::GET for getting all policies or getting policies by id, uuid, or SCI ID.
  - Added a new Director endpoint /mgmt/policy::POST for creating a new policy.
  - Added a new Director endpoint /mgmt/policy::DELETE for deleting a policy by id or uuid.
- Director Scan
  - Added a new Director endpoint /mgmt/user::GET for getting all users or getting users by id, uuid, organization ID, or SCI ID.
- Accept Risk Rule
  - Modified /acceptRiskRule::GET
    - Returns a "uuid" field, in addition to the "id" field, in the "hostValue" field if the "hostType" is "asset", and the asset list is part of your organization context.
    - Returns a "uuid" field, in addition to the "id" field, in the "repository", "organization", and "user" fields.
    - Returns a "type" field in the "repository" and "plugin" fields.

- Modified /acceptRiskRule::POST
    - Returns a "uuid" field, in addition to the "id" field, in the "hostValue" field if the "hostType" is "asset", and the asset list is part of your organization context.
    - Returns a "uuid" field, in addition to the "id" field, in the "repository", "organization", and "user" fields.
    - Returns a "type" field in the "repository" and "plugin" fields.

- Agent Results Sync
    - Modified /agentResultsSync::GET
        - Returns a "uuid" field, in addition to the "id" field, in the "repository", "creator" and "owner" fields.
        - Returns a "type" field in the "repository" field.
    - Modified /agentResultsSync::POST
        - Returns a "uuid" field, in addition to the "id" field, in the "repository", "creator" and "owner" fields.
        - Returns a "type" field in the "repository" field.
    - Modified /agentResultsSync::PATCH
        - Returns a "uuid" field, in addition to the "id" field, in the "repository", "creator" and "owner" fields.
        - Returns a "type" field in the "repository" field.
    - Modified /agentResultsSync/copy::POST
        - Returns a "uuid" field, in addition to the "id" field, in the "repository", "creator" and "owner" fields.
        - Returns a "type" field in the "repository" field.

- Alert

- Modified /alert::GET
    - Returns a "uuid" field, in addition to the "id" field, in the "action → definition → scan", "action → definition → assignee", "action → definition → users" and "action → users" fields.
    - Returns a "type" field in the "action → definition → scan" field.
- Modified /alert::POST
    - Returns a "uuid" field, in addition to the "id" field, in the "action → definition → scan", "action → definition → assignee", "action → definition → users" and "action → users" fields.
    - Returns a "type" field in the "action → definition → scan" field.
- Modified /alert::PATCH
    - Returns a "uuid" field, in addition to the "id" field, in the "action → definition → scan", "action → definition → assignee", "action → definition → users" and "action → users" fields.
    - Returns a "type" field in the "action → definition → scan" field.
- Modified /alert/execute::POST
    - Returns a "uuid" field, in addition to the "id" field, in the "action → definition → scan", "action → definition → assignee", "action → definition → users" and "action → users" fields.
    - Returns a "type" field in the "action → definition → scan" field.

- ARC
    - Modified /arc::GET
        - Returns a "uuid" field, in addition to the "id" field, in the "policyStatements → baseFilters → value", "policyStatements → compliantFilters → value" and

"policyStatements → drilldownFilters → value" fields if the filter is a type of asset list, audit file, policy, repository or user, whether it is a single record or multiple records.

- Returns a "uuid" field, in addition to the "id" field, in the "policyStatements → baseFilters → value", "policyStatements → compliantFilters → value" and "policyStatements → drilldownFilters → value" fields if the filter is a combination of assets and they are not, themselves, a combination record.
- Returns a "uuid" field, in addition to the "id" field, in the "creator" and "owner" fields.
- Returns a "type" field in the "policyStatements → baseFilters → value", "policyStatements → compliantFilters → value" and "policyStatements → drilldownFilters → value" fields if the filter (name) is "repository" or "auditFile."

- Modified /arc::POST
  - Returns a "uuid" field, in addition to the "id" field, in the "policyStatements → baseFilters → value", "policyStatements → compliantFilters → value" and "policyStatements → drilldownFilters → value" fields if the filter is a type of asset list, audit file, policy, repository or user, whether it is a single record or multiple records.
  - Returns a "uuid" field, in addition to the "id" field, in the "policyStatements → baseFilters → value", "policyStatements → compliantFilters → value" and "policyStatements → drilldownFilters → value" fields if the filter is a combination of assets and they are not, themselves, a combination record.
  - Returns a "uuid" field, in addition to the "id" field, in the "creator" and "owner" fields.
  - Returns a "type" field in the "policyStatements → baseFilters → value", "policyStatements → compliantFilters → value" and "policyStatements → drilldownFilters → value" fields if the filter (name) is "repository" or "auditFile."
- Modified /arc::PATCH.

- Returns a "uuid" field, in addition to the "id" field, in the "policyStatements → baseFilters → value", "policyStatements → compliantFilters → value" and "policyStatements → drilldownFilters → value" fields if the filter is a type of asset list, audit file, policy, repository or user, whether it is a single record or multiple records.
- Returns a "uuid" field, in addition to the "id" field, in the "policyStatements → baseFilters → value", "policyStatements → compliantFilters → value" and "policyStatements → drilldownFilters → value" fields if the filter is a combination of assets and they are not, themselves, a combination record.
- Returns a "uuid" field, in addition to the "id" field, in the "creator" and "owner" fields.
- Returns a "type" field in the "policyStatements → baseFilters → value", "policyStatements → compliantFilters → value" and "policyStatements → drilldownFilters → value" fields if the filter (name) is "repository" or "auditFile."

- Modified /arc/import::POST
  - Returns a "uuid" field, in addition to the "id" field, in the "policyStatements → baseFilters → value", "policyStatements → compliantFilters → value" and "policyStatements → drilldownFilters → value" fields if the filter is a type of asset list, audit file, policy, repository or user, whether it is a single record or multiple records.
  - Returns a "uuid" field, in addition to the "id" field, in the "policyStatements → baseFilters → value", "policyStatements → compliantFilters → value" and "policyStatements → drilldownFilters → value" fields if the filter is a combination of assets and they are not, themselves, a combination record.
  - Returns a "uuid" field, in addition to the "id" field, in the "creator" and "owner" fields.
  - Returns a "type" field in the "policyStatements → baseFilters → value",

"policyStatements → compliantFilters → value" and "policyStatements → drilldownFilters → value" fields if the filter (name) is "repository" or "auditFile."

- Modified /arc/copy::POST
    - Returns a "uuid" field, in addition to the "id" field, in the "policyStatements → baseFilters → value", "policyStatements → compliantFilters → value" and "policyStatements → drilldownFilters → value" fields if the filter is a type of asset list, audit file, policy, repository or user, whether it is a single record or multiple records.
    - Returns a "uuid" field, in addition to the "id" field, in the "policyStatements → baseFilters → value", "policyStatements → compliantFilters → value" and "policyStatements → drilldownFilters → value" fields if the filter is a combination of assets and they are not, themselves, a combination record.
    - Returns a "uuid" field, in addition to the "id" field, in the "creator" and "owner" fields.
    - Returns a "type" field in the "policyStatements → baseFilters → value", "policyStatements → compliantFilters → value" and "policyStatements → drilldownFilters → value" fields if the filter (name) is "repository" or "auditFile."
- Modified /arc/refresh::POST
    - Returns a "uuid" field, in addition to the "id" field, in the "policyStatements → baseFilters → value", "policyStatements → compliantFilters → value" and "policyStatements → drilldownFilters → value" fields if the filter is a type of asset list, audit file, policy, repository or user, whether it is a single record or multiple records.
    - Returns a "uuid" field, in addition to the "id" field, in the "policyStatements → baseFilters → value", "policyStatements → compliantFilters → value" and "policyStatements → drilldownFilters → value" fields if the filter is a combination of assets and they are not, themselves, a combination record.

- Returns a "uuid" field, in addition to the "id" field, in the "creator" and "owner" fields.
- Returns a "type" field in the "policyStatements → baseFilters → value", "policyStatements → compliantFilters → value" and "policyStatements → drilldownFilters → value" fields if the filter (name) is "repository" or "auditFile."

- Modified /arc/share::POST
  - Returns a "uuid" field, in addition to the "id" field, in the "policyStatements → baseFilters → value", "policyStatements → compliantFilters → value" and "policyStatements → drilldownFilters → value" fields if the filter is a type of asset list, audit file, policy, repository or user, whether it is a single record or multiple records.
  - Returns a "uuid" field, in addition to the "id" field, in the "policyStatements → baseFilters → value", "policyStatements → compliantFilters → value" and "policyStatements → drilldownFilters → value" fields if the filter is a combination of assets and they are not, themselves, a combination record.
  - Returns a "uuid" field, in addition to the "id" field, in the "creator" and "owner" fields.
  - Returns a "type" field in the "policyStatements → baseFilters → value", "policyStatements → compliantFilters → value" and "policyStatements → drilldownFilters → value" fields if the filter (name) is "repository" or "auditFile."

- Asset
  - Modified /asset::GET
    - Can accept the asset list resource UUID in place of the asset list ID.
    - Can accept an "orgUUID" parameter in place of the "orgID" parameter when getting a single asset while logged in as an administrator.
    - Returns a "uuid" field, in addition to the "id" field, for the resource.

- Returns a "uuid" field, in addition to the "id" field, in the "operand1" and "operand2" fields if they are not a combination record.
- Returns a "uuid" field, in addition to the "id" field, in the "repositories → repository", "viewableIPs → repository", "creator" and "owner" fields.
- Returns a "uuid" field, in addition to the "id" field, in the "organization" field, while logged in as an administrator and viewing "Full Access" Group (#0) asset lists.
- Returns a "type" field in the "repositories → repository" and "viewableIPs → repository" fields.

- Modified /asset::POST
  - Can accept a UUID record, instead of an ID record, as "operand1" and "operand2" when defining a combination list.
  - Returns a "uuid" field, in addition to the "id" field, for the resource.
  - Returns a "uuid" field, in addition to the "id" field, in the "operand1" and "operand2" fields if they are not a combination record.
  - Returns a "uuid" field, in addition to the "id" field, in the "repositories → repository", "creator" and "owner" fields.
  - Returns a "type" field in the "repositories → repository" and "viewableIPs → repository" fields.
- Modified /asset::PATCH
  - Can accept the asset list resource UUID in place of the asset list ID.
  - Can accept a UUID record, instead of an ID record, as "operand1" and "operand2" when defining a combination list.
  - Returns a "uuid" field, in addition to the "id" field, for the resource.

        - Returns a "uuid" field, in addition to the "id" field, in the "operand1" and "operand2" fields if they are not a combination record.
        - Returns a "uuid" field, in addition to the "id" field, in the "repositories → repository", "viewableIPs → repository", "creator" and "owner" fields.
        - Returns a "type" field in the "repositories → repository" and "viewableIPs → repository" fields.
    - Modified /asset::DELETE
        - Can accept the asset list resource UUID in place of the asset list ID.
    - Modified /asset/export::GET
        - Can accept the asset list resource UUID in place of the asset list ID.
    - Modified /asset/refresh::POST
        - Can accept the asset list resource UUID in place of the asset list ID.
        - Can accept an "orgUUID" parameter in place of the "orgID" parameter.
        - Can accept a "repUUIDs" parameter in place of the "repIDs" parameter.
    - Modified /asset/share::POST
        - Can accept the asset list resource UUID in place of the asset list ID.
        - Returns a "uuid" field, in addition to the "id" field, for the resource.
        - Returns a "uuid" field, in addition to the "id" field, in the "operand1" and "operand2" fields if they are not a combination record.
        - Returns a "uuid" field, in addition to the "id" field, in the "repositories → repository", "viewableIPs → repository", "creator" and "owner" fields.
        - Returns a "type" field in the "repositories → repository" and "viewableIPs → repository" fields.
- Attribute Set

- Modified /attributeSet::GET
    - Returns a "uuid" field, in addition to the "id" field, in the "creator" field.
- Modified /attributeSet::POST
    - Returns a "uuid" field, in addition to the "id" field, in the "creator" field.
- Modified /attributeSet::PATCH.
    - Returns a "uuid" field, in addition to the "id" field, in the "repository", "creator" and "owner" fields.

- Audit File
    - Modified /auditFile::GET
        - Can accept the audit file resource UUID in place of the audit file ID.
        - Returns a "uuid" field, in addition to the "id" field, for the resource.
        - Returns a "uuid" field, in addition to the "id" field, in the "creator" and "owner" fields.
    - Modified /auditFile::POST
        - Returns a "uuid" field, in addition to the "id" field, for the resource.
        - Returns a "uuid" field, in addition to the "id" field, in the "creator" and "owner" fields.
    - Modified /auditFile::PATCH
        - Can accept the audit file resource UUID in place of the audit file ID.
        - Returns a "uuid" field, in addition to the "id" field, for the resource.
        - Returns a "uuid" field, in addition to the "id" field, in the "creator" and "owner" fields.
    - Modified /auditFile::DELETE
        - Can accept the audit file resource UUID in place of the audit file ID.
    - Modified /auditFile/refresh::POST

        - Can accept the audit file resource UUID in place of the audit file ID.
        - Returns a "uuid" field, in addition to the "id" field, for the resource.
        - Returns a "uuid" field, in addition to the "id" field, in the "creator" and "owner" fields.
    - Modified /auditFile::DELETE
        - Can accept the audit file resource UUID in place of the audit file ID.
- Credential
    - Modified /credential::GET
        - Can accept the credential resource UUID in place of the credential ID.
        - Returns a "uuid" field, in addition to the "id" field, for the resource.
        - Returns a "uuid" field, in addition to the "id" field, in the "creator" and "owner" fields.
    - Modified /credential::POST
        - Returns a "uuid" field, in addition to the "id" field, for the resource.
        - Returns a "uuid" field, in addition to the "id" field, in the "creator" and "owner" fields.
    - Modified /credential::PATCH
        - Can accept the credential resource UUID in place of the credential ID.
        - Returns a "uuid" field, in addition to the "id" field, for the resource.
        - Returns a "uuid" field, in addition to the "id" field, in the "creator" and "owner" fields.
    - Modified /credential::DELETE
        - Can accept the credential resource UUID in place of the credential ID.
    - Modified /credential/share::POST

        - Can accept the audit file resource UUID in place of the audit file ID.
        - Returns a "uuid" field, in addition to the "id" field, for the resource.
        - Returns a "uuid" field, in addition to the "id" field, in the "creator" and "owner" fields.
- Current Organization
    - Modified /currentOrganization::GET
        - Returns a "uuid" field, in addition to the "id" field, in the "zones" field.
- Current User
    - Modifed /currentUser::GET
        - Returns a "uuid" field, in addition to the "id" field, in the "switchableUsers → user", "switchableUsers → organization", "responsibleAsset", "organization" and "uuid" fields. NOTE: The "switchableUsers → organization" field will not contain a UUID if the switchable user is an administrator. Likewise, the "organization" field will not contain a "uuid" if the current user is an administrator.
    - Modifed /currentUser/associateCert::POST
        - Returns a "uuid" field, in addition to the "id" field, in the "switchableUsers → user", "switchableUsers → organization", "responsibleAsset", "organization" and "uuid" fields. NOTE: The "switchableUsers → organization" field will not contain a UUID if the switchable user is an administrator. Likewise, the "organization" field will not contain a "uuid" if the current user is an administrator.
    - Modifed /currentUser/switch::POST
        - Returns a "uuid" field, in addition to the "id" field, in the "switchableUsers → user", "switchableUsers → organization", "responsibleAsset", "organization" and "uuid" fields. NOTE: The "switchableUsers → organization" field will not contain a UUID if the switchable user is an administrator. Likewise, the "organization" field will not contain a "uuid" if the current user is an administrator.
- Dashboard Tab

- Modified /dashboard::GET
    - Returns a "uuid" field, in addition to the "id" field, in the "owner" field.
- Modified /dashboard::POST
    - Returns a "uuid" field, in addition to the "id" field, in the "owner" field.
- Modified /dashboard/copy::POST
    - Returns a "uuid" field, in addition to the "id" field, in the "owner" field.
- Modified /dashboard/import::POST
    - Returns a "uuid" field, in addition to the "id" field, in the "owner" field.
- Modified /dashboard/share::POST
    - Returns a "uuid" field, in addition to the "id" field, in the "owner" field.

- Device Information
    - Modified /deviceInfo::GET
        - Clarified that the "dnsName" parameter may only be supplied with the "ip" parameter when a "uuid" parameter is not supplied.
        - Added a "sourceType" parameter to specify which data source, "cumulative" or "patched", to pull information from when not supplying the "scanResultID" parameter.
        - Returns a "uuid" field, in addition to the "id" field, in the "repository" field.
- Freeze Window
    - Modified /freeze::GET
        - Returns a "uuid" field, in addition to the "id" field, in the "assets", "repository", "creator" and "owner" fields.
    - Modified /freeze::POST

        - Returns a "uuid" field, in addition to the "id" field, in the "assets", "repository", "creator" and "owner" fields.
    - Modified /freeze::PATCH
        - Returns a "uuid" field, in addition to the "id" field, in the "assets", "repository", "creator" and "owner" fields.
- Group
    - Modified /group::GET
        - Returns a "uuid" field, in addition to the "id" field, in the "repositories", "definingAssets", "users", "assets", "policies", "credentials" and "auditFiles" fields.
        - Returns a "type" field in the "auditFiles" field.
    - Modified /group::POST
        - Returns a "uuid" field, in addition to the "id" field, in the "repositories", "definingAssets", "users", "assets", "policies", "credentials" and "auditFiles" fields.
        - Returns a "type" field in the "auditFiles" field.
    - Modified /group::PATCH
        - Returns a "uuid" field, in addition to the "id" field, in the "repositories", "definingAssets", "users", "assets", "policies", "credentials" and "auditFiles" fields.
        - Returns a "type" field in the "auditFiles" field.
- Job
    - Modified /job::GET
        - Returns a "uuid" field, in addition to the "id" field, in the "organization" and "initiator" fields.
- LCE

- Modified /lce::GET
    - Returns a "uuid" field, in addition to the "id" field, in the "organizations" and "repositories" fields.
- Modified /group::POST
    - Returns a "uuid" field, in addition to the "id" field, in the "organizations" and "repositories" fields.
- Modified /group::PATCH
    - Returns a "uuid" field, in addition to the "id" field, in the "organizations" and "repositories" fields.

- LDAP
    - Modified /ldap::GET
        - Returns a "uuid" field, in addition to the "id" field, in the "organizations" field.
    - Modified /ldap::POST
        - Returns a "uuid" field, in addition to the "id" field, in the "organizations" field.
    - Modified /ldap::PATCH
        - Returns a "uuid" field, in addition to the "id" field, in the "organizations" field.
- Organization
    - Modified /organization::GET
        - Can accept the organization resource UUID in place of the organization ID.
        - Returns a "uuid" field, in addition to the "id" field, for the resource.
        - Returns a "uuid" field, in addition to the "id" field, in the "repositories" and "zones"

fields.

    - Returns a "type" field in the "repositories" field.

- Modified /organization::POST
    - Can accept UUID records, instead of ID records, in the "repositories" and "zones" fields.
    - Returns a "uuid" field, in addition to the "id" field, in the "creator" and "owner" fields.
    - Returns a "uuid" field, in addition to the "id" field, in the "repositories" and "zones" fields.
    - Returns a "type" field in the "repositories" field.
- Modified /organization::PATCH
    - Can accept the organization resource UUID in place of the organization ID.
    - Can accept UUID records, instead of ID records, in the "repositories" and "zones" fields.
    - Returns a "uuid" field, in addition to the "id" field, for the resource.
    - Returns a "uuid" field, in addition to the "id" field, in the "repositories" and "zones" fields.
    - Returns a "type" field in the "repositories" field.
- Modified /organization::DELETE
    - Can accept the organization resource UUID in place of the organization ID.
- Modified /organization/acceptRiskRule::GET
    - Can accept the organization resource UUID in place of the organization ID.
    - Can accept the "repositoryUUIDs" field, instead of the "repositoryIDs" field.

        - Returns a "uuid" field, in addition to the "id" field, in the "hostValue" field if the "hostType" is "asset", and the asset list is part of your organization context.
        - Returns a "uuid" field, in addition to the "id" field, in the "repository", "organization", and "user" fields.
        - Returns a "type" field in the "repository" and "plugin" fields.
    - Modified /organization/recastRiskRule::GET
        - Can accept the organization resource UUID in place of the organization ID.
        - Can accept the "repositoryUUIDs" field, instead of the "repositoryIDs" field.
        - Returns a "uuid" field, in addition to the "id" field, in the "hostValue" field if the "hostType" is "asset", and the asset list is part of your organization context.
        - Returns a "uuid" field, in addition to the "id" field, in the "repository", "organization", and "user" fields.
        - Returns a "type" field in the "repository" and "plugin" fields.
- Organization Security Manager
    - Modified /organization/securityManager::GET
        - Can accept the organization resource UUID in place of the organization ID.
        - Can accept the user resource UUID (for the Security Manager) in place of the user ID.
        - Returns a "uuid" field, in addition to the "id" field, for the resource.
        - Returns a "uuid" field, in addition to the "id" field, in the "parent → user" and "responsibleAsset" fields.
    - Modified /organization/securityManager::POST

        - Can accept the organization resource UUID in place of the organization ID.
        - Can accept the "responsibleAssetUUID" field, instead of the "responsibleAssetID" field.
        - Can accept a UUID record, instead of an ID record, as the "responsibleAsset" field.
        - Returns a "uuid" field, in addition to the "id" field, for the resource.
        - Returns a "uuid" field, in addition to the "id" field, in the "parent → user" and "responsibleAsset" fields.
    - Modified /organization/securityManager::PATCH
        - Can accept the organization resource UUID in place of the organization ID.
        - Can accept the user resource UUID in place of the user ID.
        - Can accept the "responsibleAssetUUID" field, instead of the "responsibleAssetID" field.
        - Can accept a UUID record, instead of an ID record, as the "responsibleAsset" field.
        - Returns a "uuid" field, in addition to the "id" field, for the resource.
        - Returns a "uuid" field, in addition to the "id" field, in the "parent → user" and "responsibleAsset" fields.
    - Modified /organization/securityManager::DELETE
        - Can accept the organization resource UUID in place of the organization ID.
        - Can accept the user resource UUID in place of the user ID.
        - Can accept the migrate user UUID in place of the migrate user ID.
- Organization User

- Modified /organization/user::GET
    - Can accept the organization resource UUID in place of the organization ID.
    - Can accept the user resource UUID in place of the user ID.
    - Returns a "uuid" field, in addition to the "id" field, for the resource.
    - Returns a "uuid" field, in addition to the "id" field, in the "parent → user" and "responsibleAsset" fields.

- Passive Scanner (NNM)
    - Modified /passivescanner::GET
        - Returns a "uuid" field, in addition to the "id" field, in the "repositories" field.
        - Returns a "type" field in the "repositories" field.
    - Modified /passivescanner::POST
        - Returns a "uuid" field, in addition to the "id" field, in the "repositories" field.
        - Returns a "type" field in the "repositories" field.
    - Modified /passivescanner::PATCH
        - Returns a "uuid" field, in addition to the "id" field, in the "repositories" field.
        - Returns a "type" field in the "repositories" field.
- Plugin Family
    - Modified /pluginFamily::GET
        - Returns a "type" field in the "plugins" field.
- Publishing Site

- Modified /pubSite::GET
    - Returns a "uuid" field, in addition to the "id" field, in the "organizations" field.
- Modified /pubSite::POST
    - Returns a "uuid" field, in addition to the "id" field, in the "organizations" field.
- Modified /pubSite::PATCH
    - Returns a "uuid" field, in addition to the "id" field, in the "organizations" field.

- Query
    - Modified /query::GET
        - Returns a "uuid" field, in addition to the "id" field, in the "query → filters → value" field if the filter is a type of asset list, audit file, policy, repository or user, whether it is a single record or multiple records
        - Returns a "uuid" field, in addition to the "id" field, in the "query → filters → value", operand1" and "operand2" fields if the filter is a combination of assets and they are not, themselves, a combination record.
        - Returns a "uuid" field, in addition to the "id" field, in the "creator" and "owner" fields.
        - Returns a "type" field in the "query → filters → value" field if the filter (name) is "repository" or "auditFile."
    - Modified /query::POST
        - Returns a "uuid" field, in addition to the "id" field, in the "query → filters → value" field if the filter is a type of asset list, audit file, policy, repository or user, whether it is a single record or multiple records.
        - Returns a "uuid" field, in addition to the "id" field, in the "query → filters → value", operand1" and "operand2" fields if the filter is a combination of assets and they are not, themselves, a combination record.

    - Returns a "uuid" field, in addition to the "id" field, in the "creator" and "owner" fields.
    - Returns a "type" field in the "query → filters → value" field if the filter (name) is "repository" or "auditFile."
- Modified /query::PATCH
    - Returns a "uuid" field, in addition to the "id" field, in the "query → filters → value" field if the filter is a type of asset list, audit file, policy, repository or user, whether it is a single record or multiple records.
    - Returns a "uuid" field, in addition to the "id" field, in the "query → filters → value", operand1" and "operand2" fields if the filter is a combination of assets and they are not, themselves, a combination record.
    - Returns a "uuid" field, in addition to the "id" field, in the "creator" and "owner" fields.
    - Returns a "type" field in the "query → filters → value" field if the filter (name) is "repository" or "auditFile."
- Modified /query/share::POST
    - Returns a "uuid" field, in addition to the "id" field, in the "query → filters → value" field if the filter is a type of asset list, audit file, policy, repository or user, whether it is a single record or multiple records.
    - Returns a "uuid" field, in addition to the "id" field, in the "query → filters → value", operand1" and "operand2" fields if the filter is a combination of assets and they are not, themselves, a combination record.
    - Returns a "uuid" field, in addition to the "id" field, in the "creator" and "owner" fields.
    - Returns a "type" field in the "query → filters → value" field if the filter (name) is "repository" or "auditFile."
- Recast Risk Rule

- Modified /rescastRiskRule::GET
    - Returns a "uuid" field, in addition to the "id" field, in the "hostValue" field if the "hostType" is "asset", and the asset list is part of your organization context.
    - Returns a "uuid" field, in addition to the "id" field, in the "repository", "organization", and "user" fields.
    - Returns a "uuid" field, in addition to the "id" field, in the "creator" and "owner" fields.
- Modified /rescastRiskRule::POST
    - Returns a "uuid" field, in addition to the "id" field, in the "hostValue" field if the "hostType" is "asset", and the asset list is part of your organization context.
    - Returns a "uuid" field, in addition to the "id" field, in the "repository", "organization", and "user" fields.
    - Returns a "type" field in the "repository" and "plugin" fields.

- Report
    - Modified /report::GET
        - Returns a "uuid" field, in addition to the "id" field, in the "creator" and "owner" fields.

- Report Definition
    - Modified /reportDefinition::GET
        - Returns a "uuid" field, in addition to the "id" field, in the "filters → value" field of all query objects, nested under the "definition" and "xmlDefinition" fields, if the filter is a type of asset list, audit file, policy, repository or user, whether it is a single record or multiple records.
        - Returns a "uuid" field, in addition to the "id" field, in the "filters → value", operand1" and "operand2" fields of all query objects, nested under the "definition" and "xmlDefinition" fields, if the filter is a combination of assets and they are not,

themselves, a combination record.

- Returns a "uuid" field, in addition to the "id" field, in the "creator" and "owner" fields.
- Returns a "type" field in the "filters → value" field of all query objects, nested under the "definition" and "xmlDefinition" fields, if the filter (name) is "repository" or "auditFile."

- Modified /reportDefinition::POST
  - Returns a "uuid" field, in addition to the "id" field, in the "filters → value" field of all query objects, nested under the "definition" and "xmlDefinition" fields, if the filter is a type of asset list, audit file, policy, repository or user, whether it is a single record or multiple records.
  - Returns a "uuid" field, in addition to the "id" field, in the "filters → value", operand1" and "operand2" fields of all query objects, nested under the "definition" and "xmlDefinition" fields, if the filter is a combination of assets and they are not, themselves, a combination record.
  - Returns a "uuid" field, in addition to the "id" field, in the "creator" and "owner" fields.
  - Returns a "type" field in the "filters → value" field of all query objects, nested under the "definition" and "xmlDefinition" fields, if the filter (name) is "repository" or "auditFile."
- Modified /reportDefinition::PATCH
  - Returns a "uuid" field, in addition to the "id" field, in the "filters → value" field of all query objects, nested under the "definition" and "xmlDefinition" fields, if the filter is a type of asset list, audit file, policy, repository or user, whether it is a single record or multiple records.
  - Returns a "uuid" field, in addition to the "id" field, in the "query → filters → value", operand1" and "operand2" fields if the filter is a combination of assets and they are

not, themselves, a combination record.

- Returns a "uuid" field, in addition to the "id" field, in the "creator" and "owner" fields.
- Returns a "type" field in the "filters → value" field of all query objects, nested under the "definition" and "xmlDefinition" fields, if the filter (name) is "repository" or "auditFile."

- Modified /reportDefinition/copy::POST
  - Returns a "uuid" field, in addition to the "id" field, in the "filters → value" field of all query objects, nested under the "definition" and "xmlDefinition" fields, if the filter is a type of asset list, audit file, policy, repository or user, whether it is a single record or multiple records.
  - Returns a "uuid" field, in addition to the "id" field, in the "filters → value", operand1" and "operand2" fields of all query objects, nested under the "definition" and "xmlDefinition" fields, if the filter is a combination of assets and they are not, themselves, a combination record.
  - Returns a "uuid" field, in addition to the "id" field, in the "creator" and "owner" fields.
  - Returns a "type" field in the "filters → value" field of all query objects, nested under the "definition" and "xmlDefinition" fields, if the filter (name) is "repository" or "auditFile."
- Modified /reportDefinition/import::POST
  - Returns a "uuid" field, in addition to the "id" field, in the "filters → value" field of all query objects, nested under the "definition" and "xmlDefinition" fields, if the filter is a type of asset list, audit file, policy, repository or user, whether it is a single record or multiple records.
  - Returns a "uuid" field, in addition to the "id" field, in the "filters → value", operand1" and "operand2" fields of all query objects, nested under the "definition" and

"xmlDefinition" fields, if the filter is a combination of assets and they are not, themselves, a combination record.

- Returns a "uuid" field, in addition to the "id" field, in the "creator" and "owner" fields.
- Returns a "type" field in the "filters → value" field of all query objects, nested under the "definition" and "xmlDefinition" fields, if the filter (name) is "repository" or "auditFile."

- Report Image
  - Modified /report/image::GET
    - Returns a "uuid" field, in addition to the "id" field, in the "creator" field.
  - Modified /report/image::POST
    - Returns a "uuid" field, in addition to the "id" field, in the "creator" field.
  - Modified /report/image::PATCH
    - Returns a "uuid" field, in addition to the "id" field, in the "creator" field.
- Repository
  - Modified /repository::GET
    - Can accept the repository resource UUID in place of the repository ID.
    - Returns a "uuid" field, in addition to the "id" field, for the resource.
    - Returns a "uuid" field, in addition to the "id" field, in the "organizations" field.
  - Modified /repository::POST
    - Can accept UUID records, instead of ID records, in the "organizations" field.
    - Returns a "uuid" field, in addition to the "id" field, for the resource.
    - Returns a "uuid" field, in addition to the "id" field, in the "organizations" field.

- Modified /repository::PATCH
    - Can accept the repository resource UUID in place of the repository ID.
    - Can accept UUID records, instead of ID records, in the "organizations" field.
    - Returns a "uuid" field, in addition to the "id" field, for the resource.
    - Returns a "type" field in the "query → filters → value" field if the filter (name) is "repository" or "auditFile."
- Modified /repository::DELETE
    - Can accept the repository resource UUID in place of the repository ID.
- Modified /repository/acceptRiskRule::GET
    - Can accept the repository resource UUID in place of the repository ID.
    - Can accept the "organizationUUIDs" field, instead of the "organizationIDs" field.
    - Returns a "uuid" field, in addition to the "id" field, in the "hostValue" field if the "hostType" is "asset", and the asset list is part of your organization context.
    - Returns a "uuid" field, in addition to the "id" field, in the "repository", "organization", and "user" fields.
    - Returns a "type" field in the "repository" and "plugin" fields.
- Modified /repository/assetIntersections::GET
    - Can accept the repository resource UUID in place of the repository ID.
- Modified /repository/export::GET
    - Can accept the repository resource UUID in place of the repository ID.
- Modified /repository/import::POST
    - Can accept the repository resource UUID in place of the repository ID.

- Modified /repository/deviceInfo::GET
    - Clarified that the "dnsName" parameter may only be supplied with the "ip" parameter when a "uuid" parameter is not supplied.
    - Added a "sourceType" parameter to specify which data source, "cumulative" or "patched", to pull information from.
    - Can accept the repository resource UUID in place of the repository ID.
    - Returns a "uuid" field, in addition to the "id" field, in the "repository" field.
    - Returns a "type" field in the "repository" field.
- Modified /repository/recastRiskRule::GET
    - Can accept the repository resource UUID in place of the repository ID.
    - Can accept the "organizationUUIDs" field, instead of the "organizationIDs" field.
    - Returns a "uuid" field, in addition to the "id" field, in the "hostValue" field if the "hostType" is "asset", and the asset list is part of your organization context.
    - Returns a "uuid" field, in addition to the "id" field, in the "repository", "organization" and "user" fields.
    - Returns a "type" field in the "repository" and "plugin" fields.
- Modified /repository/sync::POST
    - Can accept the repository resource UUID in place of the repository ID.
- Modified /repository/updateMobileData::POST
    - Can accept the repository resource UUID in place of the repository ID.

- Role

- Modified /role::GET
    - Returns a "uuid" field, in addition to the "id" field, in the "creator" field.
- Modified /role::POST
    - Returns a "uuid" field, in addition to the "id" field, in the "creator" field.
- Modified /role::PATCH
    - Returns a "uuid" field, in addition to the "id" field, in the "creator" field.

- Scanner
    - Modified /scanner::GET
        - Returns a "uuid" field, in addition to the "id" field, in the "nessusManagerOrgs" and "zones" fields.
    - Modified /scanner::POST
        - Returns a "uuid" field, in addition to the "id" field, in the "nessusManagerOrgs" and "zones" fields.
    - Modified /scanner::PATCH
        - Returns a "uuid" field, in addition to the "id" field, in the "nessusManagerOrgs" and "zones" fields.

- Scan
    - Modified /scan::GET
        - Can accept the scan resource UUID in place of the scan ID.
        - Returns a "uuid" field, in addition to the "id" field, for the resource.
        - Returns a "uuid" field, in addition to the "id" field, in the "credentials", "policy",

"repository", "zone", "creator" and "owner" fields.

- Returns a "type" field in the "repository" field.

- Modified /scan::POST
  - Can accept UUID records, instead of ID records, in the "auditFiles" field.
  - Returns a "uuid" field, in addition to the "id" field, for the resource.
  - Returns a "uuid" field, in addition to the "id" field, in the "credentials", "policy", "repository", "zone", "creator" and "owner" fields.
  - Returns a "type" field in the "repository" field.
- Modified /scan::PATCH
  - Can accept the scan resource UUID in place of the scan ID.
  - Can accept UUID records, instead of ID records, in the "auditFiles" field.
  - Returns a "uuid" field, in addition to the "id" field, for the resource.
  - Returns a "uuid" field, in addition to the "id" field, in the "credentials", "policy", "repository", "zone", "creator" and "owner" fields.
  - Returns a "type" field in the "repository" field.
- Modified /scan::DELETE
  - Can accept the scan resource UUID in place of the scan ID.
- Modified /scan/copy::POST
  - Can accept the scan resource UUID in place of the scan ID.
  - Can accept a UUID record instead of an ID record for the "targetUser" field.
  - Returns a "uuid" field, in addition to the "id" field, for the resource.

- Returns a "uuid" field, in addition to the "id" field, in the "credentials", "policy", "repository", "zone", "creator" and "owner" fields.
- Returns a "type" field in the "repository" field.

- Modified /scan/launch::POST
  - Can accept the scan resource UUID in place of the scan ID.

- Scan Policy
  - Modified /policy::GET
    - Can accept the policy resource UUID in place of the policy ID.
    - Returns a "uuid" field, in addition to the "id" field, for the resource.
    - Returns a "uuid" field, in addition to the "id" field, in the "policy → creator", "policy → owner", "auditFiles", "creator" and "owner" fields.
    - Returns a "type" field in the "auditFiles" and "families → plugins" fields.
  - Modified /policy::POST
    - Can accept UUID records, instead of ID records, in the "auditFiles" field.
    - Returns a "uuid" field, in addition to the "id" field, for the resource.
    - Returns a "uuid" field, in addition to the "id" field, in the "policy → creator", "policy → owner", "auditFiles", "creator" and "owner" fields.
    - Returns a "type" field in the "auditFiles" and "families → plugins" fields.
  - Modified /policy::PATCH
    - Can accept the policy resource UUID in place of the policy ID.
    - Can accept UUID records, instead of ID records, in the "auditFiles" field.
    - Returns a "uuid" field, in addition to the "id" field, for the resource.

    - Returns a "uuid" field, in addition to the "id" field, in the "policy → creator", "policy → owner", "auditFiles", "creator" and "owner" fields.
    - Returns a "type" field in the "auditFiles" and "families → plugins" fields.
- Modified /policy::DELETE.
    - Can accept the policy resource UUID in place of the policy ID.
- Modified /policy/copy::POST
    - Can accept the policy resource UUID in place of the policy ID.
    - Returns a "uuid" field, in addition to the "id" field, for the resource.
    - Returns a "uuid" field, in addition to the "id" field, in the "policy → creator", "policy → owner", "auditFiles", "creator" and "owner" fields.
    - Returns a "type" field in the "auditFiles" and "families → plugins" fields.
- Modified /policy/export::GET and /policy/export::POST
    - Can accept the resource UUID in place of the ID.
- Modified /policy/import::POST
    - Returns a "uuid" field, in addition to the "id" field, for the resource.
    - Returns a "uuid" field, in addition to the "id" field, in the "policy → creator", "policy → owner", "auditFiles", "creator" and "owner" fields.
    - Returns a "type" field in the "auditFiles" and "families → plugins" fields. (NOTE: This would be the case, however audit files are not imported when polices import. This was merely documented for possible, future necessity.)
- Modified /policy/share::POST
    - Can accept the policy resource UUID in place of the policy ID.
    - Returns a "uuid" field, in addition to the "id" field, for the resource.

        - Returns a "uuid" field, in addition to the "id" field, in the "policy → creator", "policy → owner", "auditFiles", "creator" and "owner" fields.
        - Returns a "type" field in the "auditFiles" and "families → plugins" fields.
- Scan Result
    - Modified /scanResult::GET
        - Returns a "uuid" field, in addition to the "id" field, in the "scan" (if not already disassociated from the result), "repository", "initiator" and "owner" fields.
        - Returns a "type" field in the "scan" and "repository" fields.
    - Modified /scanResult/pause::POST
        - Returns a "uuid" field, in addition to the "id" field, in the "scan" (if not already disassociated from the result), "repository", "initiator" and "owner" fields.
        - Returns a "type" field in the "scan" and "repository" fields.
    - Modified /scanResult/resume::POST
        - Returns a "uuid" field, in addition to the "id" field, in the "scan" (if not already disassociated from the result), "repository", "initiator" and "owner" fields.
        - Returns a "type" field in the "scan" and "repository" fields.
    - Modified /policy::DELETE.
        - Can accept the policy resource UUID in place of the policy ID.
    - Modified /scanResult/stop::POST
        - Returns a "uuid" field, in addition to the "id" field, in the "scan" (if not already disassociated from the result), "repository", "initiator" and "owner" fields.
        - Returns a "type" field in the "scan" and "repository" fields.
- Scan Zone

- Modified /zone::GET
    - Can accept the zone resource UUID in place of the zone ID.
    - Returns a "uuid" field, in addition to the "id" field, for the resource.
    - Returns a "uuid" field, in addition to the "id" field, in the "organizations" field.
- Modified /zone::POST
    - Returns a "uuid" field, in addition to the "id" field, for the resource.
    - Returns a "uuid" field, in addition to the "id" field, in the "organizations" field.
- Modified /zone::PATCH
    - Can accept the zone resource UUID in place of the zone ID.
    - Returns a "uuid" field, in addition to the "id" field, for the resource.
    - Returns a "uuid" field, in addition to the "id" field, in the "organizations" field.
- Modified /zone::DELETE
    - Can accept the policy resource UUID in place of the policy ID.

- Status
    - Modified /status::GET
        - Returns a "uuid" field, in addition to the "id" field, in the "zones" field.
- Ticket
    - Modified /ticket::GET
        - Returns a "uuid" field, in addition to the "id" field, in the "assignee", "creator" and "owner" fields.
    - Modified /ticket::POST

        - Returns a "uuid" field, in addition to the "id" field, in the "assignee", "creator" and "owner" fields.
    - Modified /ticket::PATCH
        - Returns a "uuid" field, in addition to the "id" field, in the "assignee", "creator" and "owner" fields.
- User
    - Modified /user::GET
        - Can accept the user resource UUID in place of the user ID.
        - Returns a "uuid" field, in addition to the "id" field, for the resource.
        - Returns a "uuid" field, in addition to the "id" field, in the "parent → user", "linkedUsers" and "responsibleAsset" fields.
    - Modified /user::POST
        - Can accept the "responsibleAssetUUID" field, instead of the "responsibleAssetID" field.
        - Returns a "uuid" field, in addition to the "id" field, for the resource.
        - Returns a "uuid" field, in addition to the "id" field, in the "parent → user", "linkedUsers" and "responsibleAsset" fields.
    - Modified /user::PATCH
        - Can accept the user resource UUID in place of the user ID.
        - Can accept the "responsibleAssetUUID" field, instead of the "responsibleAssetID" field.
        - Can accept a UUID record, instead of an ID record, as the "responsibleAsset" field.
        - Returns a "uuid" field, in addition to the "id" field, for the resource.

    - Returns a "uuid" field, in addition to the "id" field, in the "parent → user", "linkedUsers" and "responsibleAsset" fields.

- Modified /user::DELETE
    - Can accept the user resource UUID in place of the user ID.
    - Can accept the "orgUUID" field instead of the "orgID" field.
    - Can accept the "migrateUserUUID" field instead of the "migrateUserID" field.

Version 5.20.x

Tenable.sc 5.20.x API includes updates for the following endpoints:

- Hosts
  - Added /host::GET endpoint for SC Exposure (Lumin-lite capabilities), which are used to retrieve a list of hosts. If a tenableUUID field is defined, the response will also include Findings (vulnerabilities) and a list of Installed Software for that specific host.
- Plugin
  - Added **agent** to the fields parameters for the /plugin::GET and /plugin/{id}::GET endpoints. Added **agent** to the response for the /plugin::GET endpoint. This field indicates if the plugin is agent capable.
- Repository
  - Added **networkDeleted** to the response for the /repository/{id}::GET endpoint as part of **luminFields**. This is boolean field that indicates if the network in Tenable.io associated with the repository in Tenable.sc (as part of the Lumin Connector) has been deleted
- Scan Policy
  - For the **families fields parameter of the /policy::GET endpoint, added the Advanced Agent Scan Template (id="25") as eligible for getting families (in addition to the Advanced Scan Template (id = "1")).**
  - For the /policy::POST endpoint, added the Advanced Agent Scan Template (id="25") as eligible for providing **families** in the request parameters. Also added **agent** to the policyTemplate object in the example response. This field indicates if the policy template is for agent scans.
  - For the **families** fields parameter of the /policy/{id}::GET endpoint, added the Advanced Agent Scan Template (id="25") as eligible for getting **families** (in addition to the Advanced Scan Template (id = "1")). Also added **agent** to the policyTemplate object in

the example response. This field indicates if the policy template is for agent scans.

- For the /policy/{id}/copy::POST endpoint, added **agent** to the policyTemplate object in the example response. This field indicates if the policy template is for agent scans.
- For the /policy/{id}/share::POST endpoint, added **agent** to the policyTemplate object in the example response. This field indicates if the policy template is for agent scans.

- Scan Policy Templates
  - Added **agent** to the fields parameters for the /policyTemplate::GET and /policyTemplate/{id}::GET endpoints. Added **agent** to the response for the /policyTemplate/{id}::GET endpoint. This is a boolean field that indicates if the policy template is for agent scans.
- User
  - Added a new /user::PATCH parameter, **currentPassword**, that is required if **password** was included in the PATCH payload.

Version 5.19.x

Tenable.sc 5.19.x API includes updates for the following endpoints:

- Credential
  - Updated /credential::GET and /credential/{id}::GET to be able to return **escalationAccount** for "ssh" type credentials.
  - Updated /credential::POST for "ssh" type "Arcon" authType credentials so that **privilegeEscalation** can be provided and **escalationAccount** can be provided for the appropriate **privilegeEscalation fields**.
- Director-Insights
  - Updated /mgmt/insights::GET endpoint to include licensing information. The data will be fetched from the SCI table. If the license information is not retrieved for a particular day, then it will consider the total and active count for that day as 0.
  - The new response will include the **licenseStatusInformation** attribute under **chart** and **usage**.
- Director-System
  - New for the 5.19 release.
  - Added /mgmt/system/logFiles::GET endpoint which returns a list of log files on a linked Tenable.sc Instance that are available to the current user.
  - Added /mgmt/system/logs::POST endpoint which returns a list of log messages on a linked Tenable.sc Instance that are available to the current user based on a query parameter.
- Lumin
  - Added a new boolean request parameter **ioNetworksEnabled** to the /lumin/repositories::PATCH endpoint. If "true", vulnerability data is synchronized to

Lumin using a separate network for each repository. The response for this endpoint has two (2) additional parameters per repository - **enabled** and **ioNetworkUUID**. The **enabled** parameter can be "true" or "false", which indicates if the repository is enabled for synchronizing to Lumin. The **ioNetworkUUID** parameteris the UUID of the network used to synchronize the vulnerability data when **ioNetworksEnabled** is set to "true."

- Added new metrics to the response parameters for the /lumin/metrics::GET endpoint including **ioRemediationMaturityGrade**, **ioRemediationMaturityGradeDelta**, **ioRemediationMaturityGradeLetter**, **ioAssessmentMaturityGradeLetter**.

- Repository
  - Added **percentCapacityCumulative** and **percentCapacityPatched** to the typeFields returned by the /repository::GET and /repository/{id}::GET endpoints. This is a percentage of the maximum capacity of cumulative and patched data for IPv4, IPv6, and Agent repositories. The current maximum is 64GB.
- Status
  - Added **lastDbBackupStatus**, **lastDbBackupSuccess**, and **lastDbBackupFailure** to the typeFields returned by the /status::GET endpoint. These fields contain the status of the last database update (0 = SUCCESS, otherwise FAILURE) and the timestamps of the last database backup success and failure.
- System
  - Added /system/logFiles::GET endpoint which returns a list of log files available to the current user.
  - Added /system/logs::POST endpoint which returns a list of log messages available to the current user based on a query parameter.
  - Added /system/logs/download::POST which downloads a list of log messages available to the current user based on a query.

Version 5.18.x

Tenable.sc 5.18.x API includes updates for the following endpoints:

- Blackout Window
  - Amended a feature name to comply with Tenable's inclusive language guidelines. The **Blackout** API's name is now changed to **Freeze** API in the Tenable.sc product.
- Configuration
  - Moved vulnerability data lifetime values from /configuration to /repository. The following are no longer available with the /configuration::GET or ::PATCH endpoints: **activeVulnsLifetime**, **passiveVulnsLifetime**, **lceVulnsLifetime**, **complianceVulnsLifetime**, and **mitigatedVulnsLifetime**. These values are now at the repository level and are a part of the /repository endpoints.
- Director Insights
  - Added /mgmt/insights::GET endpoints for Director, which retrieves the trending data for Scan Results, Scanners, and Scan Zones on Tenable.sc Instances linked to Director.
- Director Organization
  - Added /mgmt/organization endpoints for Director. GET for both /mgmt/organization and /organization/{id}, which are used to view the organization information on a linked Tenable.sc Instance. This is currently used primarily when managing Nessus Scanners through Director (see the above endpoint)
- Director Scanner
  - Added /mgmt/scanner endpoints for Director. GET and POST for both /mgmt/scanner, which are used for adding new Nessus Scanners to the linked Tenable.sc Instance through Director. GET, PATCH, and DELETE for /mgmt/scanner/{id}, which are used to view, modify, and delete the specified Scanner on its linked Tenable.sc Instance through Director.

- Director Scan Result
    - Added /mgmt/scanResult endpoints for Director customers and /all/scanResult endpoints for managed by Director users. GET for both /scanResult and /scanResult/{id}, and POST for /scanResult/{id}/email, /scanResult/{id}/stop, /scanResult/{id}/pause, /scanResult/{id}/resume, /scanResult/{id}/retrieve, and /scanResult/{id}/download. These endpoints are responsible for controlling Scan Results of SCIs linked to Director.
- Director Scan Zone
    - Added /mgmt/zone endpoints for Director. GET and POST for both /mgmt/zone, which are used for adding new Scan Zones to the linked Tenable.sc Instance through Director. GET, PATCH, and DELETE for /mgmt/zone/{id}, which are used to view, modify and delete the specified Scan Zone on its' linked Tenable.sc Instance through Director.
- LDAP
    - Added support for two new LDAP options, as customers can now provision their users on first-time logins and sync their attributes/metadata on every login. /ldap::POST and /ldap::PATCH calls can now configure the following parameters **(1) ldapUserProvisioning** and **(2) ldapUserSync**, though by default they are set to false.
- Query
    - Added to the POST envelope to support a new tool, "remediationdetail" and a new filter, "solutionID."
    - Added a clarification "NOTE" specifying that the "solutionID" filter only applies to tools "sumremediation" and "remediationdetail." Specified that the latter tool must use this "filter" to function.
    - Added a clarification "NOTE" specifying that the existing "outputAssets" filter only applies to the tool "sumasset" for both the "vuln" and "lce" query types.
- Report

- Correction of the "/report/{id}/email" description, it was incorrectly set to the description of the /copy endpoint before it in the document. This endpoint is responsible for sharing a report result to specified users and/or list of email addresses.

- Report Definition
  - Correction to the GET field names in API documentation, as the expected field values were **creator** and **owner**, but in API documentation it was written as **CreatorID** and **ownerID**, hence the following field names **creatorID** and **ownerID** have been changed to **creator** and **owner**.

- Repository
  - Added vulnerability data expiration related fields to the typeFields returned by the /repository::GET and /repository/{id}::GET endpoints. For repositories with a dataFormat of "IPv4", added: **activeVulnsLifetime**, **passiveVulnsLifetime**, **lceVulnsLifetime**, **complianceVulnsLifetime**, and **mitigatedVulnsLifetime**. For repositories with a dataFormat of "IPv6", added: **activeVulnsLifetime**, **passiveVulnsLifetime**, **complianceVulnsLifetime**, and **mitigatedVulnsLifetime**. For repositories with a dataFormat of "agent", added: **activeVulnsLifetime**, **complianceVulnsLifetime**, and **mitigatedVulnsLifetime**. The units for these fields are specified in days.
  - Added vulnerability data expiration related fields to the /repository::POST and /repository/{id}::PATCH endpoints. For repositories with a dataFormat of "IPv4", added: **activeVulnsLifetime**, **passiveVulnsLifetime**, **lceVulnsLifetime**, **complianceVulnsLifetime**, and **mitigatedVulnsLifetime**. For repositories with a dataFormat of "IPv6", added: **activeVulnsLifetime**, **passiveVulnsLifetime**, **complianceVulnsLifetime**, and **mitigatedVulnsLifetime**. For repositories with a dataFormat of "agent", added: **activeVulnsLifetime**, **complianceVulnsLifetime**, and **mitigatedVulnsLifetime**. The units for these fields are specified in days. The default value for **passiveVulnsLifetime** is "7", and for the other fields is "365."

- Scan

- Clarifications by way of a "NOTE" stating that setting the schedule type to "template" will create a scan that will not run on a schedule.

- Tenable.sc Instance
  - Added /sci endpoints for Director. GET and POST for both /sci, which are used for adding and viewing Tenable.sc Instances on Director. GET, PATCH, and DELETE for /sci/{id} which are used for managing the linked Tenable.sc Instances on Director.

Version 5.17.x

Tenable.sc 5.17.x API includes updates for the following endpoints:

- Industrial-Security
    - This entire API has been deleted and is no longer functioning. Customers must use Tenable.ot, the new Industrial Security replacement.
- Analysis
    - The /analysis endpoint now supports a "startOffset" and "endOffset" for "vuln" type requests. This is similar to the /analysis/download endpoint.
- Asset
    - Added a new filterName value, "uuid." Supported in asset::POST for assets of type "dynamic."
- Credential
    - Added support for a new Credential type, Centrify, available for SSH and Windows.
    - Added "Privilege Escalation" option to the SSH Thycotic Secret Server credential.
    - Applied a correction to the POST request values for privilege escalation for SSH CyberArk Vault, to match the SC 5.17.0 REST API.
    - Applied a correction to the POST request values for privilege escalation type "dzdo" for auth types other than SSH Thycotic Secret Server, to match the SC 5.17.0 REST API.
    - Added support for a new Credential type, Sybase ASE., available for Databses.
    - Added support for a new Credential type, Apache Cassandra, available for Databses.
    - Expanded CSV import support to SQL Server, MySQL, and DB2 database type credentials. On POST for these database types when Source = 'Import' added a new field for providing the CSV file name. This new field is returned on GET and can be

modified using PATCH.

- Added Escalation Username field for SSH credentials with privilege escalation of type pbrun. On POST when Privilege Escalation = 'pbrun' added a new field for providing the Escalation Username. This new field is returned on GET and can be modified using PATCH.

- Organization
  - Added a new field associated with an Organization, vulnScoringSystem, which holds the value of the scoring system used to compute vulnerability severity (e.g., "CVSSv2", "CVSSv3"). This field is returned on /organization::GET and /organization/{id}::GET and can be provided to /organization::POST and /organization/{id}::PATCH. The default value is "CVSSv3."
- Scan
  - Applied a change to the "type" field. Now defaulted to "policy" as we no longer support "plugin" type policies (used for Remediation scans, which now use type "policy" as well).
- User
  - Applied a correction to the GET endpoint description. Creating a request as an Admin, with orgID as a parameter, will retrieve all the Users within the provided organization.

Version 5.16.x

Tenable.sc 5.16 .x API includes updates for the following endpoints:

- User
    - As an Administrator, when viewing a list of Administrators /user::GET, return the list of Linked Users for each Administrator showing user and organization.
    - As an Administrator, when creating a Linked User /user::POST, providing the ID for the parent Administrator is required. (NOTE: Only Administrators can create Linked Users.)
    - As an Administrator, when viewing an Administrator /user/{id}::GET, return its list of Linked Users showing user and organization.
    - As an Administrator, when viewing a Linked User /user/{id}::GET, return the parent Administrator information (user, organization).
    - As an Administrator, when locking an Administrator with Linked Users /user/{id}::PATCH (/user/{id}::PATCH), the Linked Users are locked as well.
    - As an Administrator, when editing a Linked User /user/{id}::PATCH(/user/{id}::PATCH), the following fields cannot be modified: (NOTE: Only Administrators can edit Linked Users.)
        - roleID (must be "Security Manager")
        - groupID (must be Full Access group)
        - authType (must be "linked")
        - parent (Linked Users cannot change parent Administrator)
        - password
        - mustChangePassword

- As an Administrator, an Administrator cannot be deleted if it has Linked Users /user/{id}::DELETE. The Linked Users must be deleted first. (NOTE: Only Administrators can delete Linked Users.)
- As an Organization User, linked users cannot be edited or deleted, and API keys cannot be created for linked users.

- Organization Security Manager
  - Added "agentScanID" to the response of the stop, resume, and pause endpoints to indicate the ID of the Agent Scan associated with the Scan Result.

Version 5.15.x

Tenable.sc 5.15.x API includes updates for the following endpoints:

- Status
    - Added "migrationStatus" to the response of /status::GET to indicate the status of the last migration that was run. Valid values are "Running" or "Stopped." A null value indicates that the migration was successful.
- Scan Result
    - Added "agentScanID" to the response of the stop, resume, and pause endpoints to indicate the ID of the Agent Scan associated with the Scan Result.

Version 5.14.x

Tenable.sc 5.14.x API includes the following new functionality:

- Lumin
    - Added a new endpoint /lumin/assets/schedule::GET for retrieving the current schedule for the daily synchronization of Assets to Lumin.

Tenable.sc 5.14.x API includes updates for the following endpoints:

- Analysis
    - Clarified pre-existing behavior of results being inclusive of the startOffset parameter value and exclusive of the endOffset parameter value.
    - Duplicated "hostUniqueness" field to also return as original field name "uniqueness" to support integrations relying on field name.
- Credential
    - Added new authType "Hashicorp" to "SSH", "Windows", and "Database" credentials.
    - Added new authType "Arcon" to "SSH" and "Windows" credentials.
- Lumin
    - Updated the request parameters for the /lumin/assets::PATCH endpoint to allow for a schedule object to be provided for the start time for the daily synchronization of assets to Lumin.
    - Dynamic assets are now supported for syncing Lumin assets.
- Configuration Section

- For the endpoint /configSection/9::GET which returns Lumin configuration information, added a new element to the response object, "assetsSyncSchedule", which contains the schedule object for the daily synchronization of assets to IO/Lumin.

Version 5.13.x

Tenable.sc 5.13.x API includes the following new functionality:

- Lumin
    - New endpoints /lumin/repositories::PATCH and /lumin/assets::PATCH to allow for enabling Lumin Synchronization.

Tenable.sc 5.13.x API includes updates for the following endpoints:

- Scanner
    - Field "password" now supported for authType "certificate" in /scanner::GET, /scasnner:POST, and /scanner:PATCH. The conventions will follow the password field for Nessus Scanners, and return SET when a certificate password exists.
- Industrial Security
    - Field "password" now supported for authType "certificate" in /industrialSecurity::GET, /industrialSecurity::POST, and /industrialSecurity::PATCH. The conventions will follow the password field for Industrial Security Instances, and return SET when a certificate password exists.
- Passive Scanner (NNM)
    - Field "password" now supported for authType "certificate" in /passivescanner::GET, /passivescanner::POST, and /passivescanner::PATCH. The conventions will follow the password field for Passive (NNM) Scanners, and return SET when a certificate password exists.
- Configuration Section

- /configSection::GET - Added Lumin Section for ID 9.
- Added new configuration section: /configSection/9::GET.
- Added new configuration section: /configSection/9::PATCH.

- Repository
  - Added fields "luminFields" and "ipOverlaps" to /repository::GET.
  - Added field "luminFields" to /repository/{id}::GET.
- Asset
  - Added admin access to /asset::GET with a limited field subset including organization and luminFields.
  - Added admin access to /asset/{id}::GET with a limited field subset including organization and luminFields.
- Credential
  - Added fields "source" and "csv_file" to /credential::POST, /credential::PATCH, and /credential::GET.
- Configuration
  - Added new string params “ioAccessKey” and "ioSecretKey" to /config/64::GET.
  - Added new string params “ioAccessKey” and "ioSecretKey" to /config/64::PATCH.
- Analysis
  - Modified attribute "uniqueness" to "hostUniqueness" in the response for certain vuln types.

The following functionality was removed from Tenable Security Center API:

- System
    - Removed unsupported / undocumented endpoints: /system/fips::GET and /system/fips::POST.

Version 5.12.x

Tenable.sc 5.12.x API includes the following new functionality:

- System
  - Added new field "SerializationDisabled" and missing field "telemetryEnabled" to /system::GET response.
  - Added debug option "dbIOErrors" to /system/debug::GET.
  - Added fields "touchDebuggingEnabled" and "migrationFailure" to /system/diagnostic::GET.
- Scanner
  - Created endpoint /scanner/{id}/bug-report.
  - Created endpoint /scanner/{id}/health.
- Solutions (provisional)
  - Created endpoint /solutions::POST.
  - Created endpoint /solutions/{pluginID}::POST.
  - Created endpoint /solutions/{pluginID}/vuln::POST.
  - Created endpoint /solutions/{pluginID}/asset::POST.
- AuditFile
  - filename and originalFilename now required for auditFileTemplate 'id' is '-1' instead of auditFileTemplate 'id' is not '-1' for /AuditFile::POST.
- Report
  - Removed non-existent endpoint /report/{id}/pause::POST.

- MDM
    - Added new MDM types Blackberry UEM and Microsoft Intune to /mdm::GET.

The following functionality was removed from Tenable Security Center API:

- IP Information
    - The /ipInfo::GET endpoint was deleted and the IP Information page was removed from API documentation. This functionality is now available through the /deviceInfo::GET endpoint.
- Repository
    - The /repository/ipInfo::GET endpoint was deleted. This functionality is now available through the /repository/{id}/deviceInfo::GET endpoint.
- Report
    - The /report/{id}/publish::POST endpoint was deleted.

Version 5.11.x

Tenable.sc 5.11.x API includes the following new functionality:

- Group
  - Added new field "createDefaultObjects" in /group::GET and /group/<id>::GET
  - Added new parameter "createDefaultObjects" in /group::POST and /group/<id>::PATCH
- Credential
  - Added new field “beyondtrust_api_user” in /credential::POST and /credential/<id>::PATCH for beyondTrust credentials of type "ssh" and "windows"
  - Added new parameter "beyondtrust_api_user” in /credential::GET and /credential/<id>::GET in the typeFields for credentials of type "ssh" and "windows"
- Scan Result
  - Added new optional filter "optimizeCompletedScans" to /scanResult::GET to skip retrieval of progress fields (completedIPs, completedChecks, totalChecks) for scans that are no longer in progress to optimize speed.

The following functionality was deprecated (marked for future removal):

- User
  - Marked fields "importReports", "importARCs", "importDashboards", "dashboardTemplate", and "arcTemplate" in /user::POST. During the deprecation period, the default of these fields will be updated to the new "createDefaultObjects" group setting.
- Organization Security Manager
  - Marked fields "importReports", "importARCs", "importDashboards", "dashboardTemplate", and "arcTemplate" in /user::POST. During the deprecation

period, the default of these fields will be updated to the new "createDefaultObjects" group setting

Version 5.10.x

Tenable.sc 5.10 API includes the following changes:

- System
  - Added new endpoint /system/debug::GET
  - Added new endpoint /system/debug::PATCH
- Plugin
  - Added new field “vprContext” to /plugin::GET
  - Added new field “vprContext” to /plugin/{id}::GET
- Plugin Family
  - Added new field “vprContext” to /pluginFamily/{id}/plugins::GET
- Scan
  - Added new field “enabled” to the schedule object inside /scan::POST
  - Added new field “enabled” to the schedule object inside /scan/{id}::PATCH
- Scanner
  - Added fields “accessKey” and “secretKey” to /scanner::GET
  - Added fields “accessKey” and “secretKey” to /scanner/{id}::GET
  - Added fields “accessKey” and “secretKey” to /scanner/{id}::POST

Tenable Security Center API: Accept Risk Rule

-

/acceptRiskRule

Methods

GET

Gets the list of Accept Risk Rules across all reps, plugins and orgs, unless filters are provided.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
**repository
**organization
**user
**plugin
**hostType
**hostValue
**port
**protocol
**expires
**status
comments
createdTime
modifiedTime

Legend

** = always comes back*
*** = comes back if fields list not specified on GET all*

redFont = *field is a JSON object (* ***e.g.*** *"repository" :{ "id" : <id>, "name" : <name> })*

Filters

Expand

```
repositoryIDs=<number>,... DEFAULT 0 (i.e. all Repositories)
pluginID=<number> | <string> "all" DEFAULT "all" (i.e. all Plugins)
port=<number> | <string> "all" DEFAULT "all" (i.e. all Ports)
```

Session User is role "1" (administrator)

```
organizationIDs=<number>,... | <string> "all" DEFAULT "all" (i.e.
all Organizations)
```

Session User is not role "1" (administrator)

```
organizationIDs=<number>,... | <string> "all" DEFAULT :sessionOrgID:
```

Paginated results:

By default, the result set encompasses all Accept Risk Rule

To obtain paginated results, a parameter value should be included in the request as follows:

?paginated=true

Additionally, for paginated results, the following parameters can be sent:

startOffset <number> (positive integer) DEFAULT 0,
endOffset <number> (integer >= startOffset) DEFAULT 50,
sortDirection <string> "ASC" | "DESC" DEFAULT "DESC",
sortField <string> "userID" | "pluginID" | "port" | "protocol" | "expires" | "createdTime",

Example Response

Expand


```
{
      "type" : "regular",
      "response" : [
              {
                      "id" : "3",
                      "hostType" : "all",
                      "hostValue" : "",
                      "port" : "any",
                      "protocol" : "any",
                      "expires" : "-1",
```

```
                        "status" : "0",
                        "repository" : {
                                "id" : "17",
                                "name" : "New Fields Repo",
                                "description" : "",
                                "type" : "Local",
                                "uuid" : "A2FF7E13-2C0E-470E-A3C9-E077FE065A54
                        "organization" : {
                                "id" : "8",
                                "name" : "Org",
                                "description" : "Testing for Policies with New
                                "uuid" : "FF00F4D0-5B9F-4A26-998C-19430295284A
                        "user" : {
                                "id" : "1",
                                "username" : "head",
                                "firstname" : "Security Manager",
                                "lastname" : "",
                                "uuid" : "96F2AD1B-1B83-462E-908A-84E6054F6B64
                        "plugin" : {
                                "id" : "0",
                                "name" : "Open Port",
                                "description" : "",
                                "type" : "active"                               }
                }
        ],
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1410275054
}
```


POST

Adds an Accept Risk Rule to one repository.

Request Parameters

Expand

```
{
       "repositories" : [
                {
                         "id" : <number>          }...
       ],
       "plugin" : {
                "id" : <number> },
    ...
```

hostType for Universal Repository type

```
        ...
       "hostType" : <string> "all" | "asset" | "ip" | "hostUUID",
    ...
```

hostType for Agent Repository type

```
        ...
       "hostType" : <string> "all" | "asset" | "uuid",
       ...
```

hostType for IPv4 or IPv6 Repository type

```
        ...
       "hostType" : <string> "all" | "asset" | "ip" ,
       ...
```

```
        "port" : <number:1..65535> | <string> "any" DEFAULT "any",
       "protocol" : <number:1..> | <string> "any" DEFAULT "any",
       "comments" : <string> DEFAULT "",
```

```
        "expires" : <number> (integer >= -1) DEFAULT -1 (not set)
        ...
}
```

hostType "asset"

The "hostValue" parameter should contain a usable, accessible Asset ID.

```
...
        "hostValue" : {
                "id" : <number> }
...
```

hostType "ip"

The "hostValue" parameter should contain a newline-separated and/or comma-separated list of IPs.

```
...
        "hostValue" : <string>...
```

hostType "uuid"

The "hostValue" parameter should contain a newline-separated and/or comma-separated list of UUIDs.

```
...
        "hostValue" : <string>...
```

hostType "hostUUID"

The "hostValue" parameter should contain a newline-separated and/or comma-separated list of UUIDs.

```
...
        "hostValue" : <string>...
```

Example Response

Expand


```
{
	"type" : "regular",
	"response" : [
		{
			"id" : "3",
			"hostType" : "all",
			"hostValue" : "",
			"port" : "any",
			"protocol" : "any",
			"comments" : "",
			"expires" : "-1",
			"status" : "0",
			"createdTime" : "1410275013",
			"modifiedTime" : "1410275013",
			"repository" : {
				"id" : "17",
				"name" : "New Fields Repo",
				"description" : "",
				"type" : "Local",
				"uuid" : "A2FF7E13-2C0E-470E-A3C9-E077FE065A54
			"organization" : {
				"id" : "8",
				"name" : "Org",
				"description" : "Testing for Policies with New
				"uuid" : "FF00F4D0-5B9F-4A26-998C-19430295284A
			"user" : {
				"id" : "1",
				"username" : "head",
				"firstname" : "Security Manager",
				"lastname" : "",
				"uuid" : "96F2AD1B-1B83-462E-908A-84E6054F6B64
			"plugin" : {
```

```
                                "id" : "0",
                                "name" : "Open Port",
                                "description" : "",
                                "type" : "active"                                }
                        }
                ],
                "error_code" : 0,
                "error_msg" : "",
                "warnings" : [],
                "timestamp" : 1410275013
        }
```


/acceptRiskRule/{id}

Methods

GET

Gets the Accept Risk Rule associated with {id}.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
**repository
**organization
**user
**plugin
**hostType
**hostValue
**port
**protocol
**expires

**status
comments
createdTime
modifiedTime

Legend

** = always comes back*
*** = comes back if fields list not specified on GET all*

redFont = *field is a JSON object (* ***e.g.*** *"repository" :{ "id" : <id>, "name" : <name> })*

Request Query Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
        "response" : {
                "id" : "3",
                "hostType" : "all",
                "hostValue" : "",
                "port" : "any",
                "protocol" : "any",
                "comments" : "",
                "expires" : "-1",
                "status" : "0",
                "createdTime" : "1410275013",
                "modifiedTime" : "1410275013",
                "repository" : {
                        "id" : "17",
                        "name" : "New Fields Repo",
                        "description" : "",
                        "type" : "Local",
```

```
                        "uuid" : "A2FF7E13-2C0E-470E-A3C9-E077FE065A54"
                "organization" : {
                        "id" : "8",
                        "name" : "Org",
                        "description" : "Testing for Policies with New Schema"
                        "uuid" : "FF00F4D0-5B9F-4A26-998C-19430295284A"
                "user" : {
                        "id" : "1",
                        "username" : "head",
                        "firstname" : "Security Manager",
                        "lastname" : "",
                        "uuid" : "96F2AD1B-1B83-462E-908A-84E6054F6B64"
                "plugin" : {
                        "id" : "0",
                        "name" : "Open Port",
                        "description" : "",
                        "type" : "active"               }
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1410275074
}
```


DELETE

Deletes the Accept Risk Rule associated with {id}, depending on access and permissions.

Request Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
        "response" : "",
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1403100582
}
```


/acceptRiskRule/apply

Methods

POST

Applies all rules for the given repository or all (id: 0)

Request Query Parameters

Expand


```
{
        "repository" : {
                "id" : <number> }
}
```


Example Response

Expand


```
{
        "type" : "regular",
        "response" : "",
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
```

```
        "timestamp" : 1410279161
}
```

Atlassian

Tenable Security Center API: Agent Group

-

/agentGroup/{agentScanID}

Methods

GET

Gets the list of Agent Groups based on local agent scan.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
**name
**description
uuid

remoteID

nessusManagerID
createdTime
modifiedTime

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

Request Parameters

None

Expand Parameters

None

Filter Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
        "response" : [
                {
                        "id" : "1",
                        "agentScanID" : "1",
                        "remoteID" : "3",
                        "uuid" : "-1",
                        "nessusManagerID" : "2",
                        "name" : "description",
                        "description" : "Agent Group #1 Description",
                        "createdTime" : 1406828330,
                        "modifiedTime" : 1406828330
        ],
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1406828340
}
```


/agentGroup/{agentScannerID}/remote

Methods

GET

Gets the list of Agent Groups based on remote Agent Scanner.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
**name
**description
uuid

remoteID

nessusManagerID
createdTime
modifiedTime

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

Request Parameters

None

Expand Parameters

credentials

Example Response

Expand

```
{
        "type" : "regular",
        "response" : [
                {
                        "id" : "1",
                        "agentScanID" : "1",
                        "remoteID" : "3",
                        "uuid" : "-1",
                        "nessusManagerID" : "2",
                        "name" : "description",
                        "description" : "Agent Group #1 Description",
                        "createdTime" : 1406828330,
                        "modifiedTime" : 1406828330
        ],
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1406828340
}
```


Atlassian

Tenable Security Center API: Agent Results Sync

/agentResultsSync

Methods

GET

Gets the list of Agent Results Syncs.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
**name
**description
**status
nessusManager
repository
scansGlob
dhcpTracking
emailOnLaunch
emailOnFinish
createdTime
modifiedTime
ownerGroup
creator
owner
reports
numDependents
schedule
lastDownloadSuccess
downloadResultsAfter

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*
redFont = *field is a JSON object (* ***e.g.*** *"repository" :{ "id" : <id>, "name" : <name> })*

Request Parameters

None

Expand Parameters

credentials

Filter Parameters

usable - The response will be an object containing an array of usable Agent Results Syncs. By default, both usable and manageable objects are returned.
manageable - The response will be an object containing all manageable Agent Results Syncs.. By default, both usable and manageable objects are returned.

Example Response

Expand


```
{
        "type" : "regular",
        "response" : {
                "usable" : [
                        {
                                "id" : "2",
                                "name" : "test",
                                "description" : ""                      },
                        {
                                "id" : "3",
                                "name" : "test2",
                                "description" : ""                      },
                        {
                                "id" : "4",
                                "name" : "POSTtest",
                                "description" : "This is a test for POST"
                ],
                "manageable" : [
                        {
                                "id" : "2",
                                "name" : "test",
                                "description" : ""                      },
                        {
                                "id" : "3",
                                "name" : "test2",
```

```
                                "description" : ""                          },
                        {
                                "id" : "4",
                                "name" : "POSTtest",
                                "description" : "This is a test for POST"
                ]
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1406828340
}
```


POST

Adds an Agent Results Sync, depending on access and permissions.

NOTE: The field *downloadResultsAfter* is a timestamp used to determine the cut off point when synchronizing results from agents. Any results before that timestamp will not be imported. The field is ONLY accepted during POST (Not PATCH).

Request Parameters

Expand


```
{
        "name" : <string>,
        "type" : <string> "plugin" | "policy",
        "description" : <string> DEFAULT "",
        "nessusManager" : {
                "id" : <number> },
        "repository" : {
                "id" : <number> },
        "scansGlob" : <string> DEFAULT "*",
```

```
        "dhcpTracking" : <string> DEFAULT "false",
        "schedule" : {
                "type" : "ical" | "never" | "rollover" | "template" <string>
DEFAULT "template",
        },
        "downloadResultsAfter" : <string> (Valid Unix Timestamp) DEFAULT "-
1",
        "reports" : [
                {
                        "id" : <number>,
                        "reportSource" : <string> "cumulative" | "patched" | "
| "lce" | "archive" | "mobile"          }...
        ] DEFAULT [],
        "emailOnLaunch" : <string> "false" | "true" DEFAULT "false",
        "emailOnFinish" : <string> "false" | "true" DEFAULT "false"}
```

schedule type is "ical"

```
...
        "schedule" : {
                "start" : <string> (This value takes the iCal format),
                "repeatRule" : <string> (This value takes the repeat rule form
        }
...
```

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "id" : "4",
```

```
            "name" : "POSTtest",
            "description" : "This is a test for POST",
            "scansGlob" : "Agent*",
            "dhcpTracking" : "false",
            "emailOnLaunch" : "false",
            "emailOnFinish" : "false",
            "status" : "0",
            "createdTime" : "1406815242",
            "modifiedTime" : "1406815242",
            "reports" : [],
            "numDependents" : "0",
            "downloadResultsAfter" : -1,
            "lastDownloadSuccess" : -1,
        "schedule" : {
            "type" : "never",
            "start" : "",
            "repeatRule" : ""        },
               "creator" : {
                       "id" : "1",
                       "username" : "head3",
                       "firstname" : "",
                       "lastname" : "",
                       "uuid" : "48F26F3B-6A79-4153-96DB-4C63D1BF3D46"
               "owner" : {
                       "id" : "1",
                       "username" : "head3",
                       "firstname" : "",
                       "lastname" : "",
                       "uuid" : "48F26F3B-6A79-4153-96DB-4C63D1BF3D46"
               "nessusManager" : {
                       "id" : "1",
                       "name" : "test manager",
                       "description" : ""              },
```

```
                "repository" : {
                        "id" : "2",
                        "name" : "test",
                        "description" : "test",
                        "type" : "Local"
                        "uuid" : "A2FF7E13-2C0E-470E-A3C9-E077FE065A54"
                "ownerGroup" : {
                        "id" : "0",
                        "name" : "Full Access",
                        "description" : "Full Access group"             }
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1406815242
}
```


/agentResultsSync/{id}

Methods

GET

Gets the Agent Results Sync associated with {id}.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
**name
**description
**status
nessusManager

repository
scansGlob
dhcpTracking
emailOnLaunch
emailOnFinish
createdTime
modifiedTime
ownerGroup
creator
owner
reports
numDependents
schedule
lastDownloadSuccess
downloadResultsAfter

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*
redFont = *field is a JSON object (* ***e.g.*** *"repository" :{ "id" : <id>, "name" : <name> })*

Request Parameters

None

Expand Parameters

credentials

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "id" : "4",
```

```
      "name" : "POSTtest",
      "description" : "This is a test for POST",
      "scansGlob" : "Agent*",
      "dhcpTracking" : "false",
      "emailOnLaunch" : "false",
      "emailOnFinish" : "false",
      "status" : "0",
      "createdTime" : "1406815242",
      "modifiedTime" : "1406815242",
      "reports" : [],
      "numDependents" : "0",
      "lastDownloadSuccess" : -1,
      "schedule" : {
   "type" : "never",
   "start" : "",
   "repeatRule" : ""        },
      "nessusManager" : {
              "id" : "1",
              "name" : "test manager",
              "description" : ""              },
      "repository" : {
              "id" : "2",
              "name" : "test",
              "description" : "test",
              "type" : "Local"
              "uuid" : "A2FF7E13-2C0E-470E-A3C9-E077FE065A54"
      "ownerGroup" : {
              "id" : "0",
              "name" : "Full Access",
              "description" : "Full Access group"            },
      "creator" : {
              "id" : "1",
              "username" : "head3",
```

```
                        "firstname" : "",
                        "lastname" : "",
                        "uuid" : "48F26F3B-6A79-4153-96DB-4C63D1BF3D46"
                "owner" : {
                        "id" : "1",
                        "username" : "head3",
                        "firstname" : "",
                        "lastname" : "",
                        "uuid" : "48F26F3B-6A79-4153-96DB-4C63D1BF3D46"
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1406828664
}
```


PATCH

Edits the Agent Results Sync associated with {id}, changing only the passed in fields.

Request Parameters

(All fields are optional)

See /agentResultsSync::POST for parameters.

Example Response

See /agentResultsSync/{id}::GET

DELETE

Deletes the Agent Results Sync associated with {id}, depending on access and permissions.

Request Parameters

None

Example Response

Expand

```
{
        "type" : "regular",
        "response" : "",
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1406732180
}
```

/agentResultsSync/{id}/copy

Methods

POST

Copies the Agent Results Sync associated with {id}, depending on access and permissions.

Request Parameters

Expand

```
{
        "name" : <string>,
        "targetUser" : {
                "id" : <number> }
}
```

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "resultsSync" : {
                        "id" : "6",
                        "name" : "Agents Scan Copy",
```

```
                        "description" : "",
                        "scansGlob" : "*",
                        "dhcpTracking" : "true",
                        "emailOnLaunch" : "false",
                        "emailOnFinish" : "false",
                        "status" : "0",
                        "lastDownloadSuccess" : "-1",
                        "createdTime" : "1442338982",
                        "modifiedTime" : "1442338982",
                        "reports" : [],
                        "numDependents" : "0",
                        "schedule" : {
                                "id" : "98",
                                "objectType" : "synchronizeAgentResults",
                                "type" : "template",
                                "start" : "",
                                "repeatRule" : "",
                                "nextRun" : 0
                        },
                        "nessusManager" : {
                                "id" : "24",
                                "name" : "DEV nessus 6.5 cloud with agent",
                                "description" : "Chris Anderson's scanner, ple
zone"                    },
                        "repository" : {
                                "id" : "14",
                                "name" : "John's Test IPv4 Rep",
                                "description" : "",
                                "type" : "Local"
                                "uuid" : "A2FF7E13-2C0E-470E-A3C9-E077FE065A54
                        "ownerGroup" : {
                                "id" : "0",
                                "name" : "Full Access",
```

```
                                "description" : "Full Access group"
                        "creator" : {
                                "id" : "1",
                                "username" : "sm",
                                "firstname" : "Security",
                                "lastname" : "Manager",
                                "uuid" : "48F26F3B-6A79-4153-96DB-4C63D1BF3D4
                        "owner" : {
                                "id" : "2",
                                "username" : "qahead",
                                "firstname" : "",
                                "lastname" : "",
                                "uuid" : "48F26F3B-6A79-4153-96DB-4C63D1BF3D4
                }
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1442338982
}
```


/agentResultsSync/{id}/launch

Methods

POST

Launches the Agent Results Sync associated with {id}.

Request Parameters

None

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "resultsSyncID" : "1",
                "syncResult" : {
                        "initiatorID" : "1",
                        "ownerID" : "1",
                        "ownerGID" : "0"                },
                "scanID" : -1,
                "resultsSyncID" : "1",
                "repositoryID" : "14",
                "jobID" : "93484",
                "name" : "John's Agent Scan",
                "description" : "",
                "details" : "",
                "status" : "Queued",
                "importStatus" : "No Results",
                "downloadFormat" : "v2",
                "dataFormat" : "IPv4",
                "resultType" : "agents",
                "running" : false,
                "errorDetails" : "",
                "importErrorDetails" : "",
                "totalIPs" : -1,
                "scannedIPs" : 0,
                "startTime" : -1,
                "finishTime" : 0,
                "id" : "45"     },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1442339263
}
```


Atlassian

Tenable Security Center API: Agent Scan

/agentScan

Methods

GET

Gets the list of Agent Scans.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
**name
**description
**status
nessusManager
repository
scanWindow
agentGroups
createdTime
modifiedTime
ownerGroup
creator
owner
reports
schedule
policy

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

redFont = *field is a JSON object (* ***e.g.*** *"repository" :{ "id" : <id>, "name" : <name> })*

Request Parameters

None

Expand Parameters

credentials

Filter Parameters

usable - The response will be an object containing an array of usable Agent Scans. By default, both usable and manageable objects are returned.
manageable - The response will be an object containing all manageable Agent Scans. By default, both usable and manageable objects are returned.

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "usable" : [
                        {
                                "id" : "2",
                                "name" : "Agent Scan #1",
                                "description" : ""                    },
                        {
                                "id" : "3",
                                "name" : "Agent Scan #2",
                                "description" : ""                    },
                        {
```

```
                                "id" : "4",
                                "name" : "Agent Scan #3",
                                "description" : "Description for Agent Scan #3"
                ],
                "manageable" : [
                        {
                                "id" : "2",
                                "name" : "Agent Scan #4",
                                "description" : ""                      },
                        {
                                "id" : "3",
                                "name" : "Agent Scan #5",
                                "description" : ""                      },
                        {
                                "id" : "4",
                                "name" : "Agent Scan #6",
                                "description" : "Description for Agent Scan #6"
                ]
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1406828340
}
```


POST

Adds an Agent Scan, depending on access and permissions.

Request Parameters

Expand


```
{
        "name" : <string>,
```

```
        "type" : <string> "plugin" | "policy",
        "description" : <string> DEFAULT "",
        "nessusManager" : {
                "id" : <number> },
        "repository" : {
                "id" : <number> },
        "scanWindow" : <string> DEFAULT "60",
        "policy": {
        {<policy ID Record>}...
        } (Optional),
    "agentGroups" : {
         "id" : <number>,
         "name" : <string>,
                "description" : <string>,
    },
        "schedule" : {
                "type" : "ical" | "never" | "rollover" | "template" <string>
DEFAULT "template",
        },
        "reports" : [
                {
                        "id" : <number>,
                        "reportSource" : <string> "cumulative" | "individual"
        ] DEFAULT []
}
```

schedule type is "ical"

```
...
        "schedule" : {
                "start" : <string> (This value takes the iCal format),
                "repeatRule" : <string> (This value takes the repeat rule form
```

```
        }
...
```

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "id" : "4",
                "creatorID" : "1",
                "ownerID" : "1",
                "name" : "POSTtest",
                "description" : "This is a test for POST",
                "status" : "0",
         "scanWindow" : 60,
                "policy" : [],
                "agentGroup" : {
                        "id" : 5,
                        "name" : "Nessus Manager",
                        "description" : ""              },
                "createdTime" : "1406815242",
                "modifiedTime" : "1406815242",
                "reports" : [],
         "schedule" : {
             "type" : "never",
             "start" : "",
             "repeatRule" : ""        },
                "creator" : {
                        "id" : "1",
                        "username" : "head3",
                        "firstname" : "",
                        "lastname" : ""         },
```

```
                "owner" : {
                        "id" : "1",
                        "username" : "head3",
                        "firstname" : "",
                        "lastname" : ""         },
                "nessusManager" : {
                        "id" : "1",
                        "name" : "test manager",
                        "description" : ""              },
                "repository" : {
                        "id" : "2",
                        "name" : "test",
                        "description" : "test"          },
                "ownerGroup" : {
                        "id" : "0",
                        "name" : "Full Access",
                        "description" : "Full Access group"             }
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1406815242
}
```


/agentScan/{id}

Methods

GET

Gets the Agent Scan associated with {id}.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
**name
**description
**status
nessusManager
repository
scanWindow
agentGroups
createdTime
modifiedTime
ownerGroup
creator
owner
reports
schedule
policy

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

redFont = *field is a JSON object (**e.g.** "repository" :{ "id" : <id>, "name" : <name> })*

Request Parameters

None

Expand Parameters

credentials

Example Response

Expand

```
{
	"type": "regular",
	"response": {
		"id": "4",
		"name": "Agent Scan",
		"description": "Agent Scan Description",
		"scansWindow": 60,
		"agentGroups": {
			"id": 3,
			"name": "Agent Group",
			"description": "Description"		},
		"emailOnLaunch": "false",
		"emailOnFinish": "false",
		"status": "0",
		"createdTime": "1406815242",
		"modifiedTime": "1406815242",
		"policy": {
			"id": "1000002",
			"context": "",
			"name": "Policy Agent Scan",
			"description": "Description",
			"tags": "",
			"uuid": "90B2DB2A-C659-442D-B11E-78023EE7",
			"owner": {
				"id": "1",
				"username": "username",
				"firstname": "First Name",
				"lastname": "Last Name",
				"uuid": "466BE9F7-007C-4F4C-B758-16B26F3F7"
			"ownerGroup": {
				"id": "0",
				"name": "Full Access",
				"description": "Full Access group"
```

```
        },
        "reports": [],
        "schedule": {
                "type": "never",
                "start": "",
                "repeatRule": ""                },
        "nessusManager": {
                "id": "1",
                "name": "test manager",
                "description": ""               },
        "repository": {
                "id": "2",
                "name": "test",
                "description": "test"           },
        "ownerGroup": {
                "id": "0",
                "name": "Full Access",
                "description": "Full Access group"              },
        "creator": {
                "id": "1",
                "username": "head3",
                "firstname": "",
                "lastname": ""          },
        "owner": {
                "id": "1",
                "username": "head3",
                "firstname": "",
                "lastname": ""          }
},
"error_code": 0,
"error_msg": "",
"warnings": [],
"timestamp": 1406828664
```

```
}
```

PATCH

Edits the Agent Scan associated with {id}, changing only the passed in fields.

Request Parameters

(All fields are optional)

See /agentScan::POST for parameters.

Example Response

See /agentScan/{id}::GET

DELETE

Deletes the Agent Scan associated with {id}, depending on access and permissions.

Request Parameters

None

Example Response

Expand

```
{
        "type" : "regular",
        "response" : "",
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1406732180
}
```

/agentScan/{id}/launch

Methods

POST

Launches the Agent Scan associated with {id}.

Request Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
        "response" : {
                "scanID" : -1,
                "resultsSyncID" : "-1",
                "agentScanID" : "7",
                "repositoryID" : "14",
                "jobID" : "93484",
                "name" : "Agent Scan",
                "description" : "",
                "details" : "",
                "status" : "Queued",
                "importStatus" : "No Results",
                "downloadFormat" : "v2",
                "dataFormat" : "IPv4",
                "resultType" : "agents",
                "running" : false,
                "errorDetails" : "",
                "importErrorDetails" : "",
                "totalIPs" : -1,
                "scannedIPs" : 0,
                "startTime" : -1,
                "finishTime" : 0,
                "id" : "45"     },
        "error_code" : 0,
```

```
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1442339263
}
```

Atlassian

Tenable Security Center API: Alert

/alert

Methods

GET

Gets the list of Alerts.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
**name
**description
**status
owner
ownerGroup
triggerName
triggerOperator
triggerValue
modifiedTime
createdTime
lastTriggered
lastEvaluated
executeOnEveryTrigger

didTriggerLastEvaluation
schedule
action
query
canUse
canManage

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*
redFont = *field is a JSON object (**e.g.** "repository" :{ "id" : <id>, "name" : <name> })*

Filter Parameters

usable - The response will be an object containing an array of usable Alerts. By default, both usable and manageable objects are returned.
manageable - The response will be an object containing all manageable Alerts. By default, both usable and manageable objects are returned.

Request Query Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
        "response" : {
                "usable" : [
                        {
                                "id" : "1",
                                "name" : "Test Alert 1",
                                "description" : "All Action Types, vuln query"
                                "status" : "0"                  }
                ],
```

```
                "manageable" : [
                        {
                                "id" : "1",
                                "name" : "Test Alert 1",
                                "description" : "All Action Types, vuln query'
                                "status" : "0"                  }
                ]
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1424975381
}
```


POST

Adds an Alert.

NOTE: Alerts do not currently support Queries of type 'all', 'alert' or 'mobile'. Values for triggerName are based on the Query's 'type' and are as follows:

- **query type 'lce':** sumip, sumport, listdata
- **query type 'vuln':** sumip, sumport, sumid
- **query type 'ticket':** listtickets
- **query type 'user':** listusers

Request Parameters

Expand


```
{
        "name" : <string>,
        "description" : <string> DEFAULT "",
        "query" : {
                <valid Query Object> | "id" : <number>  },
```

```
        "triggerName" : <string>,
        "triggerOperator" : <string> '>=' | '<=' | '=' | '!=',
        "triggerValue" : <number>,
        "executeOnEveryTrigger" : <string> "false" | "true" DEFAULT
"false",
        "schedule" : {
                "type" : <string> "dependent" | "ical" | "never" | "rollover"
"template" DEFAULT "never"              type "ical"             -----------
                "start" : <string> (This value takes the iCal format),
                "repeatRule" : <string> (This value takes the repeat rule form
        },
        "action" : [
                {
                        "type" : <string> "email" | "notification" | "report"
"syslog" | "ticket",

                        type "email"                    ------------
                        "subject" : <string>,
                        "message" : <string> DEFAULT "",
                        "addresses" : <string> (valid email addresses separate
DEFAULT "",
                        "users" : [
                                {
                                        "id" : <number>
                        ] DEFAULT [],
                        "includeResults" : <string> "false" | "true" DEFAULT "
                        type "notification"                     ------------
                        "message" : <string>,
                        "users" : [
                                {
                                        "id" : <string>
                        ]
```

```
                        type "report"                    ------------
                        "report" : {
                                "id" : <number>                 }

                        type "scan"                      ------------
                        "scan" : {
                                "id" : <number>,
                        }

                        type "syslog"                    ------------
                        "host" : <string> (valid IP address),
                        "port" : <string> (valid server port),
                        "message"       : <string>,
                        "severity"      : <string> "Critical" | "Notice" | "Wa
"ticket"                        ------------
                        "assignee" : {
                                "id" : <number>                 },
                        "name" : <string> DEFAULT "",
                        "description" : <string> DEFAULT "",
                        "notes" : <string> DEFAULT ""           }...
        ]
}
```

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "id" : "2",
                "name" : "Test Patch",
                "description" : "All Action Types, vuln query",
                "triggerName" : "sumip",
```

```
"triggerOperator" : "=",
"triggerValue" : "1000",
"modifiedTime" : "1424978025",
"createdTime" : "1424976588",
"lastTriggered" : "0",
"lastEvaluated" : "1424978004",
"executeOnEveryTrigger" : "false",
"didTriggerLastEvaluation" : "false",
"status" : "0",
"action" : [
        {
                "id" : "61",
                "type" : "email",
                "definition" : {
                        "subject" : "Test Email Action",
                        "message" : "",
                        "addresses" : "",
                        "users" : [
                                {
                                        "id" : "1",
                                        "username" : "head",
                                        "firstname" : "Securit
                                        "lastname" : "",
                                        "uuid" : "11B3FACD-5E
                        ],
                        "includeResults" : "true"
                "objectID" : "-1",
                "status" : "0",
                "users" : [
                        {
                                "id" : "1",
                                "username" : "head",
                                "firstname" : "Security Manage
```

```
                                "lastname" : "",
                                "uuid" : "11B3FACD-5E6F-4D8D-
                        ]
                },
                {
                        "id" : "62",
                        "type" : "notification",
                        "definition" : {
                                "message" : "Test Notification Action"
                                "users" : [
                                        {
                                                "id" : "1",
                                                "username" : "head",
                                                "firstname" : "Securit
                                                "lastname" : "",
                                                "uuid" : "11B3FACD-5E
                                        ]
                        },
                        "objectID" : "-1",
                        "status" : "0",
                        "users" : [
                                {
                                        "id" : "1",
                                        "username" : "head",
                                        "firstname" : "Security Manage
                                        "lastname" : "",
                                        "uuid" : "11B3FACD-5E6F-4D8D-
                        ]
                },
                {
                        "id" : "63",
                        "type" : "report",
                        "definition" : {
```

```
                                "reportID" : "11",
                                "report" : {
                                        "id" : -1,
                                        "name" : "",
                                        "description" : ""
                                },
                                "objectID" : "11",
                                "status" : "0",
                                "users" : []
                        },
                        {
                                "id" : "64",
                                "type" : "scan",
                                "definition" : {
                                        "scan" : {
                                                "id" : "60",
                                                "name" : "Test Scan",
                                                "description" : "Used for Ale
schedule",
                                                "type" : "policy",
                                                "uuid" : "29F2B9E1-ADE9-4550-
                                },
                                "objectID" : "60",
                                "status" : "0",
                                "users" : []
                        },
                        {
                                "id" : "65",
                                "type" : "syslog",
                                "definition" : {
                                        "host" : "127.0.0.1",
                                        "port" : "22",
                                        "message" : "127.0.0.1 port 22",
```

```
                        "severity" : {
                                "id" : -1,
                                "name" : "",
                                "description" : ""
                        },
                        "objectID" : "-1",
                        "status" : "0",
                        "users" : []
                },
                {
                        "id" : "66",
                        "type" : "ticket",
                        "definition" : {
                                "name" : "",
                                "description" : "",
                                "notes" : "",
                                "assigneeID" : "1",
                                "assignee" : {
                                        "id" : "1",
                                        "username" : "head",
                                        "firstname" : "Security Manage
                                        "lastname" : "",
                                        "uuid" : "11B3FACD-5E6F-4D8D-
                        },
                        "objectID" : "-1",
                        "status" : "0",
                        "users" : []
                }
        ],
        "schedule" : {
                "type" : "never",
                "start" : "",
                "repeatRule" : ""               },
```

```
                "query" : {
                        "id" : "2",
                        "name" : "Post Copy Response Example",
                        "description" : ""              },
                "canUse" : "true",
                "canManage" : "true",
                "owner" : {
                        "id" : "1",
                        "username" : "head",
                        "firstname" : "Security Manager",
                        "lastname" : "",
                        "uuid" : "11B3FACD-5E6F-4D8D-B596-5992EECC9104"
                "ownerGroup" : {
                        "id" : "0",
                        "name" : "Full Access",
                        "description" : "Full Access group"             }
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1426867363
}
```


/alert/{id}

Methods

GET

Gets the Alert associated with {id}.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
**name
**description
**status
owner
ownerGroup
triggerName
triggerOperator
triggerValue
modifiedTime
createdTime
lastTriggered
lastEvaluated
executeOnEveryTrigger
didTriggerLastEvaluation
schedule
action
query
canUse
canManage

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*
redFont = *field is a JSON object (* ***e.g.*** *"repository" :{ "id" : <id>, "name" : <name> })*

Request Parameters

None

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "id" : "2",
                "name" : "Test Patch",
                "description" : "All Action Types, vuln query",
                "triggerName" : "sumip",
                "triggerOperator" : "=",
                "triggerValue" : "1000",
                "modifiedTime" : "1424978025",
                "createdTime" : "1424976588",
                "lastTriggered" : "0",
                "lastEvaluated" : "1424978004",
                "executeOnEveryTrigger" : "false",
                "didTriggerLastEvaluation" : "false",
                "status" : "0",
                "action" : [
                        {
                                "id" : "61",
                                "type" : "email",
                                "definition" : {
                                        "subject" : "Test Email Action",
                                        "message" : "",
                                        "addresses" : "",
                                        "users" : [
                                                {
                                                        "id" : "1",
                                                        "username" : "head",
                                                        "firstname" : "Securit
                                                        "lastname" : "",
                                                        "uuid" : "11B3FACD-5E
                                        ],
                                        "includeResults" : "true"
```

```
                        "objectID" : "-1",
                        "status" : "0",
                        "users" : [
                                {
                                        "id" : "1",
                                        "username" : "head",
                                        "firstname" : "Security Manage
                                        "lastname" : "",
                                        "uuid" : "11B3FACD-5E6F-4D8D-
                        ]
                },
                {
                        "id" : "62",
                        "type" : "notification",
                        "definition" : {
                                "message" : "Test Notification Action"
                                "users" : [
                                        {
                                                "id" : "1",
                                                "username" : "head",
                                                "firstname" : "Securit
                                                "lastname" : "",
                                                "uuid" : "11B3FACD-5E
                                ]
                        },
                        "objectID" : "-1",
                        "status" : "0",
                        "users" : [
                                {
                                        "id" : "1",
                                        "username" : "head",
                                        "firstname" : "Security Manage
                                        "lastname" : "",
```

```
                                        "uuid" : "11B3FACD-5E6F-4D8D-
                        ]
                },
                {
                        "id" : "63",
                        "type" : "report",
                        "definition" : {
                                "reportID" : "11",
                                "report" : {
                                        "id" : -1,
                                        "name" : "",
                                        "description" : ""
                        },
                        "objectID" : "11",
                        "status" : "0",
                        "users" : []
                },
                {
                        "id" : "64",
                        "type" : "scan",
                        "definition" : {
                                "scan" : {
                                        "id" : "60",
                                        "name" : "Test Scan",
                                        "description" : "Used for Ale
schedule",
                                        "type" : "policy",
                                        "uuid" : "29F2B9E1-ADE9-4550-
                        },
                        "objectID" : "60",
                        "status" : "0",
                        "users" : []
                },
```

```
                {
                        "id" : "65",
                        "type" : "syslog",
                        "definition" : {
                                "host" : "127.0.0.1",
                                "port" : "22",
                                "message" : "127.0.0.1 port 22",
                                "severity" : {
                                        "id" : -1,
                                        "name" : "",
                                        "description" : ""
                        },
                        "objectID" : "-1",
                        "status" : "0",
                        "users" : []
                },
                {
                        "id" : "66",
                        "type" : "ticket",
                        "definition" : {
                                "name" : "",
                                "description" : "",
                                "notes" : "",
                                "assigneeID" : "1",
                                "assignee" : {
                                        "id" : "1",
                                        "username" : "head",
                                        "firstname" : "Security Manage
                                        "lastname" : "",
                                        "uuid" : "11B3FACD-5E6F-4D8D-
                        },
                        "objectID" : "-1",
                        "status" : "0",
```

```
                                "users" : []
                        }
                ],
                "schedule" : {
                        "type" : "never",
                        "start" : "",
                        "repeatRule" : ""               },
                "query" : {
                        "id" : "2",
                        "name" : "Post Copy Response Example",
                        "description" : ""              },
                "canUse" : "true",
                "canManage" : "true",
                "owner" : {
                        "id" : "1",
                        "username" : "head",
                        "firstname" : "Security Manager",
                        "lastname" : "",
                        "uuid" : "11B3FACD-5E6F-4D8D-B596-5992EECC9104"
                "ownerGroup" : {
                        "id" : "0",
                        "name" : "Full Access",
                        "description" : "Full Access group"             }
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1426867363
}
```


PATCH

Edits the Alert associated with {id}, changing only the passed in fields.

Request Parameters

(All fields are optional)

See /alert::POST for parameters.

Example Response

See /alert/{id}::GET for example response.

DELETE

Deletes the Alert associated with {id}, depending on access and permissions.

Request Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
        "response" : "1",
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1401911117
}
```


/alert/{id}/execute

Methods

POST

Executes the Alert associated with {id}, depending on access and permissions

Request Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
        "response" : {
                "id" : "1",
                "name" : "Test Alert 1",
                "description" : "All Action Types, vuln query",
                "triggerName" : "sumip",
                "triggerOperator" : "=",
                "triggerValue" : "1000",
                "modifiedTime" : "1424812161",
                "createdTime" : "1424812161",
                "lastTriggered" : "0",
                "lastEvaluated" : "0",
                "executeOnEveryTrigger" : "false",
                "didTriggerLastEvaluation" : "false",
                "status" : "0",
                "action" : [
                        {
                                "id" : "1",
                                "type" : "email",
                                "definition" : {
                                        "subject" : "Test Email Action",
                                        "message" : "",
                                        "addresses" : "",
                                        "users" : [
                                                {
                                                        "id" : "1",
                                                        "username" : "head",
                                                        "firstname" : "Securit
                                                        "lastname" : "",
                                                        "uuid" : "11B3FACD-5E
                                        ],
```

```
                        "includeResults" : "true"
                "objectID" : "-1",
                "status" : "0",
                "subject" : "Test Email Action",
                "message" : "",
                "addresses" : "",
                "users" : [
                        {
                                "id" : "1",
                                "username" : "head",
                                "firstname" : "Security Manage
                                "lastname" : "",
                                "uuid" : "11B3FACD-5E6F-4D8D-
                ],
                "includeResults" : "true"
        {
                "id" : "2",
                "type" : "notification",
                "definition" : {
                        "message" : "Test Notification Action"
                        "users" : [
                                {
                                        "id" : "1",
                                        "username" : "head",
                                        "firstname" : "Securit
                                        "lastname" : "",
                                        "uuid" : "11B3FACD-5E
                        ]
                },
                "objectID" : "-1",
                "status" : "0",
                "message" : "Test Notification Action",
                "users" : [
```

```
                        {
                                "id" : "1",
                                "username" : "head",
                                "firstname" : "Security Manage
                                "lastname" : "",
                                "uuid" : "11B3FACD-5E6F-4D8D-
                        ]
                },
                {
                        "id" : "3",
                        "type" : "report",
                        "definition" : {
                                "report" : {
                                        "id" : "11"
                        },
                        "objectID" : "11",
                        "status" : "0",
                        "report" : {
                                "id" : "11"
                        "users" : []
                },
                {
                        "id" : "4",
                        "type" : "scan",
                        "definition" : {
                                "scan" : {
                                        "id" : "60",
                                        "name" : "Test Scan",
                                        "description" : "Used for Ale
schedule",
                                        "type" : "policy",
                                        "uuid" : "29F2B9E1-ADE9-4550-
                        },
```

```
                        "objectID" : "60",
                        "status" : "0",
                        "users" : []
                },
                {
                        "id" : "5",
                        "type" : "syslog",
                        "definition" : {
                                "host" : "127.0.0.1",
                                "port" : "22",
                                "message" : "127.0.0.1 port 22",
                                "severity" : {
                                        "id" : -1,
                                        "name" : "",
                                        "description" : ""
                        },
                        "objectID" : "-1",
                        "status" : "0",
                        "host" : "127.0.0.1",
                        "port" : "22",
                        "message" : "127.0.0.1 port 22",
                        "severity" : {
                                "id" : -1,
                                "name" : "",
                                "description" : ""
                        "users" : []
                },
                {
                        "id" : "6",
                        "type" : "ticket",
                        "definition" : {
                                "assignee" : {
                                        "id" : "1",
```

```
                                        "username" : "head",
                                        "firstname" : "Security Manage
                                        "lastname" : "",
                                        "uuid" : "11B3FACD-5E6F-4D8D-
                                "name" : "",
                                "description" : "",
                                "notes" : ""
                        "objectID" : "-1",
                        "status" : "0",
                        "name" : "",
                        "description" : "",
                        "notes" : "",
                        "users" : []
                }
        ],
        "schedule" : {
                "type" : "never",
                "start" : "",
                "repeatRule" : ""               },
        "query" : {
                "id" : "2"              },
        "canUse" : "true",
        "canManage" : "true",
        "owner" : {
                "id" : "1",
                "username" : "head",
                "firstname" : "Security Manager",
                "lastname" : "",
                "uuid" : "11B3FACD-5E6F-4D8D-B596-5992EECC9104"
        "ownerGroup" : {
                "id" : "0",
                "name" : "Full Access",
                "description" : "Full Access group"            }
```

```
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1424975475
}
```

Atlassian

Tenable Security Center API: Analysis

/analysis

Methods

POST

Processes a query for analysis

Request Parameters

Expand

Note

If the parameter query['id'] is not specified, the *query* parameter will require a valid query, ~~unless the type is "scLog"~~ (deprecated in 5.19.0). The format for the full query definition can be found in the Query section of the API.

Note

The results are inclusive of the startOffset parameter value and exclusive of the endOffset parameter value.

Type: vuln (Expand)

Vuln Type

```
{
	"type" : "vuln",
	"query" : {
		"id" : <number> | (valid query)
	},
	"sortDir" : <string> "ASC" | "DESC" OPTIONAL
	"sortField" : <string> (alphanumeric; any valid field returned in
the results entry for the corresponding tool.  [Some restrictions
apply.]  Must accompany sortDir),
	"sourceType" : <string> "individual" | "cumulative" | "patched",
	"startOffset" : <number>,
	"endOffset" : <number>,
}
```

When the sourceType is "individual", a scanID must be provided in the root of the request object:

```
{
	"type" : "vuln",
	"query" : {
		"id" : <number> | (valid query)
	},
	"sortDir" : <string> "ASC" | "DESC" OPTIONAL
	"sortField" : <string> (alphanumeric; any valid field returned in
the results entry for the corresponding tool.  [Some restrictions
apply.]  Must accompany sortDir),
	"sourceType" : "individual",
	"startOffset" : <number>,
	"endOffset" : <number>,
	"scanID" : <number>,
	"view" : "all" | "new" | "patched"}
```

Type: event (Expand)

Event Type

```
{
       "type" : "event",
       "query" : {
              "id" : <number> | (valid query)
       },
       "sortDir" : <string> "ASC" | "DESC" OPTIONAL
       "sortField" : <string> (alphanumeric; any valid field returned in
the results entry for the corresponding tool.  [Some restrictions
apply.]  Must accompany sortDir),
       "sourceType" : <string> "lce" | "archive"}
```

When the sourceType is "archive", lceID and view must be provided in the root of the request object:

```
{
       "type" : "event",
       "query" : {
              "id" : <number> | (valid query)
       },
       "sortDir" : <string> "ASC" | "DESC" OPTIONAL
       "sortField" : <string> (alphanumeric; any valid field returned in
the results entry for the corresponding tool.  [Some restrictions
apply.]  Must accompany sortDir),
       "sourceType" : "archive",
       "lceID" : <number>,
       "view" : <string> (silo id)
}
```

Type: user (Expand)

User Type

```
{
        "type" : "user",
        "query" : {
                "id" : <number> | (valid query)
        }
}
```

Type: scLog (Expand)

~~SCLog Type~~ (deprecated in 5.19.0)

scLog has a unique query object with its own special filters.

```
{
        "type" : "scLog",
        "date" : scLog basename (eg. "201412") | "all",
        "query": {
                "startOffset" : <number>,
                "endOffset" : <number>,
                "filters" : [
                        {
                                "filterName" : "keywords",
                                        "operator" : "=",
                                "value" : <string>                              },
                        {
                                "filterName" : "severity",
                                "value" : {
                                        "id" : <number> [0-2],
                                        "operator" : "=",
                                        "name":"INFO|WARNING|CRITICAL"
                        },
                        {
                                "filtername" : "initiator",
                                "operator" : "=",
```

```
                                "value" : {
                                        "id" : <number>,
                                        "username" : <string>
                        },
                        {
                                "filterName" : "module",
                                "operator" : "=",
                                "value" : <string> (eg. "auth")
                        },
                        {
                                "filterName" : "organization",
                                "value" : {
                                        "id" : <number>
                        }
                ]
        }
}
```

scLog basenames can be retrieved from the system::GET call, but only for a logged in user.

Type: mobile (Expand)

Mobile Type

```
{
        "type" : "mobile",
        "query" : {
                "id" : <number> | (valid query)
        },
        "sortDir" : <string> "ASC" | "DESC" OPTIONAL,
        "sortField" : <string> (alphanumeric; any valid field returned in
the results entry for the corresponding tool.  [Some restrictions
apply.]  Must accompany sortDir),
        "startOffset" : <number>,
```

```
        "endOffset" : <number>}
```

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "totalRecords" : "1",
                "returnedRecords" : 1,
                "startOffset" : "0",
                "endOffset" : "50",
                "matchingDataElementCount" : "-1",
                "results":[
                        {
                                "pluginID" : "119500",
                                "severity" : {
                                        "id" : "4",
                                        "name" : "Critical",
                                        "description" : "Critical Severity"
                                "vprScore" : "6.7",
                                "vprContext" : "[
                                        {
                                                "id" : "age_of_vuln",
                                                "name" : "Vulnerability Age",
                                                "value" : "60 - 180 days",
                                                "type" : "string"
                                        {
                                                "id" : "cvssV3_impactScore",
                                                "name" : "CvssV3 Impact Score"
                                                "value" : 5.9,
                                                "type" : "number"
                                        {
```

```
                                "id" : "exploit_code_maturity"
                                "name" : "Exploit Code Maturit
                                "value" : "Unproven",
                                "type" : "string"
                            {
                                "id" : "predicted_impactScore"
                                "name" : "Predicted Impact Sc
                                "value" : false,
                                "type" : "boolean"
                            {
                                "id" : "product_coverage",
                                "name" : "Product Coverage",
                                "value" : "Low",
                                "type" : "string"
                            {
                                "id" : "threat_intensity_last_
                                "name " : "Threat Intensity",
                                "value" : "Low",
                                "type" : "string"
                            {
                                "id" : "threat_recency",
                                "name" : "Threat Recency",
                                "value" : "7 to 30 days",
                                "type" : "string"
                            {
                                "id" : "threat_sources_last_28
                                "name" : "Threat Sources",
                                "value" : "Security Research",
                                "type" : "string"
                    ]",
                    "ip" : "172.26.48.75",
                    "uuid" : "",
                    "port" : "8080",
```

```
                        "protocol" : "TCP",
                        "name" : "Jenkins < 2.138.4 LTS \/ 2.150.1 LTS \/ 2.15
MultipleVulnerabilities",
                        "dnsName" : "",
                        "macAddress" : "00:50:56:be:27:da",
                        "netbiosName" : "TARGET\\WINDOW7X64",
                        "uniqueness" : "repositoryID,ip,dnsName",
                        "hostUniqueness" : "repositoryID,ip,dnsName",
                        "family" : {
                                        "id" : "6",
                                        "name" : "CGI abuses",
                                        "type" : "active"
                        "repository" : {
                                        "id" : "516",
                                        "name" : "repo1",
                                        "description" : "",
                                        "dataFormat" : "IPv4"
                        "pluginInfo" : "119500 (8080\/6) Jenkins < 2.138.4 LTS
LTS \/ 2.154 Multiple Vulnerabilities"                  }
                ]
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1553525692
}
```


/analysis/download

Methods

POST

Downloads an analysis of a Query

Request Parameters

Expand

Note

The "user" type of Analysis is not supported in download.

Note

The results are inclusive of the startOffset parameter value and exclusive of the endOffset parameter value.

Type: vuln (Expand)

Vuln Type

```
{
        "type" : "vuln",
        "query" : {
                "id" : <number> | (valid query)
        },
        "sourceType" : <string> "individual" | "cumulative" | "patched",
        "sortDir" : <string> "ASC" | "DESC" OPTIONAL,
        "sortField" : <string> (alphanumeric; any valid field returned in
the results entry for the corresponding tool.  [Some restrictions
apply.]  Must accompany sortDir),
        "startOffset" : <number>,
        "endOffset" : <number>,
        "columns" : [
                {
                        "name" : <string>               }
        ]
}
```

When the sourceType is "individual", scanID and view must be provided in the root of the request object:

```
{
	"type" : "vuln",
	"query" : {
		"id" : <number> | (valid query)
	},
	"sourceType" : <string> "individual",
	"sortDir" : <string> "ASC" | "DESC" OPTIONAL,
	"sortField" : <string> (alphanumeric; any valid field returned in
the results entry for the corresponding tool.  [Some restrictions
apply.]  Must accompany sortDir),
	"startOffset" : <number>,
	"endOffset" : <number>,
	"columns" : [
		{
			"name" : <string>		}
	],
	"scanID" : <number>,
	"view" : <string>}
```

Type: event (Expand)

Event Type

```
{
	"type" : "event",
	"query" : {
		"id" : <number> | (valid query)
	},
	"sourceType" : <string> "lce" | "archive",
	"sortDir" : <string> "ASC" | "DESC" OPTIONAL,
	"sortField" : <string> (alphanumeric; any valid field returned in
the results entry for the corresponding tool.  [Some restrictions
apply.]  Must accompany sortDir)
}
```

When the sourceType is "archive", lceID and view must be provided in the root of the request object:

```
{
       "type" : "event",
       "query" : {
              "id" : <number> | (valid query)
       },
       "sourceType" : <string> "lce" | "archive",
       "sortDir" : <string> "ASC" | "DESC" OPTIONAL,
       "sortField" : <string> (alphanumeric; any valid field returned in
the results entry for the corresponding tool.  [Some restrictions
apply.]  Must accompany sortDir),
       "lceID" : <number>,
       "view" : <string> (silo id)
}
```

Type: scLog (Expand)

~~SCLog Type~~ (deprecated in 5.19.0)

–

-

```
{
       "type" : "scLog",
       "offset" : <number>,
       "length" : <number>,
       "severity" : "INFO" | "WARN" | "CRITICAL",
       "keywords" : <string> keywords separated by " ", "\t", "\n", or
"\r" (eg. "Authentication User"),
       "date" : scLog basename (eg. "201412") | "all",
```

```
        "username" : <string> (Optional),
        "module" : <string> (eg. "auth") (Optional),
        "orgID" : <number> (Admins only; Optional)
}
```

Type: mobile (Expand)

Mobile Type

```
{
        "type" : "mobile",
        "query" : {
                "id" : <number> | (valid query)
        },
        "sortDir" : <string> "ASC" | "DESC" OPTIONAL,
        "sortField" : <string> (alphanumeric; any valid field returned in
the results entry for the corresponding tool.  [Some restrictions
apply.]  Must accompany sortDir),
        "startOffset" : <number>,
        "endOffset" : <number>,
        "columns" : [
                {
                        "name" : <string>               }
        ]
}
```

Example Response

None given. The response will be CSV format.

Atlassian

Tenable Security Center API: ARC

/arc

Methods

GET

Gets the list of ARCs

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
**name
**description
**running
**status
**result
****policyStatements***
creator
owner
groups
ownerGroup
targetGroup
lastUpdateTime
lastCompletedUpdateTime
lastComplianceUpdateTime
createdTIme
modifiedTIme
focusFilters
schedule
canUse
canManage
order
activated

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*
**** =** policyStatements field on /arc::GET will return a minimal set of Policy Statement fields. This includes the fields: id, label, baseStatus, compliantStatus, drilldownStatus, and displayType*

***redFont =** field is a JSON object (**e.g.** "repository" :{ "id" : <id>, "name" : <name> })*

Request Parameters

None

Filter Parameters

usable - The response will be an object containing an array of usable ARCs. By default, both usable and manageable objects are returned.
manageable - The response will be an object containing all manageable ARCs. By default, both usable and manageable objects are returned.
activated - the response returns an 'usable' object containing an array of objects with only activated ARCs for the session user. This is not compatible with usable and/or manageable filters.

Example Response

Expand


```
{
        "type" : "regular",
        "response" : {
                "usable" : [
                        {
                                "running" : "false",
                                "id" : "1",
                                "name" : "POST TEST",
                                "description" : "",
                                "policyStatements" : [
                                        {
```

```
                                        "id" : "1",
                                        "label" : "label",
                                        "baseStatus" : "0",
                                        "compliantStatus" : "0",
                                        "drilldownStatus" : "0",
                                        "displayType" : "state"
                                ],
                                "result" : "fail",
                                "status" : 0
                        }
                ],
                "manageable" : [
                        {
                                "running" : "false",
                                "id" : "1",
                                "name" : "POST TEST",
                                "description" : "",
                                "policyStatements" : [
                                        {
                                                "id" : "1",
                                                "label" : "label",
                                                "baseStatus" : "0",
                                                "compliantStatus" : "0",
                                                "drilldownStatus" : "0",
                                                "displayType" : "state"
                                ],
                                "result" : "fail",
                                "status" : 0
                        }
                ]
        },
        "error_code" : 0,
        "error_msg" : "",
```

```
        "warnings" : [],
        "timestamp" : 1413315427
}
```

POST

Adds an ARC

NOTE #1: ARC add will automatically "prepare" the files for its Assets.

NOTE #2: *For valid filternames based on queryType or combination asset format, see */query::POST*.

Request Parameters

Expand

```
{
        "name" : <string>,
        "order" : <number>,
        "description" : <string> DEFAULT "",
    "schedule" : {
         "type" : <string> "ical" | "never",
                type "ical"              -----------
         "start" : <string> (This value takes the iCal format),
         "repeatRule" : <string> (This value takes the repeat rule
format)
    },
        "ownerID" : <number> DEFAULT (Session User ID),
        "policyStatements" : [
                {
                        "label" : <string>,
                        "queryType" : <string> "vuln" | "lce",
                        "conditionalName" : <string> "hosts" | "ports" | "reco
                        "conditionalOperator" : <string> "Any" | "No" | "All"
| ">=" | "<=",
```

```
                        "displayType" : <string> "percentage" | "ratio" | "sta
                        "baseFilters" : [
                                {
                                        "filterName" : <string> (valid Query
queryType),
                                        "value : (Format depends on filter's
                                        "operator" : <string> (Options depend
parameter*)
                                }
                        ] DEFAULT [],
                        "compliantFilters" : [
                                {
                                        "filterName" : <string> (valid Query
queryType),
                                        "value : (Format depends on filter's
                                        "operator" : <string> (Options depend
parameter*)
                                }
                        ],
                        "drilldownFilters" : [
                                {
                                        "filterName" : <string> (valid Query
queryType),
                                        "value : (Format depends on filter's
                                        "operator" : <string> (Options depend
parameter*)
                                }
                        ],


                        "conditionalOperator" is ">" | "<" | ">=" | "<="
---------------------------------
                        "conditionalValue" : <number>           }...
```

```
        ],
        "focusFilters" : [
                {
                        "operator" : <string> ">" | "<" | ">=" | "<=" | "=",
                        "filterName" : <string> "asset" | "repository" | "ip",


                        "filterName" is "asset" and "operator" is "~"
----------------------------
                        "value" : {
                                (combination asset*)
                        }


                        "filterName" is "asset" and "operator" is not "~"
-------------------------------------
                        "value" : {
                                "id" : <number>                 }

                        "filterName" is "repository"                    ------
                        "value" : [
                                {
                                        "id" : <number>
                        ]

                        "filterName" is "ip"                    --------------
                        "value" : <string> (valid IP or IP list)
                }...
        ] OPTIONAL
        ...
}
```

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "id" : "1",
                "name" : "POST TEST",
                "description" : "",
                "running" : "false",
                "lastUpdateTime" : "1648781875",
                "lastCompletedUpdateTime" : "1648781875",
                "lastComplianceUpdateTime" : "1648781875",
                "createdTime" : "1648781858",
                "modifiedTime" : "1648781858",
                "focusFilters" : [
                        {
                                "filterName" : "ip",
                                "operator" : "=",
                                "value" : "172.26.20.0"                 }
                ],
                "order" : "0",
                "activated" : "true",
                "groups" : [],
                "policyStatements" : [
                        {
                                "id" : "1",
                                "arcID" : "1",
                                "label" : "POST TEST Label",
                                "baseFilters" : [
                                        {
                                                "filterName" : "ip",
                                                "operator" : "=",
                                                "value" : "172.26.20.0"
                                ],
                                "compliantFilters" : [
```

```
                {
                        "filterName" : "repository",
                        "operator" : "=",
                        "value" : {
                                "id" : "24",
                                "name" : "IPv4 Repo",
                                "description" : "",
                                "type" : "Local",
                                "uuid" : "FC6B1EF4-A8
                        }
                ],
                "drilldownFilters" : [
                        {
                                "filterName" : "asset",
                                "operator" : "=",
                                "value" : {
                                        "id" : "9",
                                        "name" : "Linux Hosts"
                                        "description" : "The
installed.",
                                        "uuid" : "2DF066B8-F3
                        }
                ],
                "baseStatus" : "0",
                "compliantStatus" : "0",
                "drilldownStatus" : "0",
                "conditionalName" : "hosts",
                "conditionalOperator" : "All",
                "conditionalValue" : "",
                "displayType" : "ratio",
                "result" : "pass",
                "resultOutput" : "{\"x\":\"0\",\"y\":\"0\"}",
                "queryType" : "vuln",
```

```
                        "drilldownQuery" : {
                                "id" : "1640"
                        }
                ],
                "result" : "pass",
                "status" : 0,
                "schedule" : {
                        "id" : "123",
                        "type" : "ical",
                        "start" : "TZID=America\/New_York:20220331T230000",
                        "repeatRule" : "FREQ=DAILY;INTERVAL=1",
                        "nextRun" : 1648782000
                },
                "canUse" : "true",
                "canManage" : "true",
                "creator" : {
                        "id" : "1",
                        "username" : "head",
                        "firstname" : "Security Manager",
                        "lastname" : "",
                        "uuid" : "48F26F3B-6A79-4153-96DB-4C63D1BF3D46"
                "owner" : {
                        "id" : "1",
                        "username" : "head",
                        "firstname" : "Security Manager",
                        "lastname" : "",
                        "uuid" : "48F26F3B-6A79-4153-96DB-4C63D1BF3D46"
                "ownerGroup" : {
                        "id" : "0",
                        "name" : "Full Access",
                        "description" : "Full Access group"             }
        },
        "error_code" : 0,
```

```
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1413315326
}
```

/arc/{id}

Methods

GET

Gets the ARC associated with {id}.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
**name
**description
**running
**status
**result
****policyStatements***
creator
owner
groups
ownerGroup
targetGroup
lastUpdateTime
lastCompletedUpdateTime
lastComplianceUpdateTime
createdTIme
modifiedTIme

focusFilters
schedule
canUse
canManage
order
activated

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*
**** =** policyStatements field on /arc/{id}::GET will return all Policy Statement fields*

***redFont =** field is a JSON object (**e.g.** "repository" :{ "id" : <id>, "name" : <name> })*

Request Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
        "response" : {
                "id" : "1",
                "name" : "POST TEST",
                "description" : "",
                "running" : "false",
                "lastUpdateTime" : "1648781875",
                "lastCompletedUpdateTime" : "1648781875",
                "lastComplianceUpdateTime" : "1648781875",
                "createdTime" : "1648781858",
                "modifiedTime" : "1648781858",
                "focusFilters" : [
                        {
```

```
                        "filterName" : "ip",
                        "operator" : "=",
                        "value" : "172.26.20.0"                 }
        ],
        "order" : "0",
        "activated" : "true",
        "groups" : [],
        "policyStatements" : [
                {
                        "id" : "1",
                        "arcID" : "1",
                        "label" : "POST TEST Label",
                        "baseFilters" : [
                                {
                                        "filterName" : "ip",
                                        "operator" : "=",
                                        "value" : "172.26.20.0"
                        ],
                        "compliantFilters" : [
                                {
                                        "filterName" : "repository",
                                        "operator" : "=",
                                        "value" : {
                                                "id" : "24",
                                                "name" : "IPv4 Repo",
                                                "description" : "",
                                                "type" : "Local",
                                                "uuid" : "FC6B1EF4-A8
                                }
                        ],
                        "drilldownFilters" : [
                                {
                                        "filterName" : "asset",
```

```
                                                "operator" : "=",
                                                "value" : {
                                                        "id" : "9",
                                                        "name" : "Linux Hosts"
                                                        "description" : "The c
installed.",
                                                        "uuid" : "2DF066B8-F31
                                                }
                                        ],
                                        "baseStatus" : "0",
                                        "compliantStatus" : "0",
                                        "drilldownStatus" : "0",
                                        "conditionalName" : "hosts",
                                        "conditionalOperator" : "All",
                                        "conditionalValue" : "",
                                        "displayType" : "ratio",
                                        "result" : "pass",
                                        "resultOutput" : "{\"x\":\"0\",\"y\":\"0\"}",
                                        "queryType" : "vuln",
                                        "drilldownQuery" : {
                                                "id" : "1640"
                                }
                        ],
                        "result" : "pass",
                        "status" : 0,
                        "schedule" : {
                                "id" : "123",
                                "type" : "ical",
                                "start" : "TZID=America\/New_York:20220331T230000",
                                "repeatRule" : "FREQ=DAILY;INTERVAL=1",
                                "nextRun" : 1648782000
                        },
                        "canUse" : "true",
```

```
                "canManage" : "true",
                "creator" : {
                        "id" : "1",
                        "username" : "head",
                        "firstname" : "Security Manager",
                        "lastname" : "",
                        "uuid" : "48F26F3B-6A79-4153-96DB-4C63D1BF3D46"
                "owner" : {
                        "id" : "1",
                        "username" : "head",
                        "firstname" : "Security Manager",
                        "lastname" : "",
                        "uuid" : "48F26F3B-6A79-4153-96DB-4C63D1BF3D46"
                "ownerGroup" : {
                        "id" : "0",
                        "name" : "Full Access",
                        "description" : "Full Access group"             }
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1413315326
}
```


PATCH

Edits the ARC associated with {id}, changing only the passed in fields.

Request Parameters

NOTE #1: All PolicyStatements and FocusFilters must be provided or they will be removed.

NOTE #2: Order can only be specified if the ARC has been activated (it is activated automatically on add, but this could apply to shares).

(All fields are optional)

[See /arc::POST for parameters.]

Activating/Deactivating Shared ARCs

A user may call this endpoint for an ARC shared to them. They will only be able to activate, change order, or deactivate a shared ARC. They may only use the following Parameters:

Expand

```
{
        "activated":"<boolean>",
        "order":"<number>" (required if activated is "true")
}
```

Example Response

See /arc/{id}::GET

DELETE

Deletes the ARC associated with {id}, depending on access and permissions.

Request Parameters

None

Example Response

Expand

```
{
    "type" : "regular",
    "response" : "",
    "error_code" : 0,
    "error_msg" : "",
    "warnings" : [],
    "timestamp" : 1403100582
}
```

/arc/import

Methods

POST

Imports an ARC Template

Request Parameters

Expand

```
{
        "filename":"<string>",
        "order":"<number>" (optional)
}
```

Example Response

See /arc/{id}::GET

/arc/{id}/export

Methods

POST

Exports the ARC associated with {id}.

Request Parameters

Expand

```
{
        "exportType":"(full|cleansed|placeholders|templates)"}
```

Example Response

Expand

```
<?xml version="1.0" encoding="UTF-8"?><arcTemplate>
<scVersion>5.0.0</scVersion>    <name>ARC with Assets</name>
<description>lkasdjflaskdj</description>
<focusFilters>YToxOntpOjA7YTozOntzOjEwOiJmaWx0ZXJOYW1lIjtzOjc6ImFzc2-
V0SUQiO3M6ODoib3BlcmF0b3IiO3M6MToifiI7czo1OiJ2YWx1ZSI7YTozOntzOjg6Im-
9wZXJhdG9yIjtzOjEyOiJpbnRlcnNlY3Rpb24iO3M6ODoib3BlcmFuZDEiO3M6MTA6Ii-
0xOlVua25vd24iO3M6ODoib3BlcmFuZDIiO3M6MTA6Ii0xOlVua25vd24iO319fQ==</-
focusFilters>    <policyStatements>        <policyStatement>
   <label>PS</label>            <displayType>state</displayType>

<definition>YTo2OntzOjExOiJiYXNlRmlsdGVycyI7YToxOntpOjA7YTozOntzOjEw-
OiJmaWx0ZXJOYW1lIjtzOjI6ImlwIjtzOjg6Im9wZXJhdG9yIjtzOjE6Ij0iO3M6NToi-
dmFsdWUiO3M6NzoiMS4xLjEuMSI7fX1zOjE2OiJjb21wbGlhbnRGaWx0ZXJzIjthOjE6-
e2k6MDthOjM6e3M6MTA6ImZpbHRlck5hbWUiO3M6MTM6ImJhc2VDVlNTU2NvcmUiO3M6-
ODoib3BlcmF0b3IiO3M6MToiPSI7czo1OiJ2YWx1ZSI7czozOiIyLTMiO319czoxNjoi-
ZHJpbGxkb3duRmlsdGVycyI7YToxOntpOjA7YTozOntzOjEwOiJmaWx0ZXJOYW1lIjtz-
OjU6ImNjZUlEIjtzOjg6Im9wZXJhdG9yIjtzOjE6Ij0iO3M6NToidmFsdWUiO3M6NDoi-
MTIzMSI7fX1zOjE1OiJjb25kaXRpb25hbE5hbWUiO3M6NToiaG9zdHMiO3M6MTk6ImNv-
bmRpdGlvbmFsT3BlcmF0b3IiO3M6MzoiQWxsIjtzOjE2OiJjb25kaXRpb25hbFZhbHVl-
IjtzOjA6IiI7fQ==</definition>        </policyStatement>
</policyStatements>
<schedule>FREQ=DAILY;INTERVAL=1</schedule></arcTemplate>
```


/arc/{id}/copy

Methods

POST

Copies an existing ARC associated with {id}, depending on access and permissions.

Request Parameters

Expand

```
{
        "name": <string>,
        "description": <string> (optional)
}
```

Example Response

See /arc/{id}::GET

/arc/{id}/refresh

Methods

POST

Refreshes the Assurance Report Card associated with {id}.

Request Parameters

None

Example Response

See /arc/{id}::GET

/arc/{id}/share

Methods

POST

Shares the ARC associated with {id}, depending on access and permissions

Request Parameters

Expand

```
{
        "groups":
                [
```

```
                        {<group ID record>},
                        ...
                ]
}
```

Every call to /arc/{id}/share will completely replace the groups that are shared to, with the groups you provide.

Example Response

See /arc/{id}::GET

Atlassian

Tenable Security Center API: ARC Template

/arcTemplate

Methods

GET

Gets the list of ARC Templates.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

**id
*name
*description
summary
enabled
focusFilters
policyStatements
tags
requirements

category
minUpgradeVersion
templatePubTime
templateModTime
definitionModTime
createdTime
modifiedTime

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*
redFont = *field is a JSON object (* ***e.g.*** *"repository" :{ "id" : <id>, "name" : <name> })*

Request Parameters

Expand

NOTE: The *searchString* parameter takes in a space-separated set of keywords/phrases (in parenthesis) and builds a fuzzy match based on them. For excluding a keyword/phrase, is preceded by a '-'. Example:

```
"searchString" : "audit" -"SCAP" ..."
```

Parameters must be passed in as query string (as opposed to JSON) in the format of: /arcTemplate?searchString=...

```
{
    "searchString" : <string> (Search String Format. See NOTE)
DEFAULT ""      "startOffset" : <number> (Positive Integer) DEFAULT "0",
       "endOffset" : <number> (Integer > startOffset) DEFAULT -1 (all
results),
       "categoryID" : <number> DEFAULT -1 (all results)
}
```

Example Response

Expand

```
{
        "type" : "regular",
        "response" : [
                {
                        "id" : "1",
                        "name" : "AA Patching Policy",
                        "description" : ""              }
        ],
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1415127035
}
```


/arcTemplate/{id}

Methods

GET

Gets the ARC Template associated with {id}.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

**id
*name
*description
summary
enabled
focusFilters
policyStatements
tags

requirements
category
minUpgradeVersion
templatePubTime
templateModTime
definitionModTime
createdTime
modifiedTime

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*
redFont = *field is a JSON object (* ***e.g.*** *"repository" :{ "id" : <id>, "name" : <name> })*

Request Query Parameters

None

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "id" : "1",
                "name" : "Example Arc Template",
                "description" : "",
                "summary" : "",
                "enabled" : "true",
                "focusFilters" : [],
                "category" : {
                        "id" : "1",
                        "name" : "Compliance",
                        "description" : ""              },
                "policyStatements" : [
```

```
{
        "label" : "Policy Statement 1",
        "baseFilters" : [
                {
                        "filterName" : "ip",
                        "operator" : "=",
                        "value" : "192.168.1.1"
        ],
        "compliantFilters" : [
                {
                        "filterName" : "baseCVSSScore"
                        "operator" : "=",
                        "value" : "2-3"
        ],
        "drilldownFilters" : [
                {
                        "filterName" : "asset",
                        "operator" : "=",
                        "value" : {
                        "template" : {
                        "id" : "35",
                        "name" : "Nessus Scanner",
                        "description" : ""
                        }
                }
        ],
        "baseStatus" : "0",
        "compliantStatus" : "0",
        "drilldownStatus" : "0",
        "conditionalName" : "hosts",
        "conditionalOperator" : "All",
        "conditionalValue" : "",
        "displayType" : "state",
```

```
                                "result" : "",
                                "resultOutput" : "{}",
                                "queryType" : "vuln"                    }
                ],
                "minUpgradeVersion" : null,
                "templatePubTime" : null,
                "templateModTime" : null,
                "definitionModTime" : null,
                "createdTime" : null,
                "modifiedTime" : null,
                "tags" : [],
                "requirements" : []
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1415313873
}
```


/arcTemplate/{templateID}/image

Methods

GET

Gets the ARC Template image associated with template {templateID}

NOTE: This endpoint is handled before token validation.

Request Query Parameters

None

Example Response

None given. The response will be a raw png file containing the requested ARC Template image.

/arcTemplate/categories

Methods

GET

Gets the list of ARCTemplate categories

Request Query Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
        "response" : [
                {
                        "id" : "2",
                        "name" : "Executive",
                        "description" : "",
                        "count" : "0",
                        "status" : ""           },
                {
                        "id" : "1",
                        "name" : "Compliance",
                        "description" : "",
                        "count" : "3",
                        "status" : "new"                }
        ],
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1426007748
}
```


Atlassian

Tenable Security Center API: Asset

/asset

Methods

GET

Gets the list of Assets. The result is broken up into two lists ("usable" and "manageable").

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
*uuid
**name
**description
type
ownerGroup

Session user not role "1" (Administrator)

**status
creator
owner
targetGroup
groups
template
typeFields
type
tags
context
createdTime
modifiedTime
repositories
ipCount

assetDataFields
viewableIPs (requesting this field for all assets may result in slow processing)

Session user role "1" (Administrator)

****organization**
luminFields

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

redFont = *field is a JSON object (* ***e.g.*** *"repository" :{ "id" : <id>, "name" : <name> })*

Template Parameter

This parameter will filter assets based on templates IDs. The IDs must be provided in a comma-separated format:

```
?template=<id1>,<id2>...
```

Filter Parameters

usable - The response will be an object containing an array of usable Assets. By default, both usable and manageable objects are returned.
manageable - The response will be an object containing all manageable Assets. By default, both usable and manageable objects are returned.
excludeAllDefined - If specified, the defined usable assets (currently id=0) will not be returned. This only applies to usable Assets.
excludeWatchlists - If specified, Assets of type 'watchlist' will be excluded from the usable and/or manageable array.

Request Query Parameters

None

Example Response

Administrator

Expand


```
{
        "type" : "regular",
        "response" : {
                "assets" : [
                        {
                                "id" : "1",
                                "name" : "dnsnameTestPost",
                                "description" : "",
                                "type" : "dnsname",
                                "status" : 0,
                                "uuid" : "1908739A-A74D-4A46-B0D1-720823ECEE1
                                "organization" : {
                                        "id" :  "1"
                                        "description" : "",
                                        "uuid" : "8FDC3F6C-9901-47B8-A720-ACF
                        },
                        {
                                "id" : "28",
                                "name" : "Test 1",
                                "description" : "",
                                "type" : "dynamic",
                                "status" : 0,
                                "uuid" : "370CDC1B-6AA9-4897-844C-01C4CAF8022
                                "organization" : {
                                        "id" :  "1"
                                        "description" : "",
                                        "uuid" : "8FDC3F6C-9901-47B8-A720-ACF
                        },
                        {
                                "id" : "29",
                                "name" : "Test 2",
                                "description" : "",
```

```
                "type" : "dynamic",
                "status" : 0,
                "uuid" : "359C3A46-CE56-420C-8305-6498A72AA3F
                "organization" : {
                        "id" :  "1"
                        "description" : "",
                        "uuid" : "8FDC3F6C-9901-47B8-A720-ACF
        },
        {
                "id" : "30",
                "name" : "Test 3",
                "description" : "",
                "type" : "dynamic",
                "status" : 0,
                "uuid" : "27351CB0-1F71-492F-AF81-EB3329F417F
                "organization" : {
                        "id" :  "1"
                        "description" : "",
                        "uuid" : "8FDC3F6C-9901-47B8-A720-ACF
        },
        {
                "id" : "31",
                "name" : "10287 TEST",
                "description" : "",
                "type" : "dynamic",
                "status" : 0,
                "uuid" : "2E1B2E39-01F4-436E-834E-06B603219B12
                "organization" : {
                        "id" :  "1"
                        "description" : "",
                        "uuid" : "8FDC3F6C-9901-47B8-A720-ACF
        },
        {
```

```
                                "id" : "32",
                                "name" : "TEST",
                                "description" : "",
                                "type" : "dynamic",
                                "status" : 0,
                                "uuid" : "9F3E4BED-6ECB-472D-BC95-3C326CBFE4A
                                "organization" : {
                                        "id" :  "1"
                                        "description" : "",
                                        "uuid" : "8FDC3F6C-9901-47B8-A720-ACF
                        },
                        {
                                "id" : "33",
                                "name" : "test",
                                "description" : "",
                                "type" : "dynamic",
                                "status" : 0,
                                "uuid" : "09075E47-BE8A-4013-88E9-57D443FA33B
                                "organization" : {
                                        "id" :  "1"
                                        "description" : "",
                                        "uuid" : "8FDC3F6C-9901-47B8-A720-ACF
                        }
                ]
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1412273607
}
```


Organization User

Expand

```
{
        "type" : "regular",
        "response" : {
                "usable" : [
                        {
                                "id" : "1",
                                "name" : "dnsnameTestPost",
                                "description" : "",
                                "type" : "dnsname",
                                "status" : 0,
                                "uuid" : "1908739A-A74D-4A46-B0D1-720823ECEE1
                        },
                        {
                                "id" : "28",
                                "name" : "Test 1",
                                "description" : "",
                                "type" : "dynamic",
                                "status" : 0,
                                "uuid" : "370CDC1B-6AA9-4897-844C-01C4CAF8022
                        },
                        {
                                "id" : "29",
                                "name" : "Test 2",
                                "description" : "",
                                "type" : "dynamic",
                                "status" : 0,
                                "uuid" : "359C3A46-CE56-420C-8305-6498A72AA3F
                        },
                        {
                                "id" : "30",
                                "name" : "Test 3",
                                "description" : "",
                                "type" : "dynamic",
```

```
                        "status" : 0,
                        "uuid" : "27351CB0-1F71-492F-AF81-EB3329F417F
                },
                {
                        "id" : "31",
                        "name" : "10287 TEST",
                        "description" : "",
                        "type" : "dynamic",
                        "status" : 0,
                        "uuid" : "2E1B2E39-01F4-436E-834E-06B603219B1
                },
                {
                        "id" : "32",
                        "name" : "TEST",
                        "description" : "",
                        "type" : "dynamic",
                        "status" : 0,
                        "uuid" : "9F3E4BED-6ECB-472D-BC95-3C326CBFE4A
                },
                {
                        "id" : "33",
                        "name" : "test",
                        "description" : "",
                        "type" : "dynamic",
                        "status" : 0,
                        "uuid" : "09075E47-BE8A-4013-88E9-57D443FA33B
                }
        ],
        "manageable" : [
                {
                        "id" : "1",
                        "name" : "dnsnameTestPost",
                        "description" : "",
```

```
                "type" : "dnsname",
                "status" : 0,
                "uuid" : "1908739A-A74D-4A46-B0D1-720823ECEE1
        },
        {
                "id" : "26",
                "name" : "Test",
                "description" : "",
                "type" : "dynamic",
                "status" : 0,
                "uuid" : "9E8E101B-D818-450F-8B8B-4F5C8F421D6
        {
                "id" : "27",
                "name" : "Test2",
                "description" : "",
                "type" : "dynamic",
                "status" : 0,
                "uuid" : "E71EC564-26B6-46E6-8E14-511BDD0A2FE
        {
                "id" : "28",
                "name" : "Test 1",
                "description" : "",
                "type" : "dynamic",
                "status" : 0,
                "uuid" : "370CDC1B-6AA9-4897-844C-01C4CAF8022
        },
        {
                "id" : "29",
                "name" : "Test 2",
                "description" : "",
                "type" : "dynamic",
                "status" : 0,
                "uuid" : "359C3A46-CE56-420C-8305-6498A72AA3F
```

```
        },
        {
                "id" : "30",
                "name" : "Test 3",
                "description" : "",
                "type" : "dynamic",
                "status" : 0,
                "uuid" : "27351CB0-1F71-492F-AF81-EB3329F417F
        },
        {
                "id" : "31",
                "name" : "10287 TEST",
                "description" : "",
                "type" : "dynamic",
                "status" : 0,
                "uuid" : "2E1B2E39-01F4-436E-834E-06B603219B1
        },
        {
                "id" : "32",
                "name" : "TEST",
                "description" : "",
                "type" : "dynamic",
                "status" : 0,
                "uuid" : "9F3E4BED-6ECB-472D-BC95-3C326CBFE4A
        },
        {
                "id" : "33",
                "name" : "test",
                "description" : "",
                "type" : "dynamic",
                "status" : 0,
                "uuid" : "09075E47-BE8A-4013-88E9-57D443FA33B
        }
```

```
                ]
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1412273607
}
```

POST

Adds an Asset.

NOTE #1: If a template ID is provided:

- The template associated with the provided ID will be retrieved and used as the default values for the Asset. These values can be overwritten.
- The 'name' will be handled by the back-end, and would default to the template name. If that name already exists for an Asset with the creatorID of the session user, it would default the name to the name plus the next-lowest integer for that user i.e. "templateName(2)"

NOTE #2: The "prepare" parameter should be set to the string "false" if this Asset pertains to an ARC that will be subsequently created. ARC add will automatically "prepare" the files for this Asset, regardless.

NOTE #3: See Lumin for Lumin synchronization settings.

Request Parameters

Expand

```
{
        "type" : <string> "combination" | "dnsname" | "dnsnameupload" |
"dynamic" | "ldapquery" | "static" | "staticeventfilter" |
"staticvulnfilter" | "templates" | "upload" | "watchlist" |
"watchlisteventfilter" | "watchlistupload",
        "prepare" : <string> "true" | "false" DEFAULT "true"...
```

```
}
```

type not "uploadmultiple"

```
...
       "name" : <string>,
       "description" : <string> DEFAULT "",
       "context" : <string> DEFAULT "",
       "tags" : <string> DEFAULT "" (not "Any" | "None",
       "assetDataFields" : [
              {
                     "fieldName" : <string> DEFAULT "" (if fieldValue not e
                     "fieldValue" : <string> DEFAULT "" (if fieldName not e
              }...
       ] OPTIONAL,
       "template" : {
              "id" : <number> } OPTIONAL,
...
```

type "uploadmultiple" | "dnsnameupload" | "upload" | "watchlistupload"

```
...
       "filename" : <string>...
```

type "combination"

NOTE: The assets you reference in the operators cannot be of type "combination" | "watchlist"

```
...
       "combinations" : {
              "operator" : <string> "complement" | "difference" | "intersect
| "union",
              "operand1" : {                  "id" : <number> (asset ID) OR
(asset UUID)
```

```
                } | <combinationRecord>,

                operator not "complement"                ----------------------
                operand2 : {
                        "id" : <number> (asset ID) OR "uuid" : <string> (asset
                } | <combinationRecord> }
...
```

type "dynamic"

```
...
        "rules": {
                "operator" : <string> "all" | "any",
                "children" : [
                        {
                                "type" : <string> "clause" | "group",
                                child type "clause"
                                "operator" : <string> "contains" | "eq" | "lt"
"gt" | "gte" | "regex" | "pcre",
                                "filterName" : <string> "dns" | "exploitAvaila
"exploitFrameworks" | "firstseen" | "hostUUID" | "mac" | "os" | "ip"
| "uuid" | "lastseen" | "netbioshost" | "netbiosworkgroup" |
"pluginid" | "plugintext" | "port" | "severity" | "sshv1" | "sshv2"
| "tcpport" | "udpport" | "xref",
                                "pluginIDConstraint" : <string> (integer or co
range) DEFAULT -1 (NOT_SET),

                                filterName "pluginid" | "severity"
------------
                                "value" : {
                                filterName not "pluginid" & not "severity"
-------------------------
                                "value" : <string>,
```

```
                                child type "group"
                                (attributes of "rules", aggregate)
                        }...
                ]
        }
...
```

type "dnsname"

```
...
        "definedDNSNames" : <string>...
```

type "ldapquery"

NOTE: Session user must have permission to create LDAP Assets

```
...
        "definedLDAPQuery" : {
                "searchString" : <string>,
                "searchBase" : <string>,
                "ldap" : {
                        "id" : <string>          }
        }
...
```

type "upload" | "watchlistupload" | "static"

```
...
        "definedIPs" : <string>...
```

type "static" | "watchlist" | "upload" | "watchlistupload" | "staticeventfilter" | "staticvulnfilter" | "watchlisteventfilter" | "uploadmultiple"

```
...
       "excludeManagedIPs" : <string> "true" | "false" OPTIONAL
...
```

type "staticeventfilter" | "staticvulnfilter" | "watchlisteventfilter"

```
...
       "filters" = [
               {
                       "filterName" : <string>,
                       "value" : <string>,
                       "operator" : <string>           }
       ]
...
```

type "staticeventfilter" | "watchlisteventfilter"

```
...
       "tool" : "sumip",
       "sourceType" : <string> "archive" | "lce",
       "startOffset" : <number> DEFAULT 0,
       "endOffset" : <number> DEFAULT 9223372036854775807 (PHP_INT_MAX),
       "view" : <string>,
       "lce" : {
               "id" : <number> }
...
```

type "staticvulnfilter"

```
...
       "tool" : <string> "iplist" | "listmailclients" | "listos" |
"listsshservers" | "listservices" | "listsoftware" |
"listwebclients" |  "listwebservers" (internally forced to tool
"iplist" with appropriate Plugin ID filter),
```

```
        "sourceType" : "cumulative" | "individual" | "patched" DEFAULT "",
        "startOffset" : <number> OPTIONAL,
        "endOffset" : <number> OPTIONAL,
        "sortField" : <string> OPTIONAL (must accompany sortDir),
        "sortDir" : <string> "ASC" | "DESC" OPTIONAL (must accompany
sortField)
...
```

type "staticvulnfilter", sourceType "individual"

```
...
        "view" : <string>,
        "scanID" : <number>...
```

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "id" : "33",
                "name" : "test",
                "type" : "combination",
                "description" : "",
                "tags" : "",
                "context" : "",
                "status" : "0",
                "templateID" : "-1",
                "createdTime" : "1412171859",
                "modifiedTime" : "1412171859",
                "typeFields" : {
                        "combinations" : {
                                "operator" : "intersection",
```

```
                        "operand1" : {
                                "id" : "28",
                                "name" : "Test 1",
                                "description" : "",
                                "uuid" : "370CDC1B-6AA9-4897-844C-01C4
                        "operand2" : {
                                "id" : "29",
                                "name" : "Test 2",
                                "description" : "",
                                "uuid" : "359C3A46-CE56-420C-8305-6498
                }
        },
        "repositories" : [
                {
                        "ipCount" : "-1",
                        "repository" : {
                                "id" : "37",
                                "name" : "ag repo1",
                                "description" : "",
                                "type" : "Local",
                                "uuid" : "488A8EE7-69F3-4E49-A53F-0B1D
                },
                {
                        "ipCount" : "-1",
                        "repository" : {
                                "id" : "38",
                                "name" : "jm ipv4",
                                "description" : "",
                                "type" : "Local",
                                "uuid" : "D7CFE6CF-8A69-4859-B9D0-9C6D
                },
                {
                        "ipCount" : "-1",
```

```
                        "repository" : {
                                "id" : "39",
                                "name" : "ipv6 rep",
                                "description" : "",
                                "type" : "Local",
                                "uuid" : "7C187636-3180-4E56-8E59-688A
                        }
                ],
                "ipCount" : -1,
                "groups" : [],
                "assetDataFields" : [],
                "creator" : {
                        "id" : "1",
                        "username" : "head",
                        "firstname" : "Security Manager",
                        "lastname" : "",
                        "uuid" : "48F26F3B-6A79-4153-96DB-4C63D1BF3D46"
                "owner" : {
                        "id" : "1",
                        "username" : "head",
                        "firstname" : "Security Manager",
                        "lastname" : "",
                        "uuid" : "48F26F3B-6A79-4153-96DB-4C63D1BF3D46"
                "ownerGroup" : {
                        "id" : "0",
                        "name" : "Full Access",
                        "description" : "Full Access group"             },
                "targetGroup" : {
                        "id" : -1,
                        "name" : "",
                        "description" : ""              }
        },
        "error_code" : 0,
```

```
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1412273575
}
```


/asset/{id}

/asset/{uuid}

Methods

GET

Gets the Asset associated with {id} or {uuid}.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
*uuid
**name
**description
**status
type
ownerGroup
Session user not role "1" (Administrator)
creator
owner
ownerGroup
targetGroup
groups
template
typeFields

viewableIPs
tags
context
createdTime
modifiedTime
repositories
ipCount
assetDataFields
Session user role "1" (Administrator)

luminFields
organization

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

redFont = *field is a JSON object (* ***e.g.*** *"repository" :{ "id" : <id>, "name" : <name> })*

Request Query Parameters

Administrator

Expand

`Parameters must be passed in as query string (as opposed to JSON) in the format of: /asset/{id}?orgID={orgID} or /asset/{uuid}?orgUUID={orgUUID}`

```
{
    "orgID" : <number> OR "orgUUID" : <string>}
```

Organization User

None

Example Response

Administrator

Expand

```
{
        "type" : "regular",
        "response" : {
                "id" : "33",
                "name" : "test",
                "type" : "combination",
                "description" : "",
                "organization" : {
                        "id" :  "1"                     "name" : "org1",
                        "description" : "",
                        "uuid" : "8FDC3F6C-9901-47B8-A720-ACF1681DE8F4"
                "ownerGroup" : {
                        "id" :  "1"                     "name" : "group1",
                        "description" : "",
                }
                "luminFields" : {
             "firstSyncTime" : "1573594357",
             "lastSyncSuccess" : "1573594357",
             "lastSyncFailure" : "-1",
             "details" : "details for LuminFields",
             "enabled" : "true",
         }
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1412273575
}
```


Organization User

Expand

```
{
	"type" : "regular",
	"response" : {
		"id" : "33",
		"name" : "test",
		"type" : "combination",
		"description" : "",
		"tags" : "",
		"context" : "",
		"status" : "0",
		"templateID" : "-1",
		"createdTime" : "1412171859",
		"modifiedTime" : "1412171859",
		"typeFields" : {
			"combinations" : {
				"operator" : "intersection",
				"operand1" : {
					"id" : "28",
					"name" : "Test 1",
					"description" : "",
					"uuid" : "370CDC1B-6AA9-4897-844C-01C4
				"operand2" : {
					"id" : "29",
					"name" : "Test 2",
					"description" : "",
					"uuid" : "359C3A46-CE56-420C-8305-6498
			}
		},
		"repositories" : [
			{
				"ipCount" : "1",
				"repository" : {
					"id" : "37",
```

```
                                "name" : "ag repo1",
                                "description" : "",
                                "type" : "Local",
                                "uuid" : "488A8EE7-69F3-4E49-A53F-0B1
                        },
                        {
                                "ipCount" : "1",
                                "repository" : {
                                        "id" : "38",
                                        "name" : "jm ipv4",
                                        "description" : "",
                                        "type" : "Local",
                                        "uuid" : "D7CFE6CF-8A69-4859-B9D0-9C6
                        },
                        {
                                "ipCount" : "0",
                                "repository" : {
                                        "id" : "39",
                                        "name" : "ipv6 rep",
                                        "description" : "",
                                        "type" : "Local",
                                        "uuid" : "7C187636-3180-4E56-8E59-688
                        }
                ],
                "ipCount" : 0,
                "groups" : [],
                "assetDataFields" : [],
                "viewableIPs" : [
                        {
                                "repository" : {
                                        "id" : "37",
                                        "name" : "ag repo1",
                                        "description" : "",
```

```
                        "type" : "Local",
                        "uuid" : "488A8EE7-69F3-4E49-A53F-0B1
                "ipList" : "192.168.1.1\n",
                "ipCount" : "1"                 },
        {
                "repository" : {
                        "id" : "38",
                        "name" : "jm ipv4",
                        "description" : "",
                        "type" : "Local",
                        "uuid" : "D7CFE6CF-8A69-4859-B9D0-9C6
                "ipList" : "192.168.1.1\n",
                "ipCount" : "1"                 },
        {
                "repository" : {
                        "id" : "39",
                        "name" : "ipv6 rep",
                        "description" : "",
                        "type" : "Local",
                        "uuid" : "7C187636-3180-4E56-8E59-688
                "ipList" : "",
                "ipCount" : "0"                 }
],
"creator" : {
        "id" : "1",
        "username" : "head",
        "firstname" : "Security Manager",
        "lastname" : "",
        "uuid" : "48F26F3B-6A79-4153-96DB-4C63D1BF3D46"
"owner" : {
        "id" : "1",
        "username" : "head",
        "firstname" : "Security Manager",
```

```
                        "lastname" : "",
                        "uuid" : "48F26F3B-6A79-4153-96DB-4C63D1BF3D46"
                "ownerGroup" : {
                        "id" : "0",
                        "name" : "Full Access",
                        "description" : "Full Access group"            },
                "targetGroup" : {
                        "id" : -1,
                        "name" : "",
                        "description" : ""              }
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1412273575
}
```


PATCH

Edits the Asset associated with {id} or {uuid}, changing only the passed in fields.

Request Parameters

(All fields are optional)

See /asset::POST for parameters.

Example Response

See /asset/{id}::GET and /asset/{uuid}::GET

DELETE

Deletes the Asset associated with {id} or {uuid}, depending on access and permissions.

Request Parameters

None

Example Response

Expand

```
{
        "type" : "regular",
        "response" : [
                {
                        "id" : "1",
                        "targetGID: : -1,
                        "name" : "Name String"          }
        ],
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1401911117
}
```

/asset/import

POST

Imports an Asset specified by a previously uploaded, plain text XML file.

NOTE: The *filename* field should contain the value of the same parameter passed back on */file/upload::POST*.

Request Parameters

Expand

```
{
        "filename" : <string>,
        "name" : <string> OPTIONAL
}
```

Example Response

Expand


```
{
        "type" : "regular",
        "response" : [
                {
                        "id" : "37",
                        "name" : "LDAP query IMPORTED",
                        "description" : "description",
                        "type" : "ldapquery",
                        "tags" : "",
                        "context" : "",
                        "status" : "0",
                        "templateID" : "-1",
                        "createdTime" : "1402582394",
                        "modifiedTime" : "1402582394",
                        "ownerGID" : "0",
                        "targetGID" : "-1",
                        "typeFields" : {
                                "definedLDAPQuery" : {
                                        "searchBase" : "DC=target,DC=tenablese
                                        "searchString" : "(objectclass=Compute
                        },
                        "ipCount" : "",
                        "groups" : [],
                        "assetDataFields" : [],
                        "canUse" : "true",
                        "canManage" : "true",
                        "creator" : {
                                "id" : "1",
                                "username" : "testorg",
                                "firstname" : "first",
                                "lastname" : "last",
```

```
                        "uuid" : "48F26F3B-6A79-4153-96DB-4C63D1BF3D4
                "owner" : {                             "id" : "1",
                        "username" : "testorg",
                        "firstname" : "first",
                        "lastname" : "last",
                        "uuid" : "48F26F3B-6A79-4153-96DB-4C63D1BF3D4
                "ownerGroup" : {
                        "id" : "0",
                        "name" : "Full Access",
                        "description" : "Full Access group"
                "targetGroup" : {
                        "id" : -1,
                        "name" : "",
                        "description" : ""                  }
        }
    ],
    "error_code" : 0,
    "error_msg" : "",
    "warnings" : [],
    "timestamp" : 1402582394
}
```


/asset/{uuid}/export

/asset/{id}/export

GET

Exports the Asset associated with {id} or {uuid} as plain text XML.

Request Parameters

None

Example Response

Expand

```
<?xml version="1.0" encoding="UTF-8"?><assets>  <asset>
<scVersion>5.0.0</scVersion>            <name>Bad Credentials</name>
<description>test</description>         <type>dynamic</type>
<templateID>35</templateID>
<definition>YToyOntzOjU6InJ1bGVzIjthOjM6e3M6ODoib3BlcmF0b3IiO3M6Mzoi-
YW55IjtzOjg6ImNoaWxkcmVuIjthOjI6e2k6MDthOjU6e3M6MTA6ImZpbHRlck5hbWUi-
O3M6ODoicGx1Z2luaWQiO3M6ODoib3BlcmF0b3IiO3M6MjoiZXEiO3M6NToidmFsdWUi-
O3M6NToiMjQ3ODYiO3M6MTg6InBsdWdpbklEQ29uc3RyYWludCI7czoyOiItMSI7czo0-
OiJ0eXBlIjtzOjY6ImNsYXVzZSI7fWk6MTthOjU6e3M6MTA6ImZpbHRlck5hbWUiO3M6-
ODoicGx1Z2luaWQiO3M6ODoib3BlcmF0b3IiO3M6MjoiZXEiO3M6NToidmFsdWUiO3M6-
NToiMjE3NDUiO3M6MTg6InBsdWdpbklEQ29uc3RyYWludCI7czoyOiItMSI7czo0OiJ0-
eXBlIjtzOjY6ImNsYXVzZSI7fX1zOjQ6InR5cGUiO3M6NToiZ3JvdXAiO31zOjE1OiJh-
c3NldERhdGFGaWVsZHMiO2E6MDp7fX0=</definition>   </asset></assets>
```

/asset/{id}/refresh

/asset/{uuid}/refresh

POST

Starts an on-demand recalculation of the Asset files associated with {id} or {uuid}, minus any LDAP querying or Hostname resolution. This includes the *Accessible Asset* files of Asset {id} or {uuid} and any, affected *Defining Assets* files.

NOTE: This can only be called by Administrators.

Request Parameters

Expand

```
{
       "orgID" : <number> OR "orgUUID" : <string>,
       "repIDs" : [
              {
                     "id" : <number>         }...
       ] OR "repUUIDs" : [
```

```
                {
                        "uuid" : <string>                }...
        ]
}
```

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "orgID" : 26,
                "repIDs" : [
                        {
                                "id" : 110
                        }
                ],
                "id" : 20
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1402579901
}
```

/asset/testLDAPQuery

POST

Tests an LDAP query, depending on access and permissions.

Note: This endpoint is restricted to users of role 1 (Admin)

Request Parameters

Expand

```
{
        "definedLDAPQuery" : {
                "searchBase" : <string> (valid dn),
                "searchString" : <string> (valid search),
                "ldap" : {
                        "id" : <string>         }
        }
}
```

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "hostnames" : [                         "system1.target.domain
                        "system2.target.domain.com",
                        "system3.target.domain.com"             ]
        }
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1402579901
}
```

/asset/{id}/share

/asset/{uuid}/share

Methods

POST

Shares the Asset associated with {id} or {uuid}, depending on access and permissions

Request Parameters

Expand

```
{
        "groups" : [
                {
                        "id" : <number>          }...
        ]
}
```

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "id" : "1",
                "name" : "dnsnameTestPost",
                "type" : "dnsname",
                "description" : "",
                "tags" : "",
                "context" : "",
                "status" : "0",
                "templateID" : "1",
                "createdTime" : "1407773915",
                "modifiedTime" : "1407773915",
                "ownerGID" : "0",
                "targetGID" : "-1",
                "definedDNSNames" : "1",
                "repositories" : "",
                "assetDataFields" : [],
                "canUse" : "true",
                "canManage" : "true",
                "creator" : {
                        "id" : "1",
```

```
                        "username" : "head",
                        "firstname" : "Security Manager",
                        "lastname" : "",
                        "uuid" : "48F26F3B-6A79-4153-96DB-4C63D1BF3D46"
                "owner" : {
                        "id" : "1",
                        "username" : "head",
                        "firstname" : "Security Manager",
                        "lastname" : "",
                        "uuid" : "48F26F3B-6A79-4153-96DB-4C63D1BF3D46"
                "ownerGroup" : {
                        "id" : "0",
                        "name" : "Full Access",
                        "description" : "Full Access group"             },
                "targetGroup" : {
                        "id" : -1,
                        "name" : "",
                        "description" : ""              }
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1409086057
}
```


/asset/tag

Methods

GET

Gets the full list of unique Asset tags

Request Parameters

none

Example Response

Expand

```
{
        "type" : "regular",
        "response" : [
                "Tag1",
                "Tag2",
                "Tag3"  ],
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1461093219
}
```

Atlassian

Tenable Security Center API: Asset Template

/assetTemplate

Methods

GET

Gets the list of AssetTemplates.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

**id
*name
*description
summary
type

category
definition
assetType
enabled
minUpgradeVersion
templatePubTime
templateModTime
templateDefModTime
definitionModTime
createdTime
modifiedTime
tags
requirements
assetTemplates

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

redFont = *field is a JSON object (* ***e.g.*** *"repository" :{ "id" : <id>, "name" : <name> })*

Expand Parameters

assetTemplates

Request Parameters

Expand

NOTE #1: Pseudo Category "0" (recent) is currently not supported

NOTE #2: The *searchString* parameter takes in a space-separated set of keywords/phrases (in parenthesis) and builds a fuzzy match based on them. For excluding a keyword/phrase, is preceded by a '-'. Example:

```
"searchString" : "audit" -"SCAP" ..."
```

Parameters must be passed in as query string (as opposed to JSON) in the format of: /assetTemplate?categoryID="1"&...

```
{
       "categoryID" : <number> "1" (OS) | "2" (Client Applications) | "3"
(Server Applications) | "4" (Virtual Technology) | "5"
(Infrastructure Technology) | "6" (Vulnerabilities) | "7"
(Compliance) | "8" (Device Behavior) | "9" (Collected Data) DEFAULT
"" (All Categories),
       "searchString" : <string> (Search String Format. See NOTE#2)
DEFAULT ""      "startOffset" : <number> (Positive Integer) DEFAULT "0",
       "endOffset" : <number> (Integer > startOffset) DEFAULT NOT_SET (all
results)
}
```

Example Response

Expand

```
{
       "type" : "regular",
       "response" : [
                {
                        "id" : "420",
                        "name" : "Helpful Assets for Getting Started",
                        "description" : "This collection of assets are some o
common assets and can be useful when getting started using
Tenable.sc.  The collection contains several assets related to
networking, operating systems, collected data, and various
enterprise applications."              },
                {
                        "id" : "421",
                        "name" : "Networking Equipment",
                        "description" : "This asset collection contains many
assets related to network equipment or network protocol usage.  Some
example assets included are Cisco, Juniper, Enterasys, and other
devices such as load balancers."               },
```

```
                {
                        "id" : "22",
                        "name" : "Linux\/Unix Operating Systems",
                        "description" : "Asset lists used to group different c
of Linux and Unix operating systems.\n\nThis will be helpful for
those getting started with Tenable.sc."         },
                {
                        "id" : "20",
                        "name" : "Windows Collection",
                        "description" : "Asset lists used to group windows and
related vulnerabilities.\n\nThis will be helpful for those getting
started with Tenable.sc."               }
        ],
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1416247907
}
```


/assetTemplate/{id}

Methods

GET

Gets the AssetTemplate associated with {id}.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

**id
*name
*description

summary
type
category
definition
assetType
enabled
minUpgradeVersion
templatePubTime
templateModTime
templateDefModTime
definitionModTime
createdTime
modifiedTime
tags
requirements
assetTemplates

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

redFont = *field is a JSON object (* ***e.g.*** *"repository" :{ "id" : <id>, "name" : <name> })*

Expand Parameters

assetTemplates

Request Parameters

None

Example Response

Expand

```
{
        "type" : "regular",
```

```
       "response" : {
              "id" : "5",
              "name" : "Bad Credentials",
              "description" : "The Nessus scanner testing the remote host ha
been given SMB credentials to log into the remote host,
               however these credentials do not have administrative privileg
Local security checks have been disabled for this host because
either the credentials supplied in the scan policy did not allow
Nessus to log into it or some other problem occurred.\n\nThis will
be helpful for those getting started with Tenable.sc.",
              "summary" : "The Nessus scanner testing the remote host has
failed.",
              "type" : "asset",
              "definition" : {
                     "rules" : {
                            "operator" : "any",
                            "children" : [
                                   {
                                          "filterName" : "pluginid",
                                          "operator" : "eq",
                                          "value" : "21745",
                                          "pluginIDConstraint" : "-1",
                                          "type" : "clause"
                                   {
                                          "filterName" : "pluginid",
                                          "operator" : "eq",
                                          "value" : "24786",
                                          "pluginIDConstraint" : "-1",
                                          "type" : "clause"
                            ],
                            "type" : "group"                          },
                     "assetDataFields" : []
              },
```

```
                "assetType" : "dynamic",
                "enabled" : "true",
                "minUpgradeVersion" : "4.7.0",
                "templatePubTime" : "1375243201",
                "templateModTime" : "1391634244",
                "templateDefModTime" : "1375446899",
                "definitionModTime" : "1413553807",
                "createdTime" : "1413553807",
                "modifiedTime" : "1413553807",
                "tags" : [
                        "credentials",
                        "failed",
                        "getting started",
                        "login",
                        "password",
                        "training",
                        "unauthorized"          ],
                "requirements" : [
                        {
                                "requirement" : "localChecks",
                                "value" : ""                    },
                        {
                                "requirement" : "nessus",
                                "value" : "5.2 : "                      }
                ],
                "category" : {
                        "id" : "9",
                        "name" : "Collected Data",
                        "description" : "Identify devices that have collected
configuration data such as patch level and user credentials."           }
        },
        "error_code" : 0,
        "error_msg" : "",
```

```
        "warnings" : [],
        "timestamp" : 1416247491
}
```


/assetTemplate/categories

Methods

GET

Gets the list of Asset Template categories

Request Query Parameters

None

Example Response

Expand


```
{
        "type":"regular",
        "response":[
                {
                        "id":"1",
                        "name":"OS",
                        "description":"Use plugins, CPE strings, and\/or other
to identify common operating systems.",
                        "count":"124",
                        "status":""             },
                {
                        "id":"2",
                        "name":"Client Applications",
                        "description":"Identify systems with client centric ap
installed.",
                        "count":"48",
                        "status":""             },
```

```
                {
                        "id":"3",
                        "name":"Server Applications",
                        "description":"Identify systems with server centric ap
such as database services, email services, and directory services.",
                        "count":"31",
                        "status":""             },
                {
                        "id":"4",
                        "name":"Virtual Technology",
                        "description":"Identify systems with virtualization te
virtual management applications installed.",
                        "count":"9",
                        "status":""             },
                {
                        "id":"5",
                        "name":"Infrastructure Technology",
                        "description":"Identify systems that are used for netw
communications infrastructure such as routers, switches, and access
points.",
                        "count":"42",
                        "status":""             },
                {
                        "id":"6",
                        "name":"Vulnerabilities",
                        "description":"Identify devices or applications based
presence of a specified severity and\/or vulnerability.",
                        "count":"9",
                        "status":""             },
                {
                        "id":"7",
                        "name":"Compliance",
                        "description":"Identify devices that have been checke
```

```
compliance against a specific audit file.",
                        "count":"25",
                        "status":""             },
                {
                        "id":"8",
                        "name":"Device Behavior",
                        "description":"Identify devices that share common tra
patterns and\/or open ports.",
                        "count":"31",
                        "status":""             },
                {
                        "id":"9",
                        "name":"Collected Data",
                        "description":"Identify devices that have collected s
configuration data such as patch level and user credentials.",
                        "count":"111",
                        "status":""             }
        ],
        "error_code":0,
        "error_msg":"",
        "warnings":[],
        "timestamp":1416249497
}
```


Atlassian

Tenable Security Center API: Attribute Set

/attributeSet

Methods

GET

Gets the list of Attribute Sets

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
**type
**name
description**
creator
createdTime
modifiedTime
attributes

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*
redFont = *field is a JSON object (**e.g.** "repository" :{ "id" : <id>, "name" : <name> })*

Request Attribute Set Parameters

None

Example Response

Expand

```
{
        "type" : "regular",
        "response" : [
                {
                        "id" : "1",
                        "type" : "arf",
                        "name" : "name",
                        "description" : "description",
                        "creator" : {
```

```
                                "id" : "1",
                                "username" : "qahead",
                        "firstname" : "QA",
                        "lastname" : "Head",
                        "uuid" : "48F26F3B-6A79-4153-96DB-4C63D1BF3D46"
                        "createdTime" : "1404335179",
                        "modifiedTime" : "1404335179"           }
                ...
        ],
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1404410691
}
```

POST

Adds an Attribute Set

Request Parameters

Expand

```
{
        "name" : <string>,
        "description" : <string> DEFAULT "",
        "type" : <string> "arf" | "lasr",
        "attributes" : {
                <name:string> : <value:string>...
                type "arf", name is "por_managed"               ----------
---
                "por_managed" : <string> "true" : "false"       }
}
```

See /attributeSet/types::GET for useful attribute name/value parameters.

Example Response

Expand


```
{
        "type" : "regular",
        "response" : {
                "attributeSet" : {
                        "id" : "1",
                        "type" : "arf",
                        "name" : "name",
                        "description" : "description",
                        "creator" : {
                            "id" : "1",
                        "username" : "qahead",
                        "firstname" : "QA",
                        "lastname" : "Head",
                        "uuid" : "48F26F3B-6A79-4153-96DB-4C63D1BF3D46",
                        },
                        "createdTime" : "1404413984",
                        "modifiedTime" : "1404413984"           }
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1404413984
}
```


/attributeSet/{id}

Methods

GET

Gets the Attribute Set associated with {id}.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
**type
**name
description**
creator
createdTime
modifiedTime
attributes

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*
redFont = *field is a JSON object (**e.g.** "repository" :{ "id" : <id>, "name" : <name> })*

Request Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
        "response" : {
                "id" : "1",
                "type" : "arf",
                "name" : "name",
                "description" : "description",
                "creator" : {
                    "id" : "1",
                        "username" : "qahead",
                        "firstname" : "QA",
```

```
                "lastname" : "Head",
                "uuid" : "48F26F3B-6A79-4153-96DB-4C63D1BF3D46",
                },
                "createdTime" : "1404335179",
                "modifiedTime" : "1404335179"   },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1404414568
}
```


PATCH

Edits the Attribute Set associated with {id}, changing only the passed in fields.

Request Parameters

(All fields are optional)

See /attributeSet::POST for parameters.

Example Response

See /attributeSet/{id}::GET

DELETE

Deletes the Attribute Set associated with {id}, depending on access and permissions.

Request Parameters

None

Example Response

Expand


```
{
    "type" : "regular",
```

```
    "response" : "",
    "error_code" : 0,
    "error_msg" : "",
    "warnings" : [],
    "timestamp" : 1403100582
}
```


/attributeSet/types

Methods

GET

Gets the list of Attribute Set Types.

Request Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
        "response" : {
                "attributes" : {
                        "arf" : [
                                "owning_unit\/name",
                                "owning_service\/name",
                                "current_aor",
                                "region",
                                "administration_unit\/name",
                                "administration_poc\/full_name\/first_name",
                                "administration_poc\/full_name\/last_name",
                                "administration_poc\/full_name\/middle_initial
```

```
                                "administration_poc\/full_name\/generational_c
                                "administration_poc\/rank_or_title",
                                "administration_poc\/e-mail",
                                "administration_poc\/position",
                                "cnd_service_provider\/name",
                                "por_managed",
                                "system_affiliation",
                                "Location\/room_identifier",
                                "Location\/building_number",
                                "Location\/street_address",
                                "Location\/city",
                                "Location\/state",
                                "Location\/postal_code",
                                "Location\/country",
                                "Location\/latitude",
                                "Location\/longitude",
                        ],
                        "lasr" : [
                                "ReportingComponent",
                                "ComponentBureau",
                                "Enclaves",
                        ]
                }
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1404415504
}
```


Atlassian

Tenable Security Center API: AuditFile

/auditFile

Methods

GET

Gets the list of AuditFiles.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

NOTE: 'typeFields' returns type-specific parameters inside of a 'typeFields." If requested, typeFields returns as follows:

> **type "scapWindows" | "scapLinux" (SCAP):** dataStreamName, benchmarkName, profileName, tailoringOriginalFilename
> **type not "scapWindows" | not "scapLinux" (Tenable): variables**

Allowed Fields

*id
*uuid
**name
**description
**type
**status
groups
creator
version
context
filename
originalFilename
createdTime
modifiedTime
lastRefreshedTime
canUse
canManage

auditFileTemplate
typeFields

Session User role not "1" (Administrator)

ownerGroup
targetGroup
owner

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*
redFont = *field is a JSON object (* ***e.g.*** *"repository" :{ "id" : <id>, "name" : <name> })*

Request Query Parameters

None

Filter Parameters

usable - The response will be an object containing an array of usable AuditFiles. By default, both usable and manageable objects are returned.
manageable - The response will be an object containing all manageable AuditFiles. By default, both usable and manageable objects are returned.

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "usable" : [
                        {
                                "id" : "5",
                                "name" : "Admin - Top 25 extended File Listene
                                "description" : "",
                                "type" : "windowsfiles",
```

```
                "status" : "0",
                "uuid" : "AC4697BA-EE58-4EBC-B05A-D3CCDF170D21
        {
                "id" : "6",
                "name" : "Admin - Top 25 lite",
                "description" : "",
                "type" : "windowsfiles",
                "status" : "0",
                "uuid" : "7F24580C-2601-44DD-96D1-1595AEB40731
        {
                "id" : "1000030",
                "name" : "Basic Audit File",
                "description" : "",
                "type" : "windowsfiles",
                "status" : "0",
                "uuid" : "6FCE9E39-A85A-4408-8796-5E892A015B69
        {
                "id" : "1000047",
                "name" : "With Scap",
                "description" : "",
                "type" : "windowsfiles",
                "status" : "0",
                "uuid" : "71479486-3ADB-461E-B0BF-2EDF615CDBDA
        {
                "id" : "1000048",
                "name" : "test12122",
                "description" : "",
                "type" : "scapWindows",
                "status" : "0",
                "uuid" : "D91B78FC-92A4-46BE-AE72-2774CE2C63DE
        {
                "id" : "1000049",
                "name" : "Test",
```

```
                        "description" : "",
                        "type" : "scapWindows",
                        "status" : "0",
                        "uuid" : "B4CED4AA-2852-42FC-8794-CCDC14E4434
                ],
                "manageable" : [
                        {
                                "id" : "1000030",
                                "name" : "Basic Audit File",
                                "description" : "",
                                "type" : "windowsfiles",
                                "status" : "0",
                                "uuid" : "6FCE9E39-A85A-4408-8796-5E892A015B6
                        {
                                "id" : "1000047",
                                "name" : "With Scap",
                                "description" : "",
                                "type" : "windowsfiles",
                                "status" : "0",
                                "uuid" : "71479486-3ADB-461E-B0BF-2EDF615CDBD
                        {
                                "id" : "1000048",
                                "name" : "test12122",
                                "description" : "",
                                "type" : "scapWindows",
                                "status" : "0",
                                "uuid" : "D91B78FC-92A4-46BE-AE72-2774CE2C63D
                        {
                                "id" : "1000049",
                                "name" : "Test",
                                "description" : "",
                                "type" : "scapWindows",
                                "status" : "0",
```

```
                                "uuid" : "B4CED4AA-2852-42FC-8794-CCDC14E4434I
                        {
                                "id" : "1000052",
                                "name" : "AuditFileTest3",
                                "description" : "",
                                "type" : "windowsfiles",
                                "status" : "0",
                                "uuid" : "6FABA32D-B409-49D6-A13B-2A29D601428
                        {
                                "id" : "1000054",
                                "name" : "AuditFile Test 5",
                                "description" : "",
                                "type" : "windowsfiles",
                                "status" : "0",
                                "uuid" : "676FDD6A-5AFC-43FC-BE28-BAF7AD451B0I
                ]
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1410981838
}
```


POST

Adds an AuditFile.

NOTE #1: The *filename* and *tailoringFilename* fields should contain the value of the same parameter passed back on a */file/upload::POST* if they are provided. The *tailoringOriginalFilename* field should contain the value of the tailoring file's original name, prior to upload if it is provided.
NOTE #2: For Tenable AuditFiles, field *type* must be sent as a blank string. SCAP AuditFile field *type* will be "scapWindows" or "scapLinux".
NOTE #3: AuditFile Template Variable names and values validation is limited to format only. They are not validated against the template's name/value pairs, nor are defaults set.

Request Parameters

Expand

```
{
        "name" : <string>,
        "description" : <string> DEFAULT "",
        "type" : <string> "scapWindows" | "scapLinux" | "" (Tenable Audit
File)
...
```

type is "" (Tenable Audit File)

```
...
        "auditFileTemplate" : {
                "id" : <number> DEFAULT -1 (NOT_SET)
        },
        "variables" : [
                {
                        "name" : <string>,
                        "value" : <string>              }...
        ],


        auditFileTemplate 'id' not '-1'
        -------------------------------
        "filename" : <string>,
        "originalFilename" : <string> DEFAULT "",
}
```

typeis "scapWindows" | "scapLinux"

```
...
        "version" : <string> "1.0" | "1.1" | "1.2",
        "benchmarkName" : <string>,
        "profileName" : <string>,
```

```
        "filename" : <string>,
        "originalFilename" : <string> DEFAULT "",
        version "1.2"   -------------
        "dataStreamName" : <string>,
        "tailoringFilename" : <string> OPTIONAL,
        "tailoringOriginalFilename" : <string> OPTIONAL


        "tailoringFilename" is provided
        --------------------------------
        "tailoringOriginalFilename" : <string>...
```

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "id" : "1000006",
                "name" : "Test Audit File",
                "description" : "Audit File Test",
                "version" : "1.12",
                "type" : "palo_alto",
                "context" : null,
                "status" : "0",
                "filename" : "scfile_KjhMPw",
                "originalFilename" : "",
                "createdTime" : "1435166011",
                "modifiedTime" : "1435249000",
                "lastRefreshedTime" : "1435249000",
                "typeFields" : {
                        "variables" : []
                },
```

```
                "groups" : [],
                "canUse" : "true",
                "canManage" : "true",
                "creator" : {
                        "id" : "1",
                        "username" : "head",
                        "firstname" : "",
                        "lastname" : "",
                        "uuid" : "48F26F3B-6A79-4153-96DB-4C63D1BF3D46"
                "owner" : {
                        "id" : "1",
                        "username" : "head",
                        "firstname" : "",
                        "lastname" : "",
                        "uuid" : "48F26F3B-6A79-4153-96DB-4C63D1BF3D46"
                "ownerGroup" : {
                        "id" : "0",
                        "name" : "Full Access",
                        "description" : "Full Access group"             },
                "targetGroup" : {
                        "id" : -1,
                        "name" : "",
                        "description" : ""              },
                "auditFileTemplate" : {
                        "id" : "186",
                        "name" : "TNS Palo Alto PAN-OS Best Practices",
                        "categoryName" : "Palo Alto Networks PAN-OS"
                "uuid" : "1981424C-2EF6-450A-9D28-B1CBEBB94C47" },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1435249000
}
```


/auditFile/{id}

/auditFile/{uuid}

Methods

GET

Gets the AuditFile associated with {id} or {uuid}.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

NOTE: 'typeFields' returns type-specific parameters inside of a 'typeFields." If requested, typeFields returns as follows:

> **type "scapWindows" | "scapLinux" (SCAP):** dataStreamName, benchmarkName, profileName, tailoringOriginalFilename
> **type not "scapWindows" | not "scapLinux" (Tenable): variables**

Allowed Fields

*id
*uuid
**name
**description
**type
**status
groups
creator
version
context
filename
originalFilename
createdTime
modifiedTime
lastRefreshedTime
canUse
canManage

auditFileTemplate

typeFields

Session User role not "1" (Administrator)

ownerGroup

targetGroup

owner

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

redFont = *field is a JSON object (* ***e.g.*** *"repository" :{ "id" : <id>, "name" : <name> })*

Request Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
        "response" : {
                "id" : "1000006",
                "name" : "Test Audit File",
                "description" : "Audit File Test",
                "version" : "1.12",
                "type" : "palo_alto",
                "context" : null,
                "status" : "0",
                "filename" : "scfile_KjhMPw",
                "originalFilename" : "",
                "createdTime" : "1435166011",
                "modifiedTime" : "1435249000",
                "lastRefreshedTime" : "1435249000",
```

```
                "typeFields" : {
                        "variables" : []
                },
                "groups" : [],
                "canUse" : "true",
                "canManage" : "true",
                "creator" : {
                        "id" : "1",
                        "username" : "head",
                        "firstname" : "",
                        "lastname" : "",
                        "uuid" : "48F26F3B-6A79-4153-96DB-4C63D1BF3D46"
                "owner" : {
                        "id" : "1",
                        "username" : "head",
                        "firstname" : "",
                        "lastname" : "",
                        "uuid" : "48F26F3B-6A79-4153-96DB-4C63D1BF3D46"
                "ownerGroup" : {
                        "id" : "0",
                        "name" : "Full Access",
                        "description" : "Full Access group"             },
                "targetGroup" : {
                        "id" : -1,
                        "name" : "",
                        "description" : ""              },
                "auditFileTemplate" : {
                        "id" : "186",
                        "name" : "TNS Palo Alto PAN-OS Best Practices",
                        "categoryName" : "Palo Alto Networks PAN-OS"
                "uuid" : "1981424C-2EF6-450A-9D28-B1CBEBB94C47" },
        "error_code" : 0,
        "error_msg" : "",
```

```
        "warnings" : [],
        "timestamp" : 1435249000
}
```


PATCH

Edits the AuditFile associated with {id} or {uuid}, changing only the passed in fields.

Request Parameters

(All fields are optional)

See /auditFile::POST for parameters.

Example Response

See /auditFile/{id}::GET or /auditFile/{uuid}::GET for example response.

DELETE

Deletes the AuditFile associated with {id} or {uuid}, depending on access and permissions.

Request Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
        "response" : "",
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1401911117
}
```


/auditFile/{id}/refresh

/auditFile/{uuid}/refresh

Methods

POST

Refreshes the AuditFile associated with {id} or {uuid} to use the latest template version, depending on access and permissions.

NOTE #1: This does not modify the template variables. If the latest template has different variables, the user must call /auditFile/{id}::PATCH.
NOTE #2: AuditFiles not based on templates or based on templates that no longer exist (likely due to deprication) will generate an error.

Request Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
        "response" : {
                "id" : "1000006",
                "name" : "Test Audit File",
                "description" : "Audit File Test",
                "version" : "1.12",
                "type" : "palo_alto",
                "context" : null,
                "status" : "0",
                "filename" : "scfile_KjhMPw",
                "originalFilename" : "",
                "createdTime" : "1435166011",
                "modifiedTime" : "1435249000",
                "lastRefreshedTime" : "1435249000",
                "typeFields" : {
```

```
                "variables" : []
        },
        "groups" : [],
        "canUse" : "true",
        "canManage" : "true",
        "creator" : {
                "id" : "1",
                "username" : "head",
                "firstname" : "",
                "lastname" : "",
                "uuid" : "48F26F3B-6A79-4153-96DB-4C63D1BF3D46"
        "owner" : {
                "id" : "1",
                "username" : "head",
                "firstname" : "",
                "lastname" : "",
                "uuid" : "48F26F3B-6A79-4153-96DB-4C63D1BF3D46"
        "ownerGroup" : {
                "id" : "0",
                "name" : "Full Access",
                "description" : "Full Access group"            },
        "targetGroup" : {
                "id" : -1,
                "name" : "",
                "description" : ""              },
        "auditFileTemplate" : {
                "id" : "186",
                "name" : "TNS Palo Alto PAN-OS Best Practices",
                "categoryName" : "Palo Alto Networks PAN-OS"
        "uuid" : "1981424C-2EF6-450A-9D28-B1CBEBB94C47" },
"error_code" : 0,
"error_msg" : "",
"warnings" : [],
```

```
        "timestamp" : 1435249000
}
```

/auditFile/{id}/share

/auditFile/{uuid}/share

Methods

POST

Shares the AuditFile associated with {id} or {uuid}, depending on access and permissions

Request Parameters

Expand

```
{
        "groups" : [
                {
                        "id" : <number>          }...
        ]
}
```

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "id" : "1000006",
                "name" : "Test Audit File",
                "description" : "Audit FIle Test",
                "version" : "1.12",
                "type" : "palo_alto",
```

```
"context" : null,
"status" : "0",
"filename" : "scfile_KjhMPw",
"originalFilename" : "",
"createdTime" : "1435166011",
"modifiedTime" : "1435249000",
"lastRefreshedTime" : "1435249000",
"typeFields" : {
        "variables" : []
},
"groups" : [],
"canUse" : "true",
"canManage" : "true",
"creator" : {
        "id" : "1",
        "username" : "head",
        "firstname" : "",
        "lastname" : "",
        "uuid" : "48F26F3B-6A79-4153-96DB-4C63D1BF3D46"
"owner" : {
        "id" : "1",
        "username" : "head",
        "firstname" : "",
        "lastname" : "",
        "uuid" : "48F26F3B-6A79-4153-96DB-4C63D1BF3D46"
"ownerGroup" : {
        "id" : "0",
        "name" : "Full Access",
        "description" : "Full Access group"            },
"targetGroup" : {
        "id" : -1,
        "name" : "",
        "description" : ""            },
```

```
                "auditFileTemplate" : {
                        "id" : "186",
                        "name" : "TNS Palo Alto PAN-OS Best Practices",
                        "categoryName" : "Palo Alto Networks PAN-OS"
                "uuid" : "1981424C-2EF6-450A-9D28-B1CBEBB94C47" },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1435249000
}
```


/auditFile/{id}/export

/auditFile/{uuid}/export

Methods

GET

Exports the AuditFile associated with {id} or {uuid} as plain text XML, depending on access and permissions

NOTE: For AuditFiles based on templates, the exported AuditFile will be merged with the indicated variables before export. There is currently no option to export with placeholders.

Request Parameters

None

Example Response

None given. The response will be a AuditFile in binary or ascii format.

Atlassian

Tenable Security Center API: AuditFile Template

/auditFileTemplate

Methods

GET

Gets the list of AuditFileTemplates.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

**id
*name
category
filename
version
editor
labels
uid
type
specType
specName
specVersion
specLink
templatePubTime
templateModTime
createdTime
modifiedTime
replaces

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*
redFont = *field is a JSON object (**e.g.** "repository" :{ "id" : <id>, "name" : <name> })*

Request Parameters

Expand

NOTE #1: The list of categories may be dynamic and is updated in the feed. See /auditFileTemplate/categories::GET for current categories.

NOTE #2: The *searchString* parameter takes in a space-separated set of keywords/phrases (in parenthesis) and builds a fuzzy match based on them. For excluding a keyword/phrase, is preceded by a '-'. Example:

```
"searchString" : "audit" -"SCAP" ..."
```

Parameters must be passed in as query string (as opposed to JSON) in the format of: /auditFileTemplate?category=1&...

```
{
	"categoryID" : <number> DEFAULT "" (all),
	"searchString" : <string> (Search String Format. See NOTE#2)
DEFAULT ""}
```

Example Response

Expand

```
{
	"type" : "regular",
	"response": [
		{
			"id" : "279",
			"name" : "DISA STIG Office 2010 OneNote v1r5"
		{
			"id" : "278",
			"name" : "DISA STIG Office 2003 InfoPath v4r3"
		{
			"id" : "277",
			"name" : "DISA STIG Office Excel 2010 v1r5"
		{
			"id" : "276",
```

```
                "name" : "DISA STIG Office Excel 2003 v4r3"
        {
                "id" : "275",
                "name" : "DISA STIG Office 2010 Access v1r5"
        {
                "id" : "274",
                "name" : "CIS Microsoft Windows 8.1 Benchmark v1.0.0"
        {
                "id" : "273",
                "name" : "TNS Best Practice RackSpace"          },
        {
                "id" : "272",
                "name" : "CIS IE 10 v1.1.0"             },
        {
                "id" : "271",
                "name" : "CIS Red Hat Enterprise Linux 6 Benchmark v1
        {
                "id" : "270",
                "name" : "PCI v2.0/v3.0 Windows Best Practices"
        {
                "id" : "269",
                "name" : "CIS SQL Server 2014 Database L1 OS v1.0.0"
        {
                "id" : "268",
                "name" : "CIS Windows 2003 DC v2.0"             },
        {
                "id" : "267",
                "name" : "CIS Windows Server 2012 R2 MS L1 v1.1.0"
        {
                "id" : "266",
                "name" : "DISA STIG Oracle 11 Instance v8r12 OS Windo
        {
                "id" : "265",
```

```
            "name" : "DISA STIG Oracle 11 Instance v8r12 OS Unix"
        {
            "id" : "264",
            "name" : "DISA STIG Oracle 11 Instance v8r12 Database"
        {
            "id" : "263",
            "name" : "DISA STIG Oracle 11 Installation v8r12 Windo
        {
            "id" : "262",
            "name" : "DISA STIG Oracle 11 Installation v8r12 Linux
        {
            "id" : "261",
            "name" : "DISA STIG Oracle 11 Installation v8r12 Datab
        {
            "id" : "260",
            "name" : "CIS Oracle Linux 7 L2 v1.0.0"         },
        {
            "id" : "259",
            "name" : "CIS VMware ESXi 5.5 v1.2.0 Level 2"
        {
            "id" : "258",
            "name" : "CIS MS Office Outlook 2010 v1.0.0"
        {
            "id" : "257",
            "name" : "MobileIron - CIS Google Android 4 v1.0.0 L1"
        {
            "id" : "256",
            "name" : "CIS Ubuntu 12.04 LTS Benchmark L2 v1.1.0"
        {
            "id" : "255",
            "name" : "AirWatch - CIS Google Android 4 v1.0.0 L1"
        {
            "id" : "254",
```

```
                "name" : "DISA Red Hat Enterprise Linux 6 STIG v1r6"
        {
                "id" : "253",
                "name" : "AirWatch - CIS Apple iOS 8 v1.0.0 L1"
        {
                "id" : "252",
                "name" : "CIS Apple OSX 10.9 Yosemite L2 v1.0.0"
        {
                "id" : "251",
                "name" : "DISA STIG HP-UX 11.31 v1r6"           },
        {
                "id" : "250",
                "name" : "CIS Apple OSX 10.9 Yosemite L1 v1.0.0"
        {
                "id" : "249",
                "name" : "CIS Windows 2003 MS v3.1.0"           },
        {
                "id" : "248",
                "name" : "CIS Windows 2003 DC v3.1.0"           },
        {
                "id" : "247",
                "name" : "CIS Apple OSX 10.10 Yosemite L2 v1.0.0"
        {
                "id" : "246",
                "name" : "CIS Apple OSX 10.10 Yosemite L1 v1.0.0"
        {
                "id" : "245",
                "name" : "DISA STIG Office 2010 Word v1r5"
        {
                "id" : "244",
                "name" : "DISA STIG Office 2003 Word v4r3"
        {
                "id" : "242",
```

```
                "name" : "DISA STIG Office 2010 Publisher v1r5"
        {
                "id" : "241",
                "name" : "DISA STIG Office 2010 Project v1r5"
        {
                "id" : "240",
                "name" : "DISA STIG Office PowerPoint 2010 v1r5"
        {
                "id" : "239",
                "name" : "DISA STIG Office 2003 PowerPoint v4r3"
        {
                "id" : "238",
                "name" : "CIS Windows Server 2012 R2 DC L1 v1.1.0"
        {
                "id" : "237",
                "name" : "DISA STIG Office 2003 Outlook v4r3"
        {
                "id" : "236",
                "name" : "MobileIron - TNS MDM Best Practices Audit v1
        {
                "id" : "235",
                "name" : "AirWatch - TNS MDM Best Practices Audit v1.0
        {
                "id" : "234",
                "name" : "Windows Nessus Installation Check"
        {
                "id" : "233",
                "name" : "Kaspersky Anti-Virus"         },
        {
                "id" : "232",
                "name" : "DISA STIG Office 2010 InfoPath v1r5"
        {
                "id" : "231",
```

```
                        "name" : "TNS File Analysis - Adult Media Browser Usag
                {
                        "id" : "230",
                        "name" : "TNS File Analysis - Source Code Errors"
                {
                        "id" : "229",
                        "name" : "TNS File Analysis - Source Code Errors"
                {
                        "id" : "228",
                        "name" : "DISA STIG Office 2003 Access v4r3"
                {
                        "id" : "227",
                        "name" : "TNS File Analysis - Source Code Leakage"
                {
                        "id" : "226",
                        "name" : "CIS Amazon 2014.09 L1 v1.0.0"         },
                {
                        "id" : "225",
                        "name" : "TNS File Analysis - Social Security Number
},
                {
                        "id" : "224",
                        "name" : "CIS IE 11 v1.0.0"             },
                {
                        "id" : "223",
                        "name" : "TNS File Analysis - Social Security Number
(International)"                 },
                {
                        "id" : "222",
                        "name" : "CIS Red Hat Enterprise Linux 6 Benchmark v1
                {
                        "id" : "221",
                        "name" : "TNS File Analysis - Classified Documents"
```

```
                {
                        "id" : "220",
                        "name" : "DISA STIG for Microsoft Dot Net Framework 4
01.24.2014"              },
                {
                        "id" : "219",
                        "name" : "TNS File Analysis - Financial Statement"
                {
                        "id" : "218",
                        "name" : "CIS Amazon 2014.09 L2 v1.0.0"          },
                {
                        "id" : "217",
                        "name" : "TNS File Analysis - Employee Salary List"
                {
                        "id" : "216",
                        "name" : "CIS SQL Server 2014 Database L1 DB v1.0.0"
                {
                        "id" : "215",
                        "name" : "TNS File Analysis - Credit Card Number"
                {
                        "id" : "214",
                        "name" : "MobileIron - CIS Google Android 4 v1.0.0 L2"
                {
                        "id" : "213",
                        "name" : "TNS File Analysis - Corporate Confidential
                 },
                {
                        "id" : "212",
                        "name" : "TNS File Analysis - Adult Media Content"
                {
                        "id" : "211",
                        "name" : "TNS File Analysis - Adult Media Content"
                {
```

```
                        "id" : "210",
                        "name" : "TNS File Analysis - Phone No. and     Addres
                {
                        "id" : "209",
                        "name" : "TNS File Analysis - Phone No. and     Addres
                {
                        "id" : "208",
                        "name" : "TNS File Analysis - SWIFT Banking Wire Trans
    },
                {
                        "id" : "207",
                        "name" : "TNS File Analysis - SWIFT Banking Wire Trans
    },
                {
                        "id" : "206",
                        "name" : "AirWatch - CIS Google Android 4 v1.0.0 L2"
                {
                        "id" : "205",
                        "name" : "TNS File Analysis - International Wire Trans
                {
                        "id" : "204",
                        "name" : "CIS Oracle Linux 7 L1 v1.0.0"         },
                {
                        "id" : "203",
                        "name" : "TNS File Analysis - Social Security Number
            },
                {
                        "id" : "202",
                        "name" : "CIS VMware ESXi 5.5 v1.2.0 Level 1"
                {
                        "id" : "201",
                        "name" : "TNS File Analysis - Non-Disclosure Agreement
                {
```

```
                "id" : "200",
                "name" : "TNS File Analysis - French Social Security N
        {
                "id" : "199",
                "name" : "TNS File Analysis - French Social Security N
        {
                "id" : "198",
                "name" : "CIS Ubuntu 12.04 LTS Benchmark L1 v1.1.0"
        {
                "id" : "197",
                "name" : "TNS File Analysis - Employee Identification
        {
                "id" : "196",
                "name" : "AirWatch - CIS Apple iOS 8 v1.0.0 L2"
        {
                "id" : "195",
                "name" : "TNS File Analysis - EDI Claim Information"
        {
                "id" : "194",
                "name" : "MobileIron - CIS Apple iOS 8 v1.0.0 L1"
        {
                "id" : "193",
                "name" : "TNS File Analysis - Drivers License"
        {
                "id" : "192",
                "name" : "VMWare vSphere 5.X Hardening Guide"
        {
                "id" : "191",
                "name" : "DISA STIG HP-UX 11.31 v1r3"           },
        {
                "id" : "190",
                "name" : "TNS VMWare vSphere Best Practices"
        {
```

```
                        "id" : "189",
                        "name" : "TNS PostgreSQL 9.1 Best Practices Windows OS
                {
                        "id" : "188",
                        "name" : "TNS PostgreSQL 9.1 Best Practices Unix OS"
                {
                        "id" : "187",
                        "name" : "TNS PostgreSQL 9.1 Best Practices DB"
                {
                        "id" : "186",
                        "name" : "TNS Palo Alto PAN-OS Best Practices"
                {
                        "id" : "185",
                        "name" : "TNS Cisco NX-OS Best Practices"
                {
                        "id" : "184",
                        "name" : "DISA STIG Office System 2010 v1r5"
                {
                        "id" : "183",
                        "name" : "TNS RedHat Enterprise Virtualization Best Pr
},
                {
                        "id" : "182",
                        "name" : "TNS MongoDB 2.6 Best Practices Windows OS Au
},
                {
                        "id" : "181",
                        "name" : "TNS MongoDB 2.6 Best Practices Linux OS Audi
                {
                        "id" : "180",
                        "name" : "TNS MongoDB 2.x Best Practices Database Audi
                {
                        "id" : "179",
```

```
                        "name" : "TNS MongoDB 2.4 Best Practices Windows OS Au
},
                {
                        "id" : "178",
                        "name" : "TNS MongoDB 2.4 Best Practices Linux OS Audi
                {
                        "id" : "177",
                        "name" : "TNS Huawei AR Series Best Practice Audit"
                {
                        "id" : "176",
                        "name" : "TNS HP ProCurve Best Practices"
                {
                        "id" : "175",
                        "name" : "TNS FortiGate FortiOS Best Practices"
                {
                        "id" : "174",
                        "name" : "TNS Extreme ExtremeXOS Best Practice Audit"
                {
                        "id" : "173",
                        "name" : "TNS Dell Force10 Best Practice Audit"
                {
                        "id" : "172",
                        "name" : "TNS Brocade Fabric OS Best Practices"
                {
                        "id" : "171",
                        "name" : "TNS BlueCoat ProxySG Benchmark"
                {
                        "id" : "170",
                        "name" : "TNS SonicWALL <= v5.8 Best Practices"
                {
                        "id" : "169",
                        "name" : "TNS Citrix XenServer Best Practices"
                {
```

```
                "id" : "168",
                "name" : "TNS FireEye Best Practices"          },
        {
                "id" : "167",
                "name" : "TNS CheckPoint GAiA Best Practices"
        {
                "id" : "166",
                "name" : "TNS Adtran AOS Best Practice Audit"
        {
                "id" : "165",
                "name" : "TNS Juniper ScreenOS Best Practices Audit"
        {
                "id" : "164",
                "name" : "PCI DSS 3.0 - Microsoft Windows"
        {
                "id" : "163",
                "name" : "PCI DSS 2.0/3.0 - Solaris 10"       },
        {
                "id" : "162",
                "name" : "PCI DSS 2.0/3.0 - Red Hat Linux"
        {
                "id" : "161",
                "name" : "PCI DSS 2.0/3.0 - AIX"              },
        {
                "id" : "160",
                "name" : "TNS NetApp Data ONTAP Best Practices"
        {
                "id" : "159",
                "name" : "MS Security Advisory 2963983 Mitigation Sett
         },
        {
                "id" : "158",
                "name" : "DISA STIG Java JRE 7 for Windows XP v1r4"
```

```
                {
                        "id" : "157",
                        "name" : "DISA STIG Java JRE 7 for Windows 7 v1r4"
                {
                        "id" : "156",
                        "name" : "DISA STIG Java JRE 7 v1r4"            },
                {
                        "id" : "155",
                        "name" : "DISA STIG Java JRE 6 for Windows XP v1r4"
                {
                        "id" : "154",
                        "name" : "DISA STIG Java JRE 6 Windows 7 v1r4"
                {
                        "id" : "153",
                        "name" : "DISA STIG Java JRE 6 v1r4"            },
                {
                        "id" : "152",
                        "name" : "IBM System i Security Reference for V7R1 and
                {
                        "id" : "151",
                        "name" : "IBM iSeries Security Reference v5r4"
                {
                        "id" : "150",
                        "name" : "TNS IBM Tivoli Enterprise Client Linux Best
        },
                {
                        "id" : "149",
                        "name" : "HIPAA Windows Audit"          },
                {
                        "id" : "148",
                        "name" : "DISA STIG Cisco Network L2 Switch v8r3"
                {
                        "id" : "147",
```

```
                        "name" : "DISA STIG VMWare ESXi vCenter 5 STIG v1r5"
                {
                        "id" : "146",
                        "name" : "DISA STIG Solaris 10 X86 v1r5"
                {
                        "id" : "145",
                        "name" : "DISA STIG SharePoint 2010 v1r1"
                {
                        "id" : "144",
                        "name" : "DISA STIG SharePoint 2010 Database v1r1"
                {
                        "id" : "143",
                        "name" : "DISA Windows Server 2012 MS STIG v1r3"
                {
                        "id" : "142",
                        "name" : "DISA STIG Windows Server 2012 MS v1r1"
                {
                        "id" : "141",
                        "name" : "DISA STIG Windows Server 2012 DC v1r3"
                {
                        "id" : "140",
                        "name" : "DISA Red Hat Enterprise Linux 6 STIG v1r5"
                {
                        "id" : "139",
                        "name" : "DISA STIG Red Hat Enterprise Linux 6 v1r3"
                {
                        "id" : "138",
                        "name" : "DISA STIG for Red Hat Enterprise Linux 5 v1
},
                {
                        "id" : "137",
                        "name" : "DISA STIG OfficeSystem 2007 v4r9"
                {
```

```
                        "id" : "136",
                        "name" : "DISA STIG Apple Mac OSX 10.6 v1r3"
                {
                        "id" : "135",
                        "name" : "DISA STIG Apple Mac OSX 10.5 v1r2"
                {
                        "id" : "134",
                        "name" : "DISA Windows 8/8.1 STIG v1r6"         },
                {
                        "id" : "133",
                        "name" : "DISA Windows 8 STIG v1r2"             },
                {
                        "id" : "132",
                        "name" : "DISA STIG Office 2010 Outlook v1r5"
                {
                        "id" : "131",
                        "name" : "DISA STIG SQL Server 2012 Database OS Audit
                {
                        "id" : "130",
                        "name" : "DISA STIG SQL Server 2012 Database Instance
v1r2"           },
                {
                        "id" : "129",
                        "name" : "DISA STIG SQL Server 2012 Database Audit v1
                {
                        "id" : "128",
                        "name" : "DISA STIG IE 9 v1r5"          },
                {
                        "id" : "127",
                        "name" : "DISA STIG IE 10 v1r2"         },
                {
                        "id" : "126",
                        "name" : "DISA STIG Google Chrome v24 v1r1"
```

```
                {
                        "id" : "125",
                        "name" : "DISA STIG Cisco Perimeter Router and L3 Swit
},
                {
                        "id" : "124",
                        "name" : "DISA STIG Cisco L2 Switch v8r17"
                {
                        "id" : "123",
                        "name" : "DISA STIG Cisco Infrastructure Router and L
v8r17"          },
                {
                        "id" : "122",
                        "name" : "DISA STIG Cisco Firewall v8r17"
                {
                        "id" : "121",
                        "name" : "DISA STIG AIX 6.1 v1r2"               },
                {
                        "id" : "120",
                        "name" : "DISA STIG Cisco Perimeter Router v8r8"
                {
                        "id" : "119",
                        "name" : "DISA Oracle 11 v8r1 8 OS Windows"
                {
                        "id" : "118",
                        "name" : "DISA STIG Oracle 11 v8r1.8 OS"
                {
                        "id" : "117",
                        "name" : "DISA STIG Oracle 11 v8r1.8"           },
                {
                        "id" : "116",
                        "name" : "DISA STIG IIS 7.0 Web Site v1r2"
                {
```

```
                "id" : "115",
                "name" : "DISA STIG IIS 7.0 Web Server v1r2"
        {
                "id" : "114",
                "name" : "DISA STIG IIS 6.0 Site Checklist v6r1"
        {
                "id" : "113",
                "name" : "DISA STIG IIS 6.0 Installation v6r1"
        {
                "id" : "112",
                "name" : "DISA STIG Web Apache v6r1.12 Section 6"
        {
                "id" : "111",
                "name" : "DISA STIG Web Apache v6r1.12 Section 5"
        {
                "id" : "110",
                "name" : "CIS Cisco IOS Device L2 v3.0.1"
        {
                "id" : "109",
                "name" : "CIS Cisco IOS Device L1 v3.0.1"
        {
                "id" : "108",
                "name" : "CIS Cisco Firewall Device L2 v3.0.1"
        {
                "id" : "107",
                "name" : "CIS Cisco Firewall Device L1 v3.0.1"
        {
                "id" : "106",
                "name" : "CIS IIS 7.0/7.5 L2 v1.2.0"            },
        {
                "id" : "105",
                "name" : "CIS IIS 7.0/7.5 L1 v1.2.0"            },
        {
```

```
                "id" : "104",
                "name" : "CIS IBM DB2 OS L2 v1.2.0"            },
        {
                "id" : "103",
                "name" : "CIS IBM DB2 OS L1 v1.2.0"            },
        {
                "id" : "102",
                "name" : "CIS v1.2.0 IBM DB2 Database Level 2"
        {
                "id" : "101",
                "name" : "CIS v1.2.0 IBM DB2 Database Level 1"
        {
                "id" : "100",
                "name" : "CIS v1.1.0 Oracle 11g OS Windows Level 2"
        {
                "id" : "99",
                "name" : "CIS v1.1.0 Oracle 11g OS Windows Level 1"
        {
                "id" : "98",
                "name" : "CIS v1.1.0 Oracle 11g OS L2"         },
        {
                "id" : "97",
                "name" : "CIS v1.1.0 Oracle 11g OS L1"         },
        {
                "id" : "96",
                "name" : "CIS v1.1.0 Oracle 11g DB Level 2"
        {
                "id" : "95",
                "name" : "CIS v1.1.0 Oracle 11g DB Level 1"
        {
                "id" : "94",
                "name" : "CIS IIS 8.0 v1.1.0 Level 2"          },
        {
```

```
                "id" : "93",
                "name" : "CIS IIS 8.0 v1.1.0 Level 1"          },
        {
                "id" : "92",
                "name" : "CIS Exchange 2007 Enterprise Edge Transport
        {
                "id" : "91",
                "name" : "CIS IIS 6.0 v1.0.0"          },
        {
                "id" : "90",
                "name" : "CIS Apache Tomcat5.5/6.0 L2 v1.0"
        {
                "id" : "89",
                "name" : "CIS Apache Tomcat5.5/6.0 L1 v1.0"
        {
                "id" : "88",
                "name" : "CIS Windows XP Pro SSLF v2.01"
        {
                "id" : "87",
                "name" : "CIS Windows XP Pro Mobile v2.01"
        {
                "id" : "86",
                "name" : "CIS Windows XP Pro Legacy v2.01"
        {
                "id" : "85",
                "name" : "CIS Windows XP Pro Enterprise v2.01"
        {
                "id" : "84",
                "name" : "CIS VMware ESXi 5.1 v1.0.1 Level 2"
        {
                "id" : "83",
                "name" : "CIS VMware ESXi 5.1 v1.0.1 Level 1"
        {
```

```
                "id" : "82",
                "name" : "CIS Ubuntu 12.04 LTS Benchmark L2 v1.0.0"
        {
                "id" : "81",
                "name" : "CIS Ubuntu 12.04 LTS Benchmark L1 v1.0.0"
        {
                "id" : "80",
                "name" : "CIS SUSE Linux Enterprise Server 9.0 v1.0"
        {
                "id" : "79",
                "name" : "CIS SUSE Linux Enterprise Server 10.0 v2.0"
        {
                "id" : "78",
                "name" : "CIS Solaris 9 v1.3"           },
        {
                "id" : "77",
                "name" : "CIS Solaris 11 v1.0"          },
        {
                "id" : "76",
                "name" : "CIS Solaris 11 L2 v1.1.0"             },
        {
                "id" : "75",
                "name" : "CIS Solaris 11 L1 v1.1.0"             },
        {
                "id" : "74",
                "name" : "CIS Solaris 11.1 L2 v1.0.0"           },
        {
                "id" : "73",
                "name" : "CIS Solaris 11.1 L1 v1.0.0"           },
        {
                "id" : "72",
                "name" : "CIS Solaris 10 v5.1"          },
        {
```

```
                "id" : "71",
                "name" : "CIS SUSE Linux Enterprise Server 11 L2 v1.0
        {
                "id" : "70",
                "name" : "CIS SUSE Linux Enterprise Server 11 L1 v1.0
        {
                "id" : "69",
                "name" : "CIS Red Hat EL7 L2 v1.0.0"            },
        {
                "id" : "68",
                "name" : "CIS Red Hat EL7 L1 v1.0.0"            },
        {
                "id" : "67",
                "name" : "CIS Red Hat Enterprise Linux 6 L2 v1.3.0"
        {
                "id" : "66",
                "name" : "CIS Red Hat Enterprise Linux 6 L1 v1.3.0"
        {
                "id" : "65",
                "name" : "CIS Red Hat Enterprise Linux 5 L2 v2.1"
        {
                "id" : "64",
                "name" : "CIS Red Hat Enterprise Linux 5 L1 v2.1"
        {
                "id" : "63",
                "name" : "CIS Oracle Server 11g R2 Windows v1.0.0"
        {
                "id" : "62",
                "name" : "CIS Oracle Server 11g R2 Unix v1.0.0"
        {
                "id" : "61",
                "name" : "CIS Oracle Server 11g R2 DB v1.0.0"
        {
```

```
                "id" : "60",
                "name" : "CIS Oracle 9 10 Windows Level2 v2.01"
        {
                "id" : "59",
                "name" : "CIS Oracle 9 10 Windows Level1 v2.01"
        {
                "id" : "58",
                "name" : "CIS Oracle 9/10 OS Audit L2 v2.01"
        {
                "id" : "57",
                "name" : "CIS Oracle 9/10 OS Audit L1 v2.01"
        {
                "id" : "56",
                "name" : "CIS Oracle 9 10 DB Level2 v2.01"
        {
                "id" : "55",
                "name" : "CIS Oracle 9 10 DB Level1 v2.01"
        {
                "id" : "54",
                "name" : "CIS Apple OSX 10.6 Snow Leopard L2 v1.0.0"
        {
                "id" : "53",
                "name" : "CIS Apple OSX 10.6 Snow Leopard L1 v1.0.0"
        {
                "id" : "52",
                "name" : "CIS MySQL 4.1/5.1 OS L2 v1.0.2"
        {
                "id" : "51",
                "name" : "CIS MySQL 4.1/5.1 OS L1 v1.0.2"
        {
                "id" : "50",
                "name" : "CIS MySQL 4.1 5.1 OS L2 v1.0.2"
        {
```

```
                "id" : "49",
                "name" : "CIS MySQL 4.1 5.1 OS L1 v1.0.2"
        {
                "id" : "48",
                "name" : "CIS MySQL 4.1 5.1 L2 v1.0.2"          },
        {
                "id" : "47",
                "name" : "CIS MySQL 4.1 5.1 L1 v1.0.2"          },
        {
                "id" : "46",
                "name" : "CIS SQL Server 2012 Database OS L1 v1.1.0"
        {
                "id" : "45",
                "name" : "CIS SQL Server 2012 Database L1 DB v1.0.0"
        {
                "id" : "44",
                "name" : "CIS SQL Server 2008 R2 DB OS L1 v1.2.0"
        {
                "id" : "43",
                "name" : "CIS SQL Server 2008 R2 DB Engine L1 v1.2.0"
        {
                "id" : "42",
                "name" : "CIS Apple OSX 10.5 Leopard L2 v1.0.0"
        {
                "id" : "41",
                "name" : "CIS Apple OSX 10.5 Leopard L1 v1.0.0"
        {
                "id" : "40",
                "name" : "CIS Windows Server 2008 R2 MS v2.1.0"
        {
                "id" : "39",
                "name" : "CIS Windows 2008 R2 DC v2.1.0"
        {
```

```
                        "id" : "38",
                        "name" : "CIS Windows 2008 MS v2.1.0"          },
                {
                        "id" : "37",
                        "name" : "CIS Windows 2008 DC v2.1.0"          },
                {
                        "id" : "36",
                        "name" : "CIS Windows 8 L1 v1.0.0"             },
                {
                        "id" : "35",
                        "name" : "CIS Windows 7 v2.1"          },
                {
                        "id" : "34",
                        "name" : "CIS Windows 7 Specialized Security Laptop Be
v1.2.0"         },
                {
                        "id" : "33",
                        "name" : "CIS Windows 7 Specialized Security Desktop v
                {
                        "id" : "32",
                        "name" : "CIS Windows 7 Enterprise Laptop v1.2.0"
                {
                        "id" : "31",
                        "name" : "CIS Windows 7 Enterprise Desktop v1.2.0"
                {
                        "id" : "30",
                        "name" : "CIS Windows 2003 MS SSLF v2.0"
                {
                        "id" : "29",
                        "name" : "CIS Windows 2012 MS L1 v1.0.0"
                {
                        "id" : "28",
                        "name" : "CIS Windows 2003 MS Legacy v2.0"
```

```
                {
                        "id" : "27",
                        "name" : "CIS Windows 2003 MS Enterprise v2.0"
                {
                        "id" : "26",
                        "name" : "CIS Windows 2008 SSLF v1.2.0"         },
                {
                        "id" : "25",
                        "name" : "CIS Windows 2008 Enterprise v1.2.0"
                {
                        "id" : "24",
                        "name" : "CIS Juniper Junos Benchmark v1.0.1 L2"
                {
                        "id" : "23",
                        "name" : "CIS Juniper Junos Benchmark v1.0.1 L1"
                {
                        "id" : "22",
                        "name" : "CIS IE 9 v1.0.0"              },
                {
                        "id" : "21",
                        "name" : "CIS IE 10 v1.0.0"             },
                {
                        "id" : "20",
                        "name" : "CIS HP-UX 11i v1.5"           },
                {
                        "id" : "19",
                        "name" : "CIS FreeBSD v1.0.5"           },
                {
                        "id" : "18",
                        "name" : "CIS Debian v1.0"              },
                {
                        "id" : "17",
                        "name" : "CIS Windows 2003 DC SSLF v2.0"
```

```
                {
                        "id" : "16",
                        "name" : "CIS Windows 2012 DC L1 v1.0.0"
                {
                        "id" : "15",
                        "name" : "CIS Windows 2003 DC Legacy v2.0"
                {
                        "id" : "14",
                        "name" : "MobileIron - CIS Apple iOS 8 v1.0.0 L2"
                {
                        "id" : "13",
                        "name" : "CIS CentOS 7 L2 v1.0.0"                },
                {
                        "id" : "12",
                        "name" : "CIS CentOS 7 L1 v1.0.0"                },
                {
                        "id" : "11",
                        "name" : "CIS CentOS 6 L2 v1.0.0"                },
                {
                        "id" : "10",
                        "name" : "CIS CentOS 6 L1 v1.0.0"                },
                {
                        "id" : "9",
                        "name" : "CIS ISC BIND 9.0/9.5 v2.0.0"           },
                {
                        "id" : "8",
                        "name" : "CIS Apple Safari v1.0.0"               },
                {
                        "id" : "7",
                        "name" : "CIS Apache HTTP Server L2 v3.1"
                {
                        "id" : "6",
                        "name" : "CIS Apache HTTP Server v3.1 L1"
```

```
                {
                        "id" : "5",
                        "name" : "CIS IBM AIX 7.1 L2 v1.1.0"            },
                {
                        "id" : "4",
                        "name" : "CIS IBM AIX 7.1 L1 v1.1.0"            },
                {
                        "id" : "3",
                        "name" : "CIS AIX 5.3/6.1 L2 v1.0.0"            },
                {
                        "id" : "2",
                        "name" : "CIS AIX 5.3/6.1 L1 v1.0.0"            }
        ],
        "error_code": 0,
        "error_msg" : "",
        "warnings": [],
        "timestamp": 1442597773
}
```


/auditFileTemplate/{id}

Methods

GET

Gets the AuditFileTemplate associated with {id}.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

**id

*name

category

filename
version
editor
labels
uid
type
specType
specName
specVersion
specLink
templatePubTime
templateModTime
createdTime
modifiedTime
replaces

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*
redFont = *field is a JSON object (* ***e.g.*** *"repository" :{ "id" : <id>, "name" : <name> })*

Request Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
        "response" : {
                "id" : "3",
                "uid" : "Unix_CIS_AIX_5.3_6.1_v1.0.0_Level_II.audit",
                "filename" : "CIS_AIX_5.3_6.1_v1.0.0_Level_II.audit",
                "name" : "CIS AIX 5.3/6.1 L2 v1.0.0",
```

```
                "version" : "0000",
                "type" : "unix",
                "editor" : "[{\"name\":\"11\",\"description\":\"NIS_
SECURENETS\",\"default\":\"127\\\\.0\\\\.0\\\\.1
[\\\\\\\\s]+255\\\\.255\\\\.255\\\\.255\",\"hint\":\"This is the
list of trusted networks that should exist in
\\/var\\/yp\\/securenets\",\"required\":\"true\",\"type\":\"entr-
y\"},{\"name\":\"10\",\"description\":\"SYSLOG_
HOST\",\"default\":\"192\\\\\\\\.168\\\\\\\\.100\\\\\\\\.1\",\"hint\-
":\"This is the IP address assigned to your organization's central
logging server\",\"required\":\"true\",\"type\":\"entry\"}]",
                "specType" : "CIS",
                "specName" : "AIX 5.3/6.1 L2",
                "specVersion" : "1.0.0",
                "specLink" : "https://benchmarks.cisecurity.org/tools2/aix/CIS
IBM_AIX_5.3-6.1_Benchmark_v1.0.0.pdf",
                "templatePubTime" : "1430393700",
                "templateModTime" : "1437762375",
                "createdTime" : "1442347946",
                "modifiedTime" : "1442348201",
                "replaces" : [],
                "labels" : [
                        "aix",
                        "aix_5.3",
                        "aix_6.1",
                        "cis",
                        "unix"          ],
                "category" : {
                        "id" : "21",
                        "name" : "Unix"         }
        },
        "error_code" : 0,
        "error_msg" : "",
```

```
        "warnings" : [],
        "timestamp" : 1442597666
}
```


/auditFileTemplate/categories

Methods

GET

Gets the list of AuditFileTemplate categories

NOTE: Categories are not static. They are updated in the feed, therefore, the example response for this endpoint should not be considered as a correct listing of AuditFileTemplate categories.

Request Query Parameters

None

Example Response

Expand


```
{
  "type": "regular",
  "response": [
    {
      "id": "1",
      "name": "IBM iSeries",
      "count": "4"    },
    {
      "id": "10",
      "name": "FireEye",
      "count": "1"    },
    {
      "id": "11",
      "name": "FortiGate FortiOS",
```

```
      "count": "1"    },
    {
      "id": "12",
      "name": "HP ProCurve",
      "count": "1"    },
    {
      "id": "13",
      "name": "Huawei VRP",
      "count": "1"    },
    {
      "id": "14",
      "name": "Juniper Junos",
      "count": "8"    },
    {
      "id": "15",
      "name": "MongoDB",
      "count": "9"    },
    {
      "id": "16",
      "name": "NetApp Data ONTAP",
      "count": "1"    },
    {
      "id": "17",
      "name": "Palo Alto Networks PAN-OS",
      "count": "11"    },
    {
      "id": "18",
      "name": "RHEV",
      "count": "1"    },
    {
      "id": "2",
      "name": "Adtran NetVanta",
      "count": "1"    },
```

```
    {
      "id": "20",
      "name": "SonicWALL SonicOS",
      "count": "1"    },
    {
      "id": "21",
      "name": "Unix",
      "count": "287"    },
    {
      "id": "22",
      "name": "Unix File Contents",
      "count": "21"    },
    {
      "id": "23",
      "name": "VMware vCenter/vSphere",
      "count": "20"    },
    {
      "id": "24",
      "name": "Windows",
      "count": "309"    },
    {
      "id": "25",
      "name": "Windows File Contents",
      "count": "22"    },
    {
      "id": "26",
      "name": "Citrix XenServer",
      "count": "1"    },
    {
      "id": "3",
      "name": "BlueCoat ProxySG",
      "count": "4"    },
    {
```

```
      "id": "31",
      "name": "WatchGuard",
      "count": "1"    },
    {
      "id": "33",
      "name": "F5",
      "count": "6"    },
    {
      "id": "34",
      "name": "Arista EOS",
      "count": "3"    },
    {
      "id": "35",
      "name": "Alcatel TiMOS",
      "count": "1"    },
    {
      "id": "37",
      "name": "Netapp API",
      "count": "1"    },
    {
      "id": "38",
      "name": "Cisco Firepower",
      "count": "1"    },
    {
      "id": "4",
      "name": "Brocade FabricOS",
      "count": "1"    },
    {
      "id": "40",
      "name": "Cisco ACI",
      "count": "1"    },
    {
      "id": "5",
```

```
      "name": "Check Point GAiA",
      "count": "1"    },
    {
      "id": "6",
      "name": "Cisco IOS",
      "count": "21"    },
    {
      "id": "7",
      "name": "Database",
      "count": "56"    },
    {
      "id": "8",
      "name": "Dell Force10 FTOS",
      "count": "1"    },
    {
      "id": "9",
      "name": "Extreme ExtremeXOS",
      "count": "1"    }
  ],
  "error_code": 0,
  "error_msg": "",
  "warnings": [],
  "timestamp": 1601418375
}
```


Atlassian

Tenable Security Center API: Blackout Window

/blackout

/blackout API is deprecated and will be phased out in 5.19.0 release, Please use /freeze API instead.

Methods

GET

Gets the list of Blackout Windows.

NOTE #1: Only users in the BlackoutWindow owner's group may view target details. For users outside of the group: Repository, Assets, ipList, and allIPs will be returned {}, [], "", and "false" respectively.

NOTE #2: If a Repository or Asset associated with a BlackoutWindow has been deleted, the ID will be returned as '-1'. If one has been unshared, the ID will be similarly returned as -1, but the name will signify the Asset ID.

NOTE #3: The "status" field represents if the BlackoutWindow has been disabled via bad Repository and if it has been degrade via Asset. The "functional" field represents if there are any valid target IPs in the BlackoutWindow (allIPs, ipList, assets) in the BlackoutWindow owner's context.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
**name
**description
**status
creator
assets
repository
owner
creator
ipList
allIPs
repeatRule
start
end
duration
enabled
createdTime

modifiedTime
active
ownerGroup
canManage
functional

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*
redFont = *field is a JSON object (* ***e.g.*** *"repository" :{ "id" : <id>, "name" : <name> })*

Request Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
        "response" : [
                {
                        "id" : "20",
                        "name" : "3",
                        "description" : "",
                        "ipList" : "",
                        "start" : "TZID=America\/New_York:20141119T235800",
                        "end" : "TZID=America\/New_York:20141119T000200",
                        "duration" : "-86160",
                        "repeatRule" : "FREQ=DAILY;INTERVAL=1",
                        "status" : "0",
                        "enabled" : "false",
                        "createdTime" : "1418327672",
                        "modifiedTime" : "1418327672",
                        "assets" : [
```

```
                        {
                                "id" : "3",
                                "name" : "Test3",
                                "description" : ""
                        ],
                        "active" : "false",
                        "creator" : {
                                "id" : "1",
                                "username" : "blackoutTest",
                                "firstname" : "",
                                "lastname" : ""                 },
                        "owner" : {
                                "id" : "1",
                                "username" : "blackoutTest",
                                "firstname" : "",
                                "lastname" : ""                 },
                        "repository" : {
                                "id" : "29",
                                "name" : "Test IPv6",
                                "description" : ""                      }
                },
                {
                        "id" : "21",
                        "name" : "4",
                        "description" : "",
                        "ipList" : "172.26.50.0\/24",
                        "start" : "TZID=America\/New_York:20141119T235800",
                        "end" : "TZID=America\/New_York:20141119T000200",
                        "duration" : "-86160",
                        "repeatRule" : "FREQ=DAILY;INTERVAL=1",
                        "status" : "0",
                        "enabled" : "false",
                        "createdTime" : "1418327716",
```

```
                        "modifiedTime" : "1418327716",
                        "assets" : [],
                        "active" : "false",
                        "creator" : {
                                "id" : "1",
                                "username" : "blackoutTest",
                                "firstname" : "",
                                "lastname" : ""                 },
                        "owner" : {
                                "id" : "1",
                                "username" : "blackoutTest",
                                "firstname" : "",
                                "lastname" : ""                 },
                        "repository" : {
                                "id" : -1,
                                "name" : "",
                                "description" : ""                      }
                }
        ],
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1418332032
}
```


POST

Adds a Blackout Window.

NOTE: If 'allIPs' is 'false', an 'ipList' and/or at least one 'assets' parameter must be provided. If 'allIPs' is 'true', the back-end will clear the target (ipList, assets, and repository) fields.

Request Parameters

Expand

```
{
        "name" : <string>,
        "description" : <string> DEFAULT "",
        "repeatRule" : <string> (ical start format) DEFAULT "",
        "start" : <string> (ical start format),
        "end" : <string> (ical end format),
        "repository" : {
                "id" : <number> } DEFAULT -1 (not set),
        "allIPs" : <string> "false" | "true" DEFAULT "true",
        "enabled" : <string> "false" | "true",
        allIPs "false"  --------------
        "ipList" : <string> (valid comma-separated IP List format) DEFAULT
"",
        "assets" : [
                {
                        "id" : <number>         }...
        ] DEFAULT []
}
```

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "id" : "21",
                "name" : "4",
                "description" : "",
                "repeatRule" : "FREQ=DAILY;INTERVAL=1",
                "start" : "TZID=America\/New_York:20141119T235800",
                "end" : "TZID=America\/New_York:20141119T000200",
                "duration" : "-86160",
                "enabled" : "false",
```

```
                "createdTime" : "1418327716",
                "modifiedTime" : "1418327716",
                "ipList" : "192.168.1.0\/24",
                "status" : "0",
                "assets" : [],
                "active" : "false",
                "creator" : {
                        "id" : "1",
                        "username" : "blackoutTest",
                        "firstname" : "",
                        "lastname" : ""         },
                "owner" : {
                        "id" : "1",
                        "username" : "blackoutTest",
                        "firstname" : "",
                        "lastname" : ""         },
                "repository" : {
                        "id" : -1,
                        "name" : "",
                        "description" : ""              }
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1418327716
}
```


/blackout/{id}

Methods

GET

Gets the Blackout Window associated with {id}.

NOTE #1: Only users in the BlackoutWindow owner's group may view target details. For users outside of the group: Repository, Assets, ipList, and allIPs will be returned {}, [], "", and "false" respectively.

NOTE #2: If a Repository or Asset associated with a BlackoutWindow has been deleted, the ID will be returned as '-1'. If one has been unshared, the ID will be similarly returned as -1, but the name will signify the Asset ID.

NOTE #3: The "status" field represents if the BlackoutWindow has been disabled via bad Repository and if it has been degrade via Asset. The "functional" field represents if there are any valid target IPs in the BlackoutWindow (allIPs, ipList, assets) in the BlackoutWindow owner's context.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
**name
**description
**status
creator
assets
repository
owner
creator
ipList
allIPs
repeatRule
start
end
duration
enabled

createdTime
modifiedTime
active
ownerGroup
canManage
functional

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*
redFont = *field is a JSON object (**e.g.** "repository" :{ "id" : <id>, "name" : <name> })*

Request Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
        "response" : {
                "id" : "21",
                "name" : "4",
                "description" : "",
                "repeatRule" : "FREQ=DAILY;INTERVAL=1",
                "start" : "TZID=America\/New_York:20141119T235800",
                "end" : "TZID=America\/New_York:20141119T000200",
                "duration" : "-86160",
                "enabled" : "false",
                "createdTime" : "1418327716",
                "modifiedTime" : "1418327716",
                "ipList" : "192.168.1.0\/24",
                "status" : "0",
                "assets" : [],
```

```
                "active" : "false",
                "creator" : {
                        "id" : "1",
                        "username" : "blackoutTest",
                        "firstname" : "",
                        "lastname" : ""         },
                "owner" : {
                        "id" : "1",
                        "username" : "blackoutTest",
                        "firstname" : "",
                        "lastname" : ""         },
                "repository" : {
                        "id" : -1,
                        "name" : "",
                        "description" : ""              }
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1418332060
}
```


PATCH

Edits the Blackout Window associated with {id}, changing only the passed in fields.

NOTE: Users that are not in the same group as the BlackoutWindow owner can ONLY patch non-target fields (i.e. name, description, and enabled).

Request Parameters

(All fields are optional)

[See /blackout::POST for parameters.]

Example Response

[See /blackout/{id}::GET for example response.]

DELETE

Deletes the Blackout Window associated with {id}, depending on access and permissions.

Request Parameters

None

Example Response

Expand

```
{
        "type" : "regular",
        "response" :    "",
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1403040206
}
```

Atlassian

Tenable Security Center API: Bulk

/bulk

The bulk endpoint is very resource intensive. Requests that are too large may fail. It is recommended to minimize the payload size of requests to bulk.

Methods

POST

Performs a bulk action, depending on access and permissions.

NOTE #1: Currently supported bulk actions (with links to their respective documentation):

- */asset::DELETE*
- */asset::POST*

- */asset/<id>::PATCH*
- */dashboard/<id>/component::POST*
- */dashboard/<id>/component/<id>::PATCH*
- */hosts/acr::PATCH*
- */query::POST*
- */query/<id>::GET*
- */query/<id>::PATCH*
- */recastRiskRule::PATCH*

NOTE #2: If a bulk post fails on one object, the bulk operation will continue to attempt other objects, return a fail response indicating failed objects, and rollback all bulk actions.

NOTE #2: For a bulk ACR edit, which is bulk action /hosts/acr::PATCH, all bulk operations that are successful will make the change to the object, and the bulk operations that fail will of course not make the change. But there will be a fail response for the overall bulk request and the returned fail response indicates which operations failed. All operations are attempted even if some fail.

Request Parameters

Expand

```
{
       "operations" : [
              {
                     "api" : <string> "/asset" | "/asset/<id>" |
"/dashboard/<id>/component" | "/dashboard/<id>/component/<id>" |
"/hosts/acr" | "/query" | "/query/<id>" | "/recastRiskRule",
                     "method" : <string> "DELETE" | "GET" | "PATCH" | "POST
                     method "GET"                    ------------
                     "params" : <valid object parameters:see NOTE #1> DEFAU

                     method not "GET"                          ------------
                     "params" : <valid object parameters:see NOTE #1>
```

```
        ]
}
```

Example Response

Expand

```
{
        "type" : "regular",
        "response" : [
                {
                        "type" : "regular",
                        "response" : {
                                "id" : "38",
                                "name" : "testBulk",
                                "type" : "dynamic",
                                "description" : "",
                                "tags" : "",
                                "context" : "",
                                "status" : "0",
                                "createdTime" : "1414436709",
                                "modifiedTime" : "1423678805",
                                "typeFields" : {
                                        "rules" : {
                                                "operator" : "any",
                                                "children" : [
                                                        {
                                                                "filterName"
                                                                "operator" : "
                                                                "value" : "192
                                                                "pluginIDConst
                                                                "type" : "clau
                                                ],
                                                "type" : "group"
```

```
                        },
                        "repositories" : [],
                        "ipCount" : 0,
                        "groups" : [],
                        "assetDataFields" : [],
                        "canUse" : "true",
                        "canManage" : "true",
                        "creator" : {
                                "id" : "1",
                                "username" : "head",
                                "firstname" : "Security Manager",
                                "lastname" : ""
                        "owner" : {
                                "id" : "1",
                                "username" : "head",
                                "firstname" : "Security Manager",
                                "lastname" : ""
                        "template" : {
                                "id" : -1,
                                "name" : "",
                                "description" : ""
                        "ownerGroup" : {
                                "id" : "0",
                                "name" : "Full Access",
                                "description" : "Full Access group"
                        "targetGroup" : {
                                "id" : -1,
                                "name" : "",
                                "description" : ""
                },
                "error_code" : 0,
                "error_msg" : "",
                "warnings" : [],
```

```
                "timestamp" : 1423678804
        },
        {
                "type" : "regular",
                "response" : {
                        "id" : "38",
                        "name" : "testBulk2",
                        "type" : "dynamic",
                        "description" : "",
                        "tags" : "",
                        "context" : "",
                        "status" : "0",
                        "createdTime" : "1414436709",
                        "modifiedTime" : "1423678805",
                        "typeFields" : {
                        "rules" : {
                                "operator" : "any",
                                "children" : [
                                        {
                                                "filterName" : "ip",
                                                "operator" : "eq",
                                                "value" : "192.168.0.0
                                                "pluginIDConstraint"
                                                "type" : "clause"
                                ],
                                "type" : "group"
                        },
                        "repositories" : [],
                        "ipCount" : 0,
                        "groups" : [],
                        "assetDataFields" : [],
                        "canUse" : "true",
                        "canManage" : "true",
```

```
                        "creator" : {
                                "id" : "1",
                                "username" : "head",
                                "firstname" : "Security Manager",
                                "lastname" : ""
                        "owner" : {
                                "id" : "1",
                                "username" : "head",
                                "firstname" : "Security Manager",
                                "lastname" : ""
                        "template" : {
                                "id" : -1,
                                "name" : "",
                                "description" : ""
                        "ownerGroup" : {
                                "id" : "0",
                                "name" : "Full Access",
                                "description" : "Full Access group"
                        "targetGroup" : {
                                "id" : -1,
                                "name" : "",
                                "description" : ""
                    },
                    "error_code" : 0,
                    "error_msg" : "",
                    "warnings" : [],
                    "timestamp" : 1423678804
            }
    ],
    "error_code" : 0,
    "error_msg" : "",
    "warnings" : [],
    "timestamp" : 1423678804
```

```
}
```

Atlassian

Tenable Security Center API: Configuration

/config

Methods

GET

Gets the system configuration types

Request Parameters

None

Example Response

Expand

```
{
        "type" : "regular",
        "response" : [
                {
                        "id" : 1,
                        "name" : "Commands"
                },
                {
                        "id" : 2,
                        "name" : "Active Plugins"
                },
```

```
        {
                "id" : 4,
                "name" : "Passive Plugins"
        },
        {
                "id" : 8,
                "name" : "SMTP"
        },
        {
                "id" : 32,
                "name" : "Scanner"
        },
        {
                "id" : 64,
                "name" : "Application"
        },
        {
                "id" : 128,
                "name" : "Expiration"
        },
        {
                "id" : 256,
                "name" : "Web Proxy"
        },
        {
                "id" : 512,
                "name" : "Status"
        },
        {
                "id" : 1024,
                "name" : "Logging"
        },
        {
```

```
                        "id" : 2048,
                        "name" : "Advanced"
                },
                {
                        "id" : 4096,
                        "name" : "Cosign"
                },
                {
                        "id" : 8192,
                        "name" : "Reporting"
                },
                {
                        "id" : 16384,
                        "name" : "Feed"
                }
        ],
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1410207176
}
```


/config/{id}

Methods

GET

Gets the configuration information associated with configuration type {id}.

Request Query Parameters

None

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "id" : "1",
                "name" : "Active Plugins",
                "CommandTAR" : "\/bin\/tar",
                "CommandRM" : "\/bin\/rm",
                "CommandGUNZIP" : "\/bin\/gunzip",
                "CommandZIP" : "\/usr\/bin\/zip",
                "CommandFILE" : "\/usr\/bin\/file",
                "CommandUNZIP" : "\/usr\/bin\/unzip",
                "CommandZCAT" : "\/bin\/zcat",
                "CommandGZIP" : "\/bin\/gzip"
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1410207242
}
```


PATCH

Edits the configuration information associated with configuration type {id}, changing only the passed in fields.

Request Parameters

(All fields are optional)

Expand

NOTE #1: For types "ScanResultExpiration" | "reportResultExpiration" | TicketExpiration" | "VulnTrendExpiration", Configuration value field must contain a positive integer (0 or greater)
NOTE #2: For valid names for types, perform config/{id}::GET on desired configuration type.

```
{
        <name:string> : <value:string>...
}
```

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "id" : "1",
                        "name" : {
                        "id" : 2,
                        "name" : "Active Plugins"
                },
                "CommandTAR" : "\/bin\/tar2",
                "CommandRM" : "\/bin\/rm",
                "CommandGUNZIP" : "\/bin\/gunzip",
                "CommandZIP" : "\/usr\/bin\/zip",
                "CommandFILE" : "\/usr\/bin\/file",
                "CommandUNZIP" : "\/usr\/bin\/unzip",
                "CommandZCAT" : "\/bin\/zcat",
                "CommandGZIP" : "\/bin\/gzip"
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1410209192
}
```

/config/query

Methods

GET

Gets the status of the configuration type(s) specified

Request Parameters

Expand

Parameters must be passed in as query string (as opposed to JSON) in the format of: /config/query?item=smtp

```
{
        "item" : <string> (comma-separated array) "smtp" &| "reportTypes"
&| "mdmTypes" &| "complianceTypes" &| "ldap" &| "saml"
}
```

Example Response

Expand

```
{
        "type" : "regular",
        "response" :
        [
                {
                        "item" : "ldap",
                        "configured" : false
                },
                {
                        "item" : "saml",
                        "configured" : false
                },
                {
                        "item" : "smtp",
                        "configured" : false
                },
                {
             "item":"reportTypes",
```

```
            "details":[
                {
                    "name":"PDF",
                    "type":"pdf",
                    "enabled":"true",
                    "attributeSets":[]
                },
                {
                                    "name":"CSV",
                    "type":"csv",
                    "enabled":"true",
                    "attributeSets":[]
                },
                {
                    "name":"RTF",
                    "type":"rtf",
                    "enabled":"true",
                    "attributeSets":[]
                },
                {
                    "name":"DISA ARF",
                    "type":"arf",
                    "enabled":"false",
                    "attributeSets":[
                        "arf"
                    ]
                },
                {
                    "name":"DISA ASR",
                    "type":"asr",
                    "enabled":"false",
                    "attributeSets":[]
                },
```

```
                {
                    "name":"CyberScope",
                    "type":"lasr",
                    "enabled":"false",
                    "attributeSets":[
                        "lasr"
                    ]
                }
            ]
        },
                {
                    "item" : "mdmTypes",
                    "details" : [
                            {
                                    "id" : "1",
                                    "name" : "ActiveSync",
                                    "description" : "",
                                    "value" : "ActiveSync",
                                    "ipPref" : "Domain Controller  : ",
                                    "pluginIDs" : [
                                            {
                                                    "id" : "60024"
                                            }
                                    ],
                                    "editor" :
"W3sidHlwZSI6ICJlbnRyeSIsIm5hbWUiOiAiRG9tYWluIENvbnRyb2xsZXIiLCJyZXF-
1aXJlZCI6InRydWUiLCJpZCI6ICJkb21haW5fY29udHJvbGxlciJ9LCB7InR5cGUiOiA-
iZW50cnkiLCJuYW1lIjogIkRvbWFpbiIsInJlcXVpcmVkIjoidHJ1ZSIsImlkIjogImR-
vbWFpbiJ9LHsidHlwZSI6ICJlbnRyeSIsIm5hbWUiOiAiRG9tYWluIFVzZXJuYW1lIiw-
icmVxdWlyZWQiOiJ0cnVlIiwiaWQiOiAiZG9tYWluX2FkbWluIn0seyJ0eXBlIjogInB-
hc3N3b3JkIiwibmFtZSI6ICJEb21haW4gUGFzc3dvcmQiLCJyZXF1aXJlZCI6InRydWU-
iLCJpZCI6ICJwYXNzd29yZCJ9XQ=="
                            },
```

```
                                {
                                        "id" : "2",
                                        "name" : "Apple Profile Manager",
                                        "description" : "",
                                        "value" : "profile_manager",
                                        "ipPref" : "Apple Profile Manager serv
                                                "pluginIDs" : [
                                                {
                                                        "id" : "60032"
                                                }
                                        ],
                                        "editor" :
"W3sidHlwZSI6ICJlbnRyeSIsIm5hbWUiOiJTZXJ2ZXIiLCJyZXF1aXJlZCI6InRydWU-
iLCJpZCI6InNlcnZlciJ9LCB7InR5cGUiOiAiZW50cnkiLCJuYW1lIjoiUG9ydCIsImR-
lZmF1bHQiOjQ0MywicmVnZXgiOiAiXihbMC05XXsxLDR9fFsxLTVdWzAtOV17NH18Nls-
wLTRdWzAtOV17M318NjVbMC00XVswLTldezJ9fDY1NVswLTJdWzAtOV18NjU1M1swLTV-
dKSQiLCJyZXF1aXJlZCI6InRydWUiLCJpZCI6InBvcnQifSx7InR5cGUiOiAiZW50cnk-
iLCJuYW1lIjoiVXNlcm5hbWUiLCJyZXF1aXJlZCI6dHJ1ZSwiaWQiOiJ1c2VybmFtZSJ-
9LHsidHlwZSI6ICJwYXNzd29yZCIsIm5hbWUiOiJQYXNzd29yZCIsInJlcXVpcmVkIjp-
0cnVlLCJpZCI6InBhc3N3b3JkIn0seyJ0eXBlIjogImNoZWNrYm94Iiwibm FtZSI6ICJ-
IVFRQUyIsImlkIjogImh0dHBzIiwiZGVmYXVsdCI6ICJ5ZXMiLCJjb25kaXRpb25hbFN-
ldHRpbmdzIjogeyJ5ZXMiOiB7ImlucHV0cyI6IFt7InR5cGUiOiAiY2hlY2tib3giLCJ-
uYW1lIjogIlZlcmlmeSBTU0wgQ2VydGlmaWNhdGUiLCJyZXF1aXJlZCI6ICJ0cnVlIiw-
iZGVmYXVsdCI6ICJ5ZXMiLCJpZCI6ICJ2ZXJpZnlfc3NsIn1dfX19XQ==="
                                },
                                {
                                        "id" : "3",
                                        "name" : "Good MDM",
                                        "description" : "",
                                        "value" : "GoodMDM",
                                        "ipPref" : "GMC Server  : ",
                                        "pluginIDs" : [
                                                {
```

```
                                                "id" : "66963"
                                        }
                                ],
                                "editor" :
"W3sidHlwZSI6ICJlbnRyeSIsIm5hbWUiOiJTZXJ2ZXIiLCJyZXF1aXJlZCI6InRydWU-
iLCJpZCI6InNlcnZlciJ9LCB7InR5cGUiOiAiZW50cnkiLCJuYW1lIjoiUG9ydCIsInJ-
lZ2V4IjogIl4oWzAtOV17MSw0fXxbMS01XVswLTldezR9fDZbMC00XVswLTldezN9fDY-
1WzAtNF1bMC05XXsyfXw2NTVbMC0yXVswLTldfDY1NTNbMC01XSkkIiwicmVxdWlyZWQ-
iOiJ0cnVlIiwiaWQiOiJwb3J0In0seyJ0eXBlIjogImVudHJ5IiwibmFtZSI6IkRvbWF-
pbiIsInJlcXVpcmVkIjoidHJ1ZSIsImlkIjoiZG9tYWluIn0seyJ0eXBlIjogImVudHJ-
5IiwibmFtZSI6IlVzZXJuYW1lIiwicmVxdWlyZWQiOiJ0cnVlIiwiaWQiOiJ1c2VybmF-
tZSJ9LHsidHlwZSI6ICJwYXNzd29yZCIsIm5hbWUiOiJQYXNzd29yZCIsInJlcXVpcmV-
kIjoidHJ1ZSIsImlkIjoicGFzc3dvcmQifSx7InR5cGUiOiAiY2hlY2tib3giLCJuYW1-
lIjogIkhUVFBTIiwiaWQiOiAiaHR0cHMiLCJkZWZhdWx0IjogInllcyIsImNvbmRpdGl-
vbmFsU2V0dGluZ3MiOiB7InllcyI6IHsiaW5wdXRzIjogW3sidHlwZSI6ICJjaGVja2J-
veCIsIm5hbWUiOiAiVmVyaWZ5IFNTTCBDZXJ0aWZpY2F0ZSIsInJlcXVpcmVkIjogInR-
ydWUiLCJkZWZhdWx0IjogInllcyIsImlkIjogInZlcmlmeV9zc2wifV19fX1d"
                                },
                                {
                                        "id" : "4",
                                        "name" : "Mobile Iron",
                                        "description" : "",
                                        "value" : "MobileIron",
                                        "ipPref" : "MobileIron VSP Admin Porta
                                        "pluginIDs" : [
                                                {
                                                        "id" : "72904"
                                                }
                                        ],
                                        "editor" :
"W3sidHlwZSI6ICJlbnRyeSIsIm5hbWUiOiJNb2JpbGVJcm9uIFZTUCBBZG1pbiBQb3J-
0YWwgVVJMIiwicmVxdWlyZWQiOiJ0cnVlIiwicGxhY2Vob2xkZXIiOiJodHRwczovL3d-
```

3dy5leGFtcGxlLm5ldC9taWZzL2xvZ2luLmpzcCIsImlkIjoicG9ydGFsX3VybCJ9LCB-
7InR5cGUiOiAiZW50cnkiLCJuYW1lIjoiTW9iaWxlSXJvbiBQb3J0IiwicmVnZXgiOiA-
iXihbMC05XXsxLDR9fFsxLTVdWzAtOV17NH18NlswLTRdWzAtOV17M318NjVbMC00XVs-
wLTldezJ9fDY1NVswLTJdWzAtOV18NjU1M1swLTVdKSQiLCJyZXF1aXJlZCI6InRydWU-
iLCJkZWZhdWx0IjoiNDQzIiwiaWQiOiJwb3J0In0seyJ0eXBlIjogImVudHJ5IiwibmF-
tZSI6IlVzZXJuYW1lIiwicmVxdWlyZWQiOnRydWUsInBsYWNlaG9sZGVyIjoiYXBpdXN-
lciIsImlkIjoidXNlcm5hbWUifSx7InR5cGUiOiAicGFzc3dvcmQiLCJuYW1lIjoiUGF-
zc3dvcmQiLCJyZXF1aXJlZCI6InRydWUiLCJpZCI6InBhc3N3b3JkIn0seyJ0eXBlIjo-
gImNoZWNrYm94IiwibmFtZSI6ICJIVFRQUyIsImlkIjogImh0dHBzIiwiZGVmYXVsdCI-
6ICJ5ZXMiLCJjb25kaXRpb25hbFNldHRpbmdzIjogeyJ5ZXMiOiB7ImlucHV0cyI6IFt-
7InR5cGUiOiAiY2hlY2tib3giLCJuYW1lIjogIlZlcmlmeSBTU0wgQ2VydGlmaWNhdGU-
iLCJyZXF1aXJlZCI6ICJ0cnVlIiwiZGVmYXVsdCI6ICJ5ZXMiLCJpZCI6ICJ2ZXJpZnl-
fc3NsIn1dfX19XQ==" },
{
"id" : "5",
"name" : "AirWatch MDM",
"description" : "",
"value" : "AirWatch",
"ipPref" : "AirWatch Environment API U
"pluginIDs" : [
{
"id" : "76460"
}
],
"editor" :
"W3sidHlwZSI6ICJlbnRyeSIsIm5hbWUiOiAiQWlyV2F0Y2ggRW52aXJvbm1lbnQgQVB-
JIFVSTCIsInBsYWNlaG9sZGVyIjoiaHR0cHM6Ly9haXJ3YXRjaC5leGFtcGxlLm5ldC9-
haXJ3YXRjaHNlcnZpY2VzLzAvIiwicmVxdWlyZWQiOiJ0cnVlIiwiaWQiOiAiYXBpX3V-
ybCJ9LCB7InR5cGUiOiAiZW50cnkiLCJuYW1lIjogIlBvcnQiLCJkZWZhdWx0IjoiNDQ-
zIiwicmVnZXgiOiAiXihbMC05XXsxLDR9fFsxLTVdWzAtOV17NH18NlswLTRdWzAtOV1-
7M318NjVbMC00XVswLTldezJ9fDY1NVswLTJdWzAtOV18NjU1M1swLTVdKSQiLCJyZXF-

```
1aXJlZCI6InRydWUiLCJpZCI6InBvcnQifSx7InR5cGUiOiAiZW50cnkiLCJuYW1lIjo-
gIlVzZXJuYW1lIiwicmVxdWlyZWQiOiJ0cnVlIiwiaWQiOiJ1c2VybmFtZSJ9LHsidHl-
wZSI6ICJwYXNzd29yZCIsIm5hbWUiOiAiUGFzc3dvcmQiLCJyZXF1aXJlZCI6InRydWU-
iLCJpZCI6InBhc3N3b3JkIn0seyJ0eXBlIjogImVudHJ5IiwibmFtZSI6ICJBUEkgS2V-
5IiwicmVxdWlyZWQiOiJ0cnVlIiwiaWQiOiJhcGlfa2V5In0seyJ0eXBlIjogImNoZWN-
rYm94IiwibmFtZSI6ICJIVFRQUyIsImlkIjogImh0dHBzIiwiZGVmYXVsdCI6ICJ5ZXM-
iLCJjb25kaXRpb25hbFNldHRpbmdzIjogeyJ5ZXMiOiB7ImlucHV0cyI6IFt7InR5cGU-
iOiAiY2hlY2tib3giLCJuYW1lIjogIlZlcmlmeSBTU0wgQ2VydGlmaWNhdGUiLCJyZXF-
1aXJlZCI6ICJ0cnVlIiwiZGVmYXVsdCI6ICJ5ZXMiLCJpZCI6ICJ2ZXJpZnlfc3NsIn1-
dfX19XQ=="
                                }
                        ]
                },
        {
            "item":"complianceTypes",
            "details":{
                "windows":{
                    "pluginID":"21156",
                    "auditFileType":"windows",
                    "displayName":"Windows"
                },
                "unix":{
                    "pluginID":"21157",
                    "auditFileType":"unix",
                    "displayName":"Unix"
                },
                "windowsfiles":{
                    "pluginID":"24760",
                    "auditFileType":"windowsfiles",
                    "displayName":"Windows Files"
                },
                "database":{
                    "pluginID":"33814",
```

```
        "auditFileType":"database",
        "displayName":"Database"
    },
    "cisco":{
        "pluginID":"46689",
        "auditFileType":"cisco",
        "displayName":"Cisco"
    },
    "as\/400":{
        "pluginID":"57860",
        "auditFileType":"as\/400",
        "displayName":"AS\/400"
    },
    "checkpoint":{
        "pluginID":"62679",
        "auditFileType":"checkpoint",
        "displayName":"Checkpoint"
    },
    "juniper":{
        "pluginID":"62680",
        "auditFileType":"juniper",
        "displayName":"Juniper"
    },
    "palo_alto":{
        "pluginID":"64095",
        "auditFileType":"palo_alto",
        "displayName":"Palo Alto"
    },
    "vmware":{
        "pluginID":"64455",
        "auditFileType":"vmware",
        "displayName":"VMWare"
    },
```

```
"scapWindows":{
    "pluginID":"66756",
    "auditFileType":"scapWindows",
    "displayName":"SCAP Windows"
},
"scapLinux":{
    "pluginID":"66757",
    "auditFileType":"scapLinux",
    "displayName":"SCAP Linux"
},
"netapp":{
    "pluginID":"66934",
    "auditFileType":"netapp",
    "displayName":"NetApp"
},
"xenserver":{
    "pluginID":"69512",
    "auditFileType":"xenserver",
    "displayName":"Citrix XenServer"
},
"hpprocurve":{
    "pluginID":"70271",
    "auditFileType":"hpprocurve",
    "displayName":"HP ProCurve"
},
"fortigate":{
    "pluginID":"70272",
    "auditFileType":"fortigate",
    "displayName":"Fortigate FortiOS"
},
"fireeye":{
    "pluginID":"70469",
    "auditFileType":"fireeye",
```

```
                "displayName":"FireEye"
            },
            "brocade":{
                "pluginID":"71842",
                "auditFileType":"brocade",
                "displayName":"Brocade FabricOS"
            },
            "sonicwall":{
                "pluginID":"71955",
                "auditFileType":"sonicwall",
                "displayName":"SonicWALL SonicOS"
            },
            "adtran":{
                "pluginID":"71991",
                "auditFileType":"adtran",
                "displayName":"Adtran AOS"
            },
            "amazon_aws":{
                "pluginID":"72426",
                "auditFileType":"amazon_aws",
                "displayName":"Amazon AWS"
            },
            "extreme_extremexos":{
                "pluginID":"73156",
                "auditFileType":"extreme_extremexos",
                "displayName":"Extreme ExtremeXOS"
            }
        }
    }
],
"error_code" : 0,
"error_msg" : "",
"warnings" : [],
```

```
        "timestamp" : 1410209808
}
```

/config/testSMTP

Methods

POST

Tests the SMTP settings

Request Parameters

Expand

```
{
        "SMTPPassword" : <string> OPTIONAL
}
```

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "status" : false,
                "message" : "Sender not accepted."
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1410210283
}
```

/config/license/register

/tes/config/license/register

/tes/config/license/register is only available in Tenable Enclave Security

Methods

POST

Registers a license file

Request Parameters

Expand

```
{
        "filename" : <string> (name of uploaded file)
}
```

Example Response

Expand


```
{
        "type" : "regular",
        "response" : {
                "config" : {
                        "Version" : "5.0.0",
                        "Banner" : "",
                        "Logo" : "assets\/mariana\/images\/sc4icon.png",
                        "LoginSessionTimeout" : "3600",
                        "LoginMaxAttempts" : "20",
                        "URL" : "https:\/\/192.168.1.1\/",
                        "VulnTrendExpiration" : "90",
                        "FreshInstall" : "no",
                        "ScanResultExpiration" : "365",
                        "ReportResultExpiration" : "365",
                        "TicketExpiration" : "365",
```

```
                        "AdvancedFields" :
"MaxNessusChunkSize,ScannerStatusConnectTimeout,ScannerStatusTimeou-
t",
                        "LicenseConfig" : {
                                "ipCount" : "0",
                                "mode" : "SC",
                                "timestamp" : 1410149400,
                                "features" : {
                                        "" : ""
                                },
                                "status" : "Valid",
                                "maxIPCount" : "500000",
                                "expiration" : 1410926400,
                                "hostname" : "name",
                                "customer" : "Customer",
                                "type" : "Demo"
                        },
                        "HeaderText" : "",
                        "PluginUpdateSiteACAS" : "",
                        "PasswordMinLength" : "3",
                        "ServerAuth" : "any",
                        "MaxNessusChunkSize" : "-1",
                        "ServerClassification" : "None",
                        "SupportV1Data" : "true",
                        "LCEPluginUpdateSiteACAS" : "",
                        "FeedActivationCode" : "",
                        "FeedSubscriptionStatus" : "Expired",
                        "FeedUpdateSite" : "downloads.nessus.org",
                        "FeedPackage" : "SecurityCenterFeed48.tar.gz",
                        "FeedUpdateSiteACAS" : "",
                        "SecurityCenterID" : "192.168.1.1",
                        "SecurityCenterIDOverride" : "",
                        "EnabledReports" : "pdf,rtf,csv,lasr"
```

```
        },
        "reportTypes" : [
                {
                        "name" : "PDF",
                        "type" : "pdf",
                        "enabled" : "true",
                        "attributeSets" : []
                },
                {
                        "name" : "CSV",
                        "type" : "csv",
                        "enabled" : "true",
                        "attributeSets" : []
                },
                {
                        "name" : "RTF",
                        "type" : "rtf",
                        "enabled" : "true",
                        "attributeSets" : []
                },
                {
                        "name" : "DISA ARF",
                        "type" : "arf",
                        "enabled" : "false",
                        "attributeSets" : ["arf"]
                },
                {
                        "name" : "DISA ASR",
                        "type" : "asr",
                        "enabled" : "false",
                        "attributeSets" : []
                },
                {
```

```
                                "name" : "CyberScope",
                                "type" : "lasr",
                                "enabled" : "true",
                                "attributeSets" : ["lasr"]
                        }
                ],
                "licenseStatus" : "Valid",
                "mode" : "SC",
                "ACAS" : "false"
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1410210722
}
```

/config/plugins/register

Methods

POST

Registers the plugin specified

Request Parameters

Expand

```
{
        "activationCode" : <string>,
        "updateSite" : <string>,
        "type" : <string> "active" | "lce" | "passive" | "industrial"
}
```

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "PluginSubscriptionStatus" : "Invalid"
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1410211133
}
```

/config/plugins/reset

Methods

POST

Resets the plugin codes for the plugin type parameter specified

Request Parameters

Expand

```
{
        "type" : <string> "active" | "lce" | "passive" | "industrial"
}
```

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "PluginSubscriptionStatus" : "Unconfigured"
        },
```

```
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1410211133
}
```


Atlassian

Tenable Security Center API: Configuration Section

/configSection

Methods

GET

Gets the Configuration Sections

Request Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
        "response" : [
                {
                        "id" : 0,
                        "name" : "Plugins",
                        "description" : "Review and apply license information
products"                 },
                {
                        "id" : 1,
                        "name" : "Mail",
                        "description" : "Configure SMTP settings for sending e
```

```
Tenable.sc"              },
                null,
                {
                        "id" : 3,
                        "name" : "Security",
                        "description" : "Configure login and display security
},
                {
                        "id" : 4,
                        "name" : "Miscellaneous",
                        "description" : "Settings for Web Proxy, Syslog, Noti
and additional report types"             },
                {
                        "id" : 5,
                        "name" : "Data Expiration",
                        "description" : "Settings for how long data is retaine
                {
                        "id" : 6,
                        "name" : "External Schedules",
                        "description" : "Configure data retrieval settings fo
LCE"             },
                {
                        "id" : 7,
                        "name" : "Plugins / Feed",
                        "description" : "Manage Tenable plugins and feeds"
                {
                        "id" : 8,
                        "name" : "SAML",
                        "description" : "Settings for SAML 2.0 identity provi
Shibboleth idenity provider"             },
                {
                        "id" : 9,
                        "name" : "Lumin",
```

```
                        "description" : "Configure settings for Lumin Synchron
    }
        ],
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1549381986
    }
```


/configSection/{id}

Methods

GET

Gets the Configuration Section associated with {id}.

NOTE: For id "8", the /saml/{id}::GET endpoint is a direct alias and may also be used (see the SAML).

Request Query Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
        "response" : {
                "id" : "1",
                "name" : "Mail",
                "description" : "This is the Mail section.",
                "SMTPHost" : "",
                "SMTPAuth" : "",
                "SMTPConnection" : "",
```

```
                "SMTPPort" : "",
                "SMTPUsername" : "",
                "SMTPPassword" : "",
                "SMTPReturnAddress" : "",
                "SMTPHostname" : ""     },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1410211451
}
```


PATCH

Edits the Configuration Section associated with {id}, changing only the passed in fields.

NOTE: For id "8", the /saml/{id}::PATCH endpoint is a direct alias and may also be used (see the SAML).

Request Parameters

(All fields are optional)

Expand

NOTE: For valid names for section types, perform /configSection/{id}::GET on desired configuration section type.

```
{
    <name:string> : <value:string>...
}
```

Example Response

See /configSection/{id}::GET

Atlassian

Tenable Security Center API: Credential

/credential

Methods

GET

Gets the list of Credentials.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

NOTE: 'typeFields' returns type-specific parameters inside of a 'typeFields." It does not consider authType, privilegeEscalation, or dbType. If requested, typeFields returns as follows:

type"database": login, password, sid, port, authType, dbType, oracleAuthType, oracle_service_type, source, csv_file, SQLServerAuthType, vault_host, vault_port, vault_username, vault_password, vault_cyberark_url, vault_safe, vault_app_id, vault_folder, vault_use_ssl, vault_verify_ssl, vault_address, vault_account_name, vault_cyberark_client_cert, vault_cyberark_private_key, vault_cyberark_private_key_passphrase, lieberman_host, lieberman_port, lieberman_pam_user, lieberman_pam_password, lieberman_use_ssl, lieberman_verify_ssl, lieberman_system_name, hashicorp_host, hashicorp_port,hashicorp_authentication_type,hashicorp_role_id,hashicorp_role_secret_id, hashicorp_client_cert, hashicorp_private_key, hashicorp_private_key_passphrase, hashicorp_auth_url,hashicorp_namespace, hashicorp_kv_url, hashicorp_username_source,hashicorp_userkey,hashicorp_passkey,hashicorp_secret,hashicorp_use_ssl,hashicorp_verify_ssl, hashicorp_vault_type,sybase_ase_auth_type,pam_user,pam_password,pam_auth_method,kdc,kdc_port,kdc_transport,pam_kdc_domain,pam_api_user,pam_api_key,pam_ssh_key

type"ssh": authType, username, password, publicKey, privateKey, passphrase, kdc_ip, kdc_port, kdc_protocol, kdc_realm, vault_host, vault_port, vault_username, vault_password, vault_cyberark_url, vault_safe, vault_app_id, vault_folder, vault_use_ssl, vault_verify_ssl, vault_address, vault_account_name, vault_cyberark_client_cert, vault_cyberark_private_key, vault_cyberark_private_key_passphrase, thycotic_secret_name, thycotic_url, thycotic_username, thycotic_password, thycotic_organization, thycotic_domain, thycotic_private_key, thycotic_ssl_verify, privilegeEscalation, escalationUsername, escalationPassword, escalationSuUser, escalationPath, escalationAccount, lieberman_host, lieberman_port, lieberman_pam_user, lieberman_pam_password, lieberman_use_ssl, lieberman_verify_ssl, beyondtrust_host,

beyondtrust_port, beyondtrust_api_key, beyondtrust_duration, beyondtrust_use_ssl, beyondtrust_verify_ssl, beyondtrust_use_private_key, beyondtrust_use_escalation, beyondtrust_api_user, hashicorp_host, hashicorp_port,hashicorp_authentication_type,hashicorp_role_id,hashicorp_role_secret_id, hashicorp_client_cert, hashicorp_private_key, hashicorp_private_key_passphrase, hashicorp_auth_url,hashicorp_namespace, hashicorp_kv_url, hashicorp_username_source,hashicorp_userkey,hashicorp_passkey,hashicorp_secret,hashicorp_use_ssl,hashicorp_verify_ssl, pam_host, pam_port, pam_api_user, pam_api_key, pam_auth_url, pam_query_url, pam_engine_url, pam_namespace, pam_duration, pam_use_ssl, pam_verify_ssl, hashicorp_vault_type,pam_secret_name,pam_ssh_key,pam_auth_method,,kdc,kdc_port,kdc_transport,realm

type"snmp": communityString
type"windows": authType, username, password, domain, kdc_ip, kdc_port, kdc_protocol, vault_host, vault_port, vault_username, vault_password, vault_cyberark_url, vault_safe, vault_app_id, vault_folder, vault_use_ssl, vault_verify_ssl, thycotic_secret_name, thycotic_url, vault_account_name, vault_cyberark_client_cert, vault_cyberark_private_key, vault_cyberark_private_key_passphrase, thycotic_username, thycotic_password, thycotic_organization, thycotic_domain, thycotic_ssl_verify, lieberman_host, lieberman_port, lieberman_pam_user, lieberman_pam_password, lieberman_use_ssl, lieberman_verify_ssl, beyondtrust_host, beyondtrust_port, beyondtrust_api_key, beyondtrust_duration, beyondtrust_use_ssl, beyondtrust_verify_ssl, beyondtrust_api_user, hashicorp_host, hashicorp_port,hashicorp_authentication_type,hashicorp_role_id,hashicorp_role_secret_id, hashicorp_client_cert, hashicorp_private_key, hashicorp_private_key_passphrase, hashicorp_auth_url,hashicorp_namespace, hashicorp_kv_url, hashicorp_username_source,hashicorp_userkey,hashicorp_passkey,hashicorp_secret,hashicorp_use_ssl,hashicorp_verify_ssl, pam_host, pam_port, pam_api_user, pam_api_key, pam_auth_url, pam_query_url, pam_engine_url, pam_namespace, pam_duration, pam_use_ssl, pam_verify_ssl, hashicorp_vault_type,kdc,kdc_port,kdc_transport

type"apiGateway": authType,datapower_client_cert, datapower_private_key, datapower_private_key_passphrase, datapower_enable_hashicorp, datapower_custom_header_key, datapower_custom_header_value

Allowed Fields

*id
*uuid
**name

**description
**type
creator
target
groups
typeFields
tags
createdTime
modifiedTime
canUse
canManage

Session user role not "1" (Administrator)

owner
ownerGroup
targetGroup

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

redFont = *field is a JSON object (* ***e.g.*** *"repository" :{ "id" : <id>, "name" : <name> })*

Request Parameters

None

Filter Parameters

usable - The response will be an object containing an array of usable Credentials. By default, both usable and manageable objects are returned.
manageable - The response will be an object containing all manageable Credentials. By default, both usable and manageable objects are returned.

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "usable" : [
                        {
                                "id" : "1000001",
                                "name" : "Test",
                                "description" : "",
                                "type" : "ssh",
                                "uuid" : "E7BC705C-9088-4F5A-81A0-A5B13F5C433
                        {
                                "id" : "1000002",
                                "name" : "test",
                                "description" : "",
                                "type" : "ssh",
                                "uuid" : "E58A2208-2776-4200-B6E5-A844AC26E338
                ],
                "manageable" : [
                        {
                                "id" : "1000001",
                                "name" : "Test",
                                "description" : "",
                                "type" : "ssh",
                                "uuid" : "E7BC705C-9088-4F5A-81A0-A5B13F5C433
                        {
                                "id" : "1000002",
                                "name" : "test",
                                "description" : "",
                                "type" : "ssh",
                                "uuid" : "E58A2208-2776-4200-B6E5-A844AC26E338
                ]
        },
        "error_code" : 0,
```

```
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1408719365
}
```

POST

Adds a Credential.

Request Parameters

Expand

```
{
        "name" : <string>,
        "tags" : <string> DEFAULT "",
        "description" : <string> DEFAULT "",
        "type" : <string> "apiGateway" | "database" | "windows" | "snmp" |
"ssh" | "webAuthentication"     ...
}
```

NOTE: webAuthentication type is only available for Security Center instances with WAS active license

type is "database"

```
{
        ...
        "login" : <string>,

        "authType" : <string> "cyberark" | "Hashicorp" | "lieberman" |
"password",
        "dbType" : <string> "Oracle" | "SQL Server" | "DB2" | "MySQL" |
"PostgreSQL" | "Informix/DRDA" | "Sybase ASE" | "Apache Cassandra",
```

```
authType "password"     -------------------
"password" : <string>,
"sid" : <string> DEFAULT "",
"port" : <string> (valid port number),

authType "cyberark"     -------------------
"vault_host" : <string> (valid IP or IP host),
"vault_port" : <string> (valid port number),
"vault_username" : <string> DEFAULT "",
"vault_password" : <string> DEFAULT "",
"vault_cyberark_url" : <string> DEFAULT "",
"vault_safe" : <string>,
"vault_app_id" : <string>,
"vault_policy_id" : <string> DEFAULT "",
"vault_folder" : <string>,
"vault_use_ssl" : <string> "no" | "yes",
"vault_verify_ssl" : <string> "no" | "yes",
"vault_address" : <string> DEFAULT "",
"vault_account_name" : <string>,
"vault_cyberark_client_cert" : <string>,
"vault_cyberark_private_key" : <string>,
"vault_cyberark_private_key_passphrase" : <string>,
"sid" : <string> DEFAULT "",
"port" : <string> (valid port number),
"dbType" : <string>,

authType "cyberarkAutoDiscovery"        -------------------
"pam_host" : <string> (valid IP or IP host),
"pam_port" : <string> (valid port number),
"pam_app_id" : <string>,
"pam_address" : <string>,
"pam_safe" : <string> DEFAULT "" ,
"pam_auth_method" : "Client Certificate" | "IIS Basic
```

```
Authentication",
       "vault_password" : <string> DEFAULT "",
       "vault_username" : <string> DEFAULT "",
       "pam_private_key_passphrase" : <string> DEFAULT "",
       "pam_user" : <string> DEFAULT "",
       "pam_password" : <string> DEFAULT "",
       "pam_use_ssl" : <string> "no" | "yes",
       "pam_verify_ssl" : <string> "no" | "yes",
       "dbType" : <string>,

       authType "senhasegura"  -------------------
       "pam_api_key" : <string>,
       "pam_api_user" : <string>,
       "pam_credential_id" : <string>,
       "pam_host" : <string> (valid IP or IP host),
       "pam_port" : <string> (valid port number),
       "pam_private_key" :  <string>,
       "pam_use_ssl" : <string> "no" | "yes",
       "pam_verify_ssl" : <string> "no" | "yes",
       "sid" : <string> DEFAULT "",
       "port" : <string> (valid port number),
       "dbType" : <string>,

       authType "wallix"       -------------------
       "pam_host" : <string> (valid IP or IP host),
       "pam_port" : <string> (valid port number),
       "pam_auth_method" : "Basic" | "API Key",
       "pam_user" : <string>,
       "pam_password" : <string>,
       "pam_api_key" : <string>,
       "pam_api_user" : <string>,
       "pam_credential_id" : <string>,
       "pam_use_ssl" : <string> "no" | "yes",
```

```
        "pam_verify_ssl" : <string> "no" | "yes",
        "sid" : <string> DEFAULT "",
        "port" : <string> (valid port number),
        "dbType" : <string>,

        authType "Hashicorp"    --------------------
        "hashicorp_host" : <string> (valid IP or IP host),
        "hashicorp_port" : <string> (valid port number),
        "hashicorp_authentication_type" : <string> "App Role" |
"Certificates",
        "hashicorp_role_id" : <string>,
        "hashicorp_role_secret_id" : <string>,
        "hashicorp_client_cert" : <string>,
        "hashicorp_private_key" : <string>,
        "hashicorp_private_key_passphrase" : <string>,
        "hashicorp_auth_url" : <string>,
        "hashicorp_namespace" : <string>,
        "hashicorp_kv_url" : <string>,
        "hashicorp_username_source" : <string> "Hashicorp Vault" | "Manual
Entry",
        "hashicorp_userkey" : <string>,
        "hashicorp_passkey" : <string>,
        "hashicorp_secret" : <string>,
        "hashicorp_use_ssl" : <string> "false" | "true",
        "hashicorp_verify_ssl" : <string> "false" | "true",
        "hashicorp_vault_type" : <string> "KV1" | "KV2" | "AD",
        "pam_auth_method" : <string> "no" | "yes",
        "kdc" : <string> (valid IP or IP host),
        "kdc_port" :  <string> (valid port number),
        "kdc_transport" :  <string>,
        "sid" : <string> DEFAULT "",
        "port" : <string> (valid port number),
        "dbType" : <string>,
```

```
       authType "lieberman"    --------------------
       "lieberman_host" : <string> (valid IP or IP host),
       "lieberman_port" : <string> (valid port number),
       "lieberman_pam_user" : <string> DEFAULT "",
       "lieberman_pam_password" : <string> DEFAULT "",
       "lieberman_use_ssl" : <string> "false" | "true",
       "lieberman_verify_ssl" : <string> "false" | "true",
       "lieberman_system_name" : <string>,
       "sid" : <string> DEFAULT "",
       "port" : <string> (valid port number),
       "dbType" : <string>,

       dbType "Oracle" ---------------
       "OracleAuthType" : <string>,
       "oracle_service_type" : <string>,
       "source" : <string>,

    dbType "Oracle" and source "Import"    -------------------------
----------
    "csv_file" : <string>,

    dbType "DB2"    ------------
    "source" : <string> "Entry" | "Import",

    dbType "DB2" and source "Import"    ----------------------------
----
    "csv_file" : <string>,

    dbType "MySQL"    --------------
    "source" : <string> "Entry" | "Import",

    dbType "MySQL" and source "Import"    -------------------------
```

```
--------
    "csv_file" : <string>,

       dbType "SQL Server"     -------------------
       "SQLServerAuthType" : <string>,
       "source" : <string> "Entry" | "Import",

    dbType "SQL Server" and source "Import"    ---------------------
------------------
    "csv_file" : <string>,

       dbType "Sybase ASE"     -------------------
       "sybase_ase_auth_type" : <string> "RSA" | "Plain Text"}
```

type is "ssh"

```
{
       ...
       "username" : <string>,
       "authType" : <string> "Arcon" | "BeyondTrust" | "Centrify" |
"certificate" | "cyberark" | "delinea" | "Hashicorp" | "kerberos" |
"lieberman" | "password" | "publickey" | "thycotic"
       authType "Arcon"        ----------------
       "pam_host" : <string> (valid IP or IP host),
       "pam_port" : <string> (valid port number),
       "pam_api_user" : <string>,
       "pam_api_key" : <string>,
       "pam_auth_url" : <string>,
       "pam_query_url" : <string>,
       "pam_engine_url" : <string>,
       "pam_namespace" : <string>,
       "pam_duration" : <string>,
       "pam_use_ssl" : <string> "no" | "yes",
       "pam_verify_ssl" : <string> "no" | "yes",
```

```
    "privilegeEscalation" : <string> "none" | "su" | "sudo" |
"su+sudo" | "dzdo" | "pbrun" | "cisco" | ".k5login"     authType
"BeyondTrust"   ----------------------
       "beyondtrust_host" : <string> (valid IP or IP host),
       "beyondtrust_port" : <string> (valid port number),
       "beyondtrust_api_key" : <string>,
       "beyondtrust_duration" : <string>,
       "beyondtrust_use_ssl" : <string> "no" | "yes",
       "beyondtrust_verify_ssl" : <string> "no" | "yes",
       "beyondtrust_use_private_key" : <string> "no" | "yes",
       "beyondtrust_use_escalation" : <string> "no" | "yes",
       "beyondtrust_api_user" : <string>,

       authType "Centrify"     ----------------
       "pam_host" : <string> (valid IP or IP host),
       "pam_port" : <string> (valid port number),
       "pam_api_user" : <string>,
       "pam_api_key" : <string>,
       "pam_namespace" : <string>,
       "pam_auth_url" : <string>,
       "pam_query_url" : <string>,
       "pam_engine_url" : <string>,
       "username" : <string>,
       "pam_duration" : <string>,
       "pam_use_ssl" : <string> "no" | "yes",
       "pam_verify_ssl" : <string> "no" | "yes"
       authType "certificate"  ----------------------
       "publicKey" : <string>,
       "privateKey" : <string>,
       "passphrase" : <string> DEFAULT "",
       "privilegeEscalation" : <string> "none" | "su" | "sudo" | "su+sudo"
| "dzdo" | "pbrun" | "cisco" | ".k5login",
```

```
        authType "cyberark"     -------------------
        "vault_host" : <string> (valid IP or IP host),
        "vault_port" : <string> (valid port number),
        "vault_username" : <string> DEFAULT "",
        "vault_password" : <string> DEFAULT "",
        "vault_cyberark_url" : <string> DEFAULT "",
        "vault_safe" : <string>,
        "vault_app_id" : <string>,
        "vault_policy_id" : <string> DEFAULT "",
        "vault_folder" : <string>,
        "vault_use_ssl" : <string> "false" | "true",
        "vault_verify_ssl" : <string> "false" | "true",
        "vault_address" : <string> DEFAULT "",
        "vault_account_name" : <string>,
        "vault_cyberark_client_cert" : <string>,
        "vault_cyberark_private_key" : <string>,
        "vault_cyberark_private_key_passphrase" : <string>,
        "privilegeEscalation" : <string> "none" | "su" | "sudo" | "su+sudo"
| "dzdo" | "pbrun" | "cisco" | ".k5login",

        authType "cyberarkAutoDiscovery"        -------------------
        "pam_host" : <string> (valid IP or IP host),
        "pam_port" : <string> (valid port number),
        "pam_app_id" : <string>,
        "pam_address" : <string>,
        "pam_safe" : <string> DEFAULT "" ,
        "pam_auth_method" : "Client Certificate" | "IIS Basic
Authentication",
        "vault_password" : <string> DEFAULT "",
        "vault_username" : <string> DEFAULT "",
        "pam_private_key_passphrase" : <string> DEFAULT "",
        "pam_user" : <string> DEFAULT "",
        "pam_password" : <string> DEFAULT "",
```

```
        "pam_use_ssl" : <string> "no" | "yes",
        "pam_verify_ssl" : <string> "no" | "yes",
        "privilegeEscalation" : <string> "none" | "sudo",

        authType "senhasegura"  -------------------
        "pam_api_key" : <string>,
        "pam_api_user" : <string>,
        "pam_credential_id" : <string>,
        "pam_host" : <string> (valid IP or IP host),
        "pam_port" : <string> (valid port number),
        "pam_private_key" :  <string>,
        "pam_use_ssl" : <string> "no" | "yes",
        "pam_verify_ssl" : <string> "no" | "yes",
        "privilegeEscalation" : <string> "none" | "su" | "sudo" | "su+sudo"
 | "dzdo" | "pbrun" | "cisco" | ".k5login",

        authType "wallix"       -------------------
        "pam_host" : <string> (valid IP or IP host),
        "pam_port" : <string> (valid port number),
        "pam_auth_method" : "Basic" | "API Key",
        "pam_user" : <string>,
        "pam_password" : <string>,
        "pam_api_key" : <string>,
        "pam_api_user" : <string>,
        "pam_credential_id" : <string>,
        "pam_use_ssl" : <string> "no" | "yes",
        "pam_verify_ssl" : <string> "no" | "yes",
        "privilegeEscalation" : <string> "none" | "su" | "sudo" | "su+sudo"
 | "dzdo" | "pbrun" | "cisco" | ".k5login",

        authType "delinea"      --------------------
        "pam_host" : <string> (valid IP or IP host),
        "pam_password" : <string>,
```

```
        "pam_port" : <string> (valid port number),
        "pam_secret_name" : <string>,
        "pam_duration" : <string> (valid duration number in hours),
        "pam_ssh_key" :  <string> "no" | "yes",
        "pam_user" : <string>,
        "pam_verify_ssl" :  <string> "no" | "yes",
        "pam_use_ssl" : <string> "no" | "yes",
        "privilegeEscalation" : <string> "none" | "su" | "sudo" | "su+sudo"
| "dzdo" | "pbrun" | "cisco" | ".k5login" | "Checkpoint Gaia
'Expert'",
    "escalationCustomPasswordPrompt" : <string>,

        authType "Hashicorp"    --------------------
        "hashicorp_host" : <string> (valid IP or IP host),
        "hashicorp_port" : <string> (valid port number),
        "hashicorp_authentication_type" : <string> "App Role" |
"Certificates",
        "hashicorp_role_id" : <string>,
        "hashicorp_role_secret_id" : <string>,
        "hashicorp_client_cert" : <string>,
        "hashicorp_private_key" : <string>,
        "hashicorp_private_key_passphrase" : <string>,
        "hashicorp_auth_url" : <string>,
        "hashicorp_namespace" : <string>,
        "hashicorp_kv_url" : <string>,
        "hashicorp_username_source" : <string> "Hashicorp Vault" | "Manual
Entry",
        "hashicorp_userkey" : <string>,
        "hashicorp_passkey" : <string>,
        "hashicorp_secret" : <string>,
        "hashicorp_use_ssl" : <string> "no" | "yes",
        "hashicorp_verify_ssl" : <string> "no" | "yes",
        "hashicorp_vault_type" : <string> "KV1" | "KV2" | "AD" | "LDAP"
```

```
"pam_auth_method" : <string> "no" | "yes",
       "kdc" : <string> (valid IP or IP host),
       "kdc_port" :  <string> (valid port number),
       "kdc_transport" :  <string>,
       "privilegeEscalation" : <string> "none" | "su" | "sudo" | "su+sudo"
| "dzdo" | "pbrun" | "cisco" | ".k5login",

       authType "kerberos"     -------------------
       "password" : <string>,
       "kdc_ip" : <string> (valid IP address),
       "kdc_port" : <string> (valid port number),
       "kdc_protocol" : <string>,
       "kdc_realm" : <string>,
       "privilegeEscalation" : <string> "none" | "su" | "sudo" | "su+sudo"
| "dzdo" | "pbrun" | "cisco" | ".k5login",

       authType "lieberman"    --------------------
       "lieberman_host" : <string> (valid IP or IP host),
       "lieberman_port" : <string> (valid port number),
       "lieberman_pam_user" : <string> DEFAULT "",
       "lieberman_pam_password" : <string> DEFAULT "",
       "lieberman_use_ssl" : <string> "false" | "true",
       "lieberman_verify_ssl" : <string> "false" | "true",

       authType "password"     -------------------
       "password" : <string>,
       "privilegeEscalation" : <string> "none" | "su" | "sudo" | "su+sudo"
| "dzdo" | "pbrun" | "cisco" | ".k5login",

       authType "publickey"    --------------------
       "privateKey" : <string>,
       "passphrase" : <string> DEFAULT "",
       "privilegeEscalation" : <string> "none" | "su" | "sudo" | "su+sudo"
```

```
| "dzdo" | "pbrun" | "cisco" | ".k5login",

       authType "thycotic"     -------------------
       "thycotic_secret_name" : <string>,
       "thycotic_url" : <string>,
       "thycotic_username" : <string>,
       "thycotic_password" : <string>,
       "thycotic_organization" : <string> DEFAULT "",
       "thycotic_domain" : <string> DEFAULT "",
       "thycotic_private_key " : <string> "no" | "yes",
       "thycotic_ssl_verify" : <string> "no" | "yes",
       "privilegeEscalation" : <string> "none" | "su" | "sudo" | "su+sudo"
| "dzdo" | "pbrun" | "cisco" | ".k5login",

       privilegeEscalation ".k5login" and authType not "cyberark"      -----
-----------------------------------------------
       "escalationUsername" : <string> privilegeEscalation ".k5login" and
authType "cyberark"     ----------------------------------------------
------
       "escalationPassword" : <string>
       privilegeEscalation "cisco" and authType not "Arcon" or "thycotic"
-------------------------------------------------------------------
       "escalationPassword" : <string> privilegeEscalation "cisco" and
authType "Arcon" or "thycotic"  ------------------------------------
-------------------------
       "escalationUsername" : <string>
       privilegeEscalation "dzdo" and authType not "Arcon" or "thycotic"
-------------------------------------------------------------------
       "escalationUsername" : <string> DEFAULT "",
       "escalationPassword" : <string> DEFAULT "",
       "escalationPath" : <string> DEFAULT ""
       privilegeEscalation "dzdo" and authType "Arcon" ------------------
---------------------------
```

```
       "escalationUsername" : <string> DEFAULT "",
       "escalationPath" : <string> DEFAULT "",
       "escalationAccount" : <string> DEFAULT ""
       privilegeEscalation "dzdo" and authType "thycotic"      ----------
---------------------------------
       "escalationUsername" : <string>, DEFAULT "",
       "escalationPath" : <string> DEFAULT ""
       privilegeEscalation "pbrun" and authType not "Arcon" or "thycotic"
-------------------------------------------------------------------
       "escalationPassword" : <string>,
       "escalationPath" : <string> DEFAULT ""  privilegeEscalation "pbrun"
and authType "Arcon"    ---------------------------------------------
-
       "escalationUsername" : <string> DEFAULT "",
       "escalationPath" : <string> DEFAULT "",
       "escalationAccount" : <string> DEFAULT ""
       privilegeEscalation "pbrun" and authType "thycotic"     ----------
-----------------------------------
       "escalationUsername" : <string>,
       "escalationPath" : <string> DEFAULT ""
       privilegeEscalation "su+sudo" and authType not "Arcon" or
"thycotic"      ------------------------------------------------------
-----------
       "escalationSuUser" : <string>,
       "escalationUsername" : <string> DEFAULT "",
       "escalationPassword" : <string> DEFAULT "",
       "escalationPath" : <string> DEFAULT ""  privilegeEscalation
"su+sudo" and authType "Arcon"  ------------------------------------
------------
       "escalationSuUser" : <string>,
       "escalationUsername" : <string> DEFAULT "",
       "escalationPath" : <string> DEFAULT "",
       "escalationAccount" : <string> DEFAULT ""
```

```
       privilegeEscalation "su+sudo" and authType "thycotic"   ------------
----------------------------------------
       "escalationSuUser" : <string>,
       "escalationUsername" : <string> DEFAULT "",
       "escalationPassword" : <string> DEFAULT "",
       "escalationPath" : <string> DEFAULT ""
       privilegeEscalation "su" | "sudo" and authType not "Arcon" or
"thycotic"      ------------------------------------------------------
---------------
       "escalationUsername" : <string> DEFAULT "",
       "escalationPassword" : <string> DEFAULT "",
       "escalationPath" : <string> DEFAULT ""  privilegeEscalation "su" |
"sudo" and authType "Arcon"     ---------------------------------------
--------------
       "escalationUsername" : <string> DEFAULT "",
       "escalationPath" : <string> DEFAULT "",
       "escalationAccount" : <string> DEFAULT ""       privilegeEscalation "s
| "sudo" and authType "thycotic"        ---------------------------------
----------------------
       "escalationUsername" : <string> DEFAULT "",
       "escalationPath" : <string> DEFAULT ""  privilegeEscalation
"Checkpoint Gaia 'Expert'" and authType "delinea"       -----------------
----------------------------------------
       "escalationUsername" : <string> DEFAULT "",
       "escalationPath" : <string> DEFAULT ""}
```

type is "snmp"

```
{
       ...
       "communityString" : <string>}
```

type is "windows"

```
{
       ...
       "username" : <string>,
       "authType" : <string> "BeyondTrust" | "Centrify" | "cyberark" |
"cyberarkAutoDiscovery" | "delinea" | "senhasegura" | "wallix" |
"Hashicorp" | "kerberos" | "lieberman" | "lm" | "ntlm" | "password"
| "thycotic",

       authType "Arcon"        ----------------
       "pam_host" : <string> (valid IP or IP host),
       "pam_port" : <string> (valid port number),
       "pam_api_user" : <string>,
       "pam_api_key" : <string>,
       "pam_auth_url" : <string>,
       "pam_query_url" : <string>,
       "pam_engine_url" : <string>,
       "pam_namespace" : <string>,
       "pam_duration" : <string>,
       "pam_use_ssl" : <string> "no" | "yes",
       "pam_verify_ssl" : <string> "no" | "yes"        authType "BeyondTrust"
--------------------
       "domain" : <string> DEFAULT "",
       "beyondtrust_host" : <string> (valid IP or IP host),
       "beyondtrust_port" : <string> (valid port number),
       "beyondtrust_api_key" : <string>,
       "beyondtrust_duration" : <string>,
       "beyondtrust_use_ssl" : <string> "no" | "yes",
       "beyondtrust_verify_ssl" : <string> "no" | "yes",
       "beyondtrust_api_user" : <string>       authType "Centrify"     ------
---
       "pam_host" : <string> (valid IP or IP host),
       "pam_port" : <string> (valid port number),
       "pam_api_user" : <string>,
```

```
        "pam_api_key" : <string>,
        "pam_namespace" : <string>,
        "pam_auth_url" : <string>,
        "pam_query_url" : <string>,
        "pam_engine_url" : <string>,
        "username" : <string>,
        "pam_duration" : <string>,
        "pam_use_ssl" : <string> "no" | "yes",
        "pam_verify_ssl" : <string> "no" | "yes"
        authType "cyberark"     -------------------
        "domain" : <string> DEFAULT "",
        "vault_host" : <string> (valid IP or IP host),
        "vault_port" : <string> (valid port number),
        "vault_username" : <string> DEFAULT "",
        "vault_password" : <string> DEFAULT "",
        "vault_cyberark_url" : <string> DEFAULT "",
        "vault_safe" : <string>,
        "vault_app_id" : <string>,
        "vault_policy_id" : <string> DEFAULT "",
        "vault_folder" : <string>,
        "vault_use_ssl" : <string>,
        "vault_verify_ssl" : <string>,
        "vault_account_name" : <string>,
        "vault_cyberark_client_cert" : <string>,
        "vault_cyberark_private_key" : <string>,
        "vault_cyberark_private_key_passphrase" : <string>      authType
"cyberarkAutoDiscovery" -------------------
        "pam_host" : <string> (valid IP or IP host),
        "pam_port" : <string> (valid port number),
        "pam_app_id" : <string>,
        "pam_address" : <string>,
        "pam_safe" : <string> DEFAULT "" ,
        "pam_auth_method" : "Client Certificate" | "IIS Basic
```

```
Authentication",
       "vault_password" : <string> DEFAULT "",
       "vault_username" : <string> DEFAULT "",
       "pam_private_key_passphrase" : <string> DEFAULT "",
       "pam_user" : <string> DEFAULT "",
       "pam_password" : <string> DEFAULT "",
       "pam_use_ssl" : <string> "no" | "yes",
       "pam_verify_ssl" : <string> "no" | "yes",

       authType "senhasegura"  -------------------
       "pam_api_key" : <string>,
       "pam_api_user" : <string>,
       "pam_credential_id" : <string>,
       "pam_host" : <string> (valid IP or IP host),
       "pam_port" : <string> (valid port number),
       "pam_private_key" :  <string>,
       "pam_use_ssl" : <string> "no" | "yes",
       "pam_verify_ssl" : <string> "no" | "yes",

       authType "wallix"       -------------------
       "pam_host" : <string> (valid IP or IP host),
       "pam_port" : <string> (valid port number),
       "pam_auth_method" : "Basic" | "API Key",
       "pam_user" : <string>,
       "pam_password" : <string>,
       "pam_api_key" : <string>,
       "pam_api_user" : <string>,
       "pam_credential_id" : <string>,
       "pam_use_ssl" : <string> "no" | "yes",
       "pam_verify_ssl" : <string> "no" | "yes",

       authType "delinea"      --------------------
       "pam_host" : <string> (valid IP or IP host),
```

```
        "pam_password" : <string>,
        "pam_port" : <string> (valid port number),
        "pam_secret_name" : <string>,
        "pam_duration" : <string> (valid duration number in hours),
        "pam_ssh_key" :  <string> "no" | "yes",
        "pam_user" : <string>,
        "pam_verify_ssl" :  <string> "no" | "yes",
        "pam_use_ssl" : <string> "no" | "yes",

        authType "Hashicorp"    --------------------
        "hashicorp_host" : <string> (valid IP or IP host),
        "hashicorp_port" : <string> (valid port number),
        "hashicorp_authentication_type" : <string> "App Role" |
"Certificates",
        "hashicorp_role_id" : <string>,
        "hashicorp_role_secret_id" : <string>,
        "hashicorp_client_cert" : <string>,
        "hashicorp_private_key" : <string>,
        "hashicorp_private_key_passphrase" : <string>,
        "hashicorp_auth_url" : <string>,
        "hashicorp_namespace" : <string>,
        "hashicorp_kv_url" : <string>,
        "hashicorp_username_source" : <string> "Hashicorp Vault" | "Manual
Entry",
        "hashicorp_userkey" : <string>,
        "hashicorp_passkey" : <string>,
        "hashicorp_secret" : <string>,
        "hashicorp_use_ssl" : <string> "false" | "true",
        "hashicorp_verify_ssl" : <string> "false" | "true",
        "hashicorp_vault_type" : <string> "KV1" | "KV2" | "AD" | "LDAP"
"pam_auth_method" : <string> "no" | "yes",
        "kdc" : <string> (valid IP or IP host),
        "kdc_port" :  <string> (valid port number),
```

```
        "kdc_transport" :  <string>,

        authType "kerberos"     -------------------
        "password" : <string>,
        "kdc_ip" : <string> (valid IP address),
        "kdc_port" : <string> (valid port number),
        "kdc_protocol" : <string>,
        "kdc_realm" : <string>  authType "lieberman"    --------------------
        "lieberman_host" : <string> (valid IP or IP host),
        "lieberman_port" : <string> (valid port number),
        "lieberman_pam_user" : <string> DEFAULT "",
        "lieberman_pam_password" : <string> DEFAULT "",
        "lieberman_use_ssl" : <string> "false" | "true",
        "lieberman_verify_ssl" : <string> "false" | "true"
        authType "lm" | "ntlm" | "password"     ------------------------------
----
        "password" : <string>,
        "domain" : <string> DEFAULT ""
        authType "thycotic"     -------------------
        "domain" : <string> DEFAULT "",
        "thycotic_secret_name" : <string>,
        "thycotic_url" : <string>,
        "thycotic_username" : <string>,
        "thycotic_password" : <string>,
        "thycotic_organization" : <string> DEFAULT "",
        "thycotic_domain" : <string> DEFAULT "",
        "thycotic_ssl_verify" : <string> "no" | "yes",
        "privilegeEscalation" : <string> "none" DEFAULT "none"}
```

type is "apiGateway"

```
{
        ...
        "authType" : <string> "ibmDPGateway",
```

```
        authType "ibmDPGateway" ----------------
        "datapower_client_cert" : <string>,
        "datapower_custom_header_key" : <string>,
        "datapower_custom_header_value" : <string>,
        "datapower_enable_hashicorp" : <string> "no" | "yes" DEFAULT "yes",
        "datapower_private_key" : <string>,
        "datapower_private_key_passphrase" : <string>}
```

type is "miscellaneous"

```
{
        ...
        "authType" : <string> "nutanix",

        authType "nutanix"      ----------------
        "nutanix_host": <string> (valid IP or IP host),
    "nutanix_port": <string> (valid port number),
    "nutanix_username": <string>,
    "nutanix_password": <string>,
    "nutanix_auto_discover_host": <string> "no" | "yes" DEFAULT
"yes",
    "nutanix_auto_discover_vm": <string> "no" | "yes" DEFAULT "yes",
    "nutanix_use_ssl": <string> "no" | "yes" DEFAULT "yes",
    "nutanix_verify_ssl": <string> "no" | "yes" DEFAULT "no",
    "context": <string>}
```

type is "webAuthentication"

```
{
        ...
        "authType" : <string> "ClientCertificate" | "HTTPServer" |
"WebApplication"        authType "ClientCertificate"    ----------------
        "client_cert" : <string> (generated name of uploaded file),
```

```
       "private_key" : <string> (generated name of uploaded file),
       "passphrase" : <string>,
       "login_check_url" : <string> (valid url - must start with http://
or https://),
       "login_check_pattern" : <string>        authType "HTTPServer"   ------
----
       "username" : <string>,
       "password" : <string>,
       "auth_type" : <string> "basic" | "ntlm" | "kerberos"    authType
"HTTPServer" and auth_type "kerberos"   "username" : <string>,
       "password" : <string>,
       "auth_type" : <string> "kerberos",
       "kerberos_domain" : <string>,
       "kdc_address" : <string>        authType "WebApplication"       ------
       "was_auth_method" : <string> "login_form" | "cookie" | "api_key" |
"selenium" | "bearer",
       ...

       authType "WebApplication" and was_auth_method "login_form"      ------
--------
       "login_page" : <string> (valid url - must start with http:// or
https://),
       "login_check" : <string>,
       "login_parameters" : <string>,
       "login_check_url" : <string> (valid url - must start with http://
or https://),
       "login_check_pattern" : <string>
       authType "WebApplication" and was_auth_method "cookie"  ------------
----
       "cookies" : <string>,
       "cookie_check_url" : <string> (valid url - must start with http://
or https://),
       "cookie_check_pattern" : <string>       authType "WebApplication" and
```

```
was_auth_method "api_key"       ----------------
       "headers" : <string>,
       "login_check_url" : <string> (valid url - must start with http://
or https://),
       "login_check_pattern" : <string>        authType "WebApplication" and
auth_method "selenium"  ----------------
       "script_contents" : <string> (generated name of uploaded file),
       "login_check_url" : <string> (valid url - must start with http://
or https://),
       "login_check_pattern" : <string>        authType "WebApplication" and
auth_method "bearer"    ----------------
       "token" : <string>,
       "login_check_url" : <string> (valid url - must start with http://
or https://),
       "login_check_pattern" : <string>}
```

NOTE: The following fields (login_parameters, cookies, headers) must have the following construct

1. Key-Value pair is delimited by the colon character ':'
2. Key and value must be base64 encoded separately
3. Parameters (Key-Value pairs) are separated by a comma

Example:

```
Construct:
<base64encoded key>:<base64encoded value>,<base64encoded
key>:<base64encoded value>,...

Example Desired Input (multiple):
Key: "Test Key 1", Value: "Test Value 1"Key: "Test Key 2", Value:
"Test Value 2"Actual Input Required:
VGVzdCBLZXkgMQ==:VGVzdCBWYWx1ZSAx,VGVzdCBLZXkgMg==:VGVzdCBWYWx1ZSAy
```

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "id" : "1000009",
                "type" : "database",
                "name" : "'database' Test PATCH",
                "description" : "Manually inputted in data for use in testing"
                "tags" : "",
                "createdTime" : "1433187223",
                "modifiedTime" : "1433265608",
                "typeFields" : {
                        "login" : "test",
                        "password" : "SET",
                        "sid" : "",
                        "port" : "49",
                        "dbType" : "Oracle",
                        "oracleAuthType" : "test",
                        "SQLServerAuthType" : ""                },
                "groups" : [],
                "canUse" : "true",
                "canManage" : "true",
                "creator" : {
                        "id" : "1",
                        "username" : "head",
                        "firstname" : "Security Manager",
                        "lastname" : "",
                         "uuid" : "48F26F3B-6A79-4153-96DB-4C63D1BF3D46"
                },
                "owner" : {
                        "id" : "1",
                        "username" : "head",
                        "firstname" : "Security Manager",
                        "lastname" : "",
```

```
                        "uuid" : "48F26F3B-6A79-4153-96DB-4C63D1BF3D46"
                },
                "ownerGroup" : {
                        "id" : "0",
                        "name" : "Full Access",
                        "description" : "Full Access group"            },
                "targetGroup" : {
                        "id" : -1,
                        "name" : "",
                        "description" : ""              },
                "uuid" : "701246AF-956F-4185-A514-62F7959B031E" },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1433279057
}
```


/credential/{id}

/credential/{uuid}

Methods

GET

Gets the Credential associated with {id} or {uuid}.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

NOTE: 'typeFields' returns type-specific parameters inside of a 'typeFields." It does not consider authType, privilegeEscalation, or dbType. If requested, typeFields returns as follows:

type"database": login, password, sid, port, dbType, oracleAuthType, oracle_service_type, SQLServerAuthType, vault_host, vault_port, vault_username, vault_password, vault_cyberark_url, vault_safe, vault_app_id, vault_folder, vault_use_ssl, vault_verify_ssl, vault_address, vault_account_name, vault_cyberark_client_cert, vault_cyberark_private_key, vault_cyberark_private_key_passphrase, lieberman_host, lieberman_port, lieberman_pam_user, lieberman_pam_password, lieberman_use_ssl, lieberman_verify_ssl, lieberman_system_name, hashicorp_host, hashicorp_port,hashicorp_authentication_type,hashicorp_role_id,hashicorp_role_secret_id, hashicorp_client_cert, hashicorp_private_key, hashicorp_private_key_passphrase, hashicorp_auth_url,hashicorp_namespace, hashicorp_kv_url, hashicorp_username_source,hashicorp_userkey,hashicorp_passkey,hashicorp_secret,hashicorp_use_ssl,hashicorp_verify_ssl, hashicorp_vault_type,sybase_ase_auth_type

type"ssh": authType, username, password, publicKey, privateKey, passphrase, kdc_ip, kdc_port, kdc_protocol, kdc_realm, vault_host, vault_port, vault_username, vault_password, vault_cyberark_url, vault_safe, vault_app_id, vault_folder, vault_use_ssl, vault_verify_ssl, vault_address, vault_account_name, vault_cyberark_client_cert, vault_cyberark_private_key, vault_cyberark_private_key_passphrase, thycotic_secret_name, thycotic_url, thycotic_username, thycotic_password, thycotic_organization, thycotic_domain, thycotic_private_key, thycotic_ssl_verify, privilegeEscalation, escalationUsername, escalationPassword, escalationSuUser, escalationPath, escalationAccount, lieberman_host, lieberman_port, lieberman_pam_user, lieberman_pam_password, lieberman_use_ssl, lieberman_verify_ssl, beyondtrust_host, beyondtrust_port, beyondtrust_api_key, beyondtrust_duration, beyondtrust_use_ssl, beyondtrust_verify_ssl, beyondtrust_use_private_key, beyondtrust_use_escalation, beyondtrust_api_user, hashicorp_host, hashicorp_port,hashicorp_authentication_type,hashicorp_role_id,hashicorp_role_secret_id, hashicorp_client_cert, hashicorp_private_key, hashicorp_private_key_passphrase, hashicorp_auth_url,hashicorp_namespace, hashicorp_kv_url,hashicorp_username_source,hashicorp_userkey,hashicorp_passkey,hashicorp_secret,hashicorp_use_ssl,hashicorp_verify_ssl, pam_host, pam_port, pam_api_user, pam_api_key, pam_auth_url, pam_query_url, pam_engine_url, pam_namespace, pam_duration, pam_use_ssl, pam_verify_ssl, hashicorp_vault_type

type"snmp": communityString

type"windows": authType, username, password, domain, kdc_ip, kdc_port, kdc_protocol, vault_host, vault_port, vault_username, vault_password, vault_cyberark_url, vault_safe, vault_app_id, vault_folder, vault_use_ssl, vault_verify_ssl, thycotic_secret_name, thycotic_url, vault_account_name, vault_cyberark_client_cert, vault_cyberark_private_key, vault_cyberark_private_key_passphrase, thycotic_username, thycotic_password, thycotic_organization,

thycotic_domain, thycotic_ssl_verify, lieberman_host, lieberman_port, lieberman_pam_user, lieberman_pam_password, lieberman_use_ssl, lieberman_verify_ssl, beyondtrust_host, beyondtrust_port, beyondtrust_api_key, beyondtrust_duration, beyondtrust_use_ssl, beyondtrust_verify_ssl, beyondtrust_api_user, hashicorp_host, hashicorp_port,hashicorp_authentication_type,hashicorp_role_id,hashicorp_role_secret_id, hashicorp_client_cert, hashicorp_private_key, hashicorp_private_key_passphrase, hashicorp_auth_url,hashicorp_namespace, hashicorp_kv_url, hashicorp_username_source,hashicorp_userkey,hashicorp_passkey,hashicorp_secret,hashicorp_use_ssl,hashicorp_verify_ssl, pam_host, pam_port, pam_api_user, pam_api_key, pam_auth_url, pam_query_url, pam_engine_url, pam_namespace, pam_duration, pam_use_ssl, pam_verify_ssl, hashicorp_vault_type

type"apiGateway": authType**,** datapower_client_cert, datapower_private_key, datapower_private_key_passphrase, datapower_enable_hashicorp, datapower_custom_header_key, datapower_custom_header_value

Allowed Fields

*id
*uuid

Allowed Fields

*id
**name
**description
**type
creator
groups
target
typeFields
tags
createdTime
modifiedTime
canUse
canManage

Session user role not "1" (Administrator)

owner
ownerGroup
targetGroup

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

redFont = *field is a JSON object (* ***e.g.*** *"repository" :{ "id" : <id>, "name" : <name> })*

Request Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
        "response" : {
                "id" : "1000009",
                "type" : "database",
                "name" : "'database' Test PATCH",192.168.1.14
                "description" : "Manually inputted in data for use in testing'
                "tags" : "",
                "createdTime" : "1433187223",
                "modifiedTime" : "1433265608",
                "typeFields" : {
                        "login" : "test",
                        "password" : "SET",
                        "sid" : "",
                        "port" : "49",
                        "dbType" : "Oracle",
                        "oracleAuthType" : "test",
                        "SQLServerAuthType" : ""                },
```

```
                "groups" : [],
                "canUse" : "true",
                "canManage" : "true",
                "creator" : {
                        "id" : "1",
                        "username" : "head",
                        "firstname" : "Security Manager",
                        "lastname" : "",
                         "uuid" : "48F26F3B-6A79-4153-96DB-4C63D1BF3D46"
                },
                "owner" : {
                        "id" : "1",
                        "username" : "head",
                        "firstname" : "Security Manager",
                        "lastname" : "",
                         "uuid" : "48F26F3B-6A79-4153-96DB-4C63D1BF3D46"
                },
                "ownerGroup" : {
                        "id" : "0",
                        "name" : "Full Access",
                        "description" : "Full Access group"            },
                "targetGroup" : {
                        "id" : -1,
                        "name" : "",
                        "description" : ""              },
                "uuid : "701246AF-956F-4185-A514-62F7959B031E"  },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1433279057
}
```


PATCH

Edits the Credential associated with {id} or {uuid}, changing only the passed in fields.

Request Parameters

Note #1: A Credential's 'type' parameter may not be modified, but 'authType' may be modified.

Note #2: When a Credential's authType, dbType, or privilegeEscalation parameters are modified, the parameters **that no longer apply** will be cleared by default.

> Parameters that still may apply, however, are maintained by default. Either may be passed to override default, though fields that no longer apply would give an error.
>
> i.e. If privilegeEscalation is modified from 'su' to 'cisco', the 'escalationPassword' parameter applies and will be maintained. The escalationUsername and escalationPath parameters no longer apply, however, and will be cleared.

Note #3: When a password field is saved, the response will be a string "SET". During PATCH, however, "SET" **should not** be passed back, or it will be considered to be the new password.

(All fields are optional)

See /credential::POST for parameters.

Example Response

See /credential/{id}::GET and /credential/{uuid}::GET.

DELETE

Deletes the Credential associated with {id} or {uuid}, depending on access and permissions.

Request Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
        "response" : "",
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
```

```
        "timestamp" : 1408723358
}
```

/credential/{id}/share

/credential/{uuid}/share

Methods

POST

Shares the Credential associated with {id} or {uuid}, depending on access and permissions.

Note: Admin users cannot share credentials. Application credentials cannot be shared.

Request Parameters

Expand

```
{
        "groups" : [
                {
                        "id" : <number>          }...
        ]
}
```

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "id" : "1000002",
                "creatorID" : "1",
                "ownerID" : "1",
                "type" : "kerberos",
```

```
"name" : "test",
"description" : "",
"tags" : "",
"createdTime" : "1407871560",
"modifiedTime" : "1407871560",
"ownerGID" : "0",
"targetGID" : "-1",
"ip" : "192.168.1.1",
"port" : "1",
"protocol" : "stuff",
"realm" : "stuff",
"canUse" : "true",
"canManage" : "true",
"creator" : {
        "id" : "1",
        "username" : "head",
        "firstname" : "Security Manager",
        "lastname" : "",
         "uuid" : "48F26F3B-6A79-4153-96DB-4C63D1BF3D46"
},
"owner" : {
        "id" : "1",
        "username" : "head",
        "firstname" : "Security Manager",
        "lastname" : "",
         "uuid" : "48F26F3B-6A79-4153-96DB-4C63D1BF3D46"
},
"ownerGroup" : {
        "id" : "0",
        "name" : "Full Access",
        "description" : "Full Access group"            },
"targetGroup" : {
        "id" : -1,
```

```
                        "name" : "",
                        "description" : ""              },
                "uuid" : "E58A2208-2776-4200-B6E5-A844AC26E338" },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1409082841
}
```


/credential/tag

Methods

GET

Gets the full list of unique Credential tags

Note: Organization user responses will contain both organization and admin policy tags. Admin user responses will contain only admin policy tags.

Request Parameters

none

Example Response

Expand


```
{
        "type" : "regular",
        "response" : [
                "Tag1",
                "Tag2",
                "Tag3"  ],
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
```

```
        "timestamp" : 1461093219
}
```

Atlassian

Tenable Security Center API: Current Organization

/currentOrganization

/tes/currentOrganization

/tes/currentOrganization is only available in Tenable Enclave Security

Methods

GET

Gets the organization of the session user.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

**name

Session User not role '1' (Administrator)

****ipInfoLinks**

**zoneSelection

****zones**

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

***redFont =** field is a JSON object (**e.g.** "repository" :{ "id" : <id>, "name" : <name> })*

Request Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
        "response" : {
                "name" : "Org3",
                "zoneSelection" : "auto_only",
                "ipInfoLinks" : [
                        {
                                "name" : "SANS",
                                "link" : "https:\/\/isc.sans.edu\/ipinfo.html
                        },
                        {
                                "name" : "ARIN",
                                "link" : "http:\/\/whois.arin.net\/rest\/ip\/
                        }
                ],
                "zones" : []
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1408974135
}
```


Atlassian

Tenable Security Center API: Current User

/currentUser

Methods

GET

Gets the Current User.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

NOTE: The 'userPrefs' field duplicates the 'preferences' field.

Allowed Fields

*id
*uuid
**username
**firstname
**lastname
**status
role
title
email
address
city
state
country
phone
fax
createdTime
modifiedTime
lastLogin
lastLoginIP
mustChangePassword
passwordExpires

passwordExpiration
passwordExpirationOverride
passwordSetDate
locked
failedLogins
authType
fingerprint
password
description
managedUsersGroups
managedObjectsGroups
userPrefs
preferences
organization
ldapUsername
ldap
orgName
switchableUsers
linkedUserRole

Session user is not role "1" (Administrator)

responsibleAsset
group

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

redFont = *field is a JSON object (* ***e.g.*** *"repository" :{ "id" : <id>, "name" : <name> })*

Request User Parameters

None

Example Response

Administrator

Expand


```
{
        "type" : "regular",
        "response" : {
                "id" : "1",
                "status" : "0",
                "username" : "admin",
                "ldapUsername" : "",
                "firstname" : "Admin",
                "lastname" : "User",
                "title" : "Application Administrator",
                "email" : "",
                "address" : "",
                "city" : "",
                "state" : "",
                "country" : "",
                "phone" : "",
                "fax" : "",
                "createdTime" : "1432921843",
                "modifiedTime" : "1453473716",
                "lastLogin" : "1454350174",
                "lastLoginIP" : "172.168.0.0",
                "mustChangePassword" : "false",
         "passwordExpires": "true",
         "passwordExpiration": "90",
                "passwordExpirationOverride": "false",
                "locked" : "false",
                "failedLogins" : "0",
                "authType" : "tns",
                "fingerprint" : null,
                "password" : "SET",
                "managedUsersGroups" : [],
                "managedObjectsGroups" : [],
```

```
                "preferences" : [
                        {
                                "name" : "timezone",
                                "value" : "America/New_York",
                                "tag" : ""                      }
                ],
                "organization" : {
                        "id" : 0,
                        "name" : "Tenable.sc Administration",
                        "description" : ""              },
                "userPrefs" : [
                        {
                                "name" : "timezone",
                                "value" : "America/New_York",
                                "tag" : ""                      }
                ],
                "role" : {
                        "id" : "1",
                        "name" : "Administrator",
                        "description" : "Role defining an administrator of the
application"            },
                "group" : {
                        "id" : -1,
                        "name" : "",
                        "description" : ""              },
                "ldap" : {
                        "id" : -1,
                        "name" : "",
                        "description" : ""              },
                "orgName" : "Tenable.sc Administration",
                "switchableUsers" : [
                        {
                                "user" {
```

```
                                        "id" : "2",
                                        "username" : "head",
                                        "firstname" : "John",
                                        "lastname" : "Doe",
                                        "locked" : "false",
                                        "uuid" : "96F2AD1B-1B83-462E-908A-84E
                                "organization" : {
                                        "id" : "1",
                                        "name" : "Organization 1",
                                        "description" : "",
                                        "uuid" : "4F7DD1CD-EB1B-40D7-BCE1-2DB
                        }, ...
                ],
                "linkedUserRole" : {
                "id": "11",
                "name": "SM-Linked",
                "description": "Role description"       },
                "uuid" : "4F7DD1CD-EB1B-40D7-BCE1-2DB3E31F6F4C" },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1454350604
}
```


Organization User

Note: If the Current User is a linked user / Non-Admin linked user, the response includes a list of the users that can be switched to including the parent Administrator / Specific organization.

Expand


```
{
        "type" : "regular",
        "response" : {
                "id" : "2",
```

```
            "status" : "0",
            "username" : "head",
            "firstname" : "",
            "lastname" : "",
            "title" : "",
            "email" : "",
            "address" : "",
            "city" : "",
            "state" : "",
            "country" : "",
            "phone" : "",
            "fax" : "",
            "createdTime" : "1433519288",
            "modifiedTime" : "1453477493",
            "lastLogin" : "1454349916",
            "lastLoginIP" : "172.20.0.0",
            "mustChangePassword" : "false",
      "passwordExpires": "true",
      "passwordExpiration": "90",
            "passwordExpirationOverride": "false",
            "locked" : "false",
            "failedLogins" : "0",
            "authType" : "tns",
            "fingerprint" : null,
            "password" : "SET",
            "managedUsersGroups" : [
                  {
                        "id" : "-1",
                        "name" : "All Groups",
                        "description" : "All Groups"
            ],
            "managedObjectsGroups" : [
                  {
```

```
                        "id" : "-1",
                        "name" : "All Groups",
                        "description" : "All Groups"
                ],
                "preferences" : [
                        {
                                "name" : "timezone",
                                "value" : "America/Nome",
                                "tag" : "system"                        }
                ],
                "organization" : {
                        "id" : 1,
                        "name" : "org1",
                        "description" : "",
                        "uuid" : "4F7DD1CD-EB1B-40D7-BCE1-2DB3E31F6F4C"
                "userPrefs" : [
                        {
                                "name" : "timezone",
                                "value" : "America/Nome",
                                "tag" : "system"                        }
                ],
                "role" : {
                        "id" : "2",
                        "name" : "Security Manager",
                        "description" : "The Security Manager role has full ac
actions at the organization level. A Security Manager has the
ability to create new groups and manage existing ones. A Security
Manager can also define how users interact with other groups.\n\nThe
ability to manage other users and their objects can be configured
using group permissions on the Access tab of User add/edit. This
includes viewing and stopping running scans and reports."               },
                "responsibleAsset" : {
                        "id" : "19",
```

```
                        "name" : "Windows Hosts",
                        "description" : "The operating system detected has Wi
installed.\n\nThis will be helpful for those getting started with
Tenable.sc."            },
                "group" : {
                        "id" : "0",
                        "name" : "Full Access",
                        "description" : "Full Access group"            },
                "orgName" : "org",
                "switchableUsers" : [
                        {
                                "user" : {
                                        "id" : "1",
                                        "username" : "admin",
                                        "firstname" : "Jane",
                                        "lastname" : "Doe",
                                        "locked" : "false",
                                        "uuid" : "18C16668-F942-407D-B7E0-4EE
                                "organization" : {
                                        "id" : "0",
                                        "name" : "Tenable.sc Administration",
                                        "description" : ""
                        }, ...
                ],
                "linkedUserRole" : {
                "id": "11",
                "name": "SM-Linked",
                "description": "Role description"       },
                "uuid" : "4F7DD1CD-EB1B-40D7-BCE1-2DB3E31F6F4C" },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1454350550
```

```
}
```

PATCH

Edits the current User, changing only the passed in fields.

Request Parameters

Expand

(All fields are optional)

```
{
       "firstname" : <string> DEFAULT "",
       "lastname" : <string> DEFAULT "",
       "title" : <string> DEFAULT "",
       "email" : <string> DEFAULT "" (required to be present and valid if
emailNotice is not empty and is not "none"),
       "address" : <string> DEFAULT "",
       "city" : <string> DEFAULT "",
       "state" : <string> DEFAULT "",
       "country" : <string> DEFAULT "",
       "phone" : <string> DEFAULT "",
       "fax" : <string> DEFAULT "",
       "fingerprint" : <string> DEFAULT null,
       "emailNotice" :  <string> "both" | "id" | "none" | "password"
DEFAULT "",
       "password" : <string> (must meet the requirements for configuration
setting, "PasswordMinLength"),
       "preferences" : [
              {
                     "name" : <string>,
                     "tag" : <string> DEFAULT "",
                     "value" : <string>              }...
       ]
}
```

Example Response

See /currentUser::GET

/currentUser/associateCert

Methods

POST

Associates a certificate that was presented to the server with the user's account, allowing for auto-login.

Note: When askAboutCert="true", then the F/E would allow you to save fingerprint.

Note: Certificates cannot be associated with linked users.

Request Parameters

Active Certificate (CAT Card, etc).

Example Response

See /currentUser::GET

/currentUser/preferences

Methods

GET

Gets the Current User's preferences specified by parameters 'name' and/or 'tag'. If neither name nor tag is provided, this gets all of the Current User's preferences.

NOTE: This functionality may also be performed in /currentUser::GET with the field 'preferences'

Request Parameters

Expand

Parameters must be passed in as query string (as opposed to JSON) in the format of: /currentUser/preferences?name=foo&tag=foo

```
{
        "name" : <string> OPTIONAL,
```

```
        "tag" : <string> OPTIONAL
}
```

Example Response

Expand

```
{
    "type" : "regular",
    "response" : [
        {
            "name" : "timezone",
            "value" : "America\/New_York",
            "tag" : ""        }
    ],
    "error_code" : 0,
    "error_msg" : "",
    "warnings" : [],
    "timestamp" : 1409327492
}
```

DELETE

Deletes the Current User's preferences specified by parameters 'name' and/or 'tag'. If neither name nor tag is provided, this deletes all of the Current User's preferences.

NOTE : This functionality may also be performed in /currentUser::PATCH with the field 'preferences'

Request Parameters

Expand

```
{
        "name" : <string> OPTIONAL,
        "tag" : <string> OPTIONAL
}
```

Example Response

Expand

```
{
    "type" : "regular",
    "response" : "",
    "error_code" : 0,
    "error_msg" : "",
    "warnings" : [],
    "timestamp" : 1410976021
}
```

PATCH

Edits or adds the preferences associated with the Current User, changing only the passed in fields.

NOTE #1: If the given preference name/tag combination exists, this will update the value. Otherwise, the preference provided will be added.

NOTE #2 : This functionality may also be performed in /currentUser::PATCH with the field 'preferences'

Request Parameters

Expand

```
{
        "name" : <string>,
        "tag" : <string> DEFAULT "",
```

```
        "value" : <string>}
```

Example Response

Expand

```
{
        "type" : "regular",
        "response" : [
                {
                        "name" : "TestNewPreference",
                        "value" : "test",
                        "tag" : ""              }
        ],
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1410977629
}
```

/currentUser/switch

Methods

POST

Switches from the current user to the specified user.

Note: You can switch

- **from an Administrator to a linked user (an organization user where *authType* = "linked" and *parentID* matches the id of the Administrator)**
- **from a linked user to another linked user with the same parent Administrator**
- **from a linked user back to the parent Administrator**

Request Parameters

Expand

```
{
        "username" : <string>}
```

Example Response

See /currentUser::GET

Atlassian

Tenable Security Center API: Custom Plugins

/customPlugins

GET

Gets the status of custom Plugin uploads.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

****custom**
****customPassive**

Legend

** = always comes back*

*** = comes back if fields list not specified*
redFont = *field is a JSON object (* ***e.g.*** *"repository" :{ "id" : <id>, "name" : <name> })*

Request Parameters

None

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "custom" : {
                        "processing" : "false",
                        "lastProcessed" : "1419284733"          },
                "customPassive" : {
                        "processing" : "false",
                        "lastProcessed" : -1
                }
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1419285119
}
```


/customPlugins/{type}/process

Methods

POST

Processes an uploaded Custom Plugin update file and sends a job to update the Custom Plugin type associated with <type>

NOTE: {type} can be one of "active" or "passive"

Request Parameters

Expand


```
{
        "filename" : <string>}
```


Example Response

Expand

```
{
        "type" : "regular",
        "response" : "",
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1419269719
}
```

Atlassian

Tenable Security Center API: Dashboard Component

/dashboard/{dID}/component

Methods

GET

Gets the Dashboard Components associated with dashboard {dID}.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

**id
*name
*description
*status
tabID
componentID
componentType
column
order
running

lastUpdatedTime
lastCompletedUpdateTime
createdTime
modifiedTime
schedule
definition
data

Legend

** = always comes back*
*** = comes back if fields list not specified on GET all*

redFont = *field is a JSON object (* ***e.g.*** *"repository" :{ "id" : <id>, "name" : <name> })*

Request Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
        "response" : [
                {
                        "id" : "1",
                        "name" : "Dashboard Component",
                        "description" : "test",
                        "tabID" : "1",
                        "componentType" : "table",
                        "column" : "1",
                        "order" : "1",
                        "status" : null,
                        "running" : "false",
                        "lastUpdatedTime" : "",
                        "lastCompletedUpdateTime" : "",
```

```
"createdTime" : "",
"modifiedTime" : "",
"definition" : {
        "allDataSources" : [
                {
                        "id" : "161",
                        "queryID" : "81",
                        "querySourceType" : "cumulativ
                        "querySourceID" : null,
                        "querySourceView" : null,
                        "sortColumn" : "score",
                        "sortDirection" : "desc",
                        "iteratorID" : "-1",
                        "dataID" : "44",
                        "context" : "report",
                        "resultStyle" : "list"
        ],
        "styleID" : "-1",
        "columns" : [
                {
                        "name" : "ip"
                {
                        "name" : "score"
                {
                        "name" : "severityLow"
                {
                        "name" : "severityMedium"
                {
                        "name" : "severityHigh"
                {
                        "name" : "severityCritical"
        ],
        "dataPoints" : "10",
```

```
                                "displayDataPoints" : "10",
                                "dataSource" : {
                                        "id" : "161",
                                        "queryID" : "81",
                                        "querySourceType" : "cumulative",
                                        "querySourceID" : null,
                                        "querySourceView" : null,
                                        "sortColumn" : "score",
                                        "sortDirection" : "desc",
                                        "iteratorID" : "-1",
                                        "dataID" : "44",
                                        "context" : "report",
                                        "resultStyle" : "list"
                        },
                        "schedule" : [],
                        "data" : -1,
                        "queryStatus" : [
                                {
                                        "id" : "1",
                                        "name" : "",
                                        "description" : """,
                                        "status" : "0"
                        ]
                }
        ],
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1414081560
}
```


POST

Adds a Dashboard Component to dashboard {dID}.

NOTE: If a template ID is provided:

- The template associated with the provided ID will be retrieved and used as the default values for the Dashboard Component.
- The template ID provided must be a "component" (not a "collection")
- The 'name' isn't enforced as unique and, therefore, there is no automation for modifying the name field automatically.
- Templates do not specify an order and/or column. These fields are still required.
- For non-matrix components, a schedule must be provided. For matrix components, there are some conversion issues with templates that are currently being discussed.

Request Parameters

Expand

```
{
        "name" : <string>,
        "template" : {
                "id" : <number> } OPTIONAL,
        "description" : <string> DEFAULT "",
        "type" : <string> "barChart" | "stackedBarChart" | pieChart" |
"table" | "areaChart" | "lineChart" | "enhancedAreaChart" |
"enhancedLineChart" | "matrix",
        "column" : <number>,
        "order" : <number>,
        "parentJob" : <number> OPTIONAL,
        ...
}
```

type is "stackedBarChart" | "barChart" | "pieChart" | "table":

NOTE: For information on valid Query object format, see */query::POST*.

```
{
        ...
        "schedule" : {
```

```
                "type" : <string> "dependent" | "ical" | "never" | "rollover"
"template"      },
        "definition" : {
                "columns" : [
                        {
                                "name" : <string>                       }...
                ],
                "labelColumns" : <string>,
                "dataSource" : {
                        "queryID" : <number> OPTIONAL,
                        "querySourceType" : "querySourceType" : "alert" | "lce
"mobile" | "ticket" | "user" | "vuln" (needs verification),
                        "querySourceID" : <number>,
                        "querySourceView" : <string>,
                        "sortColumn" : <string>,
                        "sortDirection" : <string>,
                        "iteratorID" : <number> DEFAULT "-1" (not set)

                        queryID is not provided
                        -----------------------
                        "query" : <query object>                }
        }
        ...
}
```

type is "areaChart" | "lineChart" | "enhancedAreaChart" | "enhancedLineChart"

NOTE: For information on valid Query object format, see */query::POST*.

```
{
        ...
        "schedule" : {
                "type" : <string> "dependent" | "ical" | "never" | "rollover"
"template"      },
```

```
        "definition" : {
                "lines" : [
                        {
                                "dataSource" : {
                                        "queryID" : <number> OPTIONAL
                                                "queryID" : <number> OPTIONAL,
                                                "querySourceType" : "alert" |
"user" | "vuln" (needs verification),
                                                "querySourceID" : <number>,
                                                "querySourceView" : <string>,
                                                "sortColumn" : <string>,
                                                "sortDirection" : <string>,
                                                "iteratorID" : <number> DEFAU

                                        queryID is not provided
                                        ----------------------
                                        "query" : <query object>
                        }...
                ]
        }
        ...
}
```

type is "matrix"

NOTE: For information on valid Query object format, see */query::POST*.

```
{
        ...
        "definition" : {
                "rows" : <number>,
                "columns" : <number>,
                "title" : <string>,
                "stripType" : <string>,
```

```
                "rowLabels" : [
                        {
                                "text" : <string>                       }...
                ],
                "columnLabels" : [
                        {
                                "text" : <string>                       }...
                ],
                "clusters" : [
                        {
                                "schedule" : {
                                        "type" : <string> "dependent" | "ical"
"template"                               },
                                "strips" : <string> (comma separated list of n
columns affected by the new schedule)
                        }...
                ],
                "cells" : [
                        {
                                "conditionals" : [
                                        {
                                                "conditionalName" : <string>,
                                                "conditionalOperator" : <strin
                                                "conditionalValue" : <string>,
                                                "outputType" : <string>,
                                                "outputColors" : <string>,
                                                "outputText" : <string>
                                ],
                                "dataSource" : {
                                        "queryID" : <number> OPTIONAL
                                        "querySourceType" : "alert" | "lce" |
"user" | "vuln" (needs verification),
                                        "querySourceID" : <number>,
```

```
                                        "querySourceView" : <string>,
                                        "sortColumn" : <string>,
                                        "sortDirection" : <string>,
                                        "iteratorID" : <number> DEFAULT "-1"
                                        queryID is not provided
                                        ----------------------
                                        "query" : <query object>
                                "baseDataSource" : {
                                        "queryID" : <number> OPTIONAL
                                        "querySourceType" : "alert" | "lce" |
"user" | "vuln" (needs verification),
                                        "querySourceID" : <number>,
                                        "querySourceView" : <string>,
                                        "sortColumn" : <string>,
                                        "sortDirection" : <string>,
                                        "iteratorID" : <number> DEFAULT "-1"

                                        queryID is not provided
                                        ----------------------
                                        "query" : <query object>
                        }...
                ]
        }
        ...
}
```

Schedule type is "ical"

NOTE: Applies to all types of Components. The schedule object for type matrix is located in the definition clusters. Othwerwise, the object is located in the base component.

```
{
        ...
        "schedule" : {
```

```
                "start" : <string> (This value takes the iCal format),
                "repeatRule" : <string> (This value takes the repeat rule form
        }
        ...
}
```

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "id" : "2",
                "name" : "testPOSTComponent",
                "description" : "",
                "tabID" : "1",
                "componentID" : "13",
                "componentType" : "barChart",
                "column" : "1",
                "order" : "2",
                "status" : "32768",
                "running" : "false",
                "lastUpdatedTime" : "-1",
                "lastCompletedUpdateTime" : "-1",
                "createdTime" : "1414095212",
                "modifiedTime" : "1414095212",
                "definition" : {
                        "styleID" : "-1",
                        "columns" : [
                                {
                                        "name" : "Column Name"
                        ],
                        "labelColumns" : "label",
```

```
                        "dataPoints" : "92233720368547758O7",
                        "dataSource" : {
                                "id" : "232",
                                "queryID" : "1",
                                "querySourceType" : "cumulative",
                                "querySourceID" : null,
                                "querySourceView" : null,
                                "sortColumn" : "id",
                                "sortDirection" : "ASC",
                                "iteratorID" : "-1",
                                "dataID" : "94",
                                "context" : "",
                                "resultStyle" : "list"                  }
                },
                "schedule" : {
                        "type" : "never",
                        "start" : "",
                        "repeatRule" : ""               },
                "data" : -1
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1414095212
}
```


/dashboard/{dID}/component/{cID}

Methods

GET

Gets the Dashboard Component associated with dashboard {dID} and component {cID}.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

**id
*name
*description
*status
tabID
componentID
componentType
column
order
running
lastUpdatedTime
lastCompletedUpdateTime
createdTime
modifiedTime
schedule
definition
data
queryStatus

Legend

** = always comes back*
*** = comes back if fields list not specified on GET all*

redFont = *field is a JSON object (* ***e.g.*** *"repository" :{ "id" : <id>, "name" : <name> })*

Request Parameters

None

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "id" : "1",
                "name" : "Component",
                "description" : "test",
                "tabID" : "1",
                "componentID" : "1",
                "componentType" : "table",
                "column" : "1",
                "order" : "1",
                "status" : "0",
                "running" : "false",
                "lastUpdatedTime" : "1414440714",
                "lastCompletedUpdateTime" : "1414440714",
                "createdTime" : "",
                "modifiedTime" : "",
                "definition" : {
                        "styleID" : "-1",
                        "columns" : [
                                {
                                        "name" : "ip"
                                {
                                        "name" : "score"
                                {
                                        "name" : "severityLow"
                                {
                                        "name" : "severityMedium"
                                {
                                        "name" : "severityHigh"
                                {
                                        "name" : "severityCritical"
                        ],
```

```
                        "dataPoints" : "10",
                        "displayDataPoints" : "10",
                        "dataSource" : {
                                "id" : "161",
                                "queryID" : "81",
                                "querySourceType" : "cumulative",
                                "querySourceID" : null,
                                "querySourceView" : null,
                                "sortColumn" : "score",
                                "sortDirection" : "desc",
                                "iteratorID" : "-1",
                                "dataID" : "44",
                                "context" : "report",
                                "resultStyle" : "list"                  }
                },
                "schedule" : {
                        "id" : -1,
                        "type" : "now",
                        "start" : "",
                        "repeatRule" : "",
                        "nextRun" : -1
                },
                "data" : -1,
                "queryStatus" : [
                        {
                                "id" : "1",
                                "name" : "",
                                "description" : """,
                                "status" : "0"                  }
                ]
        },
        "error_code" : 0,
        "error_msg" : "",
```

```
        "warnings" : [],
        "timestamp" : 1414440824
}
```


PATCH

Edits the Dashboard associated with dashboard {dID} and component {cID}, changing only the passed in fields.

NOTE #1: If no definition parameter is passed, the original definition is maintained. If a definition parameter is passed (***even an empty array***), the old definition is recreated.

NOTE #2: Only users in the same group as the owner (and with proper permissions) can make modifications to a component. Users in another group (with proper permissions), however, can change the order and column.

Request Parameters

(All fields are optional)

See /dashboard/{dID}/component::POST for parameters.

Example Response

See /dashboard/{dID}/component/{cID}::GET

DELETE

Deletes the Dashboard associated with dashboard {dID} and component {cID}, depending on access and permissions

Request Parameters

None

Example Response

Expand

```
{
    "type" : "regular",
    "response" : "",
    "error_code" : 0,
    "error_msg" : "",
    "warnings" : [],
    "timestamp" : 1403100582
}
```

/dashboard/{dID}/component/{cID}/copy

Methods

POST

Refreshes the Dashboard Component associated with dashboard {dID} and component {cID}.

Request Parameters

Expand

```
{
        "name" : <string>,
        "targetTabID" : <number> DEFAULT <tabID>        ...
}
```

(Additional fields are optional)

See /dashboard/{dID}/component::POST for parameters.

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
```

```
                "id" : "45",
                "name" : "Test 11\/10 12",
                "description" : "This component provides a list of infected ho
that have been identified with plugin 74442.  The systems identified
in this table are most likely compromised and should be immediately
removed from the network.  The next step would be to follow an
incident response policy and determine if an incident needs to be
declared.  Additionally, a forensic analysis should be considered to
determine the extent of the compromise.  The table uses the IP
Summary tool and is sorted based on repository, and displays the IP
Address, NetBIOS Name, FQDN, and OS CPE string.",
                "tabID" : "47",
                "componentID" : "449",
                "componentType" : "table",
                "column" : "1",
                "order" : "2",
                "status" : "32768",
                "running" : "false",
                "lastUpdatedTime" : "-1",
                "lastCompletedUpdateTime" : "-1",
                "createdTime" : "1415635146",
                "modifiedTime" : "1415635146",
                "definition" : {
                        "allDataSources" : [
                                {
                                        "id" : "888",
                                        "queryID" : "541",
                                        "querySourceType" : "cumulative",
                                        "querySourceID" : null,
                                        "querySourceView" : null,
                                        "sortColumn" : "ip",
                                        "sortDirection" : "desc",
                                        "iteratorID" : "-1",
```

```
                                "dataID" : "676",
                                "context" : "dashboard",
                                "resultStyle" : "list"
                        ],
                        "styleID" : "-1",
                        "columns" : [
                                {
                                        "name" : "ip"
                                {
                                        "name" : "netbiosName"
                                {
                                        "name" : "dnsName"
                                {
                                        "name" : "osCPE"
                        ],
                        "dataPoints" : "100",
                        "displayDataPoints" : "8",
                        "dataSource" : {
                                "id" : "888",
                                "queryID" : "541",
                                "querySourceType" : "cumulative",
                                "querySourceID" : null,
                                "querySourceView" : null,
                                "sortColumn" : "ip",
                                "sortDirection" : "desc",
                                "iteratorID" : "-1",
                                "dataID" : "676",
                                "context" : "dashboard",
                                "resultStyle" : "list"                  }
                },
                "schedule" : {
                        "id" : "164",
                        "type" : "ical",
```

```
                        "start" : "TZID=America\/New_York : 20140815T140000",
                        "repeatRule" : "FREQ=WEEKLY;INTERVAL=1;BYDAY=SU,SA",
                        "nextRun" : 1416078000
                },
                "data" : -1
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1415635146
}
```


/dashboard/{dID}/component/{cID}/refresh

Methods

POST

Refreshes the Dashboard Component associated with dashboard {dID} and component {cID}.

Request Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
        "response" : {
                "id" : "1",
                "name" : "Component",
                "description" : "test",
                "tabID" : "1",
                "componentID" : "1",
                "componentType" : "table",
```

```
"column" : "1",
"order" : "1",
"status" : "0",
"running" : "false",
"lastUpdatedTime" : "1414440714",
"lastCompletedUpdateTime" : "1414440714",
"createdTime" : "",
"modifiedTime" : "",
"definition" : {
        "styleID" : "-1",
        "columns" : [
                {
                        "name" : "ip"
                {
                        "name" : "score"
                {
                        "name" : "severityLow"
                {
                        "name" : "severityMedium"
                {
                        "name" : "severityHigh"
                {
                        "name" : "severityCritical"
        ],
        "dataPoints" : "10",
        "displayDataPoints" : "10",
        "dataSource" : {
                "id" : "161",
                "queryID" : "81",
                "querySourceType" : "cumulative",
                "querySourceID" : null,
                "querySourceView" : null,
                "sortColumn" : "score",
```

```
                                "sortDirection" : "desc",
                                "iteratorID" : "-1",
                                "dataID" : "44",
                                "context" : "report",
                                "resultStyle" : "list"                  }
                },
                "schedule" : {
                        "id" : -1,
                        "type" : "now",
                        "start" : "",
                        "repeatRule" : "",
                        "nextRun" : -1
                },
                "data" : -1
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1414440824
}
```


Atlassian

Tenable Security Center API: Dashboard Tab

/dashboard

Methods

GET

Gets the list of Dashboards

NOTE: If the Session User is an Admin, the response will be faked Dashboards.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

id*
name**
description**
owner
ownerGroup
targetGroup
groups
numColumns
columnWidths
defaultTemplateNumber
createdTime
modifiedTime
dashboardComponents
failedComponentCount
activated
order
canUse
canManage

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*
redFont = *field is a JSON object (* ***e.g.*** *"repository" :{ "id" : <id>, "name" : <name> })*

Request Parameters

None

Expand Parameters

dashboardComponents

Filter Parameters

activated - the response returns an 'usable' object containing an array of objects with only activated Dashboard Tabs for the session user. This is not compatible with usable and/or manageable filters.
usable - The response will be an object containing an array of usable Dashboards. By default, both usable and manageable objects are returned.
manageable - The response will be an object containing all manageable Dashboards. By default, both usable and manageable objects are returned.

Example Response

Expand


```
{
	"type" : "regular",
	"response" : {
		"usable" : [
			{
				"id" : "1",
				"name" : "Vulnerability Overview",
				"description" : "Vulnerability Overview tab"
			{
				"id" : "2",
				"name" : "Executive 7 Day",
				"description" : "This dashboard provides an ex
a weekly status of the current vulnerability management program.  A
series of tables, charts and graphs provide a detailed view into the
vulnerabilities discovered and mitigated within the last 7
days.\n\nThe dashboard is comprised of 18 components that provide an
overview analysis of a vulnerability management program that is easy
to understand by managers, CISO's and other executives.  \n\nThe
first set of tables show a detailed ratio of vulnerabilities to the
risk of exploitation, and if the vulnerability has been mitigated or
not.  The tables are followed by series of pie charts, which
summarize the severities and risk of exploitation.\n \nThe next two
rows provide a trend analysis of the vulnerabilities by severity and
plugin type.  Both sets of trend data are calculated every day over
```

```
the past 7 days.  The data points are designed to show the daily
changes, allowing for detection of unusual activity.  In the third
column are the trend graphs showing the vulnerabilities that have
returned after they have been previously mitigated. \n\nThe
remaining components show an analysis of assets, and the
vulnerabilities with top 10 most vulnerable assets.  Using a bar
chart and table, a high level summary is depicted."                    },
                        {
                                "id" : "3",
                                "name" : "Executive Summary",
                                "description" : "Using a series of charts, tab
this overview dashboard provides a summary for an executive to gain
a high level understanding of the vulnerability management status of
the network environment.  This dashboard contains valuable
information, including Top 10 Summaries of Assets, Networks and
Systems that are vulnerable, as well as useful trend information on
vulnerabilities and how long they have existed within the network
environment."                    },
                        {
                                "id" : "4",
                                "name" : "Vulnerability Overview",
                                "description" : "Vulnerability Overview"
                        {
                                "id" : "5",
                                "name" : "Vulnerability Overview",
                                "description" : "Vulnerability Overview tab"
                        {
                                "id" : "6",
                                "name" : "Executive 7 Day",
                                "description" : "This dashboard provides an ex
a weekly status of the current vulnerability management program.  A
series of tables, charts and graphs provide a detailed view into the
vulnerabilities discovered and mitigated within the last 7
```

days.\n\nThe dashboard is comprised of 18 components that provide an overview analysis of a vulnerability management program that is easy to understand by managers, CISO's and other executives. \n\nThe first set of tables show a detailed ratio of vulnerabilities to the risk of exploitation, and if the vulnerability has been mitigated or not. The tables are followed by series of pie charts, which summarize the severities and risk of exploitation.\n \nThe next two rows provide a trend analysis of the vulnerabilities by severity and plugin type. Both sets of trend data are calculated every day over the past 7 days. The data points are designed to show the daily changes, allowing for detection of unusual activity. In the third column are the trend graphs showing the vulnerabilities that have returned after they have been previously mitigated. \n\nThe remaining components show an analysis of assets, and the vulnerabilities with top 10 most vulnerable assets. Using a bar chart and table, a high level summary is depicted." },
{
"id" : "7",
"name" : "Executive Summary",
"description" : "Using a series of charts, tab
this overview dashboard provides a summary for an executive to gain a high level understanding of the vulnerability management status of the network environment. This dashboard contains valuable information, including Top 10 Summaries of Assets, Networks and Systems that are vulnerable, as well as useful trend information on vulnerabilities and how long they have existed within the network environment." },
{
"id" : "8",
"name" : "Vulnerability Overview",
"description" : "Vulnerability Overview"
{
"id" : "9",

```
                                "name" : "Vulnerability Overview",
                                "description" : "Vulnerability Overview tab"
                        {
                                "id" : "10",
                                "name" : "Executive 7 Day",
                                "description" : "This dashboard provides an ex
a weekly status of the current vulnerability management program.  A
series of tables, charts and graphs provide a detailed view into the
vulnerabilities discovered and mitigated within the last 7
days.\n\nThe dashboard is comprised of 18 components that provide an
overview analysis of a vulnerability management program that is easy
to understand by managers, CISO's and other executives.  \n\nThe
first set of tables show a detailed ratio of vulnerabilities to the
risk of exploitation, and if the vulnerability has been mitigated or
not.  The tables are followed by series of pie charts, which
summarize the severities and risk of exploitation.\n \nThe next two
rows provide a trend analysis of the vulnerabilities by severity and
plugin type.  Both sets of trend data are calculated every day over
the past 7 days.  The data points are designed to show the daily
changes, allowing for detection of unusual activity.  In the third
column are the trend graphs showing the vulnerabilities that have
returned after they have been previously mitigated. \n\nThe
remaining components show an analysis of assets, and the
vulnerabilities with top 10 most vulnerable assets.  Using a bar
chart and table, a high level summary is depicted."                    },
                        {
                                "id" : "11",
                                "name" : "Executive Summary",
                                "description" : "Using a series of charts, tab
this overview dashboard provides a summary for an executive to gain
a high level understanding of the vulnerability management status of
the network environment.  This dashboard contains valuable
information, including Top 10 Summaries of Assets, Networks and
```

```
Systems that are vulnerable, as well as useful trend information on
vulnerabilities and how long they have existed within the network
environment."                    },
                        {
                                "id" : "12",
                                "name" : "Vulnerability Overview",
                                "description" : "Vulnerability Overview"
                ],
                "manageable" : [
                        {
                                "id" : "1",
                                "name" : "Vulnerability Overview",
                                "description" : "Vulnerability Overview tab"
                        {
                                "id" : "2",
                                "name" : "Executive 7 Day",
                                "description" : "This dashboard provides an ex
a weekly status of the current vulnerability management program.  A
series of tables, charts and graphs provide a detailed view into the
vulnerabilities discovered and mitigated within the last 7
days.\n\nThe dashboard is comprised of 18 components that provide an
overview analysis of a vulnerability management program that is easy
to understand by managers, CISO's and other executives.  \n\nThe
first set of tables show a detailed ratio of vulnerabilities to the
risk of exploitation, and if the vulnerability has been mitigated or
not.  The tables are followed by series of pie charts, which
summarize the severities and risk of exploitation.\n \nThe next two
rows provide a trend analysis of the vulnerabilities by severity and
plugin type.  Both sets of trend data are calculated every day over
the past 7 days.  The data points are designed to show the daily
changes, allowing for detection of unusual activity.  In the third
column are the trend graphs showing the vulnerabilities that have
returned after they have been previously mitigated. \n\nThe
```

```
remaining components show an analysis of assets, and the
vulnerabilities with top 10 most vulnerable assets.  Using a bar
chart and table, a high level summary is depicted."                    },
                        {
                                "id" : "3",
                                "name" : "Executive Summary",
                                "description" : "Using a series of charts, tab
this overview dashboard provides a summary for an executive to gain
a high level understanding of the vulnerability management status of
the network environment.  This dashboard contains valuable
information, including Top 10 Summaries of Assets, Networks and
Systems that are vulnerable, as well as useful trend information on
vulnerabilities and how long they have existed within the network
environment."                    },
                        {
                                "id" : "4",
                                "name" : "Vulnerability Overview",
                                "description" : "Vulnerability Overview"
                ]
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1414177712
}
```


POST

Adds a Dashboard

Request Parameters

Expand

NOTE #1: The number of columnWidth objects must match the numColumns parameter.
NOTE #2: To activate or change the order, both activated="true' and the order parameters must be

provided.

```
{
        "name" : <string>,
        "description" : <string> DEFAULT "",
        "numColumns": <number> DEFAULT "1",
        "order" : <number> OPTIONAL,
        "activated" : <string> "false" | "true" OPTIONAL,
        "columnWidths" : [
                <numbers> (separated by commas)
        ] DEFAULT []
}
```

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "id" : "42",
                "name" : "testPOST2",
                "description" : "test of a POST",
                "numColumns" : "3",
                "columnWidths" : [
                        "1",
                        "2",
                        "3"             ],
                "defaultTemplateNumber" : "-1",
                "createdTime" : "1414185335",
                "modifiedTime" : "1414185335",
                "order" : "6",
                "activated" : "true",
                "dashboardComponents" : [],
                "groups" : [],
```

```
                "failedComponentCount" : "0",
                "canUse" : "true",
                "canManage" : "true",
                "owner" : {
                        "id" : "1",
                        "username" : "head",
                        "firstname" : "Security Manager",
                        "lastname" : "",
                        "uuid" : "4F7DD1CD-EB1B-40D7-BCE1-2DB3E31F6F4C"
                "ownerGroup" : {
                        "id" : "0",
                        "name" : "Full Access",
                        "description" : "Full Access group"             },
                "targetGroup" : {
                        "id" : -1,
                        "name" : "",
                        "description" : ""              }
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1414185335
}
```


/dashboard/{id}

Methods

GET

Gets the Dashboard associated with {id}.

NOTE: If the Session User is an Admin, the response will be a faked Dashboard.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

id*
name**
description**
owner
ownerGroup
targetGroup
groups
numColumns
columnWidths
defaultTemplateNumber
createdTime
modifiedTime
dashboardComponents
failedComponentCount
activated
order
canUse
canManage

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*
redFont = *field is a JSON object (* ***e.g.*** *"repository" :{ "id" : <id>, "name" : <name> })*

Request Parameters

None

Expand Parameters

dashboardComponents

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "id" : "1",
                "name" : "Vulnerability Overview",
                "description" : "Vulnerability Overview tab",
                "numColumns" : "2",
                "columnWidths" : [
                        "34","66"               ],
                "defaultTemplateNumber" : "-1",
                "createdTime" : "1406321532",
                "modifiedTime" : "1406321532",
                "order" : "1",
                "activated" : "true",
                "dashboardComponents" : [
                        {
                                "id" : "1",
                                "name" : "fakedDataTemplate",
                                "description" : "this was faked data"
                        {
                                "id" : "2",
                                "name" : "testPATCH 7",
                                "description" : ""                      },
                        {
                                "id" : "3",
                                "name" : "testPATCH 2",
                                "description" : ""                      }
                ],
                "groups" : [],
                "failedComponentCount" : "0",
                "canUse" : "true",
                "canManage" : "true",
                "owner" : {
```

```
                        "id" : "1",
                        "username" : "head",
                        "firstname" : "Security Manager",
                        "lastname" : "",
                        "uuid" : "4F7DD1CD-EB1B-40D7-BCE1-2DB3E31F6F4C"
                "ownerGroup" : {
                        "id" : "0",
                        "name" : "Full Access",
                        "description" : "Full Access group"             },
                "targetGroup" : {
                        "id" : -1,
                        "name" : "",
                        "description" : ""              }
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1414177737
}
```


PATCH

Edits the Dashboard associated with {id}, changing only the passed in fields.

NOTE #1: This is for patching the Dashboard tab, not the contained components.

NOTE #2: To activate, both activated="true" and the order parameter must be provided. To deactivate, only the activated="false" parameter (not the order) should be provided.

Request Parameters

(All fields are optional)

See /dashboard::POST for parameters.

Example Response

See /dashboard/{id}::GET

DELETE

Deletes the Dashboard associated with {id}, depending on access and permissions.

Request Parameters

Expand

NOTE #1: The number of columnWidth objects must match the numColumns parameter.

```
{
        "name" : <string>,
        "description" : <string> DEFAULT <original tab>,
        "numColumns": <number> DEFAULT <original tab>,
        "columnWidths" : [
                <numbers> (separated by commas)
        ]  DEFAULT <original tab>,
        "activated" : <string> "false" | "true" OPTIONAL,

        activated "true"        ----------------
        "order" : <number>}
```

Example Response

Expand

```
{
        "type" : "regular",
        "response" : "",
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1414444607
}
```

/dashboard/{id}/copy

Methods

POST

Copies the Dashboard associated with {id}.

Request Parameters

Expand

NOTE: all other parameters optional. See /dashboard::POST for parameters.

```
{
        "name" : <string>}
```

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "id" : "48",
                "name" : "testTabCopy",
                "description" : "Freshly Posted Dashboard with no Faked Compon
- order 1",
                "numColumns" : "1",
                "columnWidths" : [
                        "100"           ],
                "defaultTemplateNumber" : "-1",
                "createdTime" : "1415051442",
                "modifiedTime" : "1415051442",
                "order" : null,
                "activated" : "false",
                "dashboardComponents" : [
                        {
                                "id" : "15",
                                "name" : "DNS Error Indicator 2",
                                "description" : "This DNS indicator component
specific events such as :  DNS Servers participating in a known
botnet,
                                 URLs on part of a known botnet,
```

```
                                If DNS traffic is found on ports other than 5
                                If there have been more than 30 minutes of co
errors,
                                detected anomolies in DNS traffic or monitori
Active Directory,
                                and any found known exploits of DNS."
                        {
                                "id" : "16",
                                "name" : "Threat Intelligence - Microsoft Wind
AutoRuns and Scheduled Tasks",
                                "description" : "This component provides a lis
hosts that have been identified with plugin 74442.  The systems
identified in this table are most likely compromised and should be
immediately removed from the network.  The next step would be to
follow an incident response policy and determine if an incident
needs to be declared.  Additionally,
                                a forensic analysis should be considered to d
extent of the compromise.  The table uses the IP Summary tool and is
sorted based on repository,
                                and displays the IP Address,
                                NetBIOS Name,
                                FQDN,
                                and OS CPE string."                     }
                ],
                "groups" : [],
                "failedComponentCount" : "0",
                "canUse" : "true",
                "canManage" : "true",
                "owner" : {
                        "id" : "1",
                        "username" : "head",
                        "firstname" : "Security Manager",
                        "lastname" : "",
```

```
                        "uuid" : "4F7DD1CD-EB1B-40D7-BCE1-2DB3E31F6F4C"
                "ownerGroup" : {
                        "id" : "0",
                        "name" : "Full Access",
                        "description" : "Full Access group"             },
                "targetGroup" : {
                        "id" : -1,
                        "name" : "",
                        "description" : ""              }
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1415051442
}
```


/dashboard/import

Methods

POST

Imports a Dashboard

Request Parameters

Expand

```
{
        "name" : <string> OPTIONAL,
        "order" : <number>,
        "filename" : <string>}
```

Example Response

Expand

```
{
    "type" : "regular",
    "response" : {
        "id" : "74",
        "name" : "ARC Name",
        "description" : "",
        "lastUpdateTime" : "-1",
        "lastCompletedUpdateTime" : "-1",
        "lastComplianceUpdateTime" : "-1",
        "createdTime" : "1416430201",
        "modifiedTime" : "1416430201",
        "focusFilters" : [],
        "order" : "1",
        "activated" : "true",
        "groups":[],
        "policyStatements" : [
            {
                "id" : "289",
                "arcID" : "74",
                "label" : "All systems should have a DNS entry",
                "baseFilters":[],
                "compliantFilters" : [
                    {
                        "filterName" : "asset",
                        "operator" : "=",
                        "value" : {
                            "template" : {
                                "id" : "222",
                                "name" : "Scanned Hosts Not in DNS",
                                "description" : ""
        }
                        }
                    }
```

```
                ],
                "drilldownFilters" : [
                    {
                        "filterName" : "asset",
                        "operator" : "~",
                        "value": {
                            "operator" : "complement",
                            "operand1" : {
                                "template" : {
                                    "id" : "222",
                                    "name" : "Scanned Hosts Not in
DNS",
                                    "description" : ""
                 }
                            }
                        }
                    }
                ],
                "baseStatus" : "0",
                "compliantStatus" : "0",
                "drilldownStatus" : "0",
                "conditionalName" : "hosts",
                "conditionalOperator" : "All",
                "conditionalValue" : "",
                "displayType" : "ratio",
                "result" : "",
                "resultOutput" : "{}",
                "queryType" : "vuln",
                "drilldownQuery": {
                    "id" : "1015"               }
            }
        ],
        "result" : "fail",
```

```
        "status" : 0,
        "schedule" : {
            "id" : "134",
            "type" : "ical",
            "start" : "TZID=America\/New_York:20141119T155001",
            "repeatRule" : "FREQ=DAILY;INTERVAL=1",
            "nextRun" : 1416516601
        },
        "canUse" : "true",
        "canManage" : "true",
        "owner" : {
            "id" : "1",
            "username" : "user",
            "firstname" : "user",
            "lastname" : "Security Manager",
                        "uuid" : "4F7DD1CD-EB1B-40D7-BCE1-2DB3E31F6F4C"
        "ownerGroup" : {
            "id" : "0",
            "name" : "Full Access",
            "description" : "Full Access group"        }
    },
    "error_code" : 0,
    "error_msg" : "",
    "warnings" : [],
    "timestamp" : 1416434977
}
```


/dashboard/{id}/export

Methods

POST

Exports the Dashboard associated with {id}.

Request Parameters

Expand

```
{
       "exportType" : <string> ("full"|"cleansed"|"placeholders")
}
```

Example Response

Expand

```
<?xml version="1.0" encoding="UTF-8"?><dashboardTab>
<scVersion>5.0.0</scVersion>    <name>Default</name>
<description>Default dashboard tab</description>
<numColumns>2</numColumns>    <columnWidths>
<column>34</column>        <column>66</column>    </columnWidths>
<dashboardComponents>        <component>
<name>Vulnerability Trending</name>
<description></description>
<componentType>lineChart</componentType>
<type>lineChart</type>            <column>1</column>
<order>1</order>
<schedule>FREQ=DAILY;INTERVAL=1</schedule>
<definition>YTo1OntzOjc6InN0eWxlSUQiO3M6MjoiLTEiO3M6OToic3RhcnRUaW1l-
IjtzOjEwOiIxNDE1OTEzODQyIjtzOjc6ImVuZFRpbWUiO3M6MTA6IjE0MTY1MTg2NDIi-
O3M6OToidGltZUZyYW1lIjtzOjI6IjdkIjtzOjU6ImxpbmVzIjthOjI6e2k6MDthOjQ6-
e3M6NzoiY29sdW1ucyI7YToxOntpOjA7YToxOntzOjQ6Im5hbWUiO3M6NToidG90YWwi-
O319czo3OiJheGlzTnVtIjtzOjE6IjEiO3M6NToibGFiZWwiO3M6MzoiTmV3IjtzOjEw-
OiJkYXRhU291cmNlIjthOjk6e3M6MTU6InF1ZXJ5U291cmNlVHlwZSI7czoxMDoiY3Vt-
dWxhdGl2ZSI7czoxMzoicXVlcnlTb3VyY2VJRCI7TjtzOjE1OiJxdWVyeVNvdXJjZVZp-
ZXciO047czoxMDoic29ydENvbHVtbiI7TjtzOjEzOiJzb3J0RGlyZWN0aW9uIjtOO3M6-
MTA6Iml0ZXJhdG9ySUQiO3M6MjoiLTEiO3M6NzoiY29udGV4dCI7czo5OiJkYXNoYm9h-
cmQiO3M6MTE6InJlc3VsdFN0eWxlIjtzOjU6InRyZW5kIjtzOjU6InF1ZXJ5IjthOjEz-
OntzOjQ6Im5hbWUiO3M6MzI6Il8xMzg5MzA1MzE0LjU4OTRfMF9saW5lQ2hhcnRfMV8y-
IjtzOjExOiJkZXNjcmlwdGlvbiI7TjtzOjQ6InRvb2wiO3M6NToidHJlbmQiO3M6NDoi-
dHlwZSI7czo0OiJ2dWxuIjtzOjQ6InRhZ3MiO3M6MDoiIjtzOjc6ImNvbnRleHQiO3M6-
```

OToiZGFzaGJvYXJkIjtzOjEzOiJicm93c2VDb2x1bW5zIjtzOjA6IiI7czoxNjoiYnJv-
d3NlU29ydENvbHVtbiI7czowOiIiO3M6MTk6ImJyb3dzZVNvcnREaXJlY3Rpb24iO3M6-
MDoiIjtzOjg6Im93bmVyR0lEIjtzOjE6IjAiO3M6OToidGFyZ2V0R0lEIjtzOjI6Ii0x-
IjtzOjc6ImZpbHRlcnMiO2E6MTp7aTowO2E6Mzp7czoxMDoiZmlsdGVyTmFtZSI7czo5-
OiJmaXJzdFNlZW4iO3M6ODoib3BlcmF0b3IiO3M6MToiPSI7czo1OiJ2YWx1ZSI7czoz-
OiIwOjciO319czo2OiJncm91cHMiO2E6MDp7fX19fWk6MTthOjQ6e3M6NzoiY29sdW1u-
cyI7YToxOntpOjA7YToxOntzOjQ6Im5hbWUiO3M6NToidG90YWwiO319czo3OiJheGlz-
TnVtIjtzOjE6IjEiO3M6NToibGFiZWwiO3M6MzoiT2xkIjtzOjEwOiJkYXRhU291cmNl-
IjthOjk6e3M6MTU6InF1ZXJ5U291cmNlVHlwZSI7czoxMDoiY3VtdWxhdGl2ZSI7czox-
MzoicXVlcnlTb3VyY2VJRCI7TjtzOjE1OiJxdWVyeVNvdXJjZVZpZXciO047czoxMDoi-
c29ydENvbHVtbiI7TjtzOjEzOiJzb3J0RGlyZWN0aW9uIjtOO3M6MTA6Iml0ZXJhdG9y-
SUQiO3M6MjoiLTEiO3M6NzoiY29udGV4dCI7czo5OiJkYXNoYm9hcmQiO3M6MTE6InJl-
c3VsdFN0eWxlIjtzOjU6InRyZW5kIjtzOjU6InF1ZXJ5IjthOjEzOntzOjQ6Im5hbWUi-
O3M6MzI6Il8xMzg5MzA1MzE0LjYzMjhfMV9saW5lQ2hhcnRfMV8yIjtzOjExOiJkZXNj-
cmlwdGlvbiI7TjtzOjQ6InRvb2wiO3M6NToidHJlbmQiO3M6NDoidHlwZSI7czo0OiJ2-
dWxuIjtzOjQ6InRhZ3MiO3M6MDoiIjtzOjc6ImNvbnRleHQiO3M6OToiZGFzaGJvYXJk-
IjtzOjEzOiJicm93c2VDb2x1bW5zIjtzOjA6IiI7czoxNjoiYnJvd3NlU29ydENvbHVt-
biI7czowOiIiO3M6MTk6ImJyb3dzZVNvcnREaXJlY3Rpb24iO3M6MDoiIjtzOjg6Im93-
bmVyR0lEIjtzOjE6IjAiO3M6OToidGFyZ2V0R0lEIjtzOjI6Ii0xIjtzOjc6ImZpbHRl-
cnMiO2E6MTp7aTowO2E6Mzp7czoxMDoiZmlsdGVyTmFtZSI7czo5OiJmaXJzdFNlZW4i-
O3M6ODoib3BlcmF0b3IiO3M6MToiPSI7czo1OiJ2YWx1ZSI7czo0OiIwOjI1Ijt9fXM6-
NjoiZ3JvdXBzIjthOjA6e319fX0==</definition>
    <component> <name>Exploitable by Malware - Top 100 Vulnerabilities Exploitable by Malware</name>
<description>This component shows a top 100 summary of the vulnerabilities that have been identified to be exploitable using malware. The table is sorted by the total host column, which counts the total systems affected by the specific vulnerability.</description>
<componentType>table</componentType> <type>table</type>
        <column>1</column> <order>2</order>
<schedule>FREQ=DAILY;INTERVAL=1</schedule>

<definition>YTo1OntzOjc6InN0eWxlSUQiO3M6MjoiLTEiO3M6NzoiY29sdW1ucyI7-
YTo1OntpOjA7YToxOntzOjQ6Im5hbWUiO3M6ODoicGx1Z2luSUQiO31pOjE7YToxOntz-
OjQ6Im5hbWUiO3M6NDoibmFtZSI7fWk6MjthOjE6e3M6NDoibmFtZSI7czo4OiJmYW1p-
bHlJRCI7fWk6MzthOjE6e3M6NDoibmFtZSI7czo4OiJzZXZlcml0eSI7fWk6NDthOjE6-
e3M6NDoibmFtZSI7czo5OiJob3N0VG90YWwiO319czoxMDoiZGF0YVBvaW50cyI7czoz-
OiIxMDAiO3M6MTc6ImRpc3BsYXlEYXRhUG9pbnRzIjtzOjE6IjkiO3M6MTA6ImRhdGFT-
b3VyY2UiO2E6OTp7czoxNToicXVlcnlTb3VyY2VUeXBlIjtzOjEwOiJjdW11bGF0aXZl-
IjtzOjEzOiJxdWVyeVNvdXJjZUlEIjtOO3M6MTU6InF1ZXJ5U291cmNlVmlldyI7Tjtz-
OjEwOiJzb3J0Q29sdW1uIjtzOjk6Imhvc3RUb3RhbCI7czoxMzoic29ydERpcmVjdGlv-
biI7czo0OiJkZXNjIjtzOjEwOiJpdGVyYXRvcklEIjtzOjI6Ii0xIjtzOjc6ImNvbnRl-
eHQiO3M6OToiZGFzaGJvYXJkIjtzOjExOiJyZXN1bHRTdHlsZSI7czo0OiJsaXN0Ijtz-
OjU6InF1ZXJ5IjthOjEzOntzOjQ6Im5hbWUiO3M6MjY6Il8xMzg5NjQxMTAzLjE4NDhf-
dGFibGVfMV8yIjtzOjExOiJkZXNjcmlwdGlvbiI7TjtzOjQ6InRvb2wiO3M6NToic3Vt-
aWQiO3M6NDoidHlwZSI7czo0OiJ2dWxuIjtzOjQ6InRhZ3MiO3M6MDoiIjtzOjc6ImNv-
bnRleHQiO3M6OToiZGFzaGJvYXJkIjtzOjEzOiJicm93c2VDb2x1bW5zIjtzOjA6IiI7-
czoxNjoiYnJvd3NlU29ydENvbHVtbiI7czowOiIiO3M6MTk6ImJyb3dzZVNvcnREaXJl-
Y3Rpb24iO3M6MDoiIjtzOjg6Im93bmVyR0lEIjtzOjE6IjAiO3M6OToidGFyZ2V0R0lE-
IjtzOjI6Ii0xIjtzOjc6ImZpbHRlcnMiO2E6MTp7aTowO2E6Mzp7czoMDoiZmlsdGVy-
TmFtZSI7czoxMDoicGx1Z2luVGV4dCI7czo4OiJvcGVyYXRvciI7czoxOiI9IjtzOjU6-
InZhbHVlIjtzOjIwOiJleHBsb2l0ZWRfYnlfbWFsd2FyZSI7fX1zOjY6Imdyb3VwcyI7-
YTowOnt9fX19</definition>   </component>   <component>
       <name>Severity Trending</name>
<description></description>
<componentType>areaChart</componentType>
<type>areaChart</type>   <column>2</column>
<order>1</order>
<schedule>FREQ=DAILY;INTERVAL=1</schedule>
<definition>YTo1OntzOjc6InN0eWxlSUQiO3M6MjoiLTEiO3M6OToic3RhcnRUaW1l-
IjtzOjEwOiIxNDE0MzU4NjQzIjtzOjc6ImVuZFRpbWUiO3M6MTA6IjE0MTY1MTg2NDMi-
O3M6OToidGltZUZyYW1lIjtzOjM6IjI1ZCI7czo1OiJsaW5lcyI7YToxOntpOjA7YTo0-
OntzOjc6ImNvbHVtbnMiO2E6NDp7aTowO2E6MTp7czo0OiJuYW1lIjtzOjExOiJzZXZl-
cml0eUxvdyI7fWk6MTthOjE6e3M6NDoibmFtZSI7czoxNDoic2V2ZXJpdHlNZWRpdW0i-

O31pOjI7YToxOntzOjQ6Im5hbWUiO3M6MTI6InNldmVyaXR5SGlnaCI7fWk6MzthOjE6-
e3M6NDoibmFtZSI7czoxNjoic2V2ZXJpdHlDcml0aWNhbCI7fX1zOjc6ImF4aXNOdW0i-
O3M6MToiMSI7czo1OiJsYWJlbCI7czowOiIiO3M6MTA6ImRhdGFTb3VyY2UiO2E6OTp7-
czoxNToicXVlcnlTb3VyY2VUeXBlIjtzOjEwOiJjdW11bGF0aXZlIjtzOjEzOiJxdWVy-
eVNvdXJjZUlEIjtOO3M6MTU6InF1ZXJ5U291cmNlVmlldyI7TjtzOjEwOiJzb3J0Q29s-
dW1uIjtOO3M6MTM6InNvcnREaXJlY3Rpb24iO047czoxMDoiaXRlcmF0b3JJRCI7czoy-
OiItMSI7czo3OiJjb250ZXh0IjtzOjk6ImRhc2hib2FyZCI7czoxMToicmVzdWx0U3R5-
bGUiO3M6NToidHJlbmQiO3M6NToicXVlcnkiO2E6MTM6e3M6NDoibmFtZSI7czozMToi-
XzEzODkzMDUzMTQuNDg3XzBfYXJlYUNoYXJ0XzFfMiI7czoxMToiZGVzY3JpcHRpb24i-
O047czo0OiJ0b29sIjtzOjU6InRyZW5kIjtzOjQ6InR5cGUiO3M6NDoidnVsbiI7czo0-
OiJ0YWdzIjtzOjA6IiI7czo3OiJjb250ZXh0IjtzOjk6ImRhc2hib2FyZCI7czoxMzoi-
YnJvd3NlQ29sdW1ucyI7czowOiIiO3M6MTY6ImJyb3dzZVNvcnRDb2x1bW4iO3M6MDoi-
IjtzOjE5OiJicm93c2VTb3J0RGlyZWN0aW9uIjtzOjA6IiI7czo4OiJvd25lckdJRCI7-
czoxOiIwIjtzOjk6InRhcmdldEdJRCI7czoyOiItMSI7czo3OiJmaWx0ZXJzIjthOjA6-
e31zOjY6Imdyb3VwcyI7YTowOnt9fX19fX0=</definition>
</component> <component> <name>Top 10
Vulnerabilities</name> <description></description>
    <componentType>table</componentType>
<type>table</type> <column>2</column>
<order>2</order>
<schedule>FREQ=DAILY;INTERVAL=1</schedule>
<definition>YTo1OntzOjc6InN0eWxlSUQiO3M6MjoiLTEiO3M6NzoiY29sdW1ucyI7-
YTo1OntpOjA7YToxOntzOjQ6Im5hbWUiO3M6ODoicGx1Z2luSUQiO31pOjE7YToxOntz-
OjQ6Im5hbWUiO3M6NToidG90YWwiO31pOjI7YToxOntzOjQ6Im5hbWUiO3M6ODoic2V2-
ZXJpdHkiO31pOjM7YToxOntzOjQ6Im5hbWUiO3M6NDoibmFtZSI7fWk6NDthOjE6e3M6-
NDoibmFtZSI7czo4OiJmYW1pbHlJRCI7fX1zOjEwOiJkYXRhUG9pbnRzIjtzOjI6IjEw-
IjtzOjE3OiJkaXNwbGF5RGF0YVBvaW50cyI7czoyOiIxMCI7czoxMDoiZGF0YVNvdXJj-
ZSI7YTo5OntzOjE1OiJxdWVyeVNvdXJjZVR5cGUiO3M6MTA6ImN1bXVsYXRpdmUiO3M6-
MTM6InF1ZXJ5U291cmNlSUQiO047czoxNToicXVlcnlTb3VyY2VWaWV3IjtOO3M6MTA6-
InNvcnRDb2x1bW4iO3M6NToidG90YWwiO3M6MTM6InNvcnREaXJlY3Rpb24iO3M6NDoi-
ZGVzYyI7czoxMDoiaXRlcmF0b3JJRCI7czoyOiItMSI7czo3OiJjb250ZXh0IjtzOjk6-
ImRhc2hib2FyZCI7czoxMToicmVzdWx0U3R5bGUiO3M6NDoibGlzdCI7czo1OiJxdWVy-

eSI7YToxMzp7czo0OiJuYW1lIjtzOjI2OiJfMTM4OTMwNTMxNC43MzEyX3RhYmxlXzFf-
MiI7czoxMToiZGVzY3JpcHRpb24iO047czo0OiJ0b29sIjtzOjU6InN1bWlkIjtzOjQ6-
InR5cGUiO3M6NDoidnVsbiI7czo0OiJ0YWdzIjtzOjA6IiI7czo3OiJjb250ZXh0Ijtz-
Ojk6ImRhc2hib2FyZCI7czoxMzoiYnJvd3NlQ29sdW1ucyI7czowOiIiO3M6MTY6ImJy-
b3dzZVNvcnRDb2x1bW4iO3M6MDoiIjtzOjE5OiJicm93c2VTb3J0RGlyZWN0aW9uIjtz-
OjA6IiI7czo4OiJvd25lckdJRCI7czoxOiIwIjtzOjk6InRhcmdldEdJRCI7czoyOiIt-
MSI7czo3OiJmaWx0ZXJzIjthOjE6e2k6MDthOjM6e3M6MTA6ImZpbHRlck5hbWUiO3M6-
ODoic2V2ZXJpdHkiO3M6ODoib3BlcmF0b3IiO3M6MToiPSI7czo1OiJ2YWx1ZSI7czo3-
OiI0LDMsMiwxIjt9fXM6NjoiZ3JvdXBzIjthOjA6e319fX0=</definition>
</component> <component> <name>Top 10 IP
Summary</name> <description></description>
<componentType>table</componentType> <type>table</type>
<column>2</column> <order>3</order>
<schedule>FREQ=DAILY;INTERVAL=1</schedule>
<definition>YTo1OntzOjc6InN0eWxlSUQiO3M6MjoiLTEiO3M6NzoiY29sdW1ucyI7-
YTo1OntpOjA7YToxOntzOjQ6Im5hbWUiO3M6MjoiaXAiO31pOjE7YToxOntzOjQ6Im5h-
bWUiO3M6NToic2NvcmUiO31pOjI7YToxOntzOjQ6Im5hbWUiO3M6MTI6InJlcG9zaXRv-
cnlJRCI7fWk6MzthOjE6e3M6NDoibmFtZSI7czo1OiJ0b3RhbCI7fWk6NDthOjE6e3M6-
NDoibmFtZSI7czo3OiJ2dWxuQmFyIjt9fXM6MTA6ImRhdGFQb2ludHMiO3M6MjoiMTAi-
O3M6MTc6ImRpc3BsYXlEYXRhUG9pbnRzIjtzOjI6IjEwIjtzOjEwOiJkYXRhU291cmNl-
IjthOjk6e3M6MTU6InF1ZXJ5U291cmNlVHlwZSI7czoxMDoiY3VtdWxhdGl2ZSI7czox-
MzoicXVlcnlTb3VyY2VJRCI7TjtzOjE1OiJxdWVyeVNvdXJjZVZpZXciO047czoxMDoi-
c29ydENvbHVtbiI7czo1OiJzY29yZSI7czoxMzoic29ydERpcmVjdGlvbiI7czo0OiJk-
ZXNjIjtzOjEwOiJpdGVyYXRvcklEIjtzOjI6Ii0xIjtzOjc6ImNvbnRleHQiO3M6OToi-
ZGFzaGJvYXJkIjtzOjExOiJyZXN1bHRTdHlsZSI7czo0OiJsaXN0IjtzOjU6InF1ZXJ5-
IjthOjEzOntzOjQ6Im5hbWUiO3M6MjQ6Il8xMzg5MzA1MzE0LjgxX3RhYmxlXzFfMiI7-
czoxMToiZGVzY3JpcHRpb24iO047czo0OiJ0b29sIjtzOjU6InN1bWlwIjtzOjQ6InR5-
cGUiO3M6NDoidnVsbiI7czo0OiJ0YWdzIjtzOjA6IiI7czo3OiJjb250ZXh0IjtzOjk6-
ImRhc2hib2FyZCI7czoxMzoiYnJvd3NlQ29sdW1ucyI7czowOiIiO3M6MTY6ImJyb3dz-
ZVNvcnRDb2x1bW4iO3M6MDoiIjtzOjE5OiJicm93c2VTb3J0RGlyZWN0aW9uIjtzOjA6-
IiI7czo4OiJvd25lckdJRCI7czoxOiIwIjtzOjk6InRhcmdldEdJRCI7czoyOiItMSI7-
czo3OiJmaWx0ZXJzIjthOjA6e31zOjY6Imdyb3VwcyI7YTowOnt9fX19</definitio-
n> </component> </dashboardComponents></dashboardTab>

/dashboard/{id}/share

Methods

POST

Shares the Dashboard associated with {id}, depending on access and permissions

Request Parameters

Expand

```
{
        "groups" : [
                {
                        "id" : <number>          }...
        ]
}
```

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "id" : "42",
                "name" : "testPOST2",
                "description" : "test of a POST",
                "numColumns" : "3",
                "columnWidths" : [
                        "1",
                        "2",
                        "3"             ],
                "defaultTemplateNumber" : "-1",
                "createdTime" : "1414185335",
                "modifiedTime" : "1414185335",
                "order" : "6",
                "activated" : "true",
```

```
                "dashboardComponents" : [],
                "groups" : [
                        {
                                "id" : "3",
                                "name" : "TestGroup",
                                "description" : "Group for testing shares"
                "],
                "failedComponentCount" : "0",
                "canUse" : "true",
                "canManage" : "true",
                "owner" : {
                        "id" : "1",
                        "username" : "head",
                        "firstname" : "Security Manager",
                        "lastname" : "",
                        "uuid" : "4F7DD1CD-EB1B-40D7-BCE1-2DB3E31F6F4C"
                "ownerGroup" : {
                        "id" : "0",
                        "name" : "Full Access",
                        "description" : "Full Access group"             },
                "targetGroup" : {
                        "id" : -1,
                        "name" : "",
                        "description" : ""              }
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1414430665
}
```


Atlassian

Tenable Security Center API: Dashboard Template

/dashboardTemplate

Methods

GET

Gets the list of Dashboard Templates.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

**id
*name
*description
summary
type
category
definition
componentType
suggestedNumColumns
suggestedColumnWidths
enabled
minUpgradeVersion
templatePubTime
templateModTime
templateDefModTime
definitionModTime
createdTime
modifiedTime
tags
requirements
components

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

redFont = *field is a JSON object (* ***e.g.*** *"repository" :{ "id" : <id>, "name" : <name> })*

Expand Parameters

components

Request Parameters

Expand

NOTE #1: Pseudo Category "0" (recent) is currently not supported

NOTE #2: The *searchString* parameter takes in a space-separated set of keywords/phrases (in parenthesis) and builds a fuzzy match based on them. For excluding a keyword/phrase, is preceded by a '-'. Example:

```
"searchString" : "audit" -"SCAP" ..."
```

Parameters must be passed in as query string (as opposed to JSON) in the format of: /dashboardTemplate?categoryID="1"&...

```
{
    "categoryID" : <number> "1" (Threat Detection & Vulnerability
Assessments) | "2" (Monitoring) | "3" (Security Industry Trends) |
"4" (Executive) | "5" (Compliance & Configuration Assessment) | "6"
(Discovery & Detection) DEFAULT "" (All Categories),
    "searchString" : <string> (Search String Format. See NOTE#2)
DEFAULT ""}
```

Example Response

Expand

```
{
       "type" : "regular",
```

```
       "response" : [
                {
                        "id" : "384",
                        "name" : "Mitigated Patch Rates",
                        "description" : "This dashboard provides a great deal
information at a glance, such as comparing items like overall patch
rates to that of items with CVSS scores of 10.  The dashboard
facilitates a comparative analysis of Linux patches vs. Windows
patching over 30 day and 60 day cycle periods.  Some organizations
might be surprised how successful one patch management process is
over another."          },
                {
                        "id" : "555",
                        "name" : "Executive Summary",
                        "description" : "Using a series of charts, tables, and
this overview dashboard provides a summary for an executive to gain
a high level understanding of the vulnerability management status of
the network environment.  This dashboard contains valuable
information, including Top 10 Summaries of Assets, Networks and
Systems that are vulnerable, as well as useful trend information on
vulnerabilities and how long they have existed within the network
environment.\n\nThis will be helpful for those getting started with
Tenable.sc"             },
                {
                        "id" : "986",
                        "name" : "Executive Vulnerability Metrics",
                        "description" : "Monitoring security just got easier w
dashboard and Nessus.  This dashboard provides an executive view
into the active vulnerability detection and remediation of
discovered vulnerabilities.   Using the Nessus vulnerability
scanner, security professionals can discover vulnerabilities in
networks. This dashboard helps security professionals to communicate
metrics and status of vulnerabilities with executives.  \n\nThis
```

dashboard begins with four tables that show vulnerabilities in various states of remediation. The top left component provides a vulnerability age summary, and the top right provides a remediation summary. Both of these components show the count of vulnerabilities by the days of discovery or mitigation. \n\nThe following row of components display the number of discovered vulnerabilities by the date that a patch or vulnerability is published. The table on the left provides a focus on the patch date and severities, while the table on the right provides a summary of vulnerability publication dates. \n\nBoth tables provide columns for each severity, ranging from low to critical. The low severities are displayed with a blue background and white text, and the medium severities are black on orange. The high and critical severities are red and purple with white text. \n\nThe third row contains two trend graphs displaying a trend over the past 25 days for Windows and *nix vulnerabilities. The last two components are tables, one with a Windows user management summary, and the other with the top 10 most vulnerable systems.\n\nOverall, this dashboard provides executives with metrics to which they can oversee a risk mitigation program."
        },
        {
            "id" : "350",
            "name" : "Ticketing Summary",
            "description" : "Tenable.sc's internal workflow featu
a robust ticketing system for tracking ticket assignments. This dashboard displays the current status of tickets by classification, assignee and ticket.\n\nComprised of four components, this SC dashboard tracks the following : \n\nStatus Summary - Last 30 Days (pie chart)\nClassification Summary - Last 30 Days (pie chart)\nAssignee Summary (table) - Displays the current statistics for each user with ticket entries\nList of Tickets (table) - Displays tickets with more detail, including name, assignee, status, classification and modified date\/time\n\nThis information will help your staff and management better track what work needs to be done,

```
and the progress made for each ticket created."         },
                {
                        "id" : "862",
                        "name" : "Executive 30 Day",
                        "description" : "This dashboard provides an executive
a weekly status of the current vulnerability management program.  A
series of tables, charts and graphs provide a detailed view into the
vulnerabilities discovered and mitigated within the last 30
days.\n\nThe dashboard is comprised of 18 components that provide an
overview analysis of a vulnerability management program that is easy
to understand by managers, CISO's and other executives.  \n\nThe
first set of tables show a detailed ratio of vulnerabilities to the
risk of exploitation, and if the vulnerability has been mitigated or
not.  The tables are followed by series of pie charts, which
summarize the severities and risk of exploitation.\n \nThe next two
rows provide a trend analysis of the vulnerabilities by severity and
plugin type.  Both sets of trend data are calculated every day over
the past 30 days.  The data points are designed to show the daily
changes, allowing for detection of unusual activity.  In the third
column are the trend graphs showing the vulner"         },
                {
                        "id" : "863",
                        "name" : "Executive 30 Day - Current Vulnerabilities",
                        "description" : "This dashboard provides an executive
a weekly status of the current vulnerability management program.  A
series of tables, charts and graphs provide a detailed view into the
vulnerabilities discovered within the last 30 days.\n\nThe dashboard
is comprised of 12 components that provide an overview analysis of a
vulnerability management program that is easy to understand by
managers, CISO's and other executives.  \n\nThe first set of tables
show a detailed ratio of vulnerabilities to the risk of
exploitation, and if the vulnerability has been mitigated or not.
The tables are followed by series of pie charts, which summarize the
```

severities and risk of exploitation.\n \nThe next two rows provide a trend analysis of the vulnerabilities by severity and plugin type. Both sets of trend data are calculated every day over the past 30 days. The data points are designed to show the daily changes, allowing for detection of unusual activity. \n\nThe remaining components show an analysis of assets, and the vulnerabilities with top 10 most vulnerable assets. Using a bar chart and table, a high level summary is depicted." },
{
"id" : "709",
"name" : "Executive 7 Day",
"description" : "This dashboard provides an executive a weekly status of the current vulnerability management program. A series of tables, charts and graphs provide a detailed view into the vulnerabilities discovered and mitigated within the last 7 days.\n\nThe dashboard is comprised of 18 components that provide an overview analysis of a vulnerability management program that is easy to understand by managers, CISO's and other executives. \n\nThe first set of tables show a detailed ratio of vulnerabilities to the risk of exploitation, and if the vulnerability has been mitigated or not. The tables are followed by series of pie charts, which summarize the severities and risk of exploitation.\n \nThe next two rows provide a trend analysis of the vulnerabilities by severity and plugin type. Both sets of trend data are calculated every day over the past 7 days. The data points are designed to show the daily changes, allowing for detection of unusual activity. In the third column are the trend graphs showing the vulnerabilities that have returned after they have been previously mitigated. \n\nThe remaining components show an analysis of assets, and the vulnerabilities with top 10 most vulnerable assets. Using a bar chart and table, a high level summary is depicted." },
{
"id" : "739",

```
                        "name" : "Executive 7 Day - Current Vulnerabilities",
                        "description" : "This dashboard provides an executive
a weekly status of the current vulnerability management program.  A
series of tables, charts and graphs provide a detailed view into the
vulnerabilities discovered within the last 7 days.\n\nThe dashboard
is comprised of 12 components that provide an overview analysis of a
vulnerability management program that is easy to understand by
managers, CISO's and other executives.  \n\nThe first set of tables
show a detailed ratio of vulnerabilities to the risk of
exploitation, and if the vulnerability has been mitigated or not.
The tables are followed by series of pie charts, which summarize the
severities and risk of exploitation.\n \nThe next two rows provide a
trend analysis of the vulnerabilities by severity and plugin type.
Both sets of trend data are calculated every day over the past 7
days.  The data points are designed to show the daily changes,
allowing for detection of unusual activity.  \n\nThe remaining
components show an analysis of assets, and the vulnerabilities with
top 10 most vulnerable assets.  Using a bar chart and table, a high
level summary is depicted."             },
                {
                        "id" : "567",
                        "name" : "Ticket Management",
                        "description" : "Tenable.sc can use other data besides
vulnerabilities or events to create dashboards. In this dashboard
example, a table component is used to list recent tickets and a
matrix component is used to list ticket load for specific users."
},
                {
                        "id" : "413",
                        "name" : "Mobile Summary",
                        "description" : "This dashboard provides an executive
the current Mobile Device Management (MDM) status.  The dashboard
was created using the new features within Tenable.sc 4.7 and the
```

```
features within Nessus to collect mobile data from the MDM solution.
 There are 4 components showing a summary of mobile device types,
charts displaying the current vulnerability count, a matrix with
device and vulnerability count, and a top 50 user summary."              },
               {
                       "id" : "404",
                       "name" : "IAVM Executive Summary",
                       "description" : "This dashboard provides an executive
the current Information Assurance Vulnerability Management (IAVM)
program."               },
               {
                       "id" : "383",
                       "name" : "Mitigated Patch Rates - Remediation Rates",
                       "description" : "On the bottom, I created a matrix cha
lists some very generic columns including : \\n- Now - number of
current vulnerabilities\\n- Patched - number of vulnerabilities in
the mitigated status\\n- 30d Rate - number of patched
vulnerabilities that took 30 days or less to patch\\n- 30d Date -
number of patches that occurred within the past 30 days\\n- 30d Rate
- Lifetime - percent of patches that occurred within 30 days of
being tracked by Tenable.sc\\n- 30d Rate Past 30d - percent of
patches that occurred within 30 days of being tracked by Tenable.sc
for the past 30 calendar days\\n- 30d Rate Past 31d - 60d - percent
of patches that occurred within 30 days of being tracked by
Tenable.sc between 31 and 60 calendar days ago\\n- 30d Rate Past 61d
- 90d - percent of patches that occurred within 30 days of being
tracked by Tenable.sc between 61 and 90 calendar days ago\\n\\nFor
the rows, I created different types of arbitrary categories,
including all vulnerabilities, vulnerabilities with a CVSS score of
10, exploitable vulnerabilities, and vulnerabilities, which were
Windows or Linux in nature.\\n\\nFor each ratio, the percentage from
0 to 25 is red, 24 to 50 is yellow and higher than 50 is green."
               {
```

```
                        "id" : "382",
                        "name" : "Mitigated Patch Rates - Vulnerabilities Ove
                        "description" : "This component is a 90 day summary ch
tracking active vulnerabilities with low, medium, high, and critical
severities."             },
                {
                        "id" : "551",
                        "name" : "Executive Summary - Vulnerability Age",
                        "description" : "This component contains a matrix disp
vulnerability age. The columns identify new hosts (within the past
24 hours), and vulnerabilities from low to critical severities. The
rows are labeled by the number of days the vulnerabilities have
existed within the environment from the first discovery date, sorted
by less than 7, 30, 90 days, and greater than 90 days."         },
                {
                        "id" : "546",
                        "name" : "Executive Summary - Outstanding Patches by O
System",
                        "description" : "This component displays a summary of
vulnerabilities by operating system, using the Local Check Plugin
Families.  The data is sorted by the critical vulnerabilities."         },
                {
                        "id" : "845",
                        "name" : "Executive 30 Day - Current Vulnerability Sum
Severity",
                        "description" : "This component displays a severity su
vulnerabilities discovered over the past 30 days. Please note that
the chart is configured only to show medium, high, and critical
severities."             },
                {
                        "id" : "983",
                        "name" : "Executive Vulnerability Metrics - Vulnerabil
Mitigation",
```

```
                        "description" : "This component contains a matrix disp
mitigated vulnerability ages. The columns identify new hosts (within
the past 24 hours), and vulnerabilities from low to critical
severities. The rows are labeled by the number of days the
vulnerabilities have existed within the environment from the first
discovery date, sorted by less than 7, 30, 90 days, and greater than
90 days."                },
                {
                        "id" : "980",
                        "name" : "Executive Vulnerability Metrics - Patch Publ
Age",
                        "description" : "This component provides a summary of
vulnerabilities and patch release dates.  The dates are summarized
with 7, 30, 90 and more than 90 days.  The matrix provides columns
for each severity, ranging from low to critical.  The low severities
are displayed with a blue background and white text, and the medium
severities are black on orange.  The high and critical severities
are red and purple with white text."            },
                {
                        "id" : "981",
                        "name" : "Executive Vulnerability Metrics - 25 Day Tre
Vulnerabilities",
                        "description" : "This component provides a 25-day tren
Microsoft vulnerabilities.  The graph provides separate colors to
denote the severity.  The vulnerability trending is calculated with
24-hour data points."           },
                {
                        "id" : "982",
                        "name" : "Executive Vulnerability Metrics - Windows Us
Management",
                        "description" : "This table provides a list of informa
vulnerabilities on Microsoft user accounts.  This component selects
the 'Windows :  User management' plugin family and is then sorted by
```

```
the total of vulnerabilities discovered.  The 'Windows :  User
management' plugin family checks for issues in Microsoft Windows
user management, and includes user information disclosure, group
enumeration, and more."         },
                {
                        "id" : "984",
                        "name" : "Executive Vulnerability Metrics - Vulnerabil
Publication Age",
                        "description" : "This component provides a summary of
vulnerabilities and their release dates.  The dates are summarized
with 7, 30, 90, and more than 90 days.  The matrix provides columns
for each severity ranging from low to critical.  The low severities
are displayed with a blue background and white text, and the medium
severities are black on orange.  The high and critical severities
are red and purple with white text."             },
                {
                        "id" : "985",
                        "name" : "Executive Vulnerability Metrics - 25 Day Tre
Vulnerabilities",
                        "description" : "This component provides a 25-day tren
vulnerabilities.  The graph provides separate colors to denote the
severities.  The vulnerability trending is calculated with 24-hour
data points."           },
                {
                        "id" : "853",
                        "name" : "Executive 30 Day - Exploitable Vulnerability
by Type",
                        "description" : "This component trend analysis display
exploitable vulnerabilities discovered in the past 25 days, and by
vulnerability type. The data points for this trend analysis are
reporting newly discovered exploitable vulnerabilities within the
last 24 hours.  This allows for the understanding of newly
discovered exploitable vulnerabilities found each day over the last
```

```
25 days."               },
               {
                       "id" : "854",
                       "name" : "Executive 30 Day - Exploitable Vulnerability
Summary",
                       "description" : "This component shows an exploitable
vulnerability analysis by asset list, displaying a bar for medium,
high, and critical severities for each asset.  The data is sorted by
the count of critical severities in a descending direction."           },
               {
                       "id" : "855",
                       "name" : "Executive 30 Day - Exploitable Asset Vulnera
Breakdown",
                       "description" : "This component displays the newly dis
exploitable vulnerability count of the top 10 assets.  The counts
are vulnerabilities that have been discovered over the past 30
days."          },
               {
                       "id" : "856",
                       "name" : "Executive 30 Day - Mitigated Vulnerability T
Matrix",
                       "description" : "The component shows a summary of the
vulnerabilities that have been discovered over the past 30 days. To
allow for better understanding of risk, the data is separated by
exploit frameworks, Metasploit, Core Impact, Canvas, and malware
that are tracked by Tenable Research.\n\nThe first column shows the
percentage of remediated vulnerabilities that have public exploits.
 The subsequent columns are broken down using the exploit framework.
 The cells show the percentage of the exploitable vulnerabilities
for each framework.  If 0% is present, then less than 1% of total
vulnerabilities are identified and text is green with black text.
If 1% - 10% of vulnerabilities are exploitable by a framework, the
cell is black on orange with a ratio-bar.   If 11 - 50% are
```

```
exploitable by a framework, the cell is white on red with a ratio-
bar.   If 51% - 100% are exploitable by a framework, the cell is
white on purple with a ratio-bar."              },
               {
                       "id" : "857",
                       "name" : "Executive 30 Day - Mitigated Vulnerability S
Severity",
                       "description" : "This component displays a severity su
remediated vulnerabilities discovered over the past 30 days. Please
note that the chart is configured only to show medium, high, and
critical severities."           },
               {
                       "id" : "858",
                       "name" : "Executive 30 Day - Previously Mitigated Vuln
Trend",
                       "description" : "This component displays a trend analy
previously remediated vulnerabilities discovered over the past 25
days.  Please note that the trend line is configured only to show
the medium, high, and critical severities.  The data points for this
trend analysis are reporting newly discovered previously remediated
vulnerabilities within the last 24 hours.  This allows for the
understanding of which vulnerabilities have returned each day over
the last 25 days."               },
               {
                       "id" : "859",
                       "name" : "Executive 30 Day - Previously Mitigated Vuln
Trending by Type",
                       "description" : "This component trend analysis display
previously mitigated vulnerabilities discovered in the past 25 days,
and by vulnerability type. The data points for this trend analysis
are reporting the newly discovered previously mitigated
vulnerabilities within the last 24 hours.  This allows for the
understanding of what new vulnerabilities have returned each day
```

```
over the last 25 days."         },
                {
                        "id" : "860",
                        "name" : "Executive 30 Day - Mitigated Vulnerability A
Summary",
                        "description" : "This component shows a mitigated vuln
analysis by asset list, displaying a bar for medium, high, and
critical severities for each asset.  The data is sorted by the count
of critical severities in a descending direction."              },
                {
                        "id" : "861",
                        "name" : "Executive 30 Day - Mitigated Asset Vulnerabi
Breakdown",
                        "description" : "This component displays the newly dis
exploitable vulnerability count of the top 10 assets.  The counts
are vulnerabilities that have been discovered over the past 30 days.
 The data is sorted in descending order by the number of critical
vulnerabilities."                },
                {
                        "id" : "846",
                        "name" : "Executive 30 Day - Current Vulnerability Tre
Severity",
                        "description" : "This component displays a trend analy
vulnerabilities discovered over the past 25 days.  Please note that
the trend line is configured only to show medium, high, and critical
severities.   The data points for this trend analysis are reporting
newly discovered vulnerabilities within the last 24 hours.  This
allows for the understanding of newly discovered vulnerabilities
found each day over the last 25 days."          },
                {
                        "id" : "847",
                        "name" : "Executive 30 Day - Current Vulnerability Tre
Type",
```

```
                        "description" : "This component trend analysis displa
vulnerabilities discovered of the past 25 days, and by vulnerability
type. The data points for this trend analysis are reporting newly
discovered vulnerabilities within the last 24 hours.  This allows
for the understanding of newly discovered vulnerabilities found each
day over the last 25 days."             },
                {
                        "id" : "848",
                        "name" : "Executive 30 Day - Current Vulnerability Ass
Summary",
                        "description" : "This component shows vulnerability an
asset list, displaying a bar for medium, high, and critical
severities of each asset.  The data is sorted by the count of
critical severities in a descending direction."         },
                {
                        "id" : "849",
                        "name" : "Executive 30 Day - Current Asset Vulnerabili
Breakdown",
                        "description" : "This component displays the newly dis
vulnerability count of the top 10 assets.  The counts are
vulnerabilities that have been discovered over the past 30 days.
The data is sorted in descending order by the number of critical
vulnerabilities."               },
                {
                        "id" : "850",
                        "name" : "Executive 30 Day - Exploitable Vulnerability
Matrix",
                        "description" : "The component shows a summary of the
vulnerabilities that have been discovered over the past 30 days. To
allow for better understanding of risk, the data is separated by
exploit frameworks, Metasploit, Core Impact, Canvas, and malware
that are tracked by Tenable Research.\n\nThe first column shows the
percentage of vulnerabilities that have public exploits.   The
```

subsequent columns are broken down using the exploit framework. The cells show the percentage of the exploitable vulnerabilities for each framework. If 0% is present, then less than 1% of total vulnerabilities are identified and text is green with black text. If 1% - 10% of vulnerabilities are exploitable by a framework, the cell is black on orange with a ratio-bar. If 11 - 50% are exploitable by a framework, the cell is white on red with a ratio-bar. If 51% - 100% are exploitable by a framework, the cell is white on purple with a ratio-bar." },
{
"id" : "851",
"name" : "Executive 30 Day - Exploitable Vulnerability Severity",
"description" : "This component displays a severity su exploitable vulnerabilities discovered over the past 30 days. Please note that the chart is configured only to show medium, high, and critical severities." },
{
"id" : "852",
"name" : "Executive 30 Day - Exploitable Vulnerability by Severity",
"description" : "This component displays a trend analy exploitable vulnerabilities discovered over the past 25 days. Please note that the trend line is configured only to show medium, high, and critical severities. The data points for this trend analysis are reporting newly discovered exploitable vulnerabilities within the last 24 hours. This allows for the understanding of newly discovered exploitable vulnerabilities found each day over the last 25 days." },
{
"id" : "844",
"name" : "Executive 30 Day - Current Vulnerability Typ
"description" : "This component provides a summary of

vulnerabilities discovered within the pasts 30 days. The rows are separated by severity level. Columns are sorted by plugin type. Please note that if your deployment does not use Nessus, PVS, or LCE, some data will show as a 0 quantity, and columns can be removed if necessary."   },
                {
                        "id" : "703",
                        "name" : "Executive 7 Day - Mitigated Vulnerability Ty
                        "description" : "The component shows a summary of the vulnerabilities that have been discovered over the past 7 days. To allow for better understanding of risk, the data is separated by exploit frameworks, Metasploit, Core Impact, Canvas, and malware that are tracked by Tenable Research.\n\nThe first column shows the percentage of remediated vulnerabilities that have public exploits. The subsequent columns are broken down using the exploit framework. The cells show the percentage of the exploitable vulnerabilities for each framework. If 0% is present, then less than 1% of total vulnerabilities are identified and text is green with black text. If 1% - 10% of vulnerabilities are exploitable by a framework, the cell is black on orange with a ratio-bar. If 11 - 50% are exploitable by a framework, the cell is white on red with a ratio-bar. If 51% - 100% are exploitable by a framework, the cell is white on purple with a ratio-bar."   },
                {
                        "id" : "545",
                        "name" : "Executive Summary - Vulnerability Trend (Mec Critical) last 90 days",
                        "description" : "This component contains a trend analy medium, high and critical severity vulnerabilities over the past 90 days. This method of analysis allows executives to see how risk to the organization has changed during the previous 90 days."   },
                {
                        "id" : "547",

```
                        "name" : "Executive Summary - Most Vulnerable Hosts",
                        "description" : "This component contains a bar chart o
10 most vulnerable hosts. The bar chart contains critical, high and
medium severity vulnerabilities. The number of critical severities
is used to rank the hosts in the chart."                },
                {
                        "id" : "548",
                        "name" : "Executive Summary - CVSS Scoring",
                        "description" : "This matrix component displays curren
vulnerabilities by CVSS scores ranging from 10-7, 6.9-5, 4.9-3 and
below 2.9."             },
                {
                        "id" : "549",
                        "name" : "Executive Summary - Asset Outstanding Patche
Operating System (Medium, Highs and Criticals)",
                        "description" : "This component shows a table of the t
summary of the most vulnerable assets, sorted by the number of
critical severities. Asset lists are dynamically and\/or statically
generated lists of IP enabled devices (a.k.a. Assets) within the
organization. Assets are commonly static or dynamic, however there
are other types such as DNS and LDAP-based assets. Static assets are
a predefined set of IP addresses using either a range or subnet
boundary as the asset parameter, while dynamic asset lists are
created to group common devices together (via rules that use
vulnerability data to create a list) for more advanced functions."
},
                {
                        "id" : "550",
                        "name" : "Executive Summary - Severity Summary",
                        "description" : "This component contains a single pie
displaying a summary of the vulnerabilities by severity level. The
chart is separated in critical, high, medium and low severities."
},
```

```
                {
                        "id" : "552",
                        "name" : "Executive Summary - Most Vulnerable Networks
                        "description" : "This component contains a bar chart c
10 most vulnerable networks. The bar chart contains critical, high
and medium severity. The number of critical severities is used to
sort the assets in the graph. The network sorting is based on the
native class 'C' subnet mask boundary, which is based on masking
with 24 bits, and the result is groups of 256 IP addresses."             },
                {
                        "id" : "553",
                        "name" : "Executive Summary - CVSS Scoring (Previously
Items)",
                        "description" : "This matrix displays mitigated vulner
by CVSS scores ranging from 10-7, 6.9-5, 4.9-3 and below 2.9."           },
                {
                        "id" : "554",
                        "name" : "Executive Summary - Asset Summary by MS Bull
                        "description" : "This component is a table showing a t
summary of the most vulnerable assets with missing Microsoft
Bulletins, sorted by critical severities. The chart indicates all
critical, high, and medium severities."         },
                {
                        "id" : "691",
                        "name" : "Executive 7 Day - Current Vulnerability Type
                        "description" : "This component provides a summary of
vulnerabilities discovered within the pasts 7 days.  The rows are
separated by severity level.   Columns are sorted by plugin type.
Please note that if your deployment does not use Nessus, PVS, or
LCE, some data will show as a 0 quantity, and columns can be removed
if necessary."          },
                {
                        "id" : "692",
```

```
                        "name" : "Executive 7 Day - Current Vulnerability Summ
Severity",
                        "description" : "This component displays a severity su
vulnerabilities discovered over the past 7 days. Please note that
the chart is configured only to show medium, high, and critical
severities."            },
                {
                        "id" : "693",
                        "name" : "Executive 7 Day - Current Vulnerability Tren
Severity",
                        "description" : "This component displays a trend analy
vulnerabilities discovered over the past 7 days.  Please note that
the trend line is configured only to show medium, high, and critical
severities.   The data points for this trend analysis are reporting
newly discovered vulnerabilities within the last 24 hours.  This
allows for the understanding of newly discovered vulnerabilities
found each day over the last 7 days."           },
                {
                        "id" : "694",
                        "name" : "Executive 7 Day - Current Vulnerability Tren
Type",
                        "description" : "This component trend analysis display
vulnerabilities discovered of the past 7 days, and by vulnerability
type. The data points for this trend analysis are reporting newly
discovered vulnerabilities within the last 24 hours.  This allows
for the understanding of newly discovered vulnerabilities found each
day over the last 7 days."              },
                {
                        "id" : "695",
                        "name" : "Executive 7 Day - Current Vulnerability Asse
                        "description" : "This component shows vulnerability an
asset list, displaying a bar for medium, high, and critical
severities of each asset.  The data is sorted by the count of
```

```
critical severities in a descending direction."         },
                {
                        "id" : "696",
                        "name" : "Executive 7 Day - Current Asset Vulnerabilit
Breakdown",
                        "description" : "This component displays the newly dis
vulnerability count of the top 10 assets.  The counts are
vulnerabilities that have been discovered over the past 7 days.  The
data is sorted in descending order by the number of critical
vulnerabilities."               },
                {
                        "id" : "697",
                        "name" : "Executive 7 Day - Exploitable Vulnerability
Matrix",
                        "description" : "The component shows a summary of the
vulnerabilities that have been discovered over the past 7 days. To
allow for better understanding of risk, the data is separated by
exploit frameworks, Metasploit, Core Impact, Canvas, and malware
that are tracked by Tenable Research.\n\nThe first column shows the
percentage of vulnerabilities that have public exploits.   The
subsequent columns are broken down using the exploit framework.  The
cells show the percentage of the exploitable vulnerabilities for
each framework.  If 0% is present, then less than 1% of total
vulnerabilities are identified and text is green with black text.
If 1% - 10% of vulnerabilities are exploitable by a framework, the
cell is black on orange with a ratio-bar.   If 11 - 50% are
exploitable by a framework, the cell is white on red with a ratio-
bar.   If 51% - 100% are exploitable by a framework, the cell is
white on purple with a ratio-bar."              },
                {
                        "id" : "698",
                        "name" : "Executive 7 Day - Exploitable Vulnerability
Severity",
```

```
                        "description" : "This component displays a severity su
exploitable vulnerabilities discovered over the past 7 days. Please
note that the chart is configured only to show medium, high, and
critical severities."           },
                {
                        "id" : "699",
                        "name" : "Executive 7 Day - Exploitable Vulnerability
Severity",
                        "description" : "This component displays a trend analy
exploitable vulnerabilities discovered over the past 7 days.  Please
note that the trend line is configured only to show medium, high,
and critical severities.  The data points for this trend analysis
are reporting newly discovered exploitable vulnerabilities within
the last 24 hours.  This allows for the understanding of newly
discovered exploitable vulnerabilities found each day over the last
7 days."                },
                {
                        "id" : "700",
                        "name" : "Executive 7 Day - Exploitable Vulnerability
Type",
                        "description" : "This component trend analysis displa
exploitable vulnerabilities discovered in the past 7 days, and by
vulnerability type. The data points for this trend analysis are
reporting newly discovered exploitable vulnerabilities within the
last 24 hours.  This allows for the understanding of newly
discovered exploitable vulnerabilities found each day over the last
7 days."                },
                {
                        "id" : "701",
                        "name" : "Executive 7 Day - Exploitable Vulnerability
Summary",
                        "description" : "This component shows an exploitable
vulnerability analysis by asset list, displaying a bar for medium,
```

```
high, and critical severities for each asset.  The data is sorted by
the count of critical severities in a descending direction."            },
                {
                        "id" : "702",
                        "name" : "Executive 7 Day - Exploitable Asset Vulnerab
Breakdown",
                        "description" : "This component displays the newly dis
exploitable vulnerability count of the top 10 assets.  The counts
are vulnerabilities that have been discovered over the past 7 days."
                 },
                {
                        "id" : "704",
                        "name" : "Executive 7 Day - Mitigated Vulnerability Su
Severity",
                        "description" : "This component displays a severity su
remediated vulnerabilities discovered over the past 7 days. Please
note that the chart is configured only to show medium, high, and
critical severities."           },
                {
                        "id" : "705",
                        "name" : "Executive 7 Day - Previously Mitigated Vulne
Trend",
                        "description" : "This component displays a trend analy
previously remediated vulnerabilities discovered over the past 7
days.  Please note that the trend line is configured only to show
the medium, high, and critical severities.  The data points for this
trend analysis are reporting newly discovered previously remediated
vulnerabilities within the last 24 hours.  This allows for the
understanding of which vulnerabilities have returned each day over
the last 7 days."               },
                {
                        "id" : "706",
                        "name" : "Executive 7 Day - Previously Mitigated Vulne
```

```
Trending by Type",
                        "description" : "This component trend analysis displa
previously mitigated vulnerabilities discovered in the past 7 days,
and by vulnerability type. The data points for this trend analysis
are reporting the newly discovered previously mitigated
vulnerabilities within the last 24 hours.  This allows for the
understanding of what new vulnerabilities have returned each day
over the last 7 days."          },
                {
                        "id" : "707",
                        "name" : "Executive 7 Day - Mitigated Vulnerability As
Summary",
                        "description" : "This component shows a mitigated vuln
analysis by asset list, displaying a bar for medium, high, and
critical severities for each asset.  The data is sorted by the count
of critical severities in a descending direction."              },
                {
                        "id" : "708",
                        "name" : "Executive 7 Day - Mitigated Asset Vulnerabil
Breakdown",
                        "description" : "This component displays the newly dis
exploitable vulnerability count of the top 10 assets.  The counts
are vulnerabilities that have been discovered over the past 7 days.
The data is sorted in descending order by the number of critical
vulnerabilities."              },
                {
                        "id" : "566",
                        "name" : "Ticket Load",
                        "description" : "This component is used to list ticket
specific users."              },
                {
                        "id" : "565",
                        "name" : "This Weeks Tickets",
```

```
                        "description" : "This table component is used to list
Tenable.sc tickets."            },
                {
                        "id" : "412",
                        "name" : "Mobile Summary - Vulnerable Mobile Devices",
                        "description" : "This component contains a matrix with
for the device count, critical severity, high severity, and medium
severity.  The numeric value denotes the device count.  This
component uses multiple fields to query the displayed data.  \n\nThe
basis of each cell query within the matrix is the 'Model' type.
Please note that this field is case sensitive.  As an example, if
the model type is set to'ipad', the returned result will be 0.  To
ensure the correct values are displayed, use the Analysis > Mobile >
Model Summary to view the current device models present.\n\nWhen
device models use a common OS over several platforms (for example,
Android), an additional filter can be used.  This component
illustrates this functionality by combining the 'Model' and 'Serial
Number' fields.  The HTC devices have HTC as the serial number
prefix, while Samsung has SAMSUNG.  This allows the component to
display a more granular data view.  However, all Android based
devices don't follow this pattern. Therefore the 'Android' row uses
only the 'Model' field as the filter."          },
                {
                        "id" : "409",
                        "name" : "Mobile Summary - Device Type Summary Pie Cha
                        "description" : "This component provides a model summa
managed devices with the MDM solution.  Using the 'Model Summary'
tool and sorting devices based on the Model column, the device count
is used to create a pie chart that is easy to read and understand.
From a quick glance, the user can understand the number of managed
mobile devices."                },
                {
                        "id" : "410",
```

```
                        "name" : "Mobile Summary - Top 50 Mobile Users",
                        "description" : "This component contains a table listi
users with the most mobile devices registered to MDM. The table is
based on the 'User Summary' tool, and displays the top 50 users
based on the total number of mobile devices.  The sort column is
based on the device total count and is sorted in descending order.
The user, low, medium, high, critical, and total columns are
displayed."              },
                {
                        "id" : "411",
                        "name" : "Mobile Summary - Mobile Device Count, Critic
Severity Summary",
                        "description" : "This component displays a bar chart t
includes a device count, critical severity, and high severity. Using
the device model as the sort column with a descending sort
direction, the component provides an easy to view status of all
managed device models, with a bar representing the count of device
with critical and high severities."              },
                {
                        "id" : "401",
                        "name" : "IAVM High Severity Summary Yr 2013",
                        "description" : "This component provides a pie chart o
10 high severity IAVM vulnerabilities identified in 2013.  The pie
chart is comprised of the host count for total hosts per IAVM Notice
Number."                },
                {
                        "id" : "399",
                        "name" : "IAVM By Year (25 Day Trend)",
                        "description" : "This component displays a 25-day tren
IAVMs per year.  Each year starting with 2013 through 2010 has its
own line, while all years from 2002 - 2009 share a common line.  The
trend is calculated by using the total vulnerabilities on the
respective date."              },
```

```
                {
                        "id" : "400",
                        "name" : "IAVM Indicator by Year",
                        "description" : "This indicator style component shows
count for each severity level for the corresponding year.  The host
count is calculated by putting the year in as an IAVM filter and the
respective severity level."             },
                {
                        "id" : "402",
                        "name" : "IAVM Plugin Family Vulnerabilities for YR 20
                        "description" : "This component displays a bar chart s
the IAVM status per plugin family.  The bar chart is also filtered
to only display the top 5 plugin families."             },
                {
                        "id" : "403",
                        "name" : "IAVM Indicator By Vendor",
                        "description" : "This indicator style component provid
correlation between IAVM and software vendor.  Using the CPE and\/or
Plugin name fields, Tenable.sc is able to map the IAVM Notice Number
(s) to the software vendor and severity level."         },
                {
                        "id" : "398",
                        "name" : "IAVM Critical Severity Summary Yr 2013",
                        "description" : "This component provides a pie chart o
10 critical severity IAVM vulnerabilities identified in 2013.  The
pie chart is comprised of the host count for total hosts per IAVM
Notice Number."         },
                {
                        "id" : "348",
                        "name" : "Ticket Overview - Assignee Summary",
                        "description" : "Assignee Summary Table displays the c
statistics for each user with ticket entries"           },
                {
```

```
                        "id" : "346",
                        "name" : "Ticket Overview - Tickey Status Summary Last
                        "description" : "Status summary of tickets created in
days."          },
                {
                        "id" : "347",
                        "name" : "Ticket Overview - Ticket Classification Summ
30 Days",
                        "description" : "Classification summary of tickets cre
last 30 days."          },
                {
                        "id" : "349",
                        "name" : "Ticket Overview - List of Tickets",
                        "description" : "The 'List of Tickets' table displays
with more detail, including name, assignee, status, classification
and modified date\/time"                }
        ],
        "error_code" : 0,"error_msg" : "",
        "warnings" : [],
        "timestamp" : 1414182980
}
```


/dashboardTemplate/{id}

Methods

GET

Gets the Dashboard Template associated with {id}.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

**id
*name
*description
summary
type
category
definition
componentType
suggestedNumColumns
suggestedColumnWidths
enabled
minUpgradeVersion
templatePubTime
templateModTime
templateDefModTime
definitionModTime
createdTime
modifiedTime
tags
requirements
components

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

redFont = *field is a JSON object (* ***e.g.*** *"repository" :{ "id" : <id>, "name" : <name> })*

Expand Parameters

components

Request Parameters

None

Example Response

Expand


```
{
       "type" : "regular",
       "response" : {
              "id" : "1574",
              "name" : "FTI Security Guidelines",
              "description" : "The most recent version of IRS Publication 10
Tax Information Security Guidelines for Federal, State, and Local
Agencies took effect on January 1, 2014, and provides thorough
guidance for organizations that deal with Federal Taxpayer
Information (FTI). Not only does Publication 1075 outline the
technical and physical security requirements, but it also details
incident response and data disclosure requirements. According to
Publication 1075, the FTI guidelines not only apply to the
organization receiving FTI; they also apply to contractors or
consolidated data centers that may come into contact with the FTI as
well. This means that organizations need to take a comprehensive
approach to securing this sensitive information.\n\nThis dashboard
focuses on IRS Publication 1075. Tenable's Tenable.sc Continuous
View (SC CV) is the market-defining continuous network monitoring
platform, which includes active vulnerability detection with Nessus,
passive vulnerability detection with the Passive Vulnerability
Scanner (PVS), and log correlation with the Log Correlation Engine
(LCE). SC CV assists organizations in discovering compliance and
vulnerability concerns on the network, assessing their impact,
reporting on the results, and taking action to remediate issues. SC
CV provides the tools that state and local government agencies can
use to meet and demonstrate FTI compliance.\n\nIRS Publication 1075
is largely based on the standard NIST Special Publication 800-53,
but with special considerations for additional sensitive
information. Tenable Network Security has extensive expertise in
helping customers meet the requirements of NIST Special Publication
800-53, and as a result, the SC CV solution is well suited for
```

```
meeting IRS Publication 1075 requirements as well.",
                "summary" : "IRS Publication 1075 - Tax Information Security
Guidelines for Federal, State, and Local Agencies, 2014 edition,
provides thorough guidance for organizations that deal with Federal
Taxpayer Information (FTI). Tenable's Tenable.sc Continuous View (SC
CV) assists organizations in discovering compliance and
vulnerability concerns on the network, assessing their impact,
reporting on the results, and taking action to remediate issues. SC
CV provides the tools that state and local government agencies can
use to meet and demonstrate FTI compliance.",
                "type" : "collection",
                "suggestedNumColumns" : "3",
                "suggestedColumnWidths" : "33,34,33",
                "enabled" : "true",
                "minUpgradeVersion" : "4.8.1",
                "templatePubTime" : "1414009276",
                "templateModTime" : "1414009276",
                "templateDefModTime" : "1414009276",
                "definitionModTime" : "1414049413",
                "createdTime" : "1414049413",
                "modifiedTime" : "1414049413",
                "tags" : [
                        "anomalies",
                        "compliance",
                        "dlp",
                        "fti",
                        "mitigated",
                        "network",
                        "vulnerabilities"               ],
                "requirements" : [
                        {
                                "requirement" : "lce",
                                "value" : "4.4.0 : "                    },
```

```
                        {
                                "requirement" : "nessus",
                                "value" : "5.2.7 : "                    },
                        {
                                "requirement" : "pvs",
                                "value" : "4.0.2 : "                    }
                ],
                "components" : [
                        {
                                "id" : "786",
                                "name" : "Vulnerability Top Ten - Top 10 Remed
                                "description" : "This table displays the top 1
the network. For each remediation, the risk reduction for the
network if the remediation is implemented is shown, along with the
number of hosts affected. The list is sorted so that the highest
risk reduction is at the top of the list. Implementing the
remediations will decrease the vulnerability of the network.",
                                "order" : "1",
                                "column" : "1"                  },
                        {
                                "id" : "789",
                                "name" : "Vulnerability Top Ten - Top 10 Explo
Vulnerabilities",
                                "description" : "This table displays the top 1
vulnerabilities on the network. The list is sorted so that the most
critical vulnerability is at the top of the list. For each
vulnerability, the severity and the number of hosts affected is
shown.\n\nThis will be helpful for those getting started with
Tenable.sc",
                                "order" : "1",
                                "column" : "2"                  },
                        {
                                "id" : "787",
```

```
                                "name" : "Vulnerability Top Ten - Top 10 Most
                                "description" : "This table displays the 10 ho
that have the greatest number of exploitable critical and high
severity vulnerabilities. The list is sorted so that the most
vulnerable host is at the top of the list. For each host, a bar
graph of its critical and high severity vulnerabilities are shown.",
                                "order" : "1",
                                "column" : "3"                  },
                        {
                                "id" : "1100",
                                "name" : "Track Mitigation Progress - Vulnerab
Severity",
                                "description" : "Tenable.sc records when vulne
discovered, when patches are issued, and when vulnerabilities are
mitigated. This component assists in tracking vulnerability
mitigations. \n\nThe matrix presents vulnerability summary
information by severity. In the matrix, the row with purple is
critical severity vulnerability information, the row with red is
high severity, the row with orange is medium severity, and the row
with blue is low severity. The Mitigated column displays the total
number of mitigated vulnerabilities. The Unmitigated column displays
the total number of vulnerabilities that have not yet been
mitigated. The Exploitable column displays the percentage of those
unmitigated vulnerabilities that are known to be exploitable. The
Patch Available column displays the percentage of the unmitigated,
exploitable vulnerabilities that have had a patch available for more
than 30 days. Ideally, both of these percentages should be 0%,
because all exploitable vulnerabilities and all vulnerabilities with
patches available should have been mitigated already. The
Exploitable Hosts column displays the number of hosts on the network
that have unmitigated, exploitable vulnerabilities.\n\nThe Common
Vulnerability Scoring System (CVSS) is an open industry standard for
assessing the severity of computer system security vulnerabilities;
```


```
it attempts to establish a measure of how much concern a
vulnerability warrants, compared to other vulnerabilities, so
efforts can be prioritized. The Tenable severity levels correspond
to the CVSS scores as follows :  Critical severity = CVSS score
10.0, High = 9.9-7.0, Medium = 6.9-4.0, and Low = 3.9-0.0.",
                                "order" : "2",
                                "column" : "1"                  },
                        {
                                "id" : "1102",
                                "name" : "Detect Changes - Changes in Last 72
                                "description" : "This component assists in ma
date inventories and detecting changes. The matrix presents
indicators for network changes detected in the last 72 hours. Each
indicator is based on one or more Log Correlation Engine (LCE)
events; the indicator is highlighted yellow if the event occurred in
the last 72 hours.\n\n - New Host - New MAC address was detected on
network.\n - New Wireless Host - New wireless MAC address was
detected on network.\n - New Login - A user has logged into a new
host (and\/or a new account type on a host) for the first time, or a
user has logged into a host from a new location for the first
time.\n - New User - New user was detected on network.\n - User
Added - A log was detected indicating a user account was added.\n -
User Removed - A log was detected indicating a user account was
removed or disabled.\n - User Change - A log was detected indicating
a change to a user account.\n - New Software - A log was detected
indicating that software was installed.\n - Software Removed - A log
was detected indicating that software was uninstalled.\n - App
Change - A log was detected indicating a change to an application.\n
- Database Change - A log was detected indicating a change to a
database.\n - File\/Dir Change - A file or directory modification
was detected.\n - Sched. Task Change - A scheduled task modification
was detected.\n - Server Change - A log was detected indicating a
change in a server.\n - Firewall Change - A log was detected
```

indicating a change in a firewall.\n - Network Change - A log was detected indicating a change in the network.\n - Device Change - A log was detected indicating a change in a device.\n - Router Change - A log was detected indicating a change in a router.\n - Switch Change - A log was detected indicating a change in a switch.\n - New Website - A new website hosted on an existing web server was detected.\n - New Connection - A new trust relationship, external connection, and\/or Internet connection was detected.\n - New Open Port - A new open port was detected.\n - Change Spike - A large number of changes, compared to previous change event rates, were detected. If unexpected, this might indicate unauthorized or malicious activity.\n\nAny changes should be investigated to determine if they are authorized. More information can be obtained on these events (such as change details, time, and IP address) by clicking on the specific indicator in the dashboard component and viewing the raw syslog.\n\nNote that some of these events rely on PVS detections being forwarded to the LCE. Make sure that the PVS is configured to send syslog messages to the LCE : in Configuration > PVS Settings > Syslog, include the LCE host (with port 514) in the Realtime Syslog Server List. The LCE listens for syslog messages by default.",
"order" : "2",
"column" : "2" },
{
"id" : "1572",
"name" : "Compliance Summary - FTI Security Gu
9.3.10",
"description" : "This matrix provides a sense
complies with the security guidelines in IRS Publication 1075.
Sections from the Computer System Security chapter of the
Publication are listed. For each section, the equivalent NIST 800-53
controls are displayed, along with the number of network systems
that were audited against these controls, and ratio bars for the

```
percentage of these compliance checks that either passed (green
bar), failed (red bar), or require manual verification (orange bar).
Since the Publication specifically mentions the equivalent NIST 800-
53 controls, the displayed information will give a good sense of how
the network complies with the security guidelines in IRS Publication
1075.",
                                "order" : "2",
                                "column" : "3"                  },
                        {
                                "id" : "1103",
                                "name" : "Monitor Security Solutions - Activit
Hours",
                                "description" : "This component assists in mor
solutions. The matrix presents activity indicators for various
security solutions :  Firewall, IDS, Antivirus, Antispam, and Anti-
scanning. This component assumes that if log events were received in
the last 72 hours from a particular technology, then that technology
is active on the network, so the indicator is highlighted green.
Further investigation is warranted if a protection technology should
be active, but no events are being received.",
                                "order" : "3",
                                "column" : "1"                  },
                        {
                                "id" : "1570",
                                "name" : "Detect Suspicious Activity - Alerts
                                "description" : "This matrix presents warning
potentially suspicious network activity detected in the last 72
hours. Each indicator is based either on one or more Log Correlation
Engine (LCE) events, or on active or passive vulnerability
detections. The indicator is highlighted red if the event occurred
in the last 72 hours.\n\n- Targeted Intrusion - An intrusion attack
was detected that targeted systems and ports likely to be exploited
by the detected attack \n- Botnet Activity - Traffic to or from a
```

known malicious IP address was detected\n- Botnet Vulns - Botnet activity was actively detected\n- Data Leak - Potential data leakage was detected\n- Malware Vulns - Malware was actively or passively detected\n- Malicious Process - A malicious process was actively detected\n- Malicious Content - Malicious hosted web content was actively detected\n- Bad AutoRuns - Windows AutoRun and scheduled task registry entries known to be associated with malware were actively detected\n- Long-Term - Potentially suspicious activity occurring over a long period of time was detected\n- Crowd Surge - A large number of local hosts visiting the same server was detected\n- Long TCP - A TCP session lasting more than a day was detected\n- Large Xfr TCP - A TCP session which transferred more than 1GB was detected\n\nAny warnings should be further investigated. More information can be obtained on these events (such as details, time, and IP address) by clicking on the specific indicator and viewing the raw syslog (for events) or the detailed vulnerability list (for vulnerabilities). \n\nNote that some of these events rely on PVS detections being forwarded to the LCE. Make sure that the PVS is configured to send syslog messages to the LCE : in Configuration > PVS Settings > Syslog, include the LCE host (with port 514) in the Realtime Syslog Server List. The LCE listens for syslog messages by default.",
"order" : "3",
"column" : "2" },
{
"id" : "1573",
"name" : "Compliance Summary - FTI Security Gu
9.3.17",
"description" : "This matrix provides a sense
complies with the security guidelines in IRS Publication 1075.
Sections from the Computer System Security chapter of the
Publication are listed. For each section, the equivalent NIST 800-53
controls are displayed, along with the number of network systems

```
that were audited against these controls, and ratio bars for the
percentage of these compliance checks that either passed (green
bar), failed (red bar), or require manual verification (orange bar).
Since the Publication specifically mentions the equivalent NIST 800-
53 controls, the displayed information will give a good sense of how
the network complies with the security guidelines in IRS Publication
1075.",
                                "order" : "3",
                                "column" : "3"                  },
                        {
                                "id" : "1021",
                                "name" : "SEC Risk Alert - Potential Data Loss
                                "description" : "This matrix displays various
potential for data leakage and loss. Red indicators signify that
activity of high severity has occurred. Green indicators signify
that activity that has the potential for data loss has occurred and
further investigation may be warranted.",
                                "order" : "4",
                                "column" : "1"                  },
                        {
                                "id" : "1571",
                                "name" : "Detect Suspicious Activity - Spikes
                                "description" : "This matrix presents warning
potentially suspicious spikes in network activity detected in the
last 72 hours. Each indicator is based on one or more Log
Correlation Engine (LCE) events. The indicator is highlighted red if
the event occurred in the last 72 hours.\n\n- Firewall Spike - A
large number of firewall events, compared to previous event rates,
were detected\n- Intrusion Spike - A large number of intrusion
events, compared to previous event rates, were detected\n- Virus
Spike - A large number of virus events, compared to previous event
rates, were detected\n- Scanning Spike - A large number of scanning
events (port scans, port sweeps, and probes), compared to previous
```

event rates, were detected\n- Botnet Spike - A large number of threatlist events (traffic to or from known malicious IP addresses), compared to previous event rates, were detected\n- Process Spike - A large number of process events (such as process starts, stops, and crashes), compared to previous event rates, were detected\n- Auth Spike - A large number of login events, compared to previous event rates, were detected\n- Auth Fail Spike - A large number of login failure events, compared to previous event rates, were detected\n- File Access Spike - A large number of remote file access events (such as FTP and SMB transfers, and e-mail attachments), compared to previous event rates, were detected \n- Access Denied Spike - A large number of access denied events (attempts to retrieve objects, files, network shares and other resources that are denied), compared to previous event rates, were detected\n- Web Access Spike - A large number of web access events (successful connections to web resources), compared to previous event rates, were detected\n- Web Error Spike - A large number of web error events (web access events that are denied because the file does not exist, the server responded with an error, or a firewall or web application firewall blocked the access), compared to previous event rates, were detected\n- DNS Spike - A large number of DNS events, compared to previous event rates, were detected\n- Network Spike - A large number of network events, compared to previous event rates, were detected\n- NetFlow Spike - A large number of NetFlow events (detected by the Tenable NetFlow Monitor (TFM)), compared to previous event rates, were detected\n- Connect Spike - A large number of connection events (such as allowed connections through firewalls and established VPN sessions), compared to previous event rates, were detected\n\nAny warnings should be further investigated. More information can be obtained on these events (such as details, time, and IP address) by clicking on the specific indicator and viewing the raw syslog. \n\nNote that some of these events rely on PVS detections being forwarded to the LCE. Make sure that the PVS is

```
configured to send syslog messages to the LCE :  in Configuration >
PVS Settings > Syslog, include the LCE host (with port 514) in the
Realtime Syslog Server List. The LCE listens for syslog messages by
default.",
                                "order" : "4",
                                "column" : "2"                  }
                ],
                "category" : {
                        "id" : "5",
                        "name" : "Compliance & Configuration Assessment",
                        "description" : "Aid with configuration, change and co
management."             }
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1414182834
}
```


/dashboardTemplate/{templateID}/image

Methods

GET

Gets the Dashboard Template image associated with template {templateID}

NOTE: This endpoint is handled before token validation.

Request Query Parameters

None

Example Response

None given. The response will be a raw png file containing the requested Dashboard Template image.

/dashboardTemplate/categories

Methods

GET

Gets the list of Dashboard Template categories

Request Query Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
        "response" : [
                {
                        "id" : "1",
                        "name" : "Threat Detection & Vulnerability Assessments
                        "description" : "Aid with identifying vulnerabilities
potential threats.",
                        "collectionCount" : "74",
                        "collectionStatus" : "new",
                        "componentCount" : "388",
                        "componentStatus" : "new"               },
                {
                        "id" : "2",
                        "name" : "Monitoring",
                        "description" : "Provide intrusion monitoring, alertin
analysis.",
                        "collectionCount" : "48",
                        "collectionStatus" : "new",
                        "componentCount" : "305",
                        "componentStatus" : "new"               },
                {
                        "id" : "3",
```

```
                        "name" : "Security Industry Trends",
                        "description" : "Influenced by trends, reports, and ar
industry leaders.",
                        "collectionCount" : "15",
                        "collectionStatus" : "new",
                        "componentCount" : "90",
                        "componentStatus" : "new"               },
                {
                        "id" : "4",
                        "name" : "Executive",
                        "description" : "Provide operational insight and metri
towards executives.",
                        "collectionCount" : "11",
                        "collectionStatus" : "new",
                        "componentCount" : "70",
                        "componentStatus" : "new"               },
                {
                        "id" : "5",
                        "name" : "Compliance & Configuration Assessment",
                        "description" : "Aid with configuration, change and co
management.",
                        "collectionCount" : "48",
                        "collectionStatus" : "new",
                        "componentCount" : "288",
                        "componentStatus" : "new"               },
                {
                        "id" : "6",
                        "name" : "Discovery & Detection",
                        "description" : "Aid in trust identification,rogue det
new device discovery.",
                        "collectionCount" : "21",
                        "collectionStatus" : "new",
                        "componentCount" : "113",
```

```
                        "componentStatus" : "new"                }
        ],
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1413925223
}
```


Atlassian

Tenable Security Center API: Device Information

/deviceInfo

Methods

GET

Gets the device information for a given host.

NOTE: This will return device information for the first repository. To specify a particular repository, see /repository/{id}/deviceInfo::GET

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*ip
*uuid
*~~repositoryID~~ *(This attribute is not supported as part of fields parameter use repository instead)*
repositories
repository
score
total
severityInfo
severityLow

severityMedium
severityHigh
severityCritical
macAddress
policyName
pluginSet
netbiosName
dnsName
osCPE
biosGUID
tpmID
mcafeeGUID
lastAuthRun
lastUnauthRun
severityAll
os
hasPassive
hasCompliance
lastScan
links

Legend

** = always comes back*

redFont = *field is a JSON object (* ***e.g.*** *"repository" :{ "id" : <id>, "name" : <name> })*

Request Parameters

Expand

Parameters must be passed in as query string (as opposed to JSON) in the format of:
/deviceInfo?uuid="123e4567-e89b-12d3-a456-426655440000" or
/deviceInfo?ip="1.1.1.1"&dnsName="foo"

Parameter "hostUUID" exists

```
hostUUID=<string> (valid uuid)
```

Parameter "hostUUID" is absent and "uuid" is present

```
uuid=<string> (valid uuid)
```

Parameters "hostUUID" and "uuid" absent

```
ip=<string> (valid ip address)
&dnsName=<string> OPTIONAL
```

Parameter "scanResultID" exists

```
scanResultID=<number>
```

Parameter "sourceType" optimization when "scanResultID" is not supplied

```
sourceType=<string> "cumulative" | "patched"
```

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "repositories" : [
                        {
                                "id" : "2",
                                "name" : "Rep2",
                                "description" : "",
                "type": "Remote",
                "uuid": "998E121D-6259-436C-BA06-0289DF9617E9"
                ],
```

```
                "ip" : "192.168.0.1",
                "uuid" : "123e4567-e89b-12d3-a456-426655440000",
                "repositoryID" : "2",
                "score" : "2130",
                "total" : "322",
                "severityInfo" : "110",
                "severityLow" : "7",
                "severityMedium" : "41",
                "severityHigh" : "152",
                "severityCritical" : "12",
                "macAddress" : "00:00:00:00:00:00",
                "policyName" : "",
                "pluginSet" : "",
                "netbiosName" : "TARGET\\WIN7X64",
                "dnsName" : "win7x64.target.domain.com",
                "osCPE" : "cpe:\/o:microsoft:windows_7::gold:x64-ultimate",
                "biosGUID" : "",
                "tpmID" : "",
                "mcafeeGUID" : "",
                "lastAuthRun" : "",
                "lastUnauthRun" : "",
                "severityAll" : "12,152,41,7,110",
                "os" : "Microsoft Windows 7 Ultimate",
                "hasPassive" : "No",
                "hasCompliance" : "No",
                "lastScan" : "1408294249",
                "links" : [
                        {
                                "name" : "SANS",
                                "link" : "https:\/\/isc.sans.edu\/ipinfo.html
},
                        {
                                "name" : "ARIN",
```

```
                                "link" : "http:\/\/whois.arin.net\/rest\/ip\/1
                ],
                "repository" : {
                        "id" : "2",
                        "name" : "Rep2",
                        "description" : "",
            "type": "Remote",
            "uuid": "998E121D-6259-436C-BA06-0289DF9617E9"                }
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1409848524
}
```


Atlassian

Tenable Security Center API: Director Insights

This API resource is only usable in Tenable.sc Director.

/mgmt/insights

Methods

GET

Gets the data required to populate the Director Insights Dashboard.

Fields Parameters

None

Request Parameters

timezone - User timezone

Example Response

Expand


```
{
        "type":"regular",
        "response":{
                "scanResults":[],
                "scanResultsTrend":{
                        "last24Hours":[
                                {
                                        "timestamp":1615550400,
                                        "Completed":3,
                                        "Partial":2,
                                        "Error":1,
                                        "Stopped":0
                                },
                                {
                                        "timestamp":1615546800,
                                        "Completed":0,
                                        "Partial":0,
                                        "Error":0,
                                        "Stopped":1
                                },
                                ...
                                {
                                        "timestamp":1615467600,
                                        "Completed":0,
                                        "Partial":0,
                                        "Error":0,
                                        "Stopped":0
```

```
                        }
                ],
                "last30Days":[
                        {
                                "timestamp":1615420800,
                                "Completed":8,
                                "Partial":2,
                                "Error":,
                                "Stopped":1
                        },
                        {
                                "timestamp":1615334400,
                                "Completed":0,
                                "Partial":0,
                                "Error":0,
                                "Stopped":0
                        },
                        ...
                        {
                                "timestamp":1612915200,
                                "Completed":0,
                                "Partial":0,
                                "Error":0,
                                "Stopped":0
                        }
                ]
        },

        "scannerStatus" : {
                "count":1,
                "status" : {
                        "working":1,
                        "notWorking":0
```

```
                        }
                },
                "scanZoneStatus" : {
                        "count":1,
                        "status" : {
                                "working":1,
                                "degraded":0,
                                "notWorking":0
                        }
                },
                "sciStatus":{
                        "count":1,
                        "status":{
                                "working":1,
                                "notWorking":0
                        }
                },
                "pluginSetAge":{
                        "last24Hours":1,
                        "1-7Days":0,
                        "8-14Days":0,
                        "olderThan14Days":0
                },
                "licenseStatusInformation":{
                        "chart":[{"date":"2021-06-
08","licenseSize":2048,"licensedIPCount":1530},{"date":"2021-06-
07","licenseSize":2048,"licensedIPCount":1530},
                                        {"date":"2021-06-
06","licenseSize":2048,"licensedIPCount":1530},{"date":"2021-06-
05","licenseSize":2048,"licensedIPCount":1530},
                                        {"date":"2021-06-04","licenseSize":204
{"date":"2021-06-03","licenseSize":2048,"licensedIPCount":0},
                                        {"date":"2021-06-02","licenseSize":204
```

```
{"date":"2021-06-01","licenseSize":2048,"licensedIPCount":0},
                                        {"date":"2021-05-31","licenseSize":204
{"date":"2021-05-30","licenseSize":2048,"licensedIPCount":0},
                                        {"date":"2021-05-29","licenseSize":204
{"date":"2021-05-28","licenseSize":2048,"licensedIPCount":0},
                                        {"date":"2021-05-27","licenseSize":0,"
{"date":"2021-05-26","licenseSize":0,"licensedIPCount":0},
                                        {"date":"2021-05-25","licenseSize":0,"
                        "usage":[{"sciName":"demo
sci","licenseSize":"2048","licensedIPCount":"1530"}]
                }
        },
        "error_code":0,
        "error_msg":"",
        "warnings":[],
        "timestamp":1615554605
}
```


Atlassian

Tenable Security Center API: Director Organization

This API resource is only available for administrators in Tenable.sc Director.

/mgmt/organization

Methods

GET

Gets the list of Organizations.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
*sci
**sciOrganization
**name
**description
email
address
city
state
country
phone
fax
ipInfoLinks
zoneSelection
restrictedIPs
vulnScoreLow
vulnScoreMedium
vulnScoreHigh
vulnScoreCritical
vulnScoringSystem
createdTime
modifiedTime
userCount
lces
repositories
zones
nessusManagers
pubSites
ldaps

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

Request Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
        "response" : [
                {
                        "id" : "8",
                        "sciOrgID": "1",
                        "name" : "Org",
                        "description" : "New Org",
                        "SCI": {
                                "id": "3",
                                "name": "ChildSCI",
                                "description": "SCI example description"
                        "email" : "",
                        "address" : "",
                        "city" : "",
                        "state" : "",
                        "country" : "",
                        "phone" : "",
                        "fax" : "",
                        "ipInfoLinks" : [
                                {
                                        "name" : "SANS",
                                        "link" : "https:\/\/isc.sans.edu\/ipi
                                {
                                        "name" : "ARIN",
                                        "link" : "http:\/\/whois.arin.net\/res
                        ],
                        "zoneSelection" : "auto_only",
```

```
                "restrictedIPs" : "192.168.1.1",
                "vulnScoreLow" : "1",
                "vulnScoreMedium" : "3",
                "vulnScoreHigh" : "10",
                "vulnScoreCritical" : "40",
                "vulnScoringSystem" : "CVSSv2",
                "createdTime" : "1406321214",
                "modifiedTime" : "1414509795",
                "userCount" : "4",
                "lces" : [
                        {
                                "id" : "3",
                                "name" : "LCE 192.168.1.1",
                                "description" : "Copied from Box for t
                        {
                                "id" : "4",
                                "name" : "NEW LCE",
                                "description" : "Copied from Box for t
                        {
                                "id" : "5",
                                "name" : "qa-lce4x-lifeA",
                                "description" : "Copied from Box for t
                ],
                "repositories" : [
                        {
                                "id" : "25",
                                "name" : "IPv6 Rep",
                                "description" : "",
                                "type" : "Local",
                                "dataFormat" : "IPv6",
                                "groupAssign" : "fullAccess"
                        {
                                "id" : "26",
```

```
                                "name" : "agrepo",
                                "description" : "",
                                "type" : "Local",
                                "dataFormat" : "IPv4",
                                "groupAssign" : "fullAccess"
                        {
                                "id" : "27",
                                "name" : "mp asset tests IPv6",
                                "description" : "Copied from QA",
                                "type" : "Local",
                                "dataFormat" : "IPv6",
                                "groupAssign" : "fullAccess"
                        {
                                "id" : "29",
                                "name" : "Test IPv6",
                                "description" : "",
                                "type" : "Local",
                                "dataFormat" : "IPv6",
                                "groupAssign" : "fullAccess"
                ],
                "zones" : [],
                "ldaps" : [],
                "pubSites" : [
                        {
                                "id":"2","name":"Test1","description"
                ]
        },
        {
                "id" : "9",
                "sciOrgID": "2",
                "name" : "Test Org 1",
                "description" : "",
                "SCI": {
```

```
                "id": "3",
                "name": "ChildSCI",
                "description": "SCI example description"
        "email" : "",
        "address" : "",
        "city" : "",
        "state" : "",
        "country" : "",
        "phone" : "",
        "fax" : "",
        "ipInfoLinks" : [
                {
                        "name" : "SANS",
                        "link" : "https:\/\/isc.sans.edu\/ipi
                {
                        "name" : "ARIN",
                        "link" : "http:\/\/whois.arin.net\/re
        ],
        "zoneSelection" : "auto_only",
        "restrictedIPs" : "",
        "vulnScoreLow" : "1",
        "vulnScoreMedium" : "3",
        "vulnScoreHigh" : "10",
        "vulnScoreCritical" : "40",
        "vulnScoringSystem" : "CVSSv2",
        "createdTime" : "1409944744",
        "modifiedTime" : "1414521257",
        "userCount" : "1",
        "lces" : [],
        "repositories" : [
                {
                        "id" : "25",
                        "name" : "IPv6 Rep",
```

```
                                        "description" : "",
                                        "type" : "Local",
                                        "dataFormat" : "IPv6",
                                        "groupAssign" : "all"
                                    {
                                        "id" : "26",
                                        "name" : "agrepo",
                                        "description" : "",
                                        "type" : "Local",
                                        "dataFormat" : "IPv4",
                                        "groupAssign" : "all"
                                    {
                                        "id" : "27",
                                        "name" : "mp asset tests IPv6",
                                        "description" : "Copied from QA",
                                        "type" : "Local",
                                        "dataFormat" : "IPv6",
                                        "groupAssign" : "all"
                            ],
                            "zones" : [],
                            "ldaps" : [],
                            "nessusManagers" : [],
                            "pubSites" : []
                    }
            ],
            "error_code" : 0,
            "error_msg" : "",
            "warnings" : [],
            "timestamp" : 1418050287
    }
```


/mgmt/organization/{id}

Methods

GET

Gets the Organization associated with {id}.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
*sci
**sciOrganization
**name
**description
email
address
city
state
country
phone
fax
ipInfoLinks
zoneSelection
restrictedIPs
vulnScoreLow
vulnScoreMedium
vulnScoreHigh
vulnScoreCritical
vulnScoringSystem
createdTime
modifiedTime
userCount
lces
repositories

zones
nessusManagers
pubSites
ldaps

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

Request Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
        "response" : {
                "id" : "8",
                "sciOrgID": "1",
                "name" : "Org",
                "description" : "Testing for Policies with New Schema",
                "email" : "",
                "address" : "",
                "city" : "",
                "state" : "",
                "country" : "",
                "phone" : "",
                "fax" : "",
                "ipInfoLinks" : [
                        {
                                "name" : "SANS",
                                "link" : "https:\/\/isc.sans.edu\/ipinfo.html
```

```
                {
                        "name" : "ARIN",
                        "link" : "http:\/\/whois.arin.net\/rest\/ip\/%
        ],
        "zoneSelection" : "auto_only",
        "restrictedIPs" : "192.168.1.1",
        "vulnScoreLow" : "1",
        "vulnScoreMedium" : "3",
        "vulnScoreHigh" : "10",
        "vulnScoreCritical" : "40",
        "vulnScoringSystem" : "CVSSv2",
        "createdTime" : "1406321214",
        "modifiedTime" : "1414509795",
        "SCI": {
                "id": "3",
                "name": "ChildSCI",
                "description: "SCI example description"         },
        "userCount" : "4",
        "lces" : [
                {
                        "id" : "3",
                        "name" : "LCE 192.168.1.1",
                        "description" : "Copied from Box for testing"
                {
                        "id" : "4",
                        "name" : "NEW LCE",
                        "description" : "Copied from Box for testing"
                {
                        "id" : "5",
                        "name" : "qa-lce4x-lifeA",
                        "description" : "Copied from Box for testing"
        ],
        "repositories" : [
```

```
                {
                        "id" : "25",
                        "name" : "IPv6 Rep",
                        "description" : "",
                        "type" : "Local",
                        "dataFormat" : "IPv6",
                        "groupAssign" : "fullAccess"
                {
                        "id" : "26",
                        "name" : "agrepo",
                        "description" : "",
                        "type" : "Local",
                        "dataFormat" : "IPv4",
                        "groupAssign" : "fullAccess"
                {
                        "id" : "27",
                        "name" : "mp asset tests IPv6",
                        "description" : "Copied from QA",
                        "type" : "Local",
                        "dataFormat" : "IPv6",
                        "groupAssign" : "fullAccess"
                {
                        "id" : "29",
                        "name" : "Test IPv6",
                        "description" : "",
                        "type" : "Local",
                        "dataFormat" : "IPv6",
                        "groupAssign" : "fullAccess"
        ],
        "zones" : [],
        "ldaps" : [],
        "nessusManagers" : [],
        "pubSites" : [
```

```
                        {
                                "id":"2","name":"Test1","description":"","type
                ]
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1418050303
}
```


Atlassian

Tenable Security Center API: Director Repository

This API resource is only available for administrators in Tenable.sc Director.

/mgmt/repository

Methods

GET

Gets the list of Repositories for the specified SCI linked to Director or all SCIs if no parameter is specified.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
*uuid
*running
*type
*dataFormat
*SCI

**name
**description
createdTime
downloadFormat
lastSyncTime
remoteID
remoteIP
sciRepID
vulnCount

Legend

** = always comes back*

*** = comes back if fields list not specified*

red = *field is a JSON object (* ***e.g.*** *"SCI" : {"id" : "2", "name" : "SCI Name", "description" : "Description"})*

Request Parameters

Expand

Parameters can be passed in as a query string if specified in the format of: /mgmt/repository?sciID=<id> or in the request as JSON.

Optional

```
{
        "sciID" : <number>}
```

Example Response

Expand

No query parameters specified to get all SCI Repositories.

```
{
    "error_code": 0,
```

```
    "error_msg": "",
    "response": [
        {
            "id": "4",
            "uuid": "14556FF6-034F-453A-935A-82B5682FE3E7",
            "name": "Local IPv4 Repository",
            "description": "",
            "dataFormat": "IPv4",
            "type": "Local",
            "running": "false",
            "SCI": {
                "id": "2",
                "name": "SCI 1",
                "description": ""            }
        },
        {
            "id": "6",
            "uuid": "1A9E688C-FAFD-46A6-B97E-A9D4E6E2BAD4",
            "name": "Agent Repository",
            "description": "",
            "dataFormat": "agent",
            "type": "Local",
            "running": "false",
            "SCI": {
                "id": "3",
                "name": "SCI 1"                "description": ""
       }
        }
    ],
    "timestamp": 1643230109,
    "type": "regular",
    "warnings": []
}
```


Query parameter specified for SCI #3: /mgmt/repository?sciID=3

```
{
    "error_code": 0,
    "error_msg": "",
    "response": [
        {
            "id": "6",
            "uuid": "1A9E688C-FAFD-46A6-B97E-A9D4E6E2BAD4",
            "name": "Agent Repository",
            "description": "",
            "dataFormat": "agent",
            "type": "Local",
            "running": "false",
            "SCI": {
                "id": "3",
                "name": "SCI 1"                "description": ""
       }
        }
    ],
    "timestamp": 1643230109,
    "type": "regular",
    "warnings": []
}
```


/mgmt/repository/{id}

/mgmt/repository/{uuid}

Methods

GET

Gets the SCI Repository associated with {id} or {uuid} on Director.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
*uuid
*running
*type
*dataFormat
***SCI**
**name
**description
**createdTime
**downloadFormat
**lastSyncTime
**remoteID
**remoteIP
**sciRepID
**vulnCount

Legend

** = always comes back*

*** = comes back if fields list not specified*

***red =** field is a JSON object (**e.g.** "SCI" : {"id" : "2", "name" : "SCI Name", "description" : "Description"})*

Request Parameters

None

Example Response

Expand

```
{
    "error_code": 0,
    "error_msg": "",
    "response": [
        {
            "id": "6",
            "uuid": "1A9E688C-FAFD-46A6-B97E-A9D4E6E2BAD4",
            "name": "Agent Repository",
            "description": "",
            "type": "Local",
            "SCI": {
                "id": "3",
                "name": "SCI 1"                "description": ""
       },
                        "sciRepID": "3",
            "dataFormat": "agent",
                        "vulnCount": "0",
                        "remoteID": "",
                        "remoteIP": "",
            "running": "false",
                        "downloadFormat": "v2",
                        "lastSyncTime": "1638811912",
                        "createdTime": "1639149484"        }
    ],
    "timestamp": 1643230109,
    "type": "regular",
    "warnings": []
}
```


Atlassian

Tenable Security Center API: Director Scan

This API resource is only available for administrators in Tenable.sc Director.

/mgmt/scan

Methods

GET

Gets the list of Scans for the specified SCI linked to Director or all SCIs if no parameter is specified.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
*uuid
**name
**description
**status
**SCI
**organization
sciScanID
policy
creator
owner
repository
zone
plugin
type
ipList
dhcpTracking
classifyMitigatedAge
emailOnLaunch
emailOnFinish
timeoutAction
scanningVirtualHosts
rolloverType
status
maxScanTime

inactivityTimeout
createdTime
modifiedTime

Legend

** = always comes back*

*** = comes back if fields list not specified*

red = *field is a JSON object (* ***e.g.*** *"SCI" : {"id" : "2", "name" : "SCI Name", "description" : "Description"})*

Request Parameters

Expand

Parameters can be passed in as a query string if specified in the format of: /mgmt/scan?sciID=<id> or in the request as JSON.

Optional

```
{
        "sciID" : <number>,
    "orgID" : <number>}
```

Example Response

Expand

No query parameters specified to get all SCI Scans.

```
{
    "error_code": 0,
    "error_msg": "",
    "response": [
        {
            "id": "2",
            "uuid": "6821F741-EF4C-46BA-98AA-E1CD93456220",
```

```
            "name": "Basic Scan",
            "description": "",
            "status": "0",
            "SCI": {
                "id": "2",
                "name": "SCI 1",
                "description": ""            },
            "organization": {
                "id": "2",
                "name": "Org 1",
                "description": ""            }
        },
        {
            "id": "5",
            "uuid": "09698C92-B1A2-4526-BA9F-4B4A6B0F81BE",
            "name": "Advanced Scan",
            "description": "",
            "status": "0",
            "SCI": {
                "id": "3",
                "name": "SCI 2"               "description": ""
       },
            "organization": {
                "id": "3",
                "name": "Org 2",
                "description": ""            }
        }
    ],
    "timestamp": 1643230109,
    "type": "regular",
    "warnings": []
}
```


Query parameter specified for SCI #3: /mgmt/scan?sciID=3

```
{
    "error_code": 0,
    "error_msg": "",
    "response": [
        {
            "id": "5",
            "uuid": "09698C92-B1A2-4526-BA9F-4B4A6B0F81BE",
            "name": "Advanced Scan",
            "description": "",
            "status": "0",
            "SCI": {
                "id": "3",
                "name": "SCI 2"                "description": ""
       },
            "organization": {
                "id": "3",
                "name": "Org 2",
                "description": ""           }
        }
    ],
    "timestamp": 1643230109,
    "type": "regular",
    "warnings": []
}
```


POST

Adds a Scan to the specified SCI.

Request Parameters

Expand


```
{
       "name" : <string>,
```

```
       "type" : <string> DEFAULT "policy",
    "description" : <string> DEFAULT "",
       "sciID" : <number>,
    "userUUID" : <string>,
    "policyUUID" : <string>,
    "repositoryUUID" : <string>,
    "zoneUUID" : <string> DEFAULT "",
    "dhcpTracking" : <string> DEFAULT "false",
    "classifyMitigatedAge" : <number> DEFAULT "0",
    "schedule" : {
        "type" : "dependent" | "ical" | "never" | "rollover" |
"template" <string> DEFAULT "template"        "start" : <string>
(This value takes the iCal format),
        "repeatRule" : <string> (This value takes the repeat rule
format),
        "enabled" : <string> "false" | "true" DEFAULT "true"    },
    "assets" : [
        {
            "id" : <number>        }...
    ] DEFAULT [],
    "emailOnLaunch" : <string> "false" | "true" DEFAULT "false",
    "emailOnFinish" : <string> "false" | "true" DEFAULT "false",
    "timeoutAction" : <string> "discard" | "import" | "rollover"
DEFAULT "import",
    "scanningVirtualHosts" : <string> "false" | "true" DEFAULT
"false",
    "rolloverType" : <string> "nextDay" | "template" DEFAULT
"template",
    "ipList" : <string> DEFAULT "",
    "maxScanTime" : <number> DEFAULT "3600",
       "inactivityTimeout" : <number> DEFAULT "12"}
```

Example Response

Expand

```
{
        "type": "regular",
        "response": {
                "id": "43",
                "uuid": "B0DD6E59-850B-421B-9498-74DE0177CF64",
                "ownerUUID": "F7791B94-A722-4C77-A722-7529CF19D68D",
                "creatorUUID": "F7791B94-A722-4C77-A722-7529CF19D68D",
                "name": "Basic Scan",
                "description": "Description",
                "sciScanID": "1",
                "ipList": "192.26.28.0/24",
                "type": "policy",
                "policyUUID": "91E02A57-505A-4BF6-95B0-AA4C5CCBFBDC",
                "pluginID": "-1",
                "repositoryUUID": "6ED5492E-0D90-401B-892D-D1DAF28EAC12",
                "zoneUUID": "",
                "dhcpTracking": "true",
                "classifyMitigatedAge": "0",
                "emailOnLaunch": "false",
                "emailOnFinish": "false",
                "timeoutAction": "rollover",
                "scanningVirtualHosts": "false",
                "rolloverType": "template",
                "status": "0",
                "maxScanTime": "unlimited",
                "inactivityTimeout": "12",
                "createdTime": "1646429871",
                "modifiedTime": "1646433443",
                "SCI": {
                        "id": "4",
                        "name": "SCI 3",
                        "description": ""               },
                "organization": {
```

```
                        "id": "3",
                        "name": "Org 4",
                        "description": ""                }
        },
        "error_code": 0,
        "error_msg": "",
        "warnings": [],
        "timestamp": 1647528708
}
```


/mgmt/scan/{id}

/mgmt/scan/{uuid}

Methods

GET

Gets the SCI Scan associated with {id} or {uuid} on Director.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
*uuid
**name
**description
**status
**SCI
**organization
**sciScanID
**policy

**creator
**owner
**repository
**zone
**plugin
**type
**ipList
**dhcpTracking
**classifyMitigatedAge
**emailOnLaunch
**emailOnFinish
**timeoutAction
**scanningVirtualHosts
**rolloverType
**status
**maxScanTime
**inactivityTimeout
**createdTime
**modifiedTime

Legend

** = always comes back*

*** = comes back if fields list not specified*

red = *field is a JSON object (* ***e.g.*** *"SCI" : {"id" : "2", "name" : "SCI Name", "description" : "Description"})*

Request Parameters

None

Example Response

Expand

```
{
        "type": "regular",
        "response": {
                "id": "43",
                "uuid": "B0DD6E59-850B-421B-9498-74DE0177CF64",
                "ownerUUID": "F7791B94-A722-4C77-A722-7529CF19D68D",
                "creatorUUID": "F7791B94-A722-4C77-A722-7529CF19D68D",
                "name": "Basic Scan",
                "description": "Description",
                "sciScanID": "1",
                "ipList": "192.26.28.0/24",
                "type": "policy",
                "policyUUID": "91E02A57-505A-4BF6-95B0-AA4C5CCBFBDC",
                "pluginID": "-1",
                "repositoryUUID": "6ED5492E-0D90-401B-892D-D1DAF28EAC12",
                "zoneUUID": "",
                "dhcpTracking": "true",
                "classifyMitigatedAge": "0",
                "emailOnLaunch": "false",
                "emailOnFinish": "false",
                "timeoutAction": "rollover",
                "scanningVirtualHosts": "false",
                "rolloverType": "template",
                "status": "0",
                "maxScanTime": "unlimited",
                "inactivityTimeout": "12"               "createdTime": "16464
                "modifiedTime": "1646433443",
                "SCI": {
                        "id": "4",
                        "name": "SCI 3",
                        "description": ""               },
                "organization": {
                        "id": "3",
```

```
                        "name": "Org 4",
                        "description": ""                }
        },
        "error_code": 0,
        "error_msg": "",
        "warnings": [],
        "timestamp": 1647528708
}
```


DELETE

Deletes the Scan associated with {id} or {uuid} on Director.

Request Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
        "response" : "",
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1408733643
}
```


Atlassian

Tenable Security Center API: Director Scanner

This API resource is only usable in Tenable.sc Director.

/mgmt/scanner

Methods

GET

Gets the list of Scanners. A Director Scanner is a Director's copy of a Scanner from a SCI.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
**name
**description
ip
port
*SCI
sciScannerID
useProxy
enabled
verifyHost
managePlugins
*authType
cert
username
password
**agentCapable
accessKey
secretKey
version
webVersion
admin
msp
numScans
numHosts
numSessions

numTCPSessions
loadAvg
uptime
*status
pluginSet
loadedPluginSet
serverUUID
createdTime
modifiedTime
zones
nessusManagerOrgs
certInfo
eolDate
eouDate

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

Request Parameters

None

Example Response

Expand

```
{
        "type":"regular",
        "response":[
                {
                        "name":"172.26.102.241",
                        "ip":"172.26.102.241",
```

```
                "port":"8834",
                "version":"8.13.1",
                "status":"1",
                "uptime":"5617814",
                "modifiedTime":"1616049747",
                "msp":"false",
                "admin":"false",
                "agentCapable":"false",
                "pluginSet":"202103122332",
                "id":"1",
                "authType":"password",
                "eolDate":1672444800,
                "SCI":{
                        "id":"2",
                        "name":"172.26.103.72",
                        "description":"Update"                  }
        },
        {
                "name":"96",
                "ip":"172.26.103.96",
                "port":"8834",
                "version":"8.13.1",
                "status":"1",
                "uptime":"4146250",
                "modifiedTime":"1616061157",
                "msp":"false",
                "admin":"false",
                "agentCapable":"false",
                "pluginSet":"202103122332",
                "id":"2",
                "authType":"certificate",
                "eolDate":1672444800,
                "SCI":{
```

```
                                "id":"2",
                                "name":"172.26.103.72",
                                "description":"Update"                    }
                }
        ],
        "error_code":0,
        "error_msg":"",
        "warnings":[],
        "timestamp":1616326074
}
```


POST

Adds a Scanner to an SCI.

Request Parameters

Expand

```
{
    "name" : <string>,
    "description" : <string> DEFAULT "",
    "authType" : <string> "certificate" | "password" DEFAULT
"password",
    "ip" : <string>,
    "port" : <number>,
    "useProxy" : <string> "true" | "false" DEFAULT "false",
    "verifyHost" : <string> "true" | "false" DEFAULT "true",
    "enabled" : <string> "true" | "false" DEFAULT "true",
    "managePlugins" : <string> "true" | "false" DEFAULT "false",
    "agentCapable" : <string> "true" | "false" DEFAULT "false",
    "sciID" : <number>    "zones" : [
        {
            "id" : <number>        }...
    ] DEFAULT [],
```

```
    "nessusManagerOrgs" : [
        {
            "id" : <number>        }...
    ] DEFAULT [],
    "accessKey" : <string> DEFAULT "",
    "secretKey" : <string> DEFAULT ""...
}
```

authType "certificate"

```
...
       "cert" : <string>,
       "password" : <string> DEFAULT "",
...
```

authType "password"

```
...
       "username" : <string>,
       "password" : <string>...
```

Example Response

Expand

```
{
       "type":"regular",
       "response":{
              "id":"3",
              "name":"NewScanner",
              "description":"NewScanner",
              "ip":"172.1.2.3",
              "port":"8834",
              "sciID":"2",
```

```
            "sciScannerID":"3",
            "useProxy":"false",
            "enabled":"true",
            "verifyHost":"false",
            "managePlugins":"false",
            "authType":"password",
            "cert":null,
            "username":"nonadmin",
            "password":"SET",
            "agentCapable":"false",
            "version":null,
            "webVersion":null,
            "admin":"false",
            "msp":"false",
            "numScans":"0",
            "numHosts":"0",
            "numSessions":"0",
            "numTCPSessions":"0",
            "loadAvg":"0.0",
            "uptime":"-1",
            "status":"8192",
            "pluginSet":null,
            "loadedPluginSet":null,
            "serverUUID":null,
            "accessKey":null,
            "secretKey":null,
            "createdTime":"1616328669",
            "modifiedTime":"1616328669",
            "eolDate":-1,
            "eouDate":-1
        },
        "error_code":0,
        "error_msg":"",
```

```
        "warnings":[],
        "timestamp":1616328669
}
```


/mgmt/scanner/{id}

Methods

GET

Gets the Scanner associated with Director {id}.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
**name
**description
ip
port
*SCI
sciScannerID
useProxy
enabled
verifyHost
managePlugins
*authType
cert
username
password
**agentCapable
accessKey
secretKey

version
webVersion
admin
msp
numScans
numHosts
numSessions
numTCPSessions
loadAvg
uptime
*status
pluginSet
loadedPluginSet
serverUUID
createdTime
modifiedTime
zones
nessusManagerOrgs
certInfo
eolDate
eouDate

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

Request Parameters

None

Example Response

Expand

```
{

        "type":"regular",
        "response":{
                "authType":"password",
                "admin":"false",
                "useProxy":"false",
                "verifyHost":"false",
                "enabled":"true",
                "cert":"",
                "username":"admin",
                "password":"SET",
                "description":"",
                "createdTime":"1616049747",
                "loadedPluginSet":"202103122332",
                "pluginSet":"202103122332",
                "webVersion":"8.13.1 (Build 257)",
                "version":"8.13.1",
                "agentCapable":"false",
                "accessKey":"",
                "secretKey":"",
                "msp":"false",
                "loadAvg":"0.0",
                "numHosts":"0",
                "numScans":"0",
                "numSessions":"0",
                "numTCPSessions":"0",
                "serverUUID":"fa3e3f8e-6d15-0c5d-0b95-
691c22b9a06179f48589955bc7aa",
                "name":"172.26.102.241",
                "ip":"172.26.102.241",
                "port":"8834",
                "status":"1",
```

```
                "uptime":"5618713",
                "modifiedTime":"1616049747",
                "id":"1",
                "eolDate":1672444800,
                "zones":[
                        {
                                "id":"1",
                                "name":"Default Scan Zone",
                                "description":""                        }
                ],
                "nessusManagerOrgs" : [
                        {
                                "id" : "1",
                                "name" : "My Org",
                                "description" : ""                      }
                ]
                "SCI":{
                        "id":"2",
                        "name":"172.26.103.72",
                        "description":"Update"          }
        },
        "error_code":0,
        "error_msg":"",
        "warnings":[],
        "timestamp":1616326821
}
```


PATCH

Edits the Scanner associated with Director{id}, changing only the passed in fields.

Request Parameters

(All fields are optional)

See /scanner::POST for parameters.

Note: The `sciID` is not changeable on a Director Scanner.

Example Response

See /scanner/{id}/::GET

DELETE

Deletes the Scanner associated with Director {id}.

Request Parameters

None

Example Response

Expand

```
{
        "type" : "regular",
        "response" : "",
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1402436001
}
```

Atlassian

Tenable Security Center API: Director Scan Policy

This API resource is only available for administrators in Tenable.sc Director.

/mgmt/policy

Methods

GET

Gets the list of Scan Policies for the specified SCI linked to Director or all SCIs if no parameter is specified.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
*uuid
**name
**description
**orgUUID
**status
**SCI
sciPolicyID
policyTemplateID
creatorUUID
ownerUUID
context
tags
createdTime
modifiedTime
generateXCCDFResults
preferences
families
organization

Legend

** = always comes back*

*** = comes back if fields list not specified*

***red =** field is a JSON object (**e.g.** "SCI" : {"id" : "2", "name" : "SCI Name", "description" : "Description"})*

Request Parameters

Expand

Parameters can be passed in as a query string if specified in the format of: /mgmt/policy?sciID=<id> or in the request as JSON.

Optional

```
{
        "sciID" : <number>}
```

Example Response

Expand

No query parameters specified to get all SCI Scan Policies.

```
{
    "error_code": 0,
    "error_msg": "",
    "response": [
        {
            "id": "2",
            "uuid": "6821F741-EF4C-46BA-98AA-E1CD93456220",
            "name": "Basic Scan Policy",
            "description": "",
            "orgUUID": "00000000-0000-0000-0000-000000000000",
            "status": "0",
            "SCI": {
                "id": "2",
                "name": "SCI 1",
                "description": ""            }
        },
        {
            "id": "5",
            "uuid": "09698C92-B1A2-4526-BA9F-4B4A6B0F81BE",
            "name": "Advanced Scan Policy",
```

```
            "description": "",
            "orgUUID": "00000000-0000-0000-0000-000000000000",
            "status": "0",
            "SCI": {
                "id": "3",
                "name": "SCI 1"                "description": ""
       }
        }
    ],
    "timestamp": 1643230109,
    "type": "regular",
    "warnings": []
}
```


Query parameter specified for SCI #3: /mgmt/policy?sciID=3


```
{
    "error_code": 0,
    "error_msg": "",
    "response": [
        {
            "id": "5",
            "uuid": "09698C92-B1A2-4526-BA9F-4B4A6B0F81BE",
            "name": "Advanced Scan Policy",
            "description": "",
            "orgUUID": "00000000-0000-0000-0000-000000000000",
            "status": "0",
            "SCI": {
                "id": "3",
                "name": "SCI 1"                "description": ""
       }
        }
    ],
    "timestamp": 1643230109,
```

```
    "type": "regular",
    "warnings": []
}
```

POST

Adds a Scan Policy to the specified SCI.

NOTE: To specify a *mixed* Plugin Family, the *plugins* field must be present; otherwise, the family type defaults to *enabled*.

Request Parameters

Expand

```
{
       "name" : <string>,
    "description" : <string> DEFAULT "",
       "sciID" : <number>,
    "tags" : <string> DEFAULT "",
    "preferences" : [
        <string:name> : <string:value>...
    ] DEFAULT [],
    "auditFiles" : [
        {
            "id" : <number>        }...
    ] DEFAULT [],
    "policyTemplate" : {
        "id" : <number>    },
    "generateXCCDFResults" : <string> "false" | "true" DEFAULT
"false"}
```

policyTemplate ID "1" (Advanced Scan Template) or "25" (Advanced Agent Scan Template)

```
...
       "families" : [
```

```
                {
                        "id" : <number>,
                        "plugins" : [
                                {
                                        "id" : <number>
                        ] OPTIONAL (must be specified to effect a "mixed" Plug
type)
                }...
        ] DEFAULT []
...
```

Example Response

Expand

```
{
        "type": "regular",
        "response": {
                "id": "5",
                "uuid": "09698C92-B1A2-4526-BA9F-4B4A6B0F81BE",
                "name": "Advanced Scan Policy",
                "description": "",
                "orgUUID": "00000000-0000-0000-0000-000000000000",
                "sciPolicyID": "2",
                "policyTemplateID": "1",
                "creatorUUID": "B87BBF5A-00DD-4CAE-887F-D63F5363E136",
                "ownerUUID": null,
                "context": "",
                "tags": "",
                "status": "0",
                "createdTime": "1646752467",
                "modifiedTime": "1646752467",
                "generateXCCDFResults": "false",
                "preferences": {
```

```
                "preference1": "value1",
                "preference2": "value2"         },
        "families": [
                {
                        "familyID": "1",
                        "type": "enabled",
                        "name": "Red Hat Local Security Checks"
                {
                        "familyID": "35",
                        "type": "enabled",
                        "name": "Backdoors",
                        "plugins": [
                                {
                                        "pluginID": "10132",
                                        "name": "Kuang2 the Virus Dete
                                        "description": "Kuang2 the Vi
                                        "type": "active"
                        ]
                }
        ]
        "SCI": {
                "id": "3",
                "name": "SCI 2",
                "description": ""               },
        "organization": {
                "id": "0",
                "name": "Administrator",
                "description": ""               }
},
"error_code": 0,
"error_msg": "",
"warnings": [],
"timestamp": 1615928574
```

```
}
```

/mgmt/policy/{id}

/mgmt/policy/{uuid}

Methods

GET

Gets the SCI Scan Policy associated with {id} or {uuid} on Director.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
*uuid
**name
**description
**orgUUID
**status
**SCI
**sciPolicyID
**policyTemplateID
**creatorUUID
**ownerUUID
**context
**tags
**createdTime
**modifiedTime
**generateXCCDFResults
**preferences

**families
**organization

Legend

** = always comes back*

*** = comes back if fields list not specified*

red = *field is a JSON object (* ***e.g.*** *"SCI" : {"id" : "2", "name" : "SCI Name", "description" : "Description"})*

Request Parameters

None

Example Response

Expand


```
{
        "type": "regular",
        "response": {
                "id": "5",
                "uuid": "09698C92-B1A2-4526-BA9F-4B4A6B0F81BE",
                "name": "Advanced Scan Policy",
                "description": "",
                "orgUUID": "00000000-0000-0000-0000-000000000000",
                "sciPolicyID": "2",
                "policyTemplateID": "1",
                "creatorUUID": "B87BBF5A-00DD-4CAE-887F-D63F5363E136",
                "ownerUUID": null,
                "context": "",
                "tags": "",
                "status": "0",
                "createdTime": "1646752467",
                "modifiedTime": "1646752467",
                "generateXCCDFResults": "false",
```

```
            "preferences": {
                    "preference1": "value1",
                    "preference2": "value2"         },
            "families": [
                    {
                            "familyID": "1",
                            "type": "enabled",
                            "name": "Red Hat Local Security Checks"
                    {
                            "familyID": "35",
                            "type": "enabled",
                            "name": "Backdoors",
                            "plugins": [
                                    {
                                            "pluginID": "10132",
                                            "name": "Kuang2 the Virus Dete
                                            "description": "Kuang2 the Vi
                                            "type": "active"
                            ]
                    }
            ]
            "SCI": {
                    "id": "3",
                    "name": "SCI 2",
                    "description": ""               },
            "organization": {
                    "id": "0",
                    "name": "Administrator",
                    "description": ""               }
    },
    "error_code": 0,
    "error_msg": "",
    "warnings": [],
```

```
        "timestamp": 1615928574
}
```


DELETE

Deletes the Scan Policy associated with {id} or {uuid} on Director.

Request Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
        "response" : "",
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1408733643
}
```


Atlassian

Tenable Security Center API: Director Scan Result

This API resource is only usable in Tenable.sc Director.

/mgmt/scanResult

Methods

GET

Gets the list of Director Scan Results. A Director Scan Result is Director's copy of a Scan Result from a SCI.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
initiator
owner
scan
resultsSync
**sci
**sciOrganization
**sciScanResult
retrievalStatus
job
repository
**name
**description
details
**status
importStatus
importStart
importFinish
importDuration
ioSyncStatus
ioSyncStart
ioSyncFinish
diagnosticAvailable
downloadAvailable
downloadFormat
dataFormat
resultType
resultSource
running
errorDetails

importErrorDetails
ioSyncErrorDetails
pluginSet
agentScanUUID
totalIPs
scannedIPs
completedIPs
completedChecks
totalChecks
startTime
finishTime
createdTime
scanDuration
timeCompareField

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

Request Parameters

Expand

NOTE: The 'startTime' and 'endTime' parameters search against the field specified in the 'timeCompareField' parameter. By default this is set to 'createdTime'

```
{
        "startTime" : <number:epoch> DEFAULT {now-30 days},
        "endTime" : <number:epoch> DEFAULT {now}
}
```

Filter Parameters

running - Only Scan Results that are currently running will be returned. By default, both running and completed Scan Results are returned.

completed - Only Scan Results that have completed will be returned. By default, both running and completed Scan Results are returned.

Example Response

Expand


```
{
  "type": "regular",
  "response": [
    {
      "status": "Completed",
      "name": "Daily compliance scan",
      "details": "PCI DSS 3.0 - Microsoft Windows Audit",
      "diagnosticAvailable": "false",
      "importStatus": "Finished",
      "createdTime": "1614904201",
      "startTime": "1614904207",
      "finishTime": "1614904269",
      "importStart": "1614904273",
      "importFinish": "1614904276",
      "running": "false",
      "totalIPs": "1",
      "scannedIPs": "1",
      "completedIPs": "1",
      "completedChecks": "190",
      "totalChecks": "190",
      "dataFormat": "IPv4",
      "downloadAvailable": "true",
      "downloadFormat": "v2",
      "resultType": "active",
      "resultSource": "internal",
      "scanDuration": "62",
      "id": "37",
```

```
      "scanID": "",
      "jobID": "4967",
      "SCI": {
        "id": "3",
        "name": "Managed SCI - 192.2.0.2",
        "description": "2"      },
      "owner": {
        "id": "1672",
        "firstname": "",
        "lastname": "",
        "username": "testuser"      },
      "repository": {
        "id": "10",
        "name": "IPv4_active_compliance",
        "description": "Contains IPv4 data imported from active
Nessus scans",
        "type": "Local",
        "dataFormat" : "IPv4"      },
      "organization": {
        "id": "2",
        "name": "Org on 192.2.0.2",
        "description": "Generated by automation!"      }
    },
    {
      "status": "Completed",
      "name": "Daily compliance scan",
      "details": "PCI DSS 3.0 - Microsoft Windows Audit 2",
      "diagnosticAvailable": "false",
      "importStatus": "Finished",
      "createdTime": "1615422601",
      "startTime": "1615422607",
      "finishTime": "1615422668",
      "importStart": "1615422673",
```

```
      "importFinish": "1615422675",
      "running": "false",
      "totalIPs": "1",
      "scannedIPs": "1",
      "completedIPs": "1",
      "completedChecks": "190",
      "totalChecks": "190",
      "dataFormat": "IPv4",
      "downloadAvailable": "true",
      "downloadFormat": "v2",
      "resultType": "active",
      "resultSource": "internal",
      "scanDuration": "61",
      "id": "43",
      "scanID": "",
      "jobID": "10615",
      "SCI": {
        "id": "3",
        "name": "Managed SCI - 192.2.0.2",
        "description": "2"      },
      "owner": {
        "id": "1672",
        "firstname": "",
        "lastname": "",
        "username": "testuser"      },
      "repository": {
        "id": "10",
        "name": "IPv4_active_compliance",
        "description": "Contains IPv4 data imported from active
Nessus scans",
        "type": "Local",
        "dataFormat": "IPv4"      },
      "organization": {
```

```
        "id": "2",
        "name": "Org on 192.2.0.2",
        "description": "Generated by automation!"      }
    }
  ],
  "error_code": 0,
  "error_msg": "",
  "warnings": [],
  "timestamp": 1615490556
}
```


/mgmt/scanResult/{id}

Methods

GET

Gets the Director Scan Result associated with {id}. A Director Scan Result is Director's copy of a Scan Result from a SCI.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
initiator
owner
scan
resultsSync
**sci
**sciOrganization

**sciScanResult
retrievalStatus
job
repository
**name
**description
details
**status
importStatus
importStart
importFinish
importDuration
ioSyncStatus
ioSyncStart
ioSyncFinish
diagnosticAvailable
downloadAvailable
downloadFormat
dataFormat
resultType
resultSource
running
errorDetails
importErrorDetails
ioSyncErrorDetails
pluginSet
agentScanUUID
totalIPs
scannedIPs
completedIPs
completedChecks
totalChecks
startTime
finishTime
createdTime
scanDuration

timeCompareField

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

Request Parameters

None

Example Response

Expand


```
{
  "type": "regular",
  "response": {
    "name": "Daily compliance scan",
    "description": "",
    "diagnosticAvailable": "false",
    "importStatus": "Finished",
    "createdTime" : "1614904200",
    "importStart": "1614904273",
    "importFinish": "1614904276",
    "importDuration": "3",
    "ioSyncStatus": "",
    "ioSyncStart": "-1",
    "ioSyncFinish": "-1",
    "totalIPs": "1",
    "scannedIPs": "1",
    "completedIPs": "1",
    "completedChecks": "190",
    "totalChecks": "190",
    "status": "Completed",
```

```
    "errorDetails": "",
    "downloadAvailable": "true",
    "dataFormat": "IPv4",
    "finishTime": "1614904269",
    "downloadFormat": "v2",
    "running": "false",
    "importErrorDetails": "",
    "ioSyncErrorDetails": "",
    "startTime": "1614904207",
    "details": "PCI DSS 3.0 - Microsoft Windows Audit",
    "resultType": "active",
    "resultSource": "internal",
    "scanDuration": "62",
    "agentScanUUID": "",
    "id": "37",
    "scanID": "",
    "jobID": "4967",
    "SCI": {
      "id": "3",
      "name": "Managed SCI - 192.2.0.2",
      "description": "2"    },
    "owner": {
      "id": "1672",
      "firstname": "",
      "lastname": "",
      "username": "testuser"    },
    "repository": {
      "id": "10",
      "name": "IPv4_active_compliance",
      "description": "Contains IPv4 data imported from active Nessus
scans",
      "type": "Local",
      "dataFormat": "IPv4"    },
```

```
    "organization": {
      "id": "2",
      "name": "Org on 192.2.0.2",
      "description": "Generated by automation!"    }
  },
  "error_code": 0,
  "error_msg": "",
  "warnings": [],
  "timestamp": 1615490707
}
```


/mgmt/scanResult/{id}/email

Methods

POST

Emails the Scan Result associated with Director {id}.

For documentation please consult the normal Scan Result email endpoint documentation.

/mgmt/scanResult/{id}/stop

Methods

POST

Stops the Scan Result on the Tenable.sc Instance associated with Director {id}.

A HTTP 200 from this endpoint does *not* mean your Scan Result was paused successfully. A job is queued up on Director to check and update the Director Scan Result information for when the Scan Result actually stops.

Request Parameters

type - "discard","import", or "rollover" for what to do with the Scan Result once the stop finishes. "discard" will discard the Scan Result, "import" will import any data Tenable.sc already has, and

"rollover" will import any data Tenable.sc already has and create a rollover scan to cover any unscanned targets.

Example Response

Expand


```
{
  "type": "regular",
  "response": {
    "id": "25",
    "agentScanID": "-1",
    "resultsSyncID": "-1",
    "jobID": "12269",
    "name": "Basic Network Scan with Credentials",
    "description": "",
    "details": "Basic Network Scan Policy",
    "status": "Running",
    "importStatus": "No Results",
    "importStart": "-1",
    "importFinish": "-1",
    "ioSyncStatus": null,
    "ioSyncStart": "-1",
    "ioSyncFinish": "-1",
    "diagnosticAvailable": "false",
    "downloadAvailable": "false",
    "downloadFormat": "v2",
    "dataFormat": "IPv4",
    "resultType": "active",
    "resultSource": "internal",
    "running": "true",
    "errorDetails": "",
    "importErrorDetails": "",
    "ioSyncErrorDetails": null,
    "pluginSet": null,
```

```
"totalIPs": "256",
"scannedIPs": "8",
"agentScanUUID": "",
"agentScanContainerUUID": "",
"startTime": "1615491193",
"finishTime": "-1",
"createdTime": "1615491185",
"scanDuration": "305",
"importDuration": "-1",
"ioSyncDuration": "-1",
"completedIPs": "26",
"completedChecks": "3228449",
"totalChecks": "32645376",
"canUse": "true",
"canManage": "true",
"initiator": {
  "id": "1",
  "username": "qa",
  "firstname": "",
  "lastname": ""    },
"owner": {
  "id": "1",
  "username": "qa",
  "firstname": "",
  "lastname": ""    },
"scan": {
  "id": "1",
  "name": "Basic Network Scan with Credentials",
  "description": ""    },
"repository": {
  "id": "1",
  "name": "qarep_IPv4_active_compliance",
  "description": "Contains IPv4 data imported from active Nessus
```

```
scans"    },
    "ownerGroup": {
      "id": "0",
      "name": "Full Access",
      "description": "Full Access group"    }
  },
  "error_code": 0,
  "error_msg": "",
  "warnings": [],
  "timestamp": 1615491498
}
```


/mgmt/scanResult/{id}/pause

Methods

POST

Pauses the Scan Result on the Tenable.sc Instance associated with Director {id}.

A HTTP 200 from this endpoint does *not* mean your Scan Result was paused successfully. A job is queued up on Director to check and update the Director Scan Result information for when the Scan Result actually pauses.

Request Parameters

None

Example Response

Expand


```
{
  "type": "regular",
  "response": {
    "id": "43",
    "initiatorID": "1",
```

```
    "ownerID": "1",
    "scanID": "",
    "resultsSyncID": "-1",
    "sciID": "3",
    "sciOrgID": "1",
    "sciScanResultID": "24",
    "retrievalStatus": "0",
    "jobID": "10615",
    "repositoryID": "1",
    "name": "Daily compliance scan",
    "description": "",
    "details": "PCI DSS 3.0 - Microsoft Windows Audit",
    "status": "Completed",
    "importStatus": "Finished",
    "importStart": "1615422673",
    "importFinish": "1615422675",
    "ioSyncStatus": "",
    "ioSyncStart": "-1",
    "ioSyncFinish": "-1",
    "diagnosticAvailable": "false",
    "downloadAvailable": "true",
    "downloadFormat": "v2",
    "dataFormat": "IPv4",
    "resultType": "active",
    "resultSource": "internal",
    "running": "false",
    "acknowledged": "false",
    "errorDetails": "",
    "importErrorDetails": "",
    "ioSyncErrorDetails": "",
    "pluginSet": null,
    "agentScanUUID": "",
    "totalIPs": "1",
```

```
    "scannedIPs": "1",
    "completedIPs": "1",
    "completedChecks": "190",
    "totalChecks": "190",
    "retrievedTime": "-1",
    "startTime": "1615422607",
    "finishTime": "1615422668",
    "createdTime": "1615422601",
    "scanDuration": "61",
    "importDuration": "2",
    "ioSyncDuration": "-1",
    "username": "qa",
    "firstname": "",
    "lastname": "",
    "title": "",
    "email": "",
    "address": "",
    "city": "",
    "state": "",
    "country": "",
    "phone": "",
    "fax": ""  },
  "error_code": 0,
  "error_msg": "",
  "warnings": [],
  "timestamp": 1615491019
}
```


/mgmt/scanResult/{id}/resume

Methods

POST

Resumes the Scan Result on the Tenable.sc Instance associated with Director {id}.

A HTTP 200 from this endpoint does *not* mean your Scan Result was resumed successfully. A job is queued up on Director to check and update the Director Scan Result information for when the Scan Result actually resumes.

Request Parameters

None

Example Response

Expand


```
{
  "type": "regular",
  "response": {
    "id": "44",
    "initiatorID": "1",
    "ownerID": "1",
    "scanID": "",
    "resultsSyncID": "-1",
    "sciID": "3",
    "sciOrgID": "1",
    "sciScanResultID": "25",
    "retrievalStatus": "0",
    "jobID": "12269",
    "repositoryID": "1",
    "name": "Basic Network Scan with Credentials",
    "description": "",
    "details": "Basic Network Scan Policy",
    "status": "Resuming",
    "importStatus": "No Results",
    "importStart": "-1",
    "importFinish": "-1",
    "ioSyncStatus": "",
    "ioSyncStart": "-1",
    "ioSyncFinish": "-1",
```

```
    "diagnosticAvailable": "false",
    "downloadAvailable": "false",
    "downloadFormat": "v2",
    "dataFormat": "IPv4",
    "resultType": "active",
    "resultSource": "internal",
    "running": "true",
    "acknowledged": "false",
    "errorDetails": "",
    "importErrorDetails": "",
    "ioSyncErrorDetails": "",
    "pluginSet": null,
    "agentScanUUID": "",
    "totalIPs": "256",
    "scannedIPs": "8",
    "completedIPs": "8",
    "completedChecks": "127521",
    "totalChecks": "32645376",
    "retrievedTime": "-1",
    "startTime": "1615491193",
    "finishTime": "-1",
    "createdTime": "1615491185",
    "scanDuration": "263",
    "importDuration": "-1",
    "ioSyncDuration": "-1",
    "username": "qa",
    "firstname": "",
    "lastname": "",
    "title": "",
    "email": "",
    "address": "",
    "city": "",
    "state": "",
```

```
    "country": "",
    "phone": "",
    "fax": ""  },
  "error_code": 0,
  "error_msg": "",
  "warnings": [],
  "timestamp": 1615491456
}
```


/mgmt/scanResult/{id}/retrieve

Methods

POST

Instructs Tenable.sc director to download (retrieve) the Scan Result on the SCI associated with Director {id} from the SCI to Director.

A HTTP 200 from this endpoint does *not* mean your Scan Result was retrieved successfully. A job is queued up on Director to download the Scan Result and update the Director Scan Result information for when that Scan Result is actually retrieved.

Example Response

Expand


```
{
  "type": "regular",
  "response": {
    "id": "43",
    "initiatorID": "1",
    "ownerID": "1",
    "scanID": "",
    "resultsSyncID": "-1",
    "sciID": "3",
    "sciOrgID": "1",
```

```
    "sciScanResultID": "24",
    "retrievalStatus": "0",
    "jobID": "10615",
    "repositoryID": "1",
    "name": "Daily compliance scan",
    "description": "",
    "details": "PCI DSS 3.0 - Microsoft Windows Audit",
    "status": "Completed",
    "importStatus": "Finished",
    "importStart": "1615422673",
    "importFinish": "1615422675",
    "ioSyncStatus": "",
    "ioSyncStart": "-1",
    "ioSyncFinish": "-1",
    "diagnosticAvailable": "false",
    "downloadAvailable": "true",
    "downloadFormat": "v2",
    "dataFormat": "IPv4",
    "resultType": "active",
    "resultSource": "internal",
    "running": "false",
    "acknowledged": "false",
    "errorDetails": "",
    "importErrorDetails": "",
    "ioSyncErrorDetails": "",
    "pluginSet": null,
    "agentScanUUID": "",
    "totalIPs": "1",
    "scannedIPs": "1",
    "completedIPs": "1",
    "completedChecks": "190",
    "totalChecks": "190",
    "retrievedTime": "-1",
```

```
    "startTime": "1615422607",
    "finishTime": "1615422668",
    "createdTime": "1615422601",
    "scanDuration": "61",
    "importDuration": "2",
    "ioSyncDuration": "-1",
    "username": "qa",
    "firstname": "",
    "lastname": "",
    "title": "",
    "email": "",
    "address": "",
    "city": "",
    "state": "",
    "country": "",
    "phone": "",
    "fax": ""  },
  "error_code": 0,
  "error_msg": "",
  "warnings": [],
  "timestamp": 1615491019
}
```


/mgmt/scanResult/{id}/download

Methods

POST

Downloads the Scan Result on the SCI associated with Director {id}.

For documentation please consult the normal Scan Result download endpoint documentation.

Atlassian

Tenable Security Center API: Director Scan Zone

This API resource is only usable in Tenable.sc Director.

/mgmt/zone

Methods

GET

Gets the list of Director Scan Zones. NOTE: A Director Scan Zone is Director's copy of a Scan Zone from an SCI.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
**name
**description
*sci
**ipList
**createdTime
**modifiedTime
**organizations
**activeScanners
**totalScanners
**scanners

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

Request Parameters

None

Example Response

Expand


```
{
        "type": "regular",
        "response": [
                {
                        "id": "1",
                        "name": "sci1 scan zone",
                        "description": "",
                        "ipList": "0.0.0.0/0",
                        "createdTime": "1615926375",
                        "modifiedTime": "1615926375",
                        "scanners": [
                                {
                                        "id": "1",
                                        "name": "192.168.1.1",
                                        "description": "",
                                        "status": "2"
                        ],
                        "organizations": [],
                        "activeScanners": 0,
                        "totalScanners": 1,
                        "SCI": {
                                "id": "2",
                                "name": "sci1",
                                "description": ""                    }
                }
        ],
        "error_code": 0,
        "error_msg": "",
        "warnings": [],
        "timestamp": 1615926995
}
```

POST

Adds a Scan Zone to a specified SCI, returning a Director Scan Zone ID.

Request Parameters

Expand

```
{
        "name" : <string>,
        "description" : <string> DEFAULT "",
        "sciID" : <number>,
        "ipList" : <string> (valid IP list),
        "scanners" : [
                {
                        "id" : <number>          }...
        ],
        "organizations" : []
}
```

Example Response

Expand

```
{
        "type": "regular",
        "response": {
                "id": "2",
                "name": "Test-Zone-1615928553",
                "description": "",
                "ipList": "0.0.0.0/0",
                "sciID": "2",
                "sciZoneID": "2",
                "createdTime": "1615928574",
                "modifiedTime": "1615928574",
                "scanners": [
```

```
                        {
                                "id": "1",
                                "name": "192.168.1.2",
                                "description": "",
                                "status": "2"                   }
                ],
                "organizations": [],
                "activeScanners": 0,
                "totalScanners": 1
        },
        "error_code": 0,
        "error_msg": "",
        "warnings": [],
        "timestamp": 1615928574
}
```


/mgmt/zone/{id}

Methods

PATCH

Edits the Director Scan Zone associated with {id}, changing only the passed in fields.

Request Parameters

(All fields are optional)

See /mgmt/zone::POST for parameters.

Example Response

See /mgmt/zone/{id}::GET

DELETE

Deletes the Director Zone associated with {id}, depending on access and permissions.

Request Parameters

None

Example Response

Expand

```
{
        "type" : "regular",
        "response" : "",
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1408733643
}
```

GET

Gets the Director Scan Zone associated with {id}. A Director Scan Zone is Director's copy of a Scan Zone from an SCI.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
**name
**description
*sci
**ipList
**createdTime
**modifiedTime
**organizations
**activeScanners
**totalScanners
**scanners

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

Request Parameters

None

Example Response

Expand


```
{
        "type": "regular",
        "response": {
                "id": "1",
                "name": "sci1 scan zone",
                "description": "",
                "ipList": "0.0.0.0/0",
                "createdTime": "1615926375",
                "modifiedTime": "1615926375",
                "scanners": [
                        {
                                "id": "1",
                                "name": "192.168.1.2",
                                "description": "",
                                "status": "2"                   }
                ],
                "organizations": [],
                "activeScanners": 0,
                "totalScanners": 1,
                "SCI": {
                        "id": "2",
                        "name": "sci1",
                        "description": ""               }
```

```
        },
        "error_code": 0,
        "error_msg": "",
        "warnings": [],
        "timestamp": 1615928128
}
```


Atlassian

Tenable Security Center API: Director System

This API resource is only usable in Tenable.sc Director.

/mgmt/system/logFiles

Methods

GET

Gets the list of log files on a linked Tenable.sc Instance that are available to the user

Request Parameters

Expand


```
{
        "sciID": <number>}
```


Example Response for Admins

Expand


```
{
        "type": "regular",
        "response": [
                {
                        "organization": {
                                "id": 0,
```

```
                                "name": "Application",
                                "description": ""                       },
                        "basenames": [
                                "202106"                        ]
                },
                {
                        "organization": {
                                "id": "1",
                                "name": "Child Org",
                                "description": ""                       },
                        "basenames": [
                                "202106"                        ]
                }
        ],
        "error_code": 0,
        "error_msg": "",
        "warnings": [],
        "timestamp": 1624370508
}
```


Example Response for Security Managers

Expand


```
{
    "type": "regular",
    "response": [
        {
            "basenames": [
                "202106"            ]
        }
    ],
    "error_code": 0,
    "error_msg": "",
```

```
    "warnings": [],
    "timestamp": 1624371093
}
```

/mgmt/system/logs

Methods

POST

Returns the available log messages on a linked Tenable.sc Instance, based on user permissions and the query filters

Request Parameters

Expand

```
{
        "sciID": <number>,
        "date" : scLog basename (eg. "201412") | "all",
        "query": {
                "startOffset" : <number>,
                "endOffset" : <number>,
                "filters" : [
                        {
                                "filterName" : "keywords",
                                "operator" : "=",
                                "value" : <string>                    },
                        {
                                "filterName" : "severity",
                                "value" : {
                                        "id" : <number> [0-2],
                                        "operator" : "=",
                                        "name":"INFO|WARNING|CRITICAL"
                        },
                        {
```

```
                                "filterName" : "module",
                                "operator" : "=",
                                "value" : <string> (eg. "auth")
                        },
                        {
                                "filterName" : "organization",
                                "value" : {
                                        "id" : <number>
                        }
                ]
        }
}
```

Example Response

Expand

```
{
   "type": "regular",
    "response": {
        "skip": [],
        "totalRecords": 56,
        "endOffset": 3,
        "results": [
            {
                "rawLog": "Tue, 22 Jun 2021 10:20:28 -
0400|qahead|auth|INFO|Successful logout for 'qahead'.\n",
                "organization": {
                    "id": "1",
                    "name": "Child Org",
                    "description": ""                },
                "message": "Successful logout for 'qahead'.",
                "severity": {
                    "id": "0",
```

```
                    "name": "INFO",
                    "description": "Information"                },
                "module": "auth",
                "source": "qahead",
                "date": "Tue, 22 Jun 2021 10:20:28 -0400"
},
            {
                "rawLog": "Tue, 22 Jun 2021 09:20:01 -
0400|qahead|policy|INFO|' [qahead]' deleted organization policy
'Basic Policy' (id #1000002).\n",
                "organization": {
                    "id": "1",
                    "name": "Child Org",
                    "description": ""                },
                "message": "' [qahead]' deleted organization policy
'Basic Policy' (id #1000002).",
                "severity": {
                    "id": "0",
                    "name": "INFO",
                    "description": "Information"                },
                "module": "policy",
                "source": "qahead",
                "date": "Tue, 22 Jun 2021 09:20:01 -0400"
},
            {
                "rawLog": "Tue, 22 Jun 2021 09:18:08 -
0400|qahead|policy|INFO|' [qahead]' created organization policy
'Basic Policy' (id #1000002).\n",
                "organization": {
                    "id": "1",
                    "name": "Child Org",
                    "description": ""                },
                "message": "' [qahead]' created organization policy
```

```
'Basic Policy' (id #1000002).",
                "severity": {
                    "id": "0",
                    "name": "INFO",
                    "description": "Information"                },
                "module": "policy",
                "source": "qahead",
                "date": "Tue, 22 Jun 2021 09:18:08 -0400"
}
        ]
    },
    "error_code": 0,
    "error_msg": "",
    "warnings": [],
    "timestamp": 1624372254
}
```


Atlassian

Tenable Security Center API: Director User

This API resource is only available for administrators in Tenable.sc Director.

mgmt/user

Methods

GET

Gets the list of Users on Tenable.sc Instances linked to Director.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
*uuid
*sciUserID
*sciRoleID
*sciGroupID
***SCI**
***organization**
**username
**firstname
**lastname
email
title
address
city
state
country
phone
fax

Legend

** = always comes back*

*** = comes back if fields list not specified*

***red =** field is a JSON object (**e.g.** "SCI" : {"id" : "2", "name" : "SCI Name", "description" : "Description"})*

Request User Parameters

Expand

The *id* and *orgID* are the IDs stored in the tables local to Director. They must match ID values found with **/mgmt/user** and **/mgmt/organization** endpoints, unless you want to filter on Administrator users, in which case you can provide an orgID of "0".

To see a list of all users on a particular Tenable.sc Instance, the *sciID* parameter should be specified along the query string, and it takes the syntax

```
?sciID=<number>
```

To see a list of all users on a particular Organization, the *orgID* parameter should be specified along the query string. To see a list of all Administrator users, an orgID of "0" should be specified along the query string. This can be used in combination with the sciID filter to see a list of Administrator users for a particular Tenable.sc instance. This filter takes the syntax

```
?orgID=<number>
```

Example Response

Expand


```
{
    "type": "regular",
    "response": [
        {
            "id": "1",
            "uuid": "875A7270-E6B1-4FBF-A12E-1381DAED1A99",
            "sciUserID": "1",
            "sciRoleID": "1",
            "sciGroupID": "-1",
            "username": "admin",
            "firstname": "Admin",
            "lastname": "User",
            "email": "",
            "SCI": {
                "id": "2",
                "name": "SCI 1",
                "description": "123"            },
            "organization": {
                "id": "0",
                "name": "Administrator",
                "description": ""            }
        },
        {
            "id": "2",
            "uuid": "AB1D4170-E362-4637-AE7C-F29D77B37A8F",
```

```
            "sciUserID": "1",
            "sciRoleID": "2",
            "sciGroupID": "0",
            "username": "qa",
            "firstname": "Organization",
            "lastname": "User",
            "email": "",
            "SCI": {
                "id": "2",
                "name": "SCI 1",
                "description": "123"            },
            "organization": {
                "id": "1",
                "name": "Org 1",
                "description": ""           }
        }
    ],
    "error_code": 0,
    "error_msg": "",
    "warnings": [],
    "timestamp": 1644240279
}
```


/mgmt/user/{id}

/mgmt/user/{uuid}

Methods

GET

Gets the User associated with {id} or {uuid}.

The *id* is the ID stored in a table local to Director. It must match an ID value found with the **/mgmt/user** endpoint.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
*uuid
*sciUserID
*sciRoleID
*sciGroupID
***SCI**
***organization**
**username
**firstname
**lastname
**email
**title
**address
**city
**state
**country
**phone
**fax

Legend

** = always comes back*

*** = comes back if fields list not specified*

***red =** field is a JSON object (**e.g.** "SCI" : {"id" : "2", "name" : "SCI Name", "description" : "Description"})*

Request User Parameters

None

Example Response

Expand


```
{
   "type": "regular",
    "response": {
        "id": "2",
        "uuid": "AB1D4170-E362-4637-AE7C-F29D77B37A8F",
        "sciUserID": "1",
        "sciRoleID": "2",
        "sciGroupID": "0",
        "username": "qa",
        "firstname": "QA",
        "lastname": "User",
        "title": "",
        "email": "",
        "address": "",
        "city": "",
        "state": "",
        "country": "",
        "phone": "",
        "fax": "",
        "SCI": {
            "id": "2",
            "name": "SCI 1",
            "description": "123"        },
        "organization": {
            "id": "1",
            "name": "Org 1",
            "description": ""        }
    },
    "error_code": 0,
    "error_msg": "",
    "warnings": [],
```

```
    "timestamp": 1644240550
}
```

Atlassian

Tenable Security Center API: File

/file/upload

Methods

POST

Uploads a File.

NOTE: The *filename* and *tailoringFilename* fields should contain the value of the same parameter passed back on a */file/upload::POST* if they are provided. The *tailoringOriginalFilename* field should contain the value of the tailoring file's original name, prior to upload if it is provided.

Request Payload

Expand

```
POST /file/upload HTTP/1.1
Host: <destinationHost>[:<destinationPort>]
Origin: http://<formHost>[:<formPort>]
Content-Length: <contentLength>Content-Type: multipart/form-data;
boundary=<dataBoundary>...
<dataBoundary>Content-Disposition: form-data; name="Filedata";
filedata="<baseName>"Content-Type:
<contentType> <fileData><dataBoundary>...
```

returnContentis provided

```
...
<dataBoundary>Content-Disposition: form-data;
name="returnContent"<returnContent>...
```

contextis provided

```
...
<dataBoundary>Content-Disposition: form-data;
name="context"<context>...
```

MAX_FILE_SIZE is specified

```
...
<dataBoundary>Content-Disposition: form-data; name="MAX_FILE_
SIZE"<maxFileSize>...
```

Types and values:

- destinationHost = <string>
- destinationPort = <number> OPTIONAL (do not provide the preceding colon if not specified)
- formHost = <string>
- formPort = <number> OPTIONAL (do not provide the preceding colon if not specified)
- contentLength = <number>
- dataBoundary = <string>
- maxFileSize = <number> (maximum size allowed for an uploaded file; It is best to check this on the client first if possible)
- fileData = <string>
- baseName = <string>
- returnContent = <string> "false" | "true" DEFAULT "false"
- context = <string> "auditfile" | "tailoringfile"

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "filename" : "4fk1r0",
                "originalFilename" : "filename.zip",
                "content" : "",
                "context" : [
                        {
                                "dataStreamName" : "scap_gov.nist_datastream_U
1.2.3.1.zip"                     }
                ],
                "benchmarkName" : "benchmarkname",
                "profileName" : "profilename",
                "version" : "1.2",
                "type" : ""     }
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1404308740
}
```

/file/clear

Methods

POST

Removes the File associated with {filename}.

Request Parameters

Expand

```
{
        "filename" : <string>}
```

Example Response

Expand


```
{
        "type" : "regular",
        "response" : {
                "filename" : "\/opt\/sc4\/orgs\/26\/tmp\/\/1.1421854135.bEiuo
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1404311344
}
```


Atlassian

Tenable Security Center API: Freeze Window

In order to better align with the inclusive language guidelines, The Freeze Window API is the new API endpoint replacing Blackout Window API.

NOTE #1: In 5.18.0 both /blackout and /freeze API are supported and /blackout API is deprecated will be phased out in 5.19.0.

/freeze

Methods

GET

Gets the list of Freeze Windows.

NOTE #1: Only users in the FreezeWindow owner's group may view target details. For users outside of the group: Repository, Assets, ipList, and allIPs will be returned {}, [], "", and "false" respectively.

NOTE #2: If a Repository or Asset associated with a FreezeWindow has been deleted, the ID will be returned as '-1'. If one has been unshared, the ID will be similarly returned as -1, but the name will signify the Asset ID.

NOTE #3: The "status" field represents if the FreezeWindow has been disabled via bad Repository and if it has been degrade via Asset. The "functional" field represents if there are any valid target IPs in the FreezeWindow (allIPs, ipList, assets) in the FreezeWindow owner's context.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
**name
**description
**status
creator
assets
repository
owner
creator
ipList
allIPs
repeatRule
start
end
duration
enabled
createdTime
modifiedTime
active
ownerGroup
canManage
functional

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

***redFont =** field is a JSON object (**e.g.** "repository" :{ "id" : <id>, "name" : <name> })*

Request Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
        "response" : [
                {
                        "id" : "20",
                        "name" : "3",
                        "description" : "",
                        "ipList" : "",
                        "start" : "TZID=America\/New_York:20141119T235800",
                        "end" : "TZID=America\/New_York:20141119T000200",
                        "duration" : "-86160",
                        "repeatRule" : "FREQ=DAILY;INTERVAL=1",
                        "status" : "0",
                        "enabled" : "false",
                        "createdTime" : "1418327672",
                        "modifiedTime" : "1418327672",
                        "assets" : [
                                {
                                        "id" : "3",
                                        "name" : "Test3",
                                        "description" : "",
                    "uuid": "31075F9E-72E8-4397-AF3B-A3A61427DBE6"
                }
                        ],
                        "active" : "false",
```

```
                "creator" : {
                        "id" : "1",
                        "username" : "freezeTest",
                        "firstname" : "",
                        "lastname" : "",
                        "uuid" : "2E2B70F2-3471-428F-82AF-A6905090EAA
                "owner" : {
                        "id" : "1",
                        "username" : "freezeTest",
                        "firstname" : "",
                        "lastname" : "",
                        "uuid" : "2E2B70F2-3471-428F-82AF-A6905090EAA
                "repository" : {
                        "id" : "29",
                        "name" : "Test IPv6",
                        "description" : "",
                        "type" : "Local",
                        "uuid": "8A547FC6-5FBA-43BB-900E-683F022812CE
        },
        {
                "id" : "21",
                "name" : "4",
                "description" : "",
                "ipList" : "172.26.50.0\/24",
                "start" : "TZID=America\/New_York:20141119T235800",
                "end" : "TZID=America\/New_York:20141119T000200",
                "duration" : "-86160",
                "repeatRule" : "FREQ=DAILY;INTERVAL=1",
                "status" : "0",
                "enabled" : "false",
                "createdTime" : "1418327716",
                "modifiedTime" : "1418327716",
                "assets" : [],
```

```
                        "active" : "false",
                        "creator" : {
                                "id" : "1",
                                "username" : "freezeTest",
                                "firstname" : "",
                                "lastname" : "",
                                "uuid" : "2E2B70F2-3471-428F-82AF-A6905090EAA
                        "owner" : {
                                "id" : "1",
                                "username" : "freezeTest",
                                "firstname" : "",
                                "lastname" : "",
                                "uuid" : "2E2B70F2-3471-428F-82AF-A6905090EAA
                        "repository" : {
                                "id" : -1,
                                "name" : "",
                                "description" : "",
                                "type" : ""                     }
                }
        ],
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1418332032
}
```


POST

Adds a Freeze Window.

NOTE: If 'allIPs' is 'false', an 'ipList' and/or at least one 'assets' parameter must be provided. If 'allIPs' is 'true', the back-end will clear the target (ipList, assets, and repository) fields.

Request Parameters

Expand

```
{
        "name" : <string>,
        "description" : <string> DEFAULT "",
        "repeatRule" : <string> (ical start format) DEFAULT "",
        "start" : <string> (ical start format),
        "end" : <string> (ical end format),
        "repository" : {
                "id" : <number> } DEFAULT -1 (not set),
        "allIPs" : <string> "false" | "true" DEFAULT "true",
        "enabled" : <string> "false" | "true",
        allIPs "false"  --------------
        "ipList" : <string> (valid comma-separated IP List format) DEFAULT
"",
        "assets" : [
                {
                        "id" : <number>         }...
        ] DEFAULT []
}
```

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "id" : "21",
                "name" : "4",
                "description" : "",
                "repeatRule" : "FREQ=DAILY;INTERVAL=1",
                "start" : "TZID=America\/New_York:20141119T235800",
                "end" : "TZID=America\/New_York:20141119T000200",
                "duration" : "-86160",
                "enabled" : "false",
```

```
                "createdTime" : "1418327716",
                "modifiedTime" : "1418327716",
                "ipList" : "192.168.1.0\/24",
                "status" : "0",
                "assets" : [],
                "active" : "false",
                "creator" : {
                        "id" : "1",
                        "username" : "freezeTest",
                        "firstname" : "",
                        "lastname" : "",
                        "uuid" : "2E2B70F2-3471-428F-82AF-A6905090EAA9"
                "owner" : {
                        "id" : "1",
                        "username" : "freezeTest",
                        "firstname" : "",
                        "lastname" : "",
                        "uuid" : "2E2B70F2-3471-428F-82AF-A6905090EAA9"
                "repository" : {
                        "id" : -1,
                        "name" : "",
                        "description" : "",
             "type": ""         }
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1418327716
}
```


/freeze/{id}

Methods

GET

Gets the Freeze Window associated with {id}.

NOTE #1: Only users in the FreezeWindow owner's group may view target details. For users outside of the group: Repository, Assets, ipList, and allIPs will be returned {}, [], "", and "false" respectively.

NOTE #2: If a Repository or Asset associated with a FreezeWindow has been deleted, the ID will be returned as '-1'. If one has been unshared, the ID will be similarly returned as -1, but the name will signify the Asset ID.

NOTE #3: The "status" field represents if the FreezeWindow has been disabled via bad Repository and if it has been degrade via Asset. The "functional" field represents if there are any valid target IPs in the FreezeWindow (allIPs, ipList, assets) in the FreezeWindow owner's context.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
**name
**description
**status
creator
assets
repository
owner
creator
ipList
allIPs
repeatRule
start

end
duration
enabled
createdTime
modifiedTime
active
ownerGroup
canManage
functional

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*
redFont = *field is a JSON object (* ***e.g.*** *"repository" :{ "id" : <id>, "name" : <name> })*

Request Parameters

None

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "id" : "21",
                "name" : "4",
                "description" : "",
                "repeatRule" : "FREQ=DAILY;INTERVAL=1",
                "start" : "TZID=America\/New_York:20141119T235800",
                "end" : "TZID=America\/New_York:20141119T000200",
                "duration" : "-86160",
                "enabled" : "false",
                "createdTime" : "1418327716",
                "modifiedTime" : "1418327716",
```

```
                "ipList" : "192.168.1.0\/24",
                "status" : "0",
                "assets" : [],
                "active" : "false",
                "creator" : {
                        "id" : "1",
                        "username" : "freezeTest",
                        "firstname" : "",
                        "lastname" : "",
             "uuid": "2E2B70F2-3471-428F-82AF-A6905090EAA9"            },
                "owner" : {
                        "id" : "1",
                        "username" : "freezeTest",
                        "firstname" : "",
                        "lastname" : "",
             "uuid": "2E2B70F2-3471-428F-82AF-A6905090EAA9"            },
                "repository" : {
                        "id" : -1,
                        "name" : "",
                        "description" : "",
             "type": ""         }
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1418332060
}
```


PATCH

Edits the Freeze Window associated with {id}, changing only the passed in fields.

NOTE: Users that are not in the same group as the FreezeWindow owner can ONLY patch non-target fields (i.e. name, description, and enabled).

Request Parameters

(All fields are optional)

See /freeze::POST for parameters.

Example Response

See /freeze/{id}::GET for example response.

DELETE

Deletes the Freeze Window associated with {id}, depending on access and permissions.

Request Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
        "response" :    "",
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1403040206
}
```


Atlassian

Tenable Security Center API: Group

/group

/tes/group

/tes/group endpoint is only supported in Tenable Enclave Security

Methods

GET

Gets the list of Groups

NOTE: Only viewable shared objects will be returned. If a group retrieved contains to object shares the session user does not have permissions to view, the shares will not be returned.

Fields Parameter

Expand

NOTE: Currently, all fields come back on GET all, but the ** indicates fields which will be listed in a future release

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
**name
**description
createdTime
modifiedTime
lces
repositories
definingAssets
userCount
users
createDefaultObjects

Session User has ShareObjects Permission

assets
policies
queries
credentials
dashboardTabs
arcs
auditFiles

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

***redFont =** field is a JSON object (**e.g.** "repository" :{ "id" : <id>, "name" : <name> })*

Request Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
        "response" : [
                {
                        "id" : "0",
                        "name" : "Full Access",
                        "description" : "Full Access group"
                },
                {
                        "id" : "2",
                        "name" : "Group A",
                        "description" : ""
                },
                {
                        "id" : "3",
                        "name" : "Group B",
                        "description" : ""
                },
                {
                        "id" : "4",
                        "name" : "grunt",
                        "description" : ""
                },
```

```
                {
                        "id" : "5",
                        "name" : "Full Access Group 2",
                        "description" : ""
                }
        ],
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1445894598
}
```

POST

Adds a Group

Note: Cannot add definingAssets of type "watchlist" | "combination" in group definitions

Request Parameters

Expand

```
{
        "name" : <string>,
        "description" : <string> DEFAULT "",
        "createDefaultObjects" : <string> "false" | "true" DEFAULT "false",
        "repositories" : [
                {
                        "id" : <number>
                }...
        ] OPTIONAL,
        "lces" : [
                {
                        "id" : <number>
                }...
```

```
        ] OPTIONAL,
        "definingAssets" : [
                {
                        "id" : <number>
                }...
        ] OPTIONAL,
        "assets" : [
                {
                        "id" : <number>
                }...
        ] OPTIONAL,
        "policies" : [
                {
                        "id" : <number>
                }...
        ] OPTIONAL,
        "queries" : [
                {
                        "id" : <number>
                }...
        ] OPTIONAL,
        "credentials" : [
                {
                        "id" : <number>
                }...
        ] OPTIONAL,
        "dashboardTabs" : [
                {
                        "id" : <number>
                }...
        ] OPTIONAL,
        "arcs" : [
                {
```

```
                        "id" : <number>
                },...
        ] OPTIONAL,
        "auditFiles" : [
                {
                        "id" : <number>
                },...
        ] OPTIONAL
}
```

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "id" : "5",
                "name" : "Full Access Group test",
                "description" : "",
                "createdTime" : "1436551970",
                "modifiedTime" : "1445892755",
                "lces" : [
                        {
                                "id" : "3",
                                "name" : "test LCE",
                                "description" : "Copied from Box for testing",
                                "version" : "4.6.0"
                        },
                        {
                                "id" : "4",
                                "name" : "LCE 1",
                                "description" : "Copied from Box for testing",
                                "version" : "4.4.1"
```

```
                },
                {
                        "id" : "5",
                        "name" : "LCE 2",
                        "description" : "Copied from Box for testing",
                        "version" : "4.4.0"
                }
        ],
        "repositories" : [
                {
                        "id" : "38",
                        "name" : "ipv4",
                        "description" : "copied from QA",
                        "lastVulnUpdate" : "1445621650",
                        "type" : "Local",
                        "dataFormat" : "IPv4",
         "uuid": "49C61E1E-3D79-4345-AE79-CE3E5DF69B47"
                },
                {
                        "id" : "39",
                        "name" : "ipv6 rep",
                        "description" : "Copied from QA 2",
                        "lastVulnUpdate" : "1437805904",
                        "type" : "Local",
                        "dataFormat" : "IPv6",
                        "uuid": "2253DAE5-880E-4796-B94C-1B880841BE64"
                },
                {
                        "id" : "44",
                        "name" : "Test w/pluginPrefs",
                        "description" : "",
                        "lastVulnUpdate" : "0",
                        "type" : "Local",
```

```
                "dataFormat" : "mobile",
 "uuid": "79843218-F7CF-48C2-867D-54EA9A6B0225"
        },
        {
                "id" : "57",
                "name" : "test mobile airwatch rep",
                "description" : "",
                "lastVulnUpdate" : "0",
                "type" : "Local",
                "dataFormat" : "mobile",
 "uuid": "B0718AAC-2CDA-4A9C-B6F5-ED1F8EFFC755"
        }
],
"definingAssets" : [
        {
                "id" : "0",
                "name" : "All Defined Ranges",
                "description" : "",
 "uuid": "0A18B330-B893-4080-96F2-220A45E0B203"
        }
],
"userCount" : 0,
"users" : [],
"createDefaultObjects" : "false",
"assets" : [],
"policies" : [],
"queries" : [],
"credentials" : [],
"dashboardTabs" : [],
"auditFiles" : [],
"arcs" : [
        {
                "id" : "18",
```

```
                                "name" : "Database Settings",
                                "description" : "The Database ARC presents a s
statements that measure percentage compliance against organizational
policies such as authentication policy, privilege policy, and best
practices. These policies all share a common theme in assessing
database compliance and configuration.  Organizational policy should
in turn be based on appropriate currently accepted standards.
\n\nThe ARC and the associated policy statements rely on audit
results received from Nessus scans utilizing database audit files
for compliance scanning. The audit files and policy statements are
guides that can be customized to fit the specific policy guidelines
of the organization.\n\nBy reviewing the ARC, Compliance Managers
can easily and quickly identify compliance concerns within database-
driven systems based around these controls, and rapidly identify
gaps in the database security programs or policies."
                        }
                ]
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1445892755
}
```


/group/{id}

/tes/group/{id}

/tes/group/{id} endpoint is only supported in Tenable Enclave Security

Methods

GET

Gets the Group associated with {id}.

NOTE: Only viewable shared objects will be returned. If the group retrieved contains to object shares the session user does not have permissions to view, the shares will not be returned.

Fields Parameter

The endpoint returns minimal [which includes * and **] fields only, if all of the conditions are met:

- user has no permission to 'Manage Group'
- user has no permission to 'Share Object'
- user is not viewing self group
- the group to view is not in the list of user's 'Managable Groups'

The contents of the sharableObjects fields [as mentioned in NOTE above] shows only those objects that are shared with the Groups that is enabled using ManageObjectsOfGroup/s in user Settings.

Irrespective of the `permManageGroup`, `permShareObject` a user can always view minimal + additional fields of their own group. The sharable fields however are displayed based on the `ManageObjectsOfGroup/s` permissions as mentioned above.

The return fields are summarized below:

permManageGroup	permShareObject	ManageObjects Of Group/s	fields
Yes	Yes	Yes/No	minimal + additional fields + sharableObjects fields
Yes	No	Yes/No	minimal + additional fields
No	Yes	No	minimal + additional fields + sharableObjects fields
No	No	Yes	minimal + additional fields for

			manageObjects enabled groups minimal fields for all other groups
No	No	No [for all groups]	minimal fields for all groups

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
**name
**description
createdTime
modifiedTime
lces
repositories
definingAssets
userCount
users
createDefaultObjects

Session User has ShareObjects Permission
assets
policies
queries
credentials
dashboardTabs
arcs
auditFiles

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

redFont = *field is a JSON object (* ***e.g.*** *"repository" :{ "id" : <id>, "name" : <name> })*

Request Parameters

None

Example Response

Expand

Any user with manageGroup permission enabled


```
{
        "type" : "regular",
        "response" : {
                "id" : "5",
                "name" : "Full Access Group test",
                "description" : "",
                "createdTime" : "1436551970",
                "modifiedTime" : "1445892755",
                "lces" : [
                        {
                                "id" : "3",
                                "name" : "test LCE",
                                "description" : "Copied from Box for testing",
                                "version" : "4.6.0"
                        },
                        {
                                "id" : "4",
                                "name" : "LCE 1",
                                "description" : "Copied from Box for testing",
                                "version" : "4.4.1"
                        },
```

```
                {
                        "id" : "5",
                        "name" : "LCE 2",
                        "description" : "Copied from Box for testing",
                        "version" : "4.4.0"
                }
        ],
        "repositories" : [
                {
                        "id" : "38",
                        "name" : "ipv4",
                        "description" : "copied from QA",
                        "lastVulnUpdate" : "1445621650",
                        "type" : "Local",
                        "dataFormat" : "IPv4",
         "uuid": "49C61E1E-3D79-4345-AE79-CE3E5DF69B47"
                },
                {
                        "id" : "39",
                        "name" : "ipv6 rep",
                        "description" : "Copied from QA 2",
                        "lastVulnUpdate" : "1437805904",
                        "type" : "Local",
                        "dataFormat" : "IPv6",
         "uuid": "2253DAE5-880E-4796-B94C-1B880841BE64"
                },
                {
                        "id" : "44",
                        "name" : "Test w/pluginPrefs",
                        "description" : "",
                        "lastVulnUpdate" : "0",
                        "type" : "Local",
                        "dataFormat" : "mobile",
```

```
 "uuid": "79843218-F7CF-48C2-867D-54EA9A6B0225"
        },
        {
                "id" : "57",
                "name" : "test mobile airwatch rep",
                "description" : "",
                "lastVulnUpdate" : "0",
                "type" : "Local",
                "dataFormat" : "mobile",
 "uuid": "B0718AAC-2CDA-4A9C-B6F5-ED1F8EFFC755"
        }
],
"definingAssets" : [
        {
                "id" : "0",
                "name" : "All Defined Ranges",
                "description" : "",
 "uuid": "0A18B330-B893-4080-96F2-220A45E0B203"
        }
],
"userCount" : 0,
"users" : [],
"createDefaultObjects" : "false",
"assets" : [],
"policies" : [],
"queries" : [],
"credentials" : [],
"dashboardTabs" : [],
"auditFiles" : [],
"arcs" : [
        {
                "id" : "18",
                "name" : "Database Settings",
```

```
                                "description" : "The Database ARC presents a s
statements that measure percentage compliance against organizational
policies such as authentication policy, privilege policy, and best
practices. These policies all share a common theme in assessing
database compliance and configuration.  Organizational policy should
in turn be based on appropriate currently accepted standards.
\n\nThe ARC and the associated policy statements rely on audit
results received from Nessus scans utilizing database audit files
for compliance scanning. The audit files and policy statements are
guides that can be customized to fit the specific policy guidelines
of the organization.\n\nBy reviewing the ARC, Compliance Managers
can easily and quickly identify compliance concerns within database-
driven systems based around these controls, and rapidly identify
gaps in the database security programs or policies."
                        }
                ]
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1445892755
}
```


Any user with manageGroup permission disabled and shareObject permission disabled, but can manage objects of the group in question


```
{
        "type" : "regular",
        "response" : {
                "id" : "5",
                "name" : "Full Access Group test",
                "description" : "",
                "createdTime" : "1436551970",
```

```
"modifiedTime" : "1445892755",
"lces" : [
        {
                "id" : "3",
                "name" : "test LCE",
                "description" : "Copied from Box for testing",
                "version" : "4.6.0"
        },
        {
                "id" : "4",
                "name" : "LCE 1",
                "description" : "Copied from Box for testing",
                "version" : "4.4.1"
        },
        {
                "id" : "5",
                "name" : "LCE 2",
                "description" : "Copied from Box for testing",
                "version" : "4.4.0"
        }
],
"repositories" : [
        {
                "id" : "38",
                "name" : "ipv4",
                "description" : "copied from QA",
                "lastVulnUpdate" : "1445621650",
                "type" : "Local",
                "dataFormat" : "IPv4",
 "uuid": "49C61E1E-3D79-4345-AE79-CE3E5DF69B47"
        },
        {
                "id" : "39",
```

```
                        "name" : "ipv6 rep",
                        "description" : "Copied from QA 2",
                        "lastVulnUpdate" : "1437805904",
                        "type" : "Local",
                        "dataFormat" : "IPv6",
                "uuid": "2253DAE5-880E-4796-B94C-1B880841BE64"
                },
                {
                        "id" : "44",
                        "name" : "Test w/pluginPrefs",
                        "description" : "",
                        "lastVulnUpdate" : "0",
                        "type" : "Local",
                        "dataFormat" : "mobile",
                "uuid": "79843218-F7CF-48C2-867D-54EA9A6B0225"
                },
                {
                        "id" : "57",
                        "name" : "test mobile airwatch rep",
                        "description" : "",
                        "lastVulnUpdate" : "0",
                        "type" : "Local",
                        "dataFormat" : "mobile",
                "uuid": "B0718AAC-2CDA-4A9C-B6F5-ED1F8EFFC755"
                }
        ],
        "definingAssets" : [
                {
                        "id" : "0",
                        "name" : "All Defined Ranges",
                        "description" : "",
                "uuid": "0A18B330-B893-4080-96F2-220A45E0B203"
                }
```

```
                ],
                "userCount" : 0,
                "users" : [],
                "createDefaultObjects" : "false"
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1445892755
}
```


Any user with manageGroup permission disabled and shareObject permission disabled, and also cannot manage objects of the group in question


```
{
        "type" : "regular",
        "response" : {
                "id" : "5",
                "name" : "Full Access Group test",
                "description" : ""
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1445892755
}
```


PATCH

Edits the Group associated with {id}, changing only the passed in fields.

Request Parameters

(All fields are optional)

See /group::POST for parameters.

Example Response

See /group/{id}::GET

DELETE

Deletes the Group associated with {id}, depending on access and permissions.

Request Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
        "response" : "",
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1408726272
}
```


Atlassian

Tenable Security Center API: Hosts

/hosts

Methods

GET

Gets the list of Hosts identified from all scan results that are on Tenable Security Center.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

The *limit* parameter should be an integer greater than 0

```
?limit=<number>,...
```

The *startOffset* parameter should an integer greater than 0

```
?startOffset=<number>,...
```

The *endOffset* parameter should an integer greater than 0

```
?endOffset=<number>,...
```

The *pagination* parameter should a boolean

```
?pagination=<boolean>,..
```

Allowed Fields

**id
**uuid
*tenableUUID
*name
*ipAddress
*os
*firstSeen
*lastSeen
macAddress
source
repID
netBios
netBiosWorkgroup
createdTime
modifiedTime
acr
aes

Legend

** = always comes back*
*** = comes back if fields list not specified on GET all*

red = *field is a JSON object (* ***e.g.*** *"SCI" : {"id" : "2", "name" : "SCI Name", "description" : "Description"})*

Example Response

Expand


```
{
    "type": "regular",
    "response": [
        {
            "id": "154",
            "uuid": "68262460-941b-4762-906e-47298f79911e",
            "tenableUUID": "58bd0909-f66d-4248-8c20-2501b208bb65",
            "name": "Aerified",
            "ipAddress": "201.22.196.102",
            "os": "Linux",
            "firstSeen": "1770798",
            "lastSeen": "1685038",
        },
        {
            "id": "47",
            "uuid": "e9344880-c32f-458c-b78e-211ce81d10cb",
            "tenableUUID": "dce3a590-70f0-4530-9843-5d3c83666f75",
            "name": "Windows 10",
            "ipAddress": "90.248.112.168",
            "os": "Windows 10",
            "firstSeen": "1755893",
            "lastSeen": "1221376",
        }
    ],
    "error_code": 0,
    "error_msg": "",
    "warnings": [],
    "timestamp": 1626889388
```

```
}
```

/hosts/{uuid}/acr

Methods

PATCH

Override the Asset Criticality Rating score and reasons for the specified Host.

Request Body Parameter

Expand

```
{
  "overwrittenScore": <int> 4,
  "reasoning": [
    {
      "id": <int> 1-6,
      "label" <string> "Why score was changed"
    }
  ],
  "notes": <string> "Some details on the score change",
  "overwritten": <string> "true" | "false"
}
```

Example Response

Expand

```
{
    "type": "regular",
    "response":{
        "id": "95",
        "uuid": "c2953a1a-c19c-4128-b518-8b0ccc33cb3d",
        "tenableUUID": null,
        "name": "172.26.48.1",
        "ipAddress": "172.26.48.1",
```

```
        "os": null,
        "firstSeen": "1632765212",
        "lastSeen": "1632765212",
        "dns": null,
        "fqdnIndex": "0",
        "netBios": null,
        "netBiosWorkgroup": null,
        "macAddress": null,
        "systemType": "general-purpose",
        "createdTime": "1632765212",
        "modifiedTime": "1632765212",
        "source": [
            {
                "type": "Nessus Scan"            }
        ],
        "repository": {
            "id": "1",
            "name": "Repo",
            "description": ""        },
        "acr": {
            "hostUUID": "c2953a1a-c19c-4128-b518-8b0ccc33cb3d",
            "score": "9.0",
            "overwritten": "true",
            "notes": "We changed this because....",
            "overwrittenScore": "10.0",
            "lastEditedUserID": "1",
            "lastEditedOrgID": "1",
            "lastEvaluatedTime": "1",
            "internetExposure": null,
            "capability": null,
            "reasoning": [
                {
                    "id": "4"                }
```

```
            ],
            "user": {
                "id": "1",
                "username": "qahead",
                "firstname": "",
                "lastname": "",
                "email": ""            }
        }
    },
    "error_code": 0,
    "error_msg": "",
    "warnings": [],
    "timestamp": 1632923227
}
```


/hosts/search

Methods

POST

Gets the Asset Criticality Rating score and reasons for the specified Host.

Fields Parameter

Expand

Search the list of Hosts identified from all scan results that are on T.sc.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

The *limit* parameter should be an integer greater than 0

```
?limit=<number>,...
```

The *startOffset* parameter should be an integer greater than 0

```
?startOffset=<number>,...
```

The *endOffset* parameter should be an integer greater than 0

```
?endOffset=<number>,...
```

The *pagination* parameter should a boolean

```
?pagination=<boolean>,...
```

Allowed Fields

**id
**uuid
*tenableUUID
*name
*ipAddress
*os
*firstSeen
*lastSeen
macAddress
source
repID
netBios
netBiosWorkgroup
createdTime
modifiedTime
acr
aes

Legend

** = always comes back*
*** = comes back if fields list not specified on GET all*
***red =** field is a JSON object (**e.g.** "SCI" : {"id" : "2", "name" : "SCI Name", "description" : "Description"})*

Example Request

Expand


```
{
  "filters": {
    "and": [
      {
        "property": "systemType",
        "operator": "eq",
        "value": "general_purpose,general-purpose"
      },
      {
        "property": "ip",
        "operator": "eq",
        "value": "172.26.48.0-172.26.48.100"
      },
      {
        "property": "repositoryAll",
        "operator": "eq",
        "value": "2,1"
      },
      {
        "property": "assetCriticalityRating",
        "operator": "eq",
        "value": "1-5"
      },
      {
        "property": "assetExposureScore",
        "operator": "eq",
        "value": "100-1000"
      },
      {
        "property": "sourceType",
        "operator": "eq",
        "value": "'Nessus Scan','Agent Scan'"
      },
      {
```

```
        "property": "hostid",
        "operator": "eq",
        "value": "74d580c7-4da4-427f-9282-591d99d3ba25,60847aad-f0b1-
426c-8bf0-1e8d92da85c4"
      }
    ]
  }
}
```


Example Response

Expand


```
{
  "type": "regular",
  "response": {
    "totalRecords": "1",
    "returnedRecords": 1,
    "startOffset": "0",
    "endOffset": "50",
    "results": [
      {
        "name": "SHAREPOINT2016",
        "ipAddress": "172.xx.xx.xx",
        "os": "Microsoft Windows 10",
        "macAddress": null,
        "firstSeen": "1655319261",
        "lastSeen": "1655319261",
        "netBios": "SHAREPOINT2016",
        "dns": "sharepoint2016.target.com",
        "id": "7",
        "uuid": "xxxx-xxxx-xxxx-xxxx-xxxx",
        "source": [
          {
            "type": "Nessus Scan"
          }
```

```
      ],
      "repository": {
        "id": "1",
        "name": "Repo",
        "description": "",
        "dataFormat": "IPv4",
        "type": "Local"
      },
      "acr": {
        "score": "4",
        "overwritten": "false",
        "notes": null,
        "overwrittenScore": "-1",
        "lastEditedUserID": null,
        "lastEditedOrgID": null,
        "lastEvaluatedTime": "1655319340",
        "internetExposure": "internal",
        "capability": "",
        "deviceType": "general_purpose",
        "reasoning": [],
        "keyDrivers": {
          "internet exposure": "internal",
          "device capability": "",
          "device type": "general_purpose"
        }
      },
      "aes": {
        "score": "496"
      },
      "systemType": "general_purpose"
    }
  ]
},
"error_code": 0,
"error_msg": "",
```

```
  "warnings": [],
  "timestamp": 1655385966
}
```


/hosts/download

Methods

POST

Export the Host Assets data to a CSV file format.

Fields Parameter

Expand

Search the list of Hosts identified from all scan results that are on T.sc.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

The *sortField* parameter should be a string

```
?sortField=<field>
```

The *sortDirection* parameter should be either ASC or DESC

```
?sortDirection=<string>
```

The *startOffset* parameter should be an integer greater than 0

```
?startOffset=<number>,...
```

The *endOffset* parameter should be an integer greater than 0

```
?endOffset=<number>,...
```

Allowed Fields

*id

**uuid

**ipAddress
**os
**name
**lastSeen
**source
**netBios
**dns
**acr
**aes
**repository
**systemType

Legend

** = always comes back*
*** = comes back if fields list not specified*
green = The uuid field will be renamed to "assetID" in the CSV header

Filter Parameter

Expand

Filter parameters should be posted via the request payload.

Value field for *assetCriticalityRating* and *assetExposureScore* should be a range of unsigned integers separated by a "-". Example: "1-10"

Filter Parameter

Expand

```
{
  "filters": {
    "and": [
      {
        "property": <string> "systemType" | "assetCriticalityRating" |
"assetExposureScore",
        "operator": <string> "eq",
        "value": <string> "systemTypeId" | "<uint>-<uint>"
      }
    ]
```

```
  }
}
```

Example Response (text/csv)

Expand

```
"name","ipAddress","os","macAddress","firstSeen","lastSeen","netBios","d
ns","id","source","repository","acr","aes","systemType","assetID"
"ABCD-EFGH","0.0.0.0","Linux Kernel
123","a:b:c:d:e","1234567890","1234567890","ABCD-EFGH","abdc-efgh.hijk-
lmnop.com","1234","Nessus Scan","ipv4","10","300","","abcd-efgh-ijkl-
mnop-qrst-uvwx-yz"
"ABCD-EFGH","0.0.0.0","Linux Kernel
123","a:b:c:d:e","1234567890","1234567890","ABCD-EFGH","abdc-efgh.hijk-
lmnop.com","1234","Nessus Scan","ipv4","10","300","","abcd-efgh-ijkl-
mnop-qrst-uvwx-yz"
"ABCD-EFGH","0.0.0.0","Linux Kernel
123","a:b:c:d:e","1234567890","1234567890","ABCD-EFGH","abdc-efgh.hijk-
lmnop.com","1234","Nessus Scan","ipv4","10","300","","abcd-efgh-ijkl-
mnop-qrst-uvwx-yz"
```

Atlassian

Tenable Security Center API: Job

/job

Methods

GET

Gets the list of Jobs across the application and all Organizations.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
**organization
**type
**status
objectID
initiator
targetedTime
startTime
pid
params
priority
errorCode
attemptNumber
dependentJobID
immediateJob

Legend

** = always comes back*
*** = comes back if fields list not specified on GET all*

redFont = *field is a JSON object (* ***e.g.*** *"repository" :{ "id" : <id>, "name" : <name> })*

Example Response

Expand


```
{
        "type" : "regular",
        "response" : [
                {
                        "id" : "387413",
                        "type" : "repositorySnapshot",
                        "status" : "scheduled",
                        "organization" : {
```

```
                        "id" : -1,
                        "name" : "",
                        "description" : ""                    }
        },
        {
                "id" : "387439",
                "type" : "appStatus",
                "status" : "scheduled",
                "organization" : {
                        "id" : -1,
                        "name" : "",
                        "description" : ""                    }
        },
        {
                "id" : "387440",
                "type" : "licenseReport",
                "status" : "scheduled",
                "organization" : {
                        "id" : -1,
                        "name" : "",
                        "description" : ""                    }
        },
        {
                "id" : "387444",
                "type" : "flushAllVulns",
                "status" : "scheduled",
                "orgID" : "0"           },
        {
                "id" : "387448",
                "type" : "nightlyCleanup",
                "status" : "scheduled",
                "organization" : {
                        "id" : -1,
```

```
                        "name" : "",
                        "description" : ""                    }
                },
                {
                        "id" : "387497",
                        "type" : "updateAllLDAPAssets",
                        "status" : "scheduled",
                        "organization" : {
                                "id" : -1,
                                "name" : "",
                                "description" : ""            }
                },
                {
                        "id" : "387503",
                        "type" : "updateAllDNSAssets",
                        "status" : "scheduled",
                        "organization" : {
                                "id" : -1,
                                "name" : "",
                                "description" : ""            }
                },
                {
                        "id" : "387520",
                        "type" : "feedUpdate",
                        "status" : "scheduled",
                        "organization" : {
                                "id" : -1,
                                "name" : "",
                                "description" : ""            }
                },
                {
                        "id" : "387521",
                        "type" : "lcePluginUpdate",
```

```
                "status" : "scheduled",
                "organization" : {
                        "id" : -1,
                        "name" : "",
                        "description" : ""                    }
        },
        {
                "id" : "387529",
                "type" : "updateIDSCorrelations",
                "status" : "scheduled",
                "organization" : {
                        "id" : -1,
                        "name" : "",
                        "description" : ""                    }
        },
        {
                "id" : "387540",
                "type" : "passivePluginUpdate",
                "status" : "scheduled",
                "organization" : {
                        "id" : -1,
                        "name" : "",
                        "description" : ""                    }
        },
        {
                "id" : "387552",
                "type" : "pluginUpdate",
                "status" : "scheduled",
                "organization" : {
                        "id" : -1,
                        "name" : "",
                        "description" : ""                    }
        },
```

```
        {
                "id" : "387563",
                "type" : "updateIDSSignatures",
                "status" : "scheduled",
                "organization" : {
                        "id" : -1,
                        "name" : "",
                        "description" : ""                    }
        },
        {
                "id" : "387783",
                "type" : "expireAcceptedRisk",
                "status" : "scheduled",
                "organization" : {
                        "id" : -1,
                        "name" : "",
                        "description" : ""                    }
        },
        {
                "id" : "387790",
                "type" : "updateLCEStatus",
                "status" : "scheduled",
                "organization" : {
                        "id" : -1,
                        "name" : "",
                        "description" : ""                    }
        },
        {
                "id" : "387791",
                "type" : "updateLCETypes",
                "status" : "scheduled",
                "organization" : {
                        "id" : -1,
```

```
                                "name" : "",
                                "description" : ""                      }
                },
                {
                        "id" : "387792",
                        "type" : "updateLCESilos",
                        "status" : "scheduled",
                        "organization" : {
                                "id" : -1,
                                "name" : "",
                                "description" : ""                      }
                },
                {
                        "id" : "387793",
                        "type" : "refreshScannerStatus",
                        "status" : "scheduled",
                        "organization" : {
                                "id" : -1,
                                "name" : "",
                                "description" : ""                      }
                }
        ],
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1425331792
}
```


/job/{id}

Methods

GET

Gets the Job associated with {id}.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

```
*id
**organization
**type
**status
objectID
initiator
targetedTime
startTime
pid
params
priority
errorCode
attemptNumber
dependentJobID
immediateJob
```

Legend

** = always comes back*
*** = comes back if fields list not specified on GET all*

redFont = *field is a JSON object (**e.g.** "repository" :{ "id" : <id>, "name" : <name> })*

Request Query Parameters

None

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "id" : "387413",
                "type" : "repositorySnapshot",
                "objectID" : "-1",
                "status" : "scheduled",
                "organization" : {
                        "id" : -1,
                        "name" : "",
                        "description" : ""              },
                "initiator" : {
                        "id" : "1",
                        "username" : "admin",
                        "firstname" : "Admin",
                        "lastname" : "User",
                        "uuid" : "4F7DD1CD-EB1B-40D7-BCE1-2DB3E31F6F4C"
                "targetedTime" : "1425355200",
                "startTime" : "-1",
                "pid" : "-1",
                "params" : "a:0:{}",
                "priority" : "5",
                "errorCode" : "0",
                "attemptNumber" : "1",
                "dependentJobID" : "-1",
                "immediateJob" : "false"        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1425332851
}
```


/job/{id}/kill

Methods

POST

Kills the Job associated with {id}, depending on access.

Request Parameters

None

Example Response

Expand

```
{
        "type" : "regular",
        "response" : "",
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1425334511
}
```

Atlassian

Tenable Security Center API: LCE

/lce

Methods

GET

Gets the list of LCEs.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
**name
**description
**status
ip
ntpIP
port
username
password
privateKeyPassphrase
managedRanges
version
downloadVulns
vulnStatus
lastReportTime
createdTime
modifiedTime
silos
canUse
canManage
organizations
repositories

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*
redFont = *field is a JSON object (* ***e.g.*** *"repository" :{ "id" : <id>, "name" : <name> })*

Request Parameters

None

Example Response

Expand

```
{
    "type" : "regular",
    "response" : [
        {
            "id" : "3",
            "name" : "LCE 192.168.1.11",
            "description" : "",
            "ip" : "192.168.1.11",
            "ntpIP" : "192.168.1.1",
            "port" : "1243",
            "username" : "root",
            "password" : "SET",
                      "privateKeyPassphrase": null,
            "managedRanges" : null,
            "version" : "4.0.2",
            "downloadVulns" : "false",
            "status" : "1",
            "vulnStatus" : "2",
            "lastReportTime" : "0",
            "createdTime" : "1409837073",
            "modifiedTime" : "1409944978",
                      "silos" : [
                              {
                                      "id" : "1",
                                      "file" : "\/opt\/lce\/silo_archive\/\/
Sep132014.ndb",
                                      "startDate" : "Sep 12, 2014",
                                      "endDate" : "Sep 13, 2014",
                                      "records":"0"                   }
                      "organizations" : [
                {
                    "id" : "8",
                    "name" : "Org",
```

```
                    "description" : "Testing for Policies with New
Schema",
                                "uuid" : "4F7DD1CD-EB1B-40D7-BCE1-2DB3E31F6F4
     }
            ],
            "repositories" : [],
            "canUse" : "true",
            "canManage" : "true"        }
    ],
    "error_code" : 0,
    "error_msg" : "",
    "warnings" : [],
    "timestamp" : 1409945528
}
```


POST

Adds an LCE.

Request Parameters

Expand

```
{
       "name" : <string>,
       "description" : <string> DEFAULT "",
       "ip" : <string> (valid IP address or IP addresses separated by a
comma),
       "downloadVulns" : <string> "false" | "true",
       "organizations" : [
              {
                     "id" : <number>,
              "uuid" : <uuid>,
              }...
       ] DEFAULT [],
```

```
        ...
}
```

downloadVulns is "true"

```
{
        ...
        "ntpIP" : <string> (valid IP address, host name, IP addresses
separated by a comma, or host names separated by a comma) DEFAULT
{ip},
        "port" : <number> {valid port) DEFAULT "1243",
        "username" : <string>,
        "password" : <string>,
        "repositories" : [
                {
                        "id" : <number>,
                        "uuid" : <uuid>          }...
        ] DEFAULT []
        ...
}
```

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "organizations" : [
                        {
                                "id" : "8",
                                "name" : "Org",
                                "description" : "Testing for Policies with New
                                "uuid" : "4F7DD1CD-EB1B-40D7-BCE1-2DB3E31F6F4
```

```
                        {
                                "id" : "9",
                                "name" : "Test Org",
                                "description" : "",
                                "uuid" : "FF00F4D0-5B9F-4A26-998C-19430295284A
                ],
                "repositories" : [],
                "id" : "9",
                "name" : "TEST2",
                "description" : "",
                "ip" : "192.168.1.1",
                "ntpIP" : "192.168.1.1",
                "port" : "1243",
                "username" : "",
                "password" : "",
                "privateKeyPassphrase" : "",
                "managedRanges" : null,
                "version" : "Unknown",
                "downloadVulns" : "false",
                "status" : "2",
                "vulnStatus" : "0",
                "lastReportTime" : "0",
                "createdTime" : "1409946064",
                "modifiedTime" : "1409946074",
                "canUse" : "true",
                "canManage" : "true"    },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1409946054
}
```


/lce/authorize

Methods

POST

Authorizes the LCE associated with the provided id or ip to be installed on remote machine, changing only the passed in fields.

NOTE: Either (not both) the ip or the id field must be specified. Alternatively, an lce being authorize by ID may be performed by lce/{id}/authorize::POST

Request Parameters

Expand

```
{
        "id" : <number> OPTIONAL,
        "uuid" : <uuid> OPTIONAL,
        "ip" : <string> (valid IP address) OPTIONAL,
        "username" : <string> DEFAULT "",
        "password" : <string> DEFAULT ""}
```

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "status" : 1,
                "version" : "unknown"   },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1408726631
}
```

/lce/{id}

Methods

GET

Gets the LCE associated with {id}.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

```
*id
**name
**description
**status
ip
ntpIP
port
username
password
managedRanges
version
downloadVulns
vulnStatus
lastReportTime
createdTime
modifiedTime
canUse
canManage
organizations
repositories
```

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

redFont = *field is a JSON object (* ***e.g.*** *"repository" :{ "id" : <id>, "name" : <name> })*

Request Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
        "response" : {
                "organizations" : [
                        {
                                "id" : "8",
                                "name" : "Org",
                                "description" : "Testing for Policies with Nev
                        "uuid" : "4F7DD1CD-EB1B-40D7-BCE1-2DB3E31F6F4C"
                ],
                "repositories" : [],
                "id" : "1",
                "name" : "testlce",
                "description" : "This is being used to test fields",
                "ip" : "192.168.1.1",
                "ntpIP" : "192.168.1.1",
                "port" : "24",
                "username" : "head",
                "password" : "SET",
                "managedRanges" : null,
                "version" : "Unknown",
                "downloadVulns" : "false",
                "status" : "2",
                "vulnStatus" : "2",
                "lastReportTime" : "0",
                "createdTime" : "1408131074",
                "modifiedTime" : "1409945570",
                "canUse" : "true",
```

```
                "canManage" : "true"    },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1409945751
}
```


PATCH

Edits the LCE associated with {id}, changing only the passed in fields.

Request Parameters

(All fields are optional)

See /lce::POST for parameters.

Example Response

See /lce/{id}::GET

DELETE

Deletes the LCE associated with {id}.

Request Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
        "response" : "",
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1408726631
```

```
}
```

/lce/{id}/authorize

Methods

POST

Authorizes the LCE associated with {id} to be installed on remote machine, changing only the passed in fields.

NOTE: To authorize by IP, See /lce/authorize::POST. An ip parameter may not be provided here.

Request Parameters

Expand

```
{
        "username" : <string> DEFAULT "",
        "password" : <string> DEFAULT ""}
```

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "status" : 1,
                "version" : "unknown"   },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1408726631
}
```

/lce/eventTypes

Methods

GET

Request Parameters

Gets the list of LCE event types.

Example Response

Expand


```
{
        "type" : "regular",
        "response" : {
                "types" : [
                        "(unknown)",
                        "access-denied",
                        "application",
                        "connection",
                        "continuous",
                        "data-leak",
                        "database",
                        "detected-change",
                        "dhcp",
                        "dns",
                        "dos",
                        "error",
                        "file-access",
                        "firewall",
                        "honeypot",
                        "indicator",
                        "intrusion",
                        "lce",
                        "login",
```

```
                        "login-failure",
                        "logout",
                        "nbs",
                        "network",
                        "process",
                        "restart",
                        "scanning",
                        "social-networks",
                        "spam",
                        "stats",
                        "system",
                        "threatlist",
                        "unnormalized",
                        "usb",
                        "virus",
                        "vulnerability",
                        "web-access",
                        "web-error"             ]
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1409946200
}
```


Atlassian

Tenable Security Center API: LCE Client

/lce/{id}/client

Methods

GET

Gets the list of LCE Clients associated with LCE server <id>, depending on access and permissions.

Request Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
        "response" : [
                {
                        "clientIP" : "192.168.1.1",
                        "clientType" : "tenableclient",
                        "version" : "v4.x.x.x",
                        "id" : "1",
                        "authorized" : "No",
                        "sensorName" : "unknown",
                        "osType" : "windows",
                        "osNumber" : "2008",
                        "serverIP" : "192.168.1.1",
                        "serverPort" : "31300",
                        "lastUpdated" : -1,
                        "lifeState" : -1,
                        "authState" : -1,
                        "policyFile" : "default_windows_tenableclient.lcp"
                {
                        "clientIP" : "192.168.1.2",
                        "clientType" : "tenableclient",
                        "version" : "v4.x.x.x",
                        "id" : "2",
                        "authorized" : "Yes",
                        "sensorName" : "unknown",
                        "osType" : "windows",
                        "osNumber" : "2008",
                        "serverIP" : "192.168.1.1",
                        "serverPort" : "31300",
```

```
                "lastUpdated" : -1,
                "lifeState" : -1,
                "authState" : -1,
                "policyFile" : "default_windows_tenableclient.lcp"
        {
                "clientIP" : "192.168.1.3",
                "clientType" : "tenableclient",
                "version" : "v4.x.x.x",
                "id" : "3",
                "authorized" : "No",
                "sensorName" : "unknown",
                "osType" : "windows",
                "osNumber" : "2003",
                "serverIP" : "192.168.1.1",
                "serverPort" : "31300",
                "lastUpdated" : -1,
                "lifeState" : -1,
                "authState" : -1,
                "policyFile" : "default_windows_tenableclient.lcp"
        {
                "clientIP" : "192.168.1.4",
                "clientType" : "tenableclient",
                "version" : "v4.x.x.x",
                "id" : "4",
                "authorized" : "No",
                "sensorName" : "unknown",
                "osType" : "windows",
                "osNumber" : "2008",
                "serverIP" : "192.168.1.1",
                "serverPort" : "31300",
                "lastUpdated" : -1,
                "lifeState" : -1,
                "authState" : -1,
```

```
                        "policyFile" : "default_windows_tenableclient.lcp"
                {
                        "clientIP" : "192.168.1.5",
                        "clientType" : "tenableclient",
                        "version" : "v4.x.x.x",
                        "id" : "5",
                        "authorized" : "No",
                        "sensorName" : "unknown",
                        "osType" : "windows",
                        "osNumber" : "2003",
                        "serverIP" : "192.168.1.1",
                        "serverPort" : "31300",
                        "lastUpdated" : -1,
                        "lifeState" : -1,
                        "authState" : -1,
                        "policyFile" : "default_windows_tenableclient.lcp"
        ],
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1409767843
}
```


/lce/{id}/client/types

Methods

GET

Gets the types for the LCE Client associated with {id}.

Request Parameters

None

Example Response

Expand

```
{
        "type" : "regular",
        "response" : [
                "networkmonitor",
                "opsec",
                "netflowclient",
                "sdee",
                "lceclient",
                "wmimonitor",
                "rdep",
                "lcesplunk",
                "tenableclient",
                "reserved"      ],
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1411393801
}
```


/lce/{id}/client/osTypes

Methods

GET

Gets the OS Types for the LCE Client associated with {id}.

Request Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
```

```
        "response" : [
                "rhel",
                "freebsd",
                "debian",
                "osx",
                "windows",
                "aix",
                "solaris",
                "hpux",
                "dragon",
                "fedora",
                "ubuntu",
                "suse",
                "appliance"     ],
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1411393910
}
```

/lce/{serverID}/client/{clientID}

Methods

PATCH

Edits the LCE Client associated with {clientID} in server {serverID}, changing only the passed in fields.

Request Parameters

Expand

```
{
        "sensorName" : <string> OPTIONAL,
        "policyFile" : <string> OPTIONAL
```

```
}
```

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "clientIP" : "192.168.1.1",
                "clientType" : "networkmonitor",
                "version" : "v4.0.1.0",
                "id" : "1",
                "authorized" : "Yes",
                "sensorName" : "unknown",
                "osType" : "rhel",
                "osNumber" : "0",
                "serverIP" : "192.168.1.1",
                "serverPort" : "31300",
                "lastUpdated" : 1409839920,
                "lifeState" : "Alive",
                "authState" : "AUTH_SUCCEEDED",
                "policyFile" : "RMS2_rhel_networkmonitor.lcp"   },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1409839975
}
```

/lce/{serverID}/client/{clientID}/authorize

Methods

POST

Authorizes the LCE Client associated with LCE {lceID} and client {clientID}, depending on access and permissions.

Request Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
        "response" : {
                "clientIP" : "192.168.1.1",
                "clientType" : "wmimonitor",
                "version" : "v4.x.x.x",
                "id" : "1",
                "authorized" : "Yes",
                "sensorName" : "unknown",
                "osType" : "rhel",
                "osNumber" : "5",
                "serverIP" : "192.168.1.1",
                "serverPort" : "31300",
                "lastUpdated" : -1,
                "lifeState" : -1,
                "authState" : -1,
                "policyFile" : "default_rhel_wmimonitor.lcp"    },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1409768302
}
```


/lce/{serverID}/client/{clientID}/revoke

Methods

POST

Revokes authorization for the LCE Client associated with LCE {serverID} and client {clientID}.

Request Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
        "response" : {
                "clientIP" : "192.168.1.1",
                "clientType" : "wmimonitor",
                "version" : "v4.x.x.x",
                "id" : "1",
                "authorized" : "No",
                "sensorName" : "unknown",
                "osType" : "rhel",
                "osNumber" : "5",
                "serverIP" : "192.168.1.1",
                "serverPort" : "31300",
                "lastUpdated" : -1,
                "lifeState" : -1,
                "authState" : -1,
                "policyFile" : "default_rhel_wmimonitor.lcp"    },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1409768331
}
```


Atlassian

Tenable Security Center API: LCE Policy

/lce/{id}/policy

Methods

GET

Gets the list of LCE Policies associated with LCE Server {id}.

Request Parameters

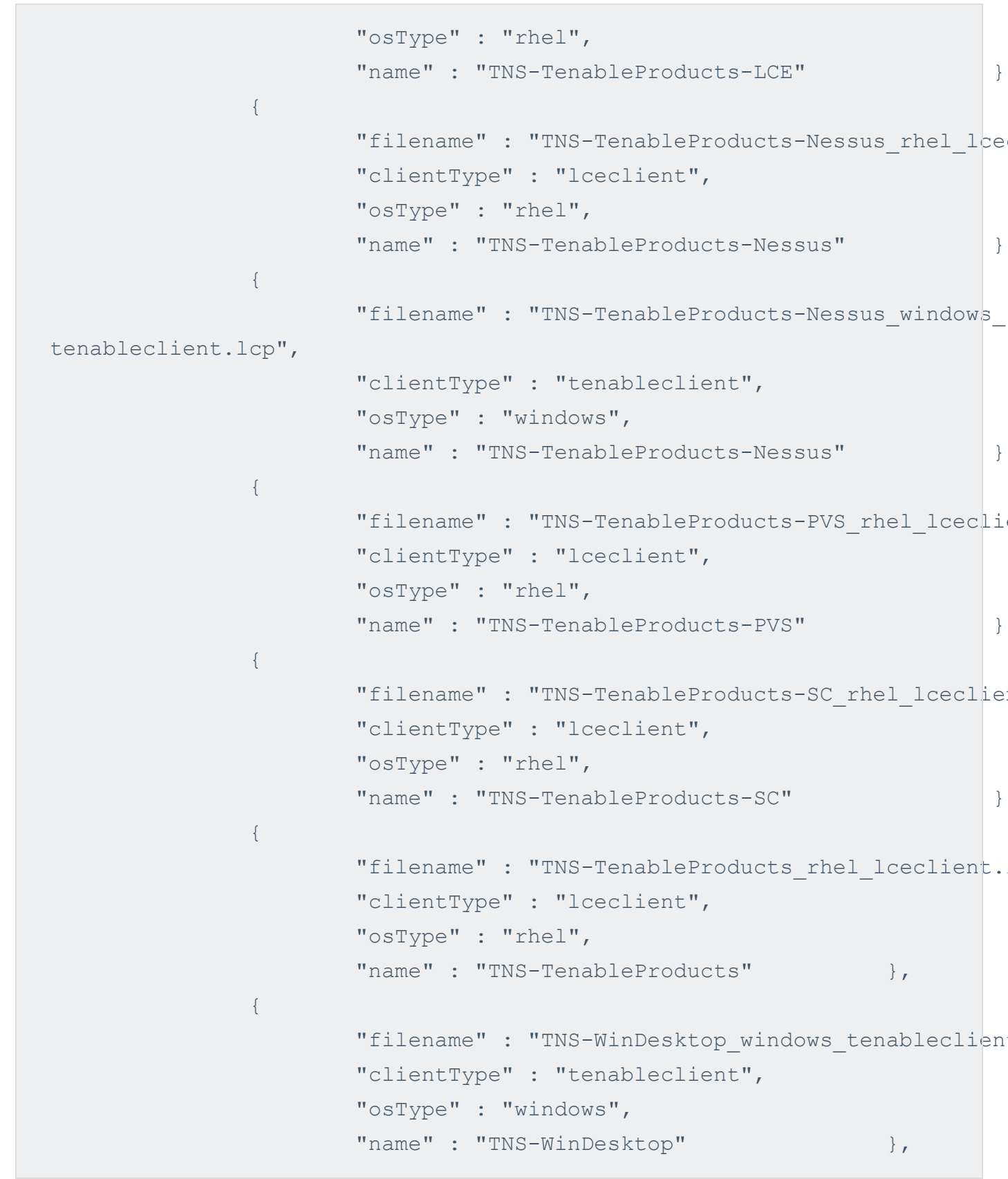
None

Example Response

Expand


```
{
        "type" : "regular",
        "response" : [
                {
                        "filename" : "TNS-MSExchangeServer_windows_tenableclie
                        "clientType" : "tenableclient",
                        "osType" : "windows",
                        "name" : "TNS-MSExchangeServer"         },
                {
                        "filename" : "TNS-MSSQLServer_windows_tenableclient.lc
                        "clientType" : "tenableclient",
                        "osType" : "windows",
                        "name" : "TNS-MSSQLServer"              },
                {
                        "filename" : "TNS-MalwareDetectionOnly_osx_lceclient.l
                        "clientType" : "lceclient",
                        "osType" : "osx",
                        "name" : "TNS-MalwareDetectionOnly"             },
                {
                        "filename" : "TNS-MalwareDetectionOnly_rhel_lceclient
                        "clientType" : "lceclient",
                        "osType" : "rhel",
                        "name" : "TNS-MalwareDetectionOnly"             },
                {
                        "filename" : "TNS-MalwareDetectionOnly_windows_
```

```
tenableclient.lcp",
                        "clientType" : "tenableclient",
                        "osType" : "windows",
                        "name" : "TNS-MalwareDetectionOnly"             },
                {
                        "filename" : "TNS-NTevents-FileSysMon_windows_tenablec
                        "clientType" : "tenableclient",
                        "osType" : "windows",
                        "name" : "TNS-NTevents-FileSysMon"              },
                {
                        "filename" : "TNS-NTevents_windows_tenableclient.lcp",
                        "clientType" : "tenableclient",
                        "osType" : "windows",
                        "name" : "TNS-NTevents"         },
                {
                        "filename" : "TNS-ProcessExecutionOnly_osx_lceclient.l
                        "clientType" : "lceclient",
                        "osType" : "osx",
                        "name" : "TNS-ProcessExecutionOnly"             },
                {
                        "filename" : "TNS-ProcessExecutionOnly_rhel_lceclient
                        "clientType" : "lceclient",
                        "osType" : "rhel",
                        "name" : "TNS-ProcessExecutionOnly"             },
                {
                        "filename" : "TNS-ProcessExecutionOnly_windows_
tenableclient.lcp",
                        "clientType" : "tenableclient",
                        "osType" : "windows",
                        "name" : "TNS-ProcessExecutionOnly"             },
                {
                        "filename" : "TNS-TenableProducts-LCE_rhel_lceclient.l
                        "clientType" : "lceclient",
```


"osType" : "rhel",
"name" : "TNS-TenableProducts-LCE" },
{
"filename" : "TNS-TenableProducts-Nessus_rhel_lceclien
"clientType" : "lceclient",
"osType" : "rhel",
"name" : "TNS-TenableProducts-Nessus" },
{
"filename" : "TNS-TenableProducts-Nessus_windows_
tenableclient.lcp",
"clientType" : "tenableclient",
"osType" : "windows",
"name" : "TNS-TenableProducts-Nessus" },
{
"filename" : "TNS-TenableProducts-PVS_rhel_lceclient.l
"clientType" : "lceclient",
"osType" : "rhel",
"name" : "TNS-TenableProducts-PVS" },
{
"filename" : "TNS-TenableProducts-SC_rhel_lceclient.lc
"clientType" : "lceclient",
"osType" : "rhel",
"name" : "TNS-TenableProducts-SC" },
{
"filename" : "TNS-TenableProducts_rhel_lceclient.lcp",
"clientType" : "lceclient",
"osType" : "rhel",
"name" : "TNS-TenableProducts" },
{
"filename" : "TNS-WinDesktop_windows_tenableclient.lcp
"clientType" : "tenableclient",
"osType" : "windows",
"name" : "TNS-WinDesktop" },

```
        {
                "filename" : "default_aix_lceclient.lcp",
                "clientType" : "lceclient",
                "osType" : "aix",
                "name" : "default"              },
        {
                "filename" : "default_appliance_lceclient.lcp",
                "clientType" : "lceclient",
                "osType" : "appliance",
                "name" : "default"              },
        {
                "filename" : "default_appliance_netflowclient.lcp",
                "clientType" : "netflowclient",
                "osType" : "appliance",
                "name" : "default"              },
        {
                "filename" : "default_appliance_networkmonitor.lcp",
                "clientType" : "networkmonitor",
                "osType" : "appliance",
                "name" : "default"              },
        {
                "filename" : "default_debian_lceclient.lcp",
                "clientType" : "lceclient",
                "osType" : "debian",
                "name" : "default"              },
        {
                "filename" : "default_dragon_lceclient.lcp",
                "clientType" : "lceclient",
                "osType" : "dragon",
                "name" : "default"              },
        {
                "filename" : "default_fedora_lceclient.lcp",
                "clientType" : "lceclient",
```

```
            "osType" : "fedora",
            "name" : "default"              },
        {
            "filename" : "default_freebsd_lceclient.lcp",
            "clientType" : "lceclient",
            "osType" : "freebsd",
            "name" : "default"              },
        {
            "filename" : "default_hpux_lceclient.lcp",
            "clientType" : "lceclient",
            "osType" : "hpux",
            "name" : "default"              },
        {
            "filename" : "default_osx_lceclient.lcp",
            "clientType" : "lceclient",
            "osType" : "osx",
            "name" : "default"              },
        {
            "filename" : "default_rhel_lceclient.lcp",
            "clientType" : "lceclient",
            "osType" : "rhel",
            "name" : "default"              },
        {
            "filename" : "default_rhel_lcesplunk.lcp",
            "clientType" : "lcesplunk",
            "osType" : "rhel",
            "name" : "default"              },
        {
            "filename" : "default_rhel_netflowclient.lcp",
            "clientType" : "netflowclient",
            "osType" : "rhel",
            "name" : "default"              },
        {
```

```
                "filename" : "default_rhel_networkmonitor.lcp",
                "clientType" : "networkmonitor",
                "osType" : "rhel",
                "name" : "default"              },
        {
                "filename" : "default_rhel_opsec.lcp",
                "clientType" : "opsec",
                "osType" : "rhel",
                "name" : "default"              },
        {
                "filename" : "default_rhel_rdep.lcp",
                "clientType" : "rdep",
                "osType" : "rhel",
                "name" : "default"              },
        {
                "filename" : "default_rhel_sdee.lcp",
                "clientType" : "sdee",
                "osType" : "rhel",
                "name" : "default"              },
        {
                "filename" : "default_rhel_wmimonitor.lcp",
                "clientType" : "wmimonitor",
                "osType" : "rhel",
                "name" : "default"              },
        {
                "filename" : "default_solaris_lceclient.lcp",
                "clientType" : "lceclient",
                "osType" : "solaris",
                "name" : "default"              },
        {
                "filename" : "default_suse_lceclient.lcp",
                "clientType" : "lceclient",
                "osType" : "suse",
```

```
                        "name" : "default"              },
                {
                        "filename" : "default_ubuntu_lceclient.lcp",
                        "clientType" : "lceclient",
                        "osType" : "ubuntu",
                        "name" : "default"              },
                {
                        "filename" : "default_windows_tenableclient.lcp",
                        "clientType" : "tenableclient",
                        "osType" : "windows",
                        "name" : "default"              }
        ],
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1409778749
}
```


PUT

Adds an LCE Client to an exiting LCE.

Request Parameters

Expand


```
{
        "overwrite" : <string> "false" | "true" DEFAULT "false",
        "content" : <string>,
        "filePrefix" : <string>,
        "clientType" : <string> "networkmonitor" | "opsec" |
"netflowclient" | "sdee" | "lceclient" | "wmimonitor" | "rdep" |
"lcesplunk" | "tenableclient",
        "osType" : <string> "rhel" | "freebsd" | "debian" | "osx" |
"windows" | "aix" | "solaris" | "hpux" | "dragon" | "fedora" |
```

```
"ubuntu" | "suse"}
```

Example Response

Expand

```
{
       "type" : "regular",
       "response" : {
              "filename" : "file_rhel_networkmonitor.lcp",
              "clientType" : "networkmonitor",
              "osType" : "rhel",
              "name" : "file",
              "content" : "<?xml version=\"1.0\" encoding=\"UTF-8\"
standalone=\"no\"?>\n<options xmlns : xi=\"http :
\/\/www.w3.org\/2003\/XInclude\">\n<example>\n<one>File<\/one>\n<bod-
y>Content<\/body>\n<\/example>\n<\/options>"    },
       "error_code" : 0,
       "error_msg" : "",
       "warnings" : [],
       "timestamp" : 1409933333
}
```

DELETE

Deletes the LCE Policy associated with {id}.

Request Parameters

Expand

```
{
       "filename" : <string>}
```

Example Response

Expand

```
{
    "type" : "regular",
    "response" : "",
    "error_code" : 0,
    "error_msg" : "",
    "warnings" : [],
    "timestamp" : 1409932735
}
```

Atlassian

Tenable Security Center API: LDAP

/ldap

Methods

GET

Gets the list of LDAPS.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

```
*id
**name
**description
**searchString
```

Session user role "1" (Administrator)

host
port
encryption
dn

dnsField
lowercase
timeLimit
password
username
attrEmail
attrName
attrPhone
attrUsername

ldapUserProvisioning

ldapUserSync
createdTime
modifiedTime
organizations

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*
redFont = *field is a JSON object (* ***e.g.*** *"repository" :{ "id" : <id>, "name" : <name> })*

Request Parameters

None

Example Response

Expand

```
{
        "type" : "regular",
        "response" : [
                {
                        "id" : "1",
                        "name" : "Test Name",
                        "description" : "Test Description",
```

```
                        "searchString" : "SearchString"         },
                {
                        "id" : "2",
                        "name" : "testName",
                        "description" : "testDescription",
                        "searchString" : "SearchString"         }
        ],
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1500911088
}
```

POST

Adds an LDAP.

Note: This endpoint is restricted to users of role 1 (Admin)

Request Parameters

Expand

```
{
        "name" : <string>,
        "description" : <string> DEFAULT "",
        "host" : <string> (valid IP or hostname),
        "port" : <string> <valid port),
        "encryption" : <string> "ldaps" | "none" | "tls",
        "dn" : <string>,
        "dnsField" : <string> DEFAULT "dNSHostName",
        "lowercase" : <string> "false" | "true" DEFAULT "false",
        "timeLimit" : <string> DEFAULT "3600",
        "password" : <string> DEFAULT "",
        "username" : <string> DEFAULT "",
        "attrEmail" : <string> DEFAULT "",
```

```
        "attrName" : <string> DEFAULT "",
        "attrPhone" : <string> DEFAULT "",
        "attrUsername" : <string> DEFAULT "",
        "searchString" : <string> DEFAULT "",
        "ldapUserProvisioning : <string> "false" | "true" DEFAULT "false",
        "ldapUserSync" : <string> "false" | "true" DEFAULT "false",
        "organizations" : [
                {
                        "id" : <string>         },...
        ] DEFAULT []
}
```

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "id" : "6",
                "name" : "Test Add LDAP",
                "description" : "Test Description",
                "host" : "127.0.0.1",
                "port" : "80",
                "encryption" : "none",
                "dn" : "Test DN",
                "dnsField" : "Test DNS",
                "lowercase" : "false",
                "timeLimit" : "3600",
                "password" : "SET",
                "username" : "username",
                "attrEmail" : "AttrEmail",
                "attrName" : "AttrName",
                "attrPhone" : "AttrPhone",
```

```
                "attrUsername" : "AttrUsername",
                "ldapUserProvisioning" : "false",
                "ldapUserSync" : "false",
                "searchString" : "SearchString",
                "createdTime" : "1500911435",
                "modifiedTime" : "1500911435",
                "organizations" : [
                        {
                                "id" : "1",
                                "name" : "org1",
                                "description" : "",
                        "uuid" : "4F7DD1CD-EB1B-40D7-BCE1-2DB3E31F6F4C"
                ]
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1500911573
}
```


/ldap/{id}

Methods

GET

Gets the LDAP associated with {id}.

Fields Parameter .

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
**name
**description
**searchString

Session user role "1" (Administrator)

host
port
encryption
dn
dnsField
lowercase
timeLimit
password
username
attrEmail
attrName
attrPhone
attrUsername

ldapUserProvisioning

ldapUserSync
createdTime
modifiedTime
organizations

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*
redFont = *field is a JSON object (* ***e.g.*** *"repository" :{ "id" : <id>, "name" : <name> })*

Request Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
        "response" : {
                "id" : "1",
                "name" : "Test Name",
                "description" : "Test Description",
                "host" : "127.0.0.1",
                "port" : "80",
                "encryption" : "none",
                "dn" : "Test DN",
                "dnsField" : "Test DNS",
                "lowercase" : "false",
                "timeLimit" : "3600",
                "password" : "SET",
                "username" : "username",
                "attrEmail" : "AttrEmail",
                "attrName" : "AttrName",
                "attrPhone" : "AttrPhone",
                "attrUsername" : "AttrUsername",
                "ldapUserProvisioning" : "false",
                "ldapUserSync" : "false",
                "searchString" : "SearchString",
                "createdTime" : "1500911435",
                "modifiedTime" : "1500911435",
                "organizations" : [
                        {
                                "id" : "1",
                                "name" : "org1",
                                "description" : "",
                        "uuid" : "4F7DD1CD-EB1B-40D7-BCE1-2DB3E31F6F4C"
                ]
        },
```

```
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1500911088
}
```


PATCH

Edits the LDAP associated with {id}, changing only the passed in fields.

Note: This endpoint is restricted to users of role 1 (Admin)

Request Parameters

(All fields are optional)

See /ldap::POST for parameters.

Example Response

See /ldap/{id}::GET

DELETE

Deletes the LDAP associated with {id}.

Note: This endpoint is restricted to users of role 1 (Admin)

Request Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
        "response" : "",
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
```

```
        "timestamp" : 1408723358
}
```

/ldap/{id}/query

POST

Retrieves users for the LDAP associated with {id}, depending on access and permissions.

Request Parameters

Expand

```
{
        "match" : <string> DEFAULT "<string:attrUsername>=*" (attrUsername
derived from LDAP)
}
```

Example Response

Expand

```
{
        "type" : "regular",
        "response" : [
                {
                        "name" : "John Doe",
                        "email" : "",
                        "phone" : "",
                        "username" : "JohnDoe"          },
                {
                        "name" : "Jane Doe",
                        "email" : "",
                        "phone" : "",
                        "username" : "Jane Doe"         }
        ],
```

```
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1503416024
}
```

/ldap/test

Methods

POST

Tests the LDAP settings

Note: This endpoint is restricted to users of role 1 (Admin)

Request Parameters

Expand

```
{
        "host" : <string> (valid IP or hostname),
        "port" : <string> <valid port),
        "encryption" : <string> "ldaps" | "none" | "tls",
        "dn" : <string>,
        "dnsField" : <string> DEFAULT "dNSHostName",
        "lowercase" : <string> "false" | "true" DEFAULT "false",
        "timeLimit" : <string> DEFAULT "3600",
        "password" : <string> DEFAULT "",
        "username" : <string> DEFAULT "",
        "attrEmail" : <string> DEFAULT "",
        "attrName" : <string> DEFAULT "",
        "attrPhone" : <string> DEFAULT "",
        "attrUsername" : <string> DEFAULT "",
        "searchString" : <string> DEFAULT ""}
```

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "status" : false,
                "message" : "Verification failed."       },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1410210283}
```


/ldap/{id}/test

Methods

POST

Tests the LDAP settings associated with {id}

Note: This endpoint is restricted to users of role 1 (Admin)

Request Parameters

(All fields are optional)

See /ldap/test::POST for parameters.

Example Response

Expand


```
{
        "type" : "regular",
        "response" : {
                "status" : false,
                "message" : "Verification failed."       },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
```

```
        "timestamp" : 1410210283}
```


Atlassian

Tenable Security Center API: LicenseInfo

/all/licenseInfo

Methods

GET

Gets the license information of the sci this API can only be accessed by admin.

Example Response

Expand


```
{
      "type" : "regular",
      "response" : [{
     "date": 1619496600,
     "licenseLimit": "3840",
     "activeIPs": "72"    },
   {
     "date": 1619583000,
     "licenseLimit": "3840",
     "activeIPs": "72"    },{
     "date": 1619596600,
     "licenseLimit": "3840",
     "activeIPs": "1024"    },
   {
     "date": 1619683000,
     "licenseLimit": "3840",
     "activeIPs": "526"    }],
      "error_code" : 0,
      "error_msg" : "",
```

```
        "warnings" : [],
        "timestamp" : 1410275054
}
```

Atlassian

Tenable Security Center API: Lumin

/lumin/repositories

Methods

PATCH

Edits the Lumin Repositories configuration. Repositories that become enabled are synchronized to Lumin. Synchronization continues for new data from scan results as long as the repository remains enabled. If networks are enabled, the vulnerability data for each repository is synchronized to separate networks in Lumin. Once networks are enabled, this cannot be reversed.

Request Parameters

Expand

```
{
        "ioNetworksEnabled" : <string> "false" | "true",
        "repositories" : [
                {
                        "repID": <string>,
                        "enabledForIOSync": <string> "false" | "true"
        ] DEFAULT []
}
```

Example Response

Expand

```
{
        "type": "regular",
        "response": {
                "2" : {
                        "enabled" : "true",
                        "ioNetworkUUID" : "990a9c09-222d-4771-b25a-1fa7a836432
                        "firstSyncTime" : "1573843474",
                        "lastSyncSuccess" : "1573843474",
                        "lastSyncFailure" : "-1",
                        "details" : ""          },
                "3" : {
                        "enabled" : "true",
                        "ioNetworkUUID" : "b3a472c5-823f-477f-a082-70b32d279d3
                        "firstSyncTime" : "1573843433",
                        "lastSyncSuccess" : "1573843433",
                        "lastSyncFailure" : "-1",
                        "details" : ""          }
                "6" : {
                        "enabled" : "false",
                        "ioNetworkUUID" : "",
                        "firstSyncTime" : "1573843479",
                        "lastSyncSuccess" : "1573843479",
                        "lastSyncFailure" : "-1",
                        "details" : ""          }
                "11" : {
                        "enabled" : "false",
                        "ioNetworkUUID" : "",
                        "firstSyncTime" : "1573843468",
                        "lastSyncSuccess" : "1573843468",
                        "lastSyncFailure" : "-1",
                        "details" : ""          }
        },
        "error_code": 0,
```

```
        "error_msg": "",
        "warnings": [],
        "timestamp": 1572462204
}
```

/lumin/assets

Methods

PATCH

Edits the Lumin Assets configuration. Enabled assets are synchronized to Lumin immediately. Assets are then scheduled to synchronize to Lumin daily at either a random off hours time that is generated automatically or a custom time specified by the user.

NOTE #1: Only static and dynamic Assets are supported.

NOTE #2: Only Assets from the full access group are supported.

Request Parameters

Expand

```
{
        "assets" : [
                {
                        "orgID": <string>,
                        "assetID": <string>,
                        "enabledForIOSync": <string> "false" | "true"
        ] DEFAULT [],
        "schedule" : {
                "type" : "ical" <string> DEFAULT "ical",
                "start" : <string> (This value takes the iCal format) | "auto"
DEFAULT "auto"  }
}
```

Example Response

Expand

```
{
        "type": "regular",
        "response": "",
        "error_code": 0,
        "error_msg": "",
        "warnings": [],
        "timestamp": 1572462204
}
```


/lumin/assets/schedule

Methods

GET

Gets the schedule for daily synchronization of Assets to Lumin.

Request Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
        "response" : {
                "id" : "8",
                "type" : "ical",
                "start" : "TZID=America\/New_York:20200305T230000",
                "repeatRule" : "FREQ=DAILY;INTERVAL=1",
                "nextRun" : 1583467200,
                "autoGenerated" : "true"        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : (Array),
```

```
        "timestamp" : 1583349312
}
```


/lumin/metrics

GET

Gets the Lumin metrics for cyber exposure score, assessment maturity grade, and remediation maturity grade and associated deltas showing the changes from the previous day's calculations.

Request Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
        "response" : {
                "ioCyberExposureScore" : "541",
                "ioAssessmentMaturityGrade" : "50",
                "ioRemediationMaturityGrade" : 24,
                "ioCyberExposureScoreDelta" : "71",
                "ioAssessmentMaturityGradeDelta" : "-20",
                "ioRemediationMaturityGradeDelta" : 5,
                "ioImportHostname" : "cloud.tenable.com",
                "ioAssessmentMaturityGradeLetter" : "C",
                "ioRemediationMaturityGradeLetter" : "D"        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : (Array),
        "timestamp" : 1593098664
}
```


/lumin/test

GET

Tests the connection to Lumin. The connection status returned can be one of the following:

- 0 - connection was successful
- 1 - connection failed
- 2 - connection was successful, but Lumin is not enabled
- 3 - connection was successful, Lumin is enabled, but the Lumin license has expired
- 4 - connection was successful, but the IO container license has expired

Request Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
        "response" : {
                "ioConnectionStatus" : "0"      },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : (Array),
        "timestamp" : 1593098664
}
```


Atlassian

Tenable Security Center API: MDM

/mdm

Methods

GET

Gets the list of MDMs.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

**id
*name
*description
value
editor
ipPref
pluginIDs

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*
redFont = *field is a JSON object (**e.g.** "repository" :{ "id" : <id>, "name" : <name> })*

Request Parameters

None

Example Response

Expand

```
{
        "type" : "regular",
        "response" : [
                {
                        "name" : "ActiveSync",
                        "description" : "",
                        "id" : "1"              },
                {
                        "name" : "Apple Profile Manager",
```

```
                        "description" : "",
                        "id" : "2"              },
                {
                        "name" : "Good MDM",
                        "description" : "",
                        "id" : "3"              },
                {
                        "name" : "Mobile Iron",
                        "description" : "",
                        "id" : "4"              },
                {
                        "name" : "AirWatch MDM",
                        "description" : "",
                        "id" : "5"              },
        {
            "name" : "Blackberry UEM",
            "description" : "",
            "id" : "6"        },
        {
            "name" : "Microsoft Intune",
            "description" : "",
            "id" : "7"        }
        ],
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1425311916
}
```


/mdm/{id}

Methods

GET

Gets the MDM associated with {id}.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

**id
*name
*description
value
editor
ipPref
pluginIDs

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*
redFont = *field is a JSON object (**e.g.** "repository" :{ "id" : <id>, "name" : <name> })*

Request Parameters

None

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "name" : "Apple Profile Manager",
                "value" : "profile_manager",
                "ipPref" : "Apple Profile Manager server  : ",
                "pluginIDs" : [
                        {
```

```
                                "id" : "60032"                  }
                ],
                "description" : "",
                "id" : "2",
                "editor" : "[]" },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1425311962
}
```


Atlassian

Tenable Security Center API: Notification

/notification

Methods

GET

Gets the list of notifications.

NOTE #1: There is currently no means to get all notifications. Rather, only notifications in the valid timeframe values.
NOTE #2: If a retrieved message had a status of 'new', it will be updated to 'sent'

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

**id
initiator
action
type
time

target
changes
effects
status
text

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*
redFont = *field is a JSON object (**e.g.** "repository" :{ "id" : <id>, "name" : <name> })*

Request Parameters

Expand

Parameters must be passed in as query string (as opposed to JSON) in the format of:
/notification?timeframe=24h

```
{
        "timeframe" : "24h" | "7d" | "30d" DEFAULT "24h"}
```

Example Response

Expand

```
{
        "type" : "regular",
        "response" : [
                {
                        "id" : "31",
                        "initiator" : "FeedUpdate",
                        "action" : "end",
                        "type" : "feed",
                        "time" : "1424709857",
                        "target" : {
                                "id" : -1,
```

```
                                "name" : "",
                                "description" : ""                    },
                        "changes" : null,
                        "effects" : [],
                        "status" : "sent",
                        "text" : "Feed Update job completed."          }
        ],
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1425923484
}
```

/notification/{id}

Methods

GET

Gets the notification associated with {id}.

NOTE: If a retrieved message had a status of 'new', it will be updated to 'sent'

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

**id
initiator
action
type
time
target
changes

effects
status
text

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*
redFont = *field is a JSON object (**e.g.** "repository" :{ "id" : <id>, "name" : <name> })*

Request Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
        "response" : {
                "id" : "39",
                "initiator" : "Scan",
                "action" : "end",
                "type" : "scan",
                "time" : "1427230966",
                "target" : {
                        "id" : "15",
                        "name" : "Weekly Scan",
                        "description" : ""              },
                "changes" : null,
                "effects" : [],
                "status" : "sent",
                "text" : "The Scan completed normally." },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
```

```
        "timestamp" : 1427311911
}
```


/notification

Methods

PATCH

Patch the notification update particular id or All notification

NOTE: If required to update status id wise then pass id ex. '1,2,3' and for all notification update pass 'All'

Fields Parameter

None

Request Parameters

Expand

Parameters must be passed in as query string (as opposed to JSON) in the format of: /notification?timeframe=24h


```
{
    "id": "All",
    "status": "new"}
```


Example Response

Expand


```
{
    "type": "regular",
    "response": 0,
    "error_code": 0,
    "error_msg": "",
    "warnings": [],
```

```
    "timestamp": 1664517168
}
```

Atlassian

Tenable Security Center API: Organization

Adds an Organization

This endpoint may only be used by administrators.

/organization

Methods

GET

Gets the list of Organizations

Fields Parameter

Expand

NOTE: This endpoint is still set to return all fields on this call by default. Eventually, this will be merged to provide the minimal set as noted by the legend below.

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
*uuid
**name
**description
email
address
city
state
country
phone

fax
ipInfoLinks
zoneSelection
restrictedIPs
vulnScoreLow
vulnScoreMedium
vulnScoreHigh
vulnScoreCritical
vulnScoringSystem
createdTime
modifiedTime
passwordExpires
passwordExpiration
userCount
lces
repositories
zones
nessusManagers
pubSites
ldaps

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

redFont = *field is a JSON object (* ***e.g.*** *"repository" :{ "id" : <id>, "name" : <name> })*

Request Parameters

None

Example Response

Expand

```
{
        "type" : "regular",
        "response" : [
                {
                        "id" : "8",
                        "name" : "Org",
                        "description" : "New Org",
                        "email" : "",
                        "address" : "",
                        "city" : "",
                        "state" : "",
                        "country" : "",
                        "phone" : "",
                        "fax" : "",
                        "ipInfoLinks" : [
                                {
                                        "name" : "SANS",
                                        "link" : "https:\/\/isc.sans.edu\/ipi
                                {
                                        "name" : "ARIN",
                                        "link" : "http:\/\/whois.arin.net\/res
                        ],
                        "zoneSelection" : "auto_only",
                        "restrictedIPs" : "192.168.1.1",
                        "vulnScoreLow" : "1",
                        "vulnScoreMedium" : "3",
                        "vulnScoreHigh" : "10",
                        "vulnScoreCritical" : "40",
                        "vulnScoringSystem" : "CVSSv2",
                        "createdTime" : "1406321214",
                        "modifiedTime" : "1414509795",
                   "passwordExpires": "true",
               "passwordExpiration": "90",
```

```
                "userCount" : "4",
                    "lces" : [
                            {
                                    "id" : "3",
                                    "name" : "LCE 192.168.1.1",
                                    "description" : "Copied from Box for t
                            {
                                    "id" : "4",
                                    "name" : "NEW LCE",
                                    "description" : "Copied from Box for t
                            {
                                    "id" : "5",
                                    "name" : "qa-lce4x-lifeA",
                                    "description" : "Copied from Box for t
                    ],
                    "repositories" : [
                            {
                                    "id" : "25",
                                    "name" : "IPv6 Rep",
                                    "description" : "",
                                    "type" : "Local",
                                    "dataFormat" : "IPv6",
                                    "groupAssign" : "fullAccess",
                                    "uuid" : "A2FF7E13-2C0E-470E-A3C9-E07
                            {
                                    "id" : "26",
                                    "name" : "agrepo",
                                    "description" : "",
                                    "type" : "Local",
                                    "dataFormat" : "IPv4",
                                    "groupAssign" : "fullAccess",
                                    "uuid" : "29F2B9E1-ADE9-4550-B63C-CEA
                            {
```

```
                                "id" : "27",
                                "name" : "mp asset tests IPv6",
                                "description" : "Copied from QA",
                                "type" : "Local",
                                "dataFormat" : "IPv6",
                                "groupAssign" : "fullAccess",
                                "uuid" : "96F2AD1B-1B83-462E-903A-84E
                        {
                                "id" : "29",
                                "name" : "Test IPv6",
                                "description" : "",
                                "type" : "Local",
                                "dataFormat" : "IPv6",
                                "groupAssign" : "fullAccess",
                                "uuid" : "2DF066B8-F310-44BB-B63E-BC6
                ],
                "zones" : [],
                "ldaps" : [],
                "pubSites" : [
                        {
                                "id":"2","name":"Test1","description"
                ],
                "uuid" : "FF00F4D0-5B9F-4A26-998C-19430295284A"
        {
                "id" : "9",
                "name" : "Test Org 1",
                "description" : "",
                "email" : "",
                "address" : "",
                "city" : "",
                "state" : "",
                "country" : "",
                "phone" : "",
```

```
                "fax" : "",
                "ipInfoLinks" : [
                        {
                                "name" : "SANS",
                                "link" : "https:\/\/isc.sans.edu\/ipi
                        {
                                "name" : "ARIN",
                                "link" : "http:\/\/whois.arin.net\/re
                ],
                "zoneSelection" : "auto_only",
                "restrictedIPs" : "",
                "vulnScoreLow" : "1",
                "vulnScoreMedium" : "3",
                "vulnScoreHigh" : "10",
                "vulnScoreCritical" : "40",
                "vulnScoringSystem" : "CVSSv2",
                "createdTime" : "1409944744",
                "modifiedTime" : "1414521257",
           "passwordExpires": "true",
        "passwordExpiration": "90",
              "userCount" : "1",
                "lces" : [],
                "repositories" : [
                        {
                                "id" : "25",
                                "name" : "IPv6 Rep",
                                "description" : "",
                                "type" : "Local",
                                "dataFormat" : "IPv6",
                                "groupAssign" : "fullAccess",
                                "uuid" : "A2FF7E13-2C0E-470E-A3C9-E07
                        {
                                "id" : "26",
```

```
                                    "name" : "agrepo",
                                    "description" : "",
                                    "type" : "Local",
                                    "dataFormat" : "IPv4",
                                    "groupAssign" : "fullAccess",
                                    "uuid" : "29F2B9E1-ADE9-4550-B63C-CEA
                                {
                                    "id" : "27",
                                    "name" : "mp asset tests IPv6",
                                    "description" : "Copied from QA",
                                    "type" : "Local",
                                    "dataFormat" : "IPv6",
                                    "groupAssign" : "fullAccess",
                                    "uuid" : "96F2AD1B-1B83-462E-903A-84E
                        ],
                        "zones" : [],
                        "ldaps" : [],
                        "nessusManagers" : [],
                        "pubSites" : [],
                        "uuid" : "F8F1B126-1B50-4A65-851A-1168F3283D7B"
        ],
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1418050287
}
```


POST

Adds an Organization

Request Parameters

Expand

NOTE: "zoneSelection" has specific "zone" restrictions noted below:

- *auto_only* cannot have any zones assigned
- *locked* must have one zone assigned
- *selectable* and *selectable+auto_restricted* must have at least one zone assigned
- *selectable+auto* has no restrictions

```
{
       "name" : <string>,
       "passwordExpires" : <string> "false" | "true" OPTIONAL,
       "passwordExpiration" : <number> (a number between 1 and 365)
OPTIONAL,
       "zoneSelection" : <string> "auto_only" | "locked" | "selectable" |
"selectable+auto" | "selectable+auto_restricted",
       "restrictedIPs" : <string> (valid IP address or range of IP
addresses) OPTIONAL,
       "lces" : [
              {
                     "id" : <number>         }...
       ] DEFAULT [],
       "repositories" : [
              {
                     "id" : <number> OR "uuid" : <string>           }...
       ] DEFAULT [],
       "pubSites" : [
              {
                     "id" : <number>         }...
       ] DEFAULT [],
       "zones" : [
              {
                     "id" : <number> OR "uuid" : <string>           }...
       ] DEFAULT [],
       "ldaps" : [
```

```
                {
                        "id" : <number>         }...
        ] DEFAULT [],
        "nessusManagers" : [
                {
                        "id" : <number>         }...
        ] DEFAULT [],
        "vulnScoreLow" : <number> DEFAULT 1,
        "vulnScoreMedium" : <number> DEFAULT 3,
        "vulnScoreHigh" : <number> DEFAULT 10,
        "vulnScoreCritical" : <number> DEFAULT 40,
        "vulnScoringSystem" : <string> "CVSSv2" | "CVSSv3",
        "ipInfoLinks" : [
                {
                        "link" : <string>,
                        "name" : <string>               }
                {
                        "link" : <string>,
                        "name" : <string>               }
        ] DEFAULT []
        ...
}
```

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "id" : "10",
                "name" : "Org Post",
                "description" : "",
                "email" : "",
```

```
            "address" : "",
            "city" : "",
            "state" : "",
            "country" : "",
            "phone" : "",
            "fax" : "",
            "ipInfoLinks" : [
                    {
                            "name" : "SANS",
                            "link" : "https:\/\/isc.sans.edu\/ipinfo.html
                    {
                            "name" : "ARIN",
                            "link" : "http:\/\/whois.arin.net\/rest\/ip\/
            ],
            "zoneSelection" : "auto_only",
            "restrictedIPs" : "",
            "vulnScoreLow" : "1",
            "vulnScoreMedium" : "3",
            "vulnScoreHigh" : "10",
            "vulnScoreCritical" : "40",
            "vulnScoringSystem" : "CVSSv2",
            "createdTime" : "1418052290",
            "modifiedTime" : "1418052290",
       "passwordExpires": "true",
    "passwordExpiration": "90",
            "userCount" : "0",
            "lces" : [
                    {
                            "id" : "5",
                            "name" : "qa-lce4x-lifeA",
                            "description" : "Copied from Box for testing"
            ],
            "repositories" : [
```

```
                        {
                                "id" : "26",
                                "name" : "agrepo",
                                "description" : "",
                                "type" : "Local",
                                "dataFormat" : "IPv4",
                                "groupAssign" : "all",
                                "uuid" : "51C9083D-3AF6-4557-9492-7B25FCF6BAEE
                ],
                "passwordExpires" : "true",
                "passwordExpiration" : "90",
                "zones" : [],
                "ldaps" : [],
                "nessusManagers" : [],
                "pubSites" : [],
                "uuid" : "FF00F4D0-5B9F-4A26-998C-19430295284A" },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1418052290
}
```


/organization/{id}

/organization/{uuid}

Methods

GET

Gets the Organization associated with {id} or {uuid}.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
*uuid
**name
**description
email
address
city
state
country
phone
fax
ipInfoLinks
zoneSelection
restrictedIPs
vulnScoreLow
vulnScoreMedium
vulnScoreHigh
vulnScoreCritical
vulnScoringSystem
createdTime
modifiedTime
passwordExpires
passwordExpiration
userCount
lces
repositories
zones
nessusManagers
pubSites
ldaps

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

redFont = *field is a JSON object (* ***e.g.*** *"repository" :{ "id" : <id>, "name" : <name> })*

Request Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
        "response" : {
                "id" : "8",
                "name" : "Org",
                "description" : "Testing for Policies with New Schema",
                "email" : "",
                "address" : "",
                "city" : "",
                "state" : "",
                "country" : "",
                "phone" : "",
                "fax" : "",
                "ipInfoLinks" : [
                        {
                                "name" : "SANS",
                                "link" : "https:\/\/isc.sans.edu\/ipinfo.html
                        {
                                "name" : "ARIN",
                                "link" : "http:\/\/whois.arin.net\/rest\/ip\/
                ],
                "zoneSelection" : "auto_only",
                "restrictedIPs" : "192.168.1.1",
                "vulnScoreLow" : "1",
                "vulnScoreMedium" : "3",
                "vulnScoreHigh" : "10",
```

```
            "vulnScoreCritical" : "40",
            "vulnScoringSystem" : "CVSSv2",
            "createdTime" : "1406321214",
            "modifiedTime" : "1414509795",
          "passwordExpires": "true",
        "passwordExpiration": "90",
            "userCount" : "4",
            "lces" : [
                    {
                            "id" : "3",
                            "name" : "LCE 192.168.1.1",
                            "description" : "Copied from Box for testing"
                    {
                            "id" : "4",
                            "name" : "NEW LCE",
                            "description" : "Copied from Box for testing"
                    {
                            "id" : "5",
                            "name" : "qa-lce4x-lifeA",
                            "description" : "Copied from Box for testing"
            ],
            "repositories" : [
                    {
                            "id" : "25",
                            "name" : "IPv6 Rep",
                            "description" : "",
                            "type" : "Local",
                            "dataFormat" : "IPv6",
                            "groupAssign" : "fullAccess",
                            "uuid" : "A2FF7E13-2C0E-470E-A3C9-E077FE065A54
                    {
                            "id" : "26",
                            "name" : "agrepo",
```

```
                        "description" : "",
                        "type" : "Local",
                        "dataFormat" : "IPv4",
                        "groupAssign" : "fullAccess",
                        "uuid" : "29F2B9E1-ADE9-4550-B63C-CEA1423E52F
                },
                        "id" : "27",
                        "name" : "mp asset tests IPv6",
                        "description" : "Copied from QA",
                        "type" : "Local",
                        "dataFormat" : "IPv6",
                        "groupAssign" : "fullAccess",
                        "uuid" : "96F2AD1B-1B83-462E-908A-84E6054F6B6
                {
                        "id" : "29",
                        "name" : "Test IPv6",
                        "description" : "",
                        "type" : "Local",
                        "dataFormat" : "IPv6",
                        "groupAssign" : "fullAccess",
                        "uuid" : "2DF066B8-F310-44BB-B6BE-BC6D53DEE0A
        ],
        "zones" : [],
        "ldaps" : [],
        "nessusManagers" : [],
        "pubSites" : [
                {
                        "id":"2","name":"Test1","description":"","type
        ],
        "uuid" : "FF00F4D0-5B9F-4A26-998C-19430295284A" },
"error_code" : 0,
"error_msg" : "",
"warnings" : [],
```

```
        "timestamp" : 1418050303
}
```

PATCH

Edits the Organization associated with {id} or {uuid}, changing only the passed in fields.

Request Parameters

Click here to expand...

All fields are optional.

See /organization::POST for parameters.

NOTE: Additionally, each "repositories" object may have an extra parameter "allUsers" not listed for the POST:

```
{
        ...
        "repositories" : [
                {
                        "id" : <number> OR "uuid" : <string>,
                        "allUsers" : <string> "false" | "true" OPTIONAL
                }...
        ]
        ...
}
```

Example Response

See /organization/{id}::GET

DELETE

Deletes the Organization associated with {id} or {uuid}, depending on access and permissions.

Request Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
        "response" : "",
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1408726272
}
```


/organization/{id}/acceptRiskRule

/organization/{uuid}/acceptRiskRule

Methods

GET

Gets the list of Accept Risk Rules in the Organization associated with {id} or {uuid}, unless filters are provided.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
**repository
**organization
**user
**plugin
**hostType
**hostValue
**port
**protocol

**expires
**status
comments
createdTime
modifiedTime

Legend

** = always comes back*
*** = comes back if fields list not specified on GET all*

redFont = *field is a JSON object (* ***e.g.*** *"repository" :{ "id" : <id>, "name" : <name> })*

Filters

Expand

```
repositoryIDs=<number>,... DEFAULT 0 (i.e. all Repositories) OR
repositoryUUIDs=<string>,...
pluginID=<number> | <string> "all" DEFAULT "all" (i.e. all Plugins)
port=<number> | <string> "all" DEFAULT "all" (i.e. all Ports)
```

Example Response

Expand

```
{
      "type" : "regular",
      "response" : [
              {
                      "id" : "3",
                      "hostType" : "all",
                      "hostValue" : "",
                      "port" : "any",
                      "protocol" : "any",
                      "expires" : "-1",
                      "status" : "0",
                      "repository" : {
```

```
                                "id" : "17",
                                "name" : "New Fields Repo",
                                "description" : "",
                                "type" : "Local",
                                "uuid" : "FF00F4D0-5B9F-4A26-998C-19430295284
                        "organization" : {
                                "id" : "8",
                                "name" : "Org",
                                "description" : "Testing for Policies with Ne
                                "uuid" : "2E950182-08B6-4737-830B-4ACC8F6B92F
                        "user" : {
                                "id" : "1",
                                "username" : "head",
                                "firstname" : "Security Manager",
                                "lastname" : "",
                                "uuid" : "A2FF7E13-2C0E-470E-A3C9-E077FE065A5
                        "plugin" : {
                                "id" : "0",
                                "name" : "Open Port",
                                "description" : "",
                 "type" : "active"                      }
                }
        ],
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1410275054
}
```


/organization/{id}/recastRiskRule

/organization/{uuid}/recastRiskRule

Methods

GET

Gets the list of Recast Risk Rules in the Organization associated with {id} or {uuid}, unless filters are provided.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
**repository
**organization
**user
**plugin
**newSeverity
**hostType
**hostValue
**port
**protocol
**order
**status
comments
createdTime
modifiedTime

Legend

** = always comes back*
*** = comes back if fields list not specified on GET all*

redFont = *field is a JSON object (* ***e.g.*** *"repository" :{ "id" : <id>, "name" : <name> })*

Filters

Expand

```
repositoryIDs=<number>,... DEFAULT 0 (i.e. all Repositories) OR
repositoryUUIDs=<string>,...
pluginID=<number> | <string> "all" DEFAULT "all" (i.e. all Plugins)
port=<number> | <string> "all" DEFAULT "all" (i.e. all Ports)
```

Example Response

Expand


```
{
	"type" : "regular",
	"response" : [
		{
			"id" : "1",
			"newSeverity" : "0",
			"hostType" : "all",
			"hostValue" : "",
			"port" : "any",
			"protocol" : "any",
			"order" : "1",
			"status" : "0",
			"repository" : {
				"id" : "18",
				"name" : "New Rep 1",
				"description" : "",
				"type" : "Local",
				"uuid" : "FF00F4D0-5B9F-4A26-998C-19430295284A
			"organization" : {
				"id" : "8",
				"name" : "Org",
				"description" : "Testing for Policies with New
				"uuid" : "2E950182-08B6-4737-830B-4ACC8F6B92F9
			"user" : {
				"id" : "1",
```

```
                                "username" : "head",
                                "firstname" : "Security Manager",
                                "lastname" : "",
                                "uuid" : "A2FF7E13-2C0E-470E-A3C9-E077FE065A54
                        "plugin" : {
                                "id" : "0",
                                "name" : "Open Port",
                                "description" : "",
                    "type" : "active"                       }
                }
        ],
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1410281615
}
```


Atlassian

Tenable Security Center API: Organization Security Manager

passwordSetDate

This endpoint should only be used by administrators and will only impact Security Managers in the Full Access Group.

/organization/{orgID}/securityManager

/organization/{orgUUID}/securityManager

Methods

GET

Retrieves all Security Managers in an Organization.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
*uuid
**firstname
**lastname
**status
role
username
title
email
address
city
state
country
phone
fax
createdTime
modifiedTime
lastLogin
lastLoginIP
mustChangePassword
passwordExpires
passwordExpiration
passwordExpirationOverride
passwordSetDate
locked
failedLogins
authType
fingerprint
password
description
managedUsersGroups
managedObjectsGroups

canUse
canManage
preferences
responsibleAsset
group
ldapUsername
ldap
parent

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

redFont = *field is a JSON object (* ***e.g.*** *"repository" :{ "id" : <id>, "name" : <name> })*

Request Parameters

None

Example Response

Expand

```
{
        "type" : "regular",
        "response" : [
                {
                        "id" : "1",
                        "status" : "0",
                        "username" : "head",
                        "ldapUsername" : "head",
                        "firstname" : "",
                        "lastname" : "",
                        "title" : "",
                        "email" : "",
                        "address" : "",
```

```
"city" : "",
"state" : "",
"country" : "",
"phone" : "",
"fax" : "",
"createdTime" : "1433519288",
"modifiedTime" : "1453477493",
"lastLogin" : "1454347644",
"lastLoginIP" : "172.26.0.0",
"mustChangePassword" : "false",
"passwordExpires": "true",
"passwordExpiration": "90",
"passwordExpirationOverride": "false",
"passwordSetDate": "1433519288",
"locked" : "false",
"failedLogins" : "0",
"authType" : "tns",
"fingerprint" : null,
"password" : "SET",
"managedUsersGroups" : [
        {
                "id" : "-1",
                "name" : "All Groups",
                "description" : "All Groups"
],
"managedObjectsGroups" : [
        {
                "id" : "-1",
                "name" : "All Groups",
                "description" : "All Groups"
],
"preferences" : [
        {
```

```
                                        "name" : "timezone",
                                        "value" : "America/Nome",
                                        "tag" : "system"
                        ],
                        "canUse" : true,
                        "canManage" : true,
                        "role" : {
                                "id" : "2",
                                "name" : "Security Manager",
                                "description" : "The Security Manager role has
all actions at the organization level. A Security Manager has the
ability to create new groups and manage existing ones. A Security
Manager can also define how users interact with other groups.\n\nThe
ability to manage other users and their objects can be configured
using group permissions on the Access tab of User add/edit. This
includes viewing and stopping running scans and reports."
                        "responsibleAsset" : {
                                "id" : "19",
                                "name" : "Windows Hosts",
                                "description" : "The operating system detected
installed.\n\nThis will be helpful for those getting started with
Tenable.sc.",
                                "uuid" : "2DF066B8-F310-44BB-B6BE-BC6D53DEE0AE
                        "group" : {
                                "id" : "0",
                                "name" : "Full Access",
                                "description" : "Full Access group"
                        "ldap" : {
                                "id" : -1,
                                "name" : "",
                                "description" : ""                    },
                        "parent" : {
                                "user" {
```

```
                                        "id" : "1",
                                        "username" : "admin",
                                        "firstname" : "Jane",
                                        "lastname" : "Doe",
                                        "uuid" : "C7FBF99F-DA90-4E67-893F-9245
                                "organization" : {
                                        "id" : "0",
                                        "name" : "Tenable.sc Administration",
                                        "description" : ""
                        },
                        "uuid" : "48F26F3B-6A79-4153-96DB-4C63D1BF3D46"
                }
        ],
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1454349445
}
```


POST

Adds a Security Manager.

Request Parameters

Expand

```
{
        "roleID" : <number>,
        "username" : <string>,
        "firstname" : <string> DEFAULT "",
        "lastname" : <string> DEFAULT "",
        "title" : <string> DEFAULT "",
        "email" : <string> DEFAULT "" (required to be present and valid if
emailNotice is not empty and is not "none"),
```

```
        "address" : <string> DEFAULT "",
        "city" : <string> DEFAULT "",
        "state" : <string> DEFAULT "",
        "country" : <string> DEFAULT "",
        "phone" : <string> DEFAULT "",
        "fax" : <string> DEFAULT "",
        "locked" : <string> "false" | "true" DEFAULT "false",
        "authType" : <string> "ldap" | "legacy" |  "saml" | "tns",
        "fingerprint" : <string> DEFAULT null,
        "mustChangePassword" : <string> "false" | "true" DEFAULT "false",
        "emailNotice" :  <string> "both" | "id" | "none" | "password"
DEFAULT "",
        "responsibleAssetID" : <number> OR "responsibleAssetUUID" :
<string>,
        "preferences" : [
                {
                        "name" : <string>,
                        "tag" : <string> DEFAULT "",
                        "value" : <string>              }...
        ] DEFAULT [
                {
                        "name" : "timezone",
                        "tag" : "system",
                        "value" : <string> (default timezone)
                }
        ]
}
```

authType "ldap"

Note: The "ldapUsername" attribute will be set to mirror the "username" attribute.

```
...
        "mustChangePassword" : <string> "false" DEFAULT "false",
```

```
        "ldap" : {
                "id" : <string> }
...
```

authType "saml"

```
...
        "mustChangePassword" : <string> "false" DEFAULT "false"...
```

authType not "ldap" or "saml"

```
...
        "password" : <string> (must meet the requirements for configuration
setting, "PasswordMinLength"),
        "mustChangePassword" : <string> "false" | "true" DEFAULT "false",
        "passwordExpires" : <string> "false" | "true" DEFAULT "false",
        "passwordExpiration" : <number> (a number between 1 and 365)
DEFAULT 90,
        "passwordExpirationOverride" : <string> "false" | "true" DEFAULT
"false",
...
```

authType "linked" or "linked_non_admin"

Note: If the authType is linked_non_admin, the roleID must be the SM-Linked roleID.

```
...
        "parent" : {
                "id" : <number> DEFAULT "-1"    }
...
```

Session user's role can manage group relationships or Session user role "1" (Administrator)

```
...
       "managedUsersGroups" : [
                {
                        "id" : <number>         }...
       ],
       "managedObjectsGroups" : [
                {
                        "id" : <number>         }...
       ]
...
```

roleID not "1" (Administrator)

WARNING: The parameters in this section have been DEPRECATED as of Tenable.sc 5.11.0. Relying on their usage is highly discouraged. See /group::POST (createDefaultObjects parameter).

```
...
       "importReports" : <string> "false" | "true" DEFAULT <Target Group's
createDefaultObjects setting> ,
       "importDashboards" : <string> "false" | "true" DEFAULT <Target
Group's createDefaultObjects setting>,
       "importARCs" : <string> "false" | "true" DEFAULT <Target Group's
createDefaultObjects setting>,

       "importDashboards" is "true"    ----------------------------
       "dashboardTemplate" : <string> (File path to template) DEFAULT
<Default filepath>,

       "importARCs" is "true"  ----------------------
       "arcTemplate" : <string> (File path to template) DEFAULT <Default
filepath>,
...
```

Example Response

Expand


```
{
        "type" : "regular",
        "response" : {
                "id" : "1",
                "status" : "0",
                "username" : "head",
                "ldapUsername" : "",
                "firstname" : "",
                "lastname" : "",
                "title" : "",
                "email" : "",
                "address" : "",
                "city" : "",
                "state" : "",
                "country" : "",
                "phone" : "",
                "fax" : "",
                "createdTime" : "1433519288",
                "modifiedTime" : "1453477493",
                "lastLogin" : "1454347644",
                "lastLoginIP" : "172.20.0.0",
                "mustChangePassword" : "false",
                "passwordExpires": "true",
                "passwordExpiration": "90",
                "passwordExpirationOverride": "false",
                "passwordSetDate": "1433519288",
                "locked" : "false",
                "failedLogins" : "0",
                "authType" : "tns",
                "fingerprint" : null,
                "password" : "SET",
                "managedUsersGroups" : [
```

```
                        {
                                "id" : "-1",
                                "name" : "All Groups",
                                "description" : "All Groups"
                ],
                "managedObjectsGroups" : [
                        {
                                "id" : "-1",
                                "name" : "All Groups",
                                "description" : "All Groups"
                ],
                "preferences" : [
                        {
                                "name" : "timezone",
                                "value" : "America/Nome",
                                "tag" : "system"                        }
                ],
                "canUse" : true,
                "canManage" : true,
                "role" : {
                        "id" : "2",
                        "name" : "Security Manager",
                        "description" : "The Security Manager role has full ac
actions at the organization level. A Security Manager has the
ability to create new groups and manage existing ones. A Security
Manager can also define how users interact with other groups.\n\nThe
ability to manage other users and their objects can be configured
using group permissions on the Access tab of User add/edit. This
includes viewing and stopping running scans and reports."               },
                "responsibleAsset" : {
                        "id" : "19",
                        "name" : "Windows Hosts",
                        "description" : "The operating system detected has Wi
```

```
installed.\n\nThis will be helpful for those getting started with
Tenable.sc.",
                        "uuid" : "2DF066B8-F310-44BB-B6BE-BC6D5BDEE0AB"
                "group" : {
                        "id" : "0",
                        "name" : "Full Access",
                        "description" : "Full Access group"            },
                "ldap" : {
                        "id" : -1,
                        "name" : "",
                        "description" : ""              },
                "parent" : {
                        "user" {
                                "id" : "1",
                                "username" : "admin",
                                "firstname" : "Jane",
                                "lastname" : "Doe",
                                "uuid" : "C7FBF99F-DA90-4E67-898F-9245CC21BDCE
                        "organization" : {
                                "id" : "0",
                                "name" : "Tenable.sc Administration",
                                "description" : ""                      }
                },
                "uuid" : "48F26F3B-6A79-4153-96DB-4C63D1BF3D46"
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1454349746
}
```


/organization/{orgID}/securityManager/{id}

/organization/{orgUUID}/securityManager/{uuid}

Methods

GET

Gets a specific Security Manager.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
*uuid
**firstname
**lastname
**status
role
username
title
email
address
city
state
country
phone
fax
createdTime
modifiedTime
lastLogin
lastLoginIP
mustChangePassword
passwordExpires
passwordExpiration
passwordExpirationOverride
passwordSetDate
locked

failedLogins
authType
fingerprint
password
description
managedUsersGroups
managedObjectsGroups
canUse
canManage
preferences
responsibleAsset
group
ldap
ldapUsername
parent
linkedUserRole

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

redFont = *field is a JSON object (* ***e.g.*** *"repository" :{ "id" : <id>, "name" : <name> })*

Request User Parameters

None

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "id" : "1",
                "status" : "0",
```

```
"username" : "head",
"ldapUsername" : "",
"firstname" : "",
"lastname" : "",
"title" : "",
"email" : "",
"address" : "",
"city" : "",
"state" : "",
"country" : "",
"phone" : "",
"fax" : "",
"createdTime" : "1433519288",
"modifiedTime" : "1453477493",
"lastLogin" : "1454347644",
"lastLoginIP" : "172.20.0.0",
"mustChangePassword" : "false",
"passwordExpires": "true",
"passwordExpiration": "90",
"passwordExpirationOverride": "false",
"passwordSetDate": "1433519288",
"locked" : "false",
"failedLogins" : "0",
"authType" : "tns",
"fingerprint" : null,
"password" : "SET",
"managedUsersGroups" : [
        {
                "id" : "-1",
                "name" : "All Groups",
                "description" : "All Groups"
],
"managedObjectsGroups" : [
```

```
                        {
                                "id" : "-1",
                                "name" : "All Groups",
                                "description" : "All Groups"
                ],
                "preferences" : [
                        {
                                "name" : "timezone",
                                "value" : "America/Nome",
                                "tag" : "system"                        }
                ],
                "canUse" : true,
                "canManage" : true,
                "role" : {
                        "id" : "2",
                        "name" : "Security Manager",
                        "description" : "The Security Manager role has full ac
actions at the organization level. A Security Manager has the
ability to create new groups and manage existing ones. A Security
Manager can also define how users interact with other groups.\n\nThe
ability to manage other users and their objects can be configured
using group permissions on the Access tab of User add/edit. This
includes viewing and stopping running scans and reports."               },
                "responsibleAsset" : {
                        "id" : "19",
                        "name" : "Windows Hosts",
                        "description" : "The operating system detected has Wi
installed.\n\nThis will be helpful for those getting started with
Tenable.sc.",
                        "uuid" : "2DF066B8-F310-44BB-B6BE-BC6D5BDEE0AB"
                "group" : {
                        "id" : "0",
                        "name" : "Full Access",
```

```
                        "description" : "Full Access group"             },
                "ldap" : {
                        "id" : -1,
                        "name" : "",
                        "description" : ""              },
                "parent" : {
                        "user" {
                                "id" : "0",
                                "username" : "admin",
                                "firstname" : "Jane",
                                "lastname" : "Doe",
                                "uuid" : "C7FBF99F-DA90-4E67-898F-9245CC21BDCE
                        "organization" : {
                                "id" : "0",
                                "name" : "Tenable.sc Administration",
                                "description" : ""                      }
                },
                "linkedUserRole": {
                "id": "8",
                "name": "SM-Linked",
                "description": "description"           },
                "uuid" : "48F26F3B-6A79-4153-96DB-4C63D1BF3D46"
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1454349746
}
```


PATCH

Edits the Security Manager associated with {id} or {uuid}.

If editing a linked user (a user whose *authType* = "linked" or *authType* = "linked_non_admin"), you cannot modify *roleID*, *groupID*, *authType* , *parent, password, or mustChangePassword,*

passwordExpires, passwordExpirationOverride.

Request Parameters

(All fields are optional)

See /organization/{orgID}/securityManager::POST and /organization/{orgUUID}/securityManager::POST for parameters.

Example Response

See /organization/{orgID}/securityManager/{id}::GET and /organization/orgUUID/securityManager/{uuid}::GET.

DELETE

Deletes the Security Manager associated with {id} or {uuid}.

The objects owned by the user being deleted can be migrated to another user in the same organization by passing in the optional *migrateUserID* (or *migrateUserUUID*) parameter.

Request Parameters

Expand

```
{
    "migrateUserID": <number> OPTIONAL OR "migrateUserUUID":
<number> OPTIONAL
}
```

Example Response

Expand

```
{
       "type" : "regular",
       "response" : "",
       "error_code" : 0,
       "error_msg" : "",
       "warnings" : [],
       "timestamp" : 1402436001
```

```
}
```

Atlassian

Tenable Security Center API: Organization User

This endpoint may only be used by administrators.

/organization/{orgID}/user

/organization/{orgUUID}/user

Methods

GET

Gets the list of Security Managers in an organization.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
*uuid
**firstname
**lastname
**username
canUse
canManage

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

Request User Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
        "response" : [
                {
                        "id" : "1",
                        "username" : "head",
                        "firstname" : "",
                        "lastname" : "",
                        "canUse" : true,
                        "canManage" : true,
                        "uuid": "48F26F3B-6A79-4153-96DB-4C63D1BF3D46"
                {
                        "id" : "36",
                        "username" : "GroupA",
                        "firstname" : "",
                        "lastname" : "",
                        "canUse" : true,
                        "canManage" : true,
                        "uuid" : "85EE961D-6DB0-47F9-88C9-F210055E37CF"
                },
                {
                        "id" : "37",
                        "username" : "GroupB",
                        "firstname" : "",
                        "lastname" : "",
                        "canUse" : true,
                        "canManage" : true,
                        "uuid" : "C4368F74-77F3-4723-8399-D3C88348D5D1"
```

```
        ],
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1454348491
}
```


/organization/{orgID}/user/{id}

/organization/{orgUUID}/user/{uuid}

Methods

GET

Gets a specific Security Manager.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
*uuid
**firstname
**lastname
**status
role
username
title
email
address
city
state
country

phone
fax
createdTime
modifiedTime
lastLogin
lastLoginIP
mustChangePassword
locked
failedLogins
authType
fingerprint
password
description
responsibleAsset
group
managedUsersGroups
managedObjectsGroups
orgName
canUse
canManage
preferences
ldap
ldapUsername
parent

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

redFont = *field is a JSON object (**e.g.** "repository" :{ "id" : <id>, "name" : <name> })*

Request User Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
        "response" : {
                "id" : "1",
                "status" : "0",
                "username" : "head",
                "ldapUsername" : "",
                "firstname" : "",
                "lastname" : "",
                "title" : "",
                "email" : "",
                "address" : "",
                "city" : "",
                "state" : "",
                "country" : "",
                "phone" : "",
                "fax" : "",
                "createdTime" : "1433519288",
                "modifiedTime" : "1453477493",
                "lastLogin" : "1454347644",
                "lastLoginIP" : "172.168.0.1",
                "mustChangePassword" : "false",
                "locked" : "false",
                "failedLogins" : "0",
                "authType" : "tns",
                "fingerprint" : null,
                "password" : "SET",
                "managedUsersGroups" : [
                        {
                                "id" : "-1",
                                "name" : "All Groups",
                                "description" : "All Groups"
```

```
                ],
                "managedObjectsGroups" : [
                        {
                                "id" : "-1",
                                "name" : "All Groups",
                                "description" : "All Groups"
                ],
                "preferences" : [
                        {
                                "name" : "timezone",
                                "value" : "America/Nome",
                                "tag" : "system"                        }
                ],
                "canUse" : true,
                "canManage" : true,
                "role" : {
                        "id" : "2",
                        "name" : "Security Manager",
                        "description" : "The Security Manager role has full ac
actions at the organization level. A Security Manager has the
ability to create new groups and manage existing ones. A Security
Manager can also define how users interact with other groups.\n\nThe
ability to manage other users and their objects can be configured
using group permissions on the Access tab of User add/edit. This
includes viewing and stopping running scans and reports."               },
                "responsibleAsset" : {
                        "id" : "19",
                        "name" : "Windows Hosts",
                        "description" : "The operating system detected has Wi
installed.\n\nThis will be helpful for those getting started with
Tenable.sc."            },
                "group" : {
                        "id" : "0",
```

```
                        "name" : "Full Access",
                        "description" : "Full Access group"            },
                "ldap" : {
                        "id" : "-1",
                        "name" : "",
                        "description" : ""              },
                "parent" : {
                        "user" : {
                                "id" : "1",
                                "username" : "admin",
                                "firstname" : "Jane",
                                "lastname" : "Doe",
                                "uuid" : "18C16668-F942-407D-B7E0-4EEB8523F42
                        "organization" : {
                                "id" :"0",
                                "name" : "Tenable.sc Administration",
                                "description" : ""                      }
                }
                "uuid" : "48F26F3B-6A79-4153-96DB-4C63D1BF3D46" },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1454348768
}
```


Atlassian

Tenable Security Center API: Passive Scanner (NNM)

/passivescanner

Methods

GET

Gets the list of Nessus Network Monitors.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
**name
**description
**status
ip
port
useProxy
enabled
verifyHost
authType
cert
username
password
version
webVersion
admin
uptime
pluginSet
loadedPluginSet
lastReportTime
createdTime
modifiedTime
repositories

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

Request Query Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
        "response" : [
                {
                        "id" : "1",
                        "name" : "My Nessus Network Monitor",
                        "description" : "",
                        "ip" : "192.168.1.1",
                        "port" : "8835",
                        "useProxy" : "false",
                        "enabled" : "true",
                        "verifyHost" : "true",
                        "authType" : "password",
                        "cert" : null,
                        "username" : "nonadmin",
                        "password" : "SET",
                        "version" : null,
                        "webVersion" : null,
                        "admin" : "false",
                        "uptime" : -1,
                        "status" : "8",
                        "pluginSet" : null,
                        "loadedPluginSet" : null,
                        "lastReportTime" : "0",
                        "lastCommunication" : "0",
                        "createdTime" : "1402434305",
                        "modifiedTime" : "1402434804",
                        "repositories" : [
                                {
```

```
                                        "id" : "100",
                                        "name" : "Test Repo 192.168.1.0\/16",
                                        "description" : "",
                                        "dataFormat" : "IPv4",
                    "type": "Local",
                    "uuid": "FC06DB42-AA49-4BDC-B28F-C60818292339"
                 },
                        ]
                }
        ],
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1402434305
}
```


POST

Adds a Nessus Network Monitor.

Request Parameters

Expand


```
{
        "name" : <string>,
        "description" : <string> DEFAULT "",
        "authType" : <string> "certificate" | "password" DEFAULT
"password",
        "ip" : <string>,
        "port" : <number>,
        "useProxy" : <string> "true" | "false" DEFAULT "false",
        "verifyHost" : <string> "true" | "false" DEFAULT "true",
        "enabled" : <string> "true" | "false" DEFAULT "true",
        "repositories" : [
```

```
                {
                        "id" : <number>          }
        ] DEFAULT []
...
}
```

authType "certificate"

```
...
        "cert" : <string>,
        "password" : <string> DEFAULT "".
...
```

authType "password"

```
...
        "username" : <string>,
        "password" : <string>,
        "certificatePassword" : <string>...
```

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "id" : "1",
                "name" : "My Nessus Network Monitor",
                "description" : "",
                "ip" : "192.168.1.1",
                "port" : "8835",
                "useProxy" : "false",
                "enabled" : "true",
```

```
                "verifyHost" : "true",
                "authType" : "password",
                "cert" : null,
                "username" : "nonadmin",
                "password" : "SET",
                "version" : null,
                "webVersion" : null,
                "admin" : "false",
                "uptime" : -1,
                "status" : "8",
                "pluginSet" : null,
                "loadedPluginSet" : null,
                "lastReportTime" : "0",
                "lastCommunication" : "0",
                "createdTime" : "1402434305",
                "modifiedTime" : "1402434804",
                "repositories" : [
                        {
                                "id" : "100",
                                "name" : "Test Repo 192.168.1.0\/16",
                                "description" : "",
                                "dataFormat" : "IPv4",
                 "type": "Local",
                 "uuid": "FC06DB42-AA49-4BDC-B28F-C60818292339"
                ]
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1401827513
}
```


/passivescanner/{id}

Methods

GET

Gets the Nessus Network Monitor associated with {id}.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
**name
**description
**status
ip
port
useProxy
enabled
verifyHost
authType
cert
username
password
version
webVersion
admin
uptime
pluginSet
loadedPluginSet
lastReportTime
createdTime
modifiedTime
repositories

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

Request Query Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
        "response" : {
                "id" : "1",
                "name" : "My Nessus Network Monitor",
                "description" : "",
                "ip" : "192.168.1.1",
                "port" : "8835",
                "useProxy" : "false",
                "enabled" : "true",
                "verifyHost" : "true",
                "authType" : "password",
                "cert" : null,
                "username" : "nonadmin",
                "password" : "SET",
                "version" : null,
                "webVersion" : null,
                "admin" : "false",
                "uptime" : -1,
                "status" : "8",
                "pluginSet" : null,
                "loadedPluginSet" : null,
                "lastReportTime" : "0",
                "lastCommunication" : "0",
                "createdTime" : "1402434305",
                "modifiedTime" : "1402434804",
```

```
                "repositories" : [
                        {
                                "id" : "100",
                                "name" : "Test Repo 192.168.1.0\/16",
                                "description" : "",
                                "dataFormat" : "IPv4",
                 "type": "Local",
                 "uuid": "FC06DB42-AA49-4BDC-B28F-C60818292339"
                ]
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1401834305
}
```


PATCH

Edits the Nessus Network Monitor Scanner associated with {id}, changing only the passed in fields.

Request Parameters

(All fields are optional)

See /passivescanner::POST for parameters.

Example Response

See /passivescanner/{id}::GET

DELETE

Deletes the Nessus Network Monitor associated with {id}, depending on access and permissions.

Request Parameters

None

Example Response

Expand

```
{
        "type" : "regular",
        "response" : "",
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1402435235
}
```


/passivescanner/updateStatus

POST

Starts an on-demand scanner status update for all Nessus Network Monitors.

Request Parameters

None.

Example Response

Expand


```
{
        "type" : "regular",
        "response" : [
                {
                        "id" : "1",
                        "name" : "My Nessus Network Monitor Scanner",
                        "description" : "",
                        "status" : "8200"               }
        ],
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1402435137
}
```

Tenable Security Center API: Plugin

/plugin

Methods

GET

Gets all the Plugins matching the filters, if provided.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
**name
**description
family
type
copyright
version
sourceFile
dependencies
requiredPorts
requiredUDPPorts
cpe
srcPort
dstPort
protocol
riskFactor
solution
seeAlso
synopsis
checkType

exploitEase
exploitAvailable
exploitFrameworks
cvssVector
cvssVectorBF
baseScore
temporalScore
cvssV3Vector
cvssV3VectorBF
cvssV3BaseScore
cvssV3TemporalScore
vprScore
vprContext
stigSeverity
pluginPubDate
pluginModDate
patchPubDate
patchModDate
vulnPubDate
modifiedTime
md5
agent
xrefs

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

Request Parameters

Expand

Parameters must be passed in as query string (as opposed to JSON) in the format of: /plugin?filterField=id&op=eq&value=1&...

NOTE #1: parameter "since" refers to plugins that have been modified since a given date.

NOTE #2: The <string> portion of the "xrefs:<string>" parameter is associated with a valid Xref field type. Valid Xref types at the time of this documentation are:

"ALAS" | "APPLE-SA" | "AUSCERT" | "BID" | "CERT" | "CERT-CC" | "CERT-FI" | "CERTA" | "CISCO-BUG-ID" | "CISCO-SA" | "CISCO-SR" | "CLSA" | "CONECTIVA" | "CVE" | "CWE" | "DSA" | "EDB-ID" | "FEDORA" | "FLSA" | "FreeBSD" | "GLSA" | "HP" | "HPSB" | "IAVA" | "IAVB" | "IAVT" | "ICS-ALERT" | "ICSA" | "MDKSA" | "MDVSA" | "MGASA" | "MSFT" | "MSVR" | "NSFOCUS" | "NessusID" | "OSVDB" | "OWASP" | "OpenPKG-SA" | "RHSA" | "SSA" | "Secunia" | "SuSE" | "TLSA" | "TSLSA" | "USN" | "VMSA" | "zone-h"

NOTE #3: The parameter "filters" allows filtering using multiple filters sent as json object.

- The values for index filterField in filters param is same as the 'filterField' request param.
- The values for index filterOperator in filters param is same as the 'op' request param.

If filterField param is send in request then filters param cannot be used.

```
{
       "filterField" : <string>  "copyright" | "description" |
"exploitAvailable" | "family" | "id" | "name" | "patchPubDate" |
"patchModDate" | "pluginPubDate" | "pluginModDate" | "sourceFile" |
"type" | "version" | "vulnPubDate" | "xrefs" | "xrefs:<string>" (see
Note #2 above) OPTIONAL,
       "sortDirection" : <string> "ASC" | "DESC" DEFAULT "DESC",
       "sortField" : <string> "modifiedTime" | "id" | "name" | "family" |
"type" DEFAULT "modifiedTime",
       "type" : <string> "active" | "all" | "compliance" | "custom" |
"lce" | "notPassive" | "passive" DEFAULT "all",
       "startOffset" : <number> (positive integer) DEFAULT 0,
       "endOffset" : <number> (integer >= startOffset) DEFAULT 50,
       "since" : <number> (Epoch Seconds) DEFAULT 0,
       "filters": <string>
[{"filterField":"","filterOperator":"","filterString":""}...]
OPTIONAL,
       ...
}
```

filterField is specified and filterField is not "type"

```
{
        ...
        "op" : <string> "eq" | "gt" | "gte" | "like" | "lt" | "lte",
        "value" : <string>      ...
}
```

filterField is "type"

```
{
        ...
        "op" : <string> "eq" | "gt" | "gte" | "like" | "lt" | "lte",
        "value" : <string> "active" | "passive" | "lce" | "compliance" |
"custom"        ...
}
```

Example Response

Expand

```
{
        "type":"regular",
        "response":[
                {
                        "id":"15000",
                        "name":"Debian DSA-163-1 : mhonarc - XSS",
                        "description":"Jason Molenda and Hiromitsu Takagi fou
exploit cross site\nscripting bugs in mhonarc, a mail to HTML
converter. When processing\nmaliciously crafted mails of type
text\/html mhonarc does not\ndeactivate all scripting parts
properly. This is fixed in upstream\nversion 2.5.3.\n\nIf you are
worried about security, it is recommended that you disable\nsupport
of text\/html messages in your mail archives. There is no\nguarantee
that the mhtxthtml.pl library is robust enough to eliminate\nall
```

```
possible exploits that can occur with HTML data.\n\nTo exclude HTML
data, you can use the MIMEEXCS resource. For example :\n\n
<MIMEExcs> text\/html text\/x-html <\/MIMEExcs>\n\nThe type
'text\/x-html' is probably not used any more, but is good
to\ninclude it, just-in-case.\n\nIf you are concerned that this
could block out the entire contents of\nsome messages, then you
could do the following instead :\n\n    <MIMEFilters> text\/html;
m2h_text_plain::filter; mhtxtplain.pl\n    text\/x-html; m2h_text_
plain::filter; mhtxtplain.pl <\/MIMEFilters>\n\nThis treats the HTML
as text\/plain.\n\nThe above problems have been fixed in version
2.5.2-1.1 for the\ncurrent stable distribution (woody), in version
2.4.4-1.1 for the old\nstable distribution (potato) and in version
2.5.11-1 for the unstable\ndistribution (sid)."         },
               {
                       "id":"15004",
                       "name":"Debian DSA-167-1 : kdelibs - XSS",
                       "description":"A cross site scripting problem has beer
in Konqueror, a\nfamous browser for KDE and other programs using
KHTML. The KDE team\nreportsthat Konqueror's cross site scripting
protection fails to\ninitialize the domains on sub-(i)frames
correctly. As a result,\nJavaScript is able to access any foreign
subframe which is defined in\nthe HTML source. Users of Konqueror
and other KDE software that uses\nthe KHTML rendering engine may
become victim of a cookie stealing and\nother cross site scripting
attacks."               }
      ],
      "error_code":0,
      "error_msg":"",
      "warnings":[],
      "timestamp":1411668488
}
```


/plugin/{id}

Methods

GET

Gets the Plugin associated with {id}.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
**name
**description
family
type
copyright
version
sourceFile
source
dependencies
requiredPorts
requiredUDPPorts
cpe
srcPort
dstPort
protocol
riskFactor
solution
seeAlso
synopsis
checkType
exploitEase
exploitAvailable
exploitFrameworks
cvssVector

cvssVectorBF
baseScore
temporalScore
cvssV3Vector
cvssV3VectorBF
cvssV3BaseScore
cvssV3TemporalScore
vprScore
vprContext
stigSeverity
pluginPubDate
pluginModDate
patchPubDate
patchModDate
vulnPubDate
modifiedTime
md5
agent
xrefs

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

Request Parameters

None

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "id" : "0",
```

```
            "name" : "Open Port",
            "description" : "",
            "type" : "active",
            "copyright" : "",
            "version" : "",
            "sourceFile" : "",
            "dependencies" : "",
            "requiredPorts" : "",
            "requiredUDPPorts" : "",
            "cpe" : "",
            "srcPort" : null,
            "dstPort" : null,
            "protocol" : "",
            "riskFactor" : "",
            "solution" : "",
            "seeAlso" : "",
            "synopsis" : "",
            "checkType" : "",
            "exploitEase" : "",
            "exploitAvailable" : "",
            "exploitFrameworks" : "",
            "cvssVector" : "",
            "cvssVectorBF" : "0",
            "baseScore" : null,
            "temporalScore" : null,
            "cvssV3Vector" : "",
            "cvssV3VectorBF" : "0",
            "cvssV3BaseScore" : null,
            "cvssV3TemporalScore" : null,
            "vprScore" : "6.1",
        "vprContext" : [
                        {
                                "id" : "age_of_vuln",
```

```
                "name" : "Vulnerability Age",
                "value" : "730 days +",
                "type" : "string"                    },
            {
                "id" : "cvssV3_impactScore",
                "name" : "CvssV3 Impact Score",
                "value" : 5.5,
                "type" : "number"                    },
            {
                "id" : "exploit_code_maturity",
                "name" : "Exploit Code Maturity",
                "value" : "PoC",
                "type" : "string"                    },
            {
                "id" : "generated_at",
                "name" : "Generated At",
                "value" : 1551695021993,
                "type" : "number"                    },
            {
                "id" : "predicted_impactScore",
                "name" : "Predicted Impact Score",
                "value" : true,
                "type" : "boolean"                   },
            {
                "id" : "product_coverage",
                "name" : "Product Coverage",
                "value" : "Low",
                "type" : "string"                    },
            {
                "id" : "threat_model_type",
                "name" : "Threat Model Type",
                "value" : "non_early_life",
                "type" : "string"                    },
```

```
                {
                        "id" : "threat_model_version",
                        "name" : "Threat Model Version",
                        "value" : "v0",
                        "type" : "string"                       },
                {
                        "id" : "threat_intensity_last_28",
                        "name" : "Threat Intensity Last 28",
                        "value" : "Very Low",
                        "type" : "string"                       },
                {
                        "id" : "threat_recency",
                        "name" : "Threat Recency",
                        "value" :  "No recorded events",
                        "type" : "string"                       },
                {
                        "id" : "threat_sources_last_28",
                        "name" : "Threat Sources Last 28",
                        "value" : "No recorded events",
                        "type" : "string"                       }
        ],
        "stigSeverity" : null,
        "pluginPubDate" : "-1",
        "pluginModDate" : "-1",
        "patchPubDate" : "-1",
        "patchModDate" : "-1",
        "vulnPubDate" : "-1",
        "modifiedTime" : "1400516102",
        "md5" : "",
        "agent" : "false",
        "xrefs" : "",
        "source" : "",
        "family" : {
```

```
                        "id" : "42",
                        "name" : "Port scanners",
                        "type" : "active"                }
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1408727888
}
```


Atlassian

Tenable Security Center API: Plugin Family

/pluginFamily

Methods

GET

Gets the list of Plugin Families

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
**name
type
count*

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

** = The field "count" signifies how many plugins in the family match the filter (if provided), not how many plugins are in the family. To get the total count of plugins in a family, do not provide any filters.*

Request Parameters

Expand

Parameters must be passed in as query string (as opposed to JSON) in the format of: /plugin?filterField=id&op=eq&value=1&...

NOTE #1: The parameters below are plugin filter parameters that are applied to get a list of families that contain plugins matching the defined filters.

NOTE #2: parameter "since" refers to plugins that have been modified since a given date.

NOTE #3: The <string> portion of the "xrefs:<string>" parameter is associated with a valid Xref field type. Valid Xref types at the time of this documentation are:

"ALAS" | "APPLE-SA" | "AUSCERT" | "BID" | "CERT" | "CERT-CC" | "CERT-FI" | "CERTA" | "CISCO-BUG-ID" | "CISCO-SA" | "CISCO-SR" | "CLSA" | "CONECTIVA" | "CVE" | "CWE" | "DSA" | "EDB-ID" | "FEDORA" | "FLSA" | "FreeBSD" | "GLSA" | "HP" | "HPSB" | "IAVA" | "IAVB" | "IAVT" | "ICS-ALERT" | "ICSA" | "MDKSA" | "MDVSA" | "MGASA" | "MSFT" | "MSVR" | "NSFOCUS" | "NessusID" | "OSVDB" | "OWASP" | "OpenPKG-SA" | "RHSA" | "SSA" | "Secunia" | "SuSE" | "TLSA" | "TSLSA" | "USN" | "VMSA" | "zone-h"

```
{
      "filterField" : <string>  "copyright" | "description" |
"exploitAvailable" | "family" | "id" | "name" | "patchPubDate" |
"patchModDate" | "pluginPubDate" | "pluginModDate" | "sourceFile" |
"type" | "version" | "vulnPubDate" | "xrefs" | "xrefs:<string>" (see
Note #3 above) OPTIONAL,
      "sortDirection" : <string> "ASC" | "DESC" DEFAULT "DESC",
      "sortField" : <string> "modifiedTime" | "id" | "name" | "family" |
"type" DEFAULT "modifiedTime",
      "type" : <string> "active" | "all" | "compliance" | "custom" |
"lce" | "notPassive" | "passive" DEFAULT "all",
      "since" : <number> (Epoch Seconds) DEFAULT 0,
      ...
```

```
}
```

filterField is specified and filterField is not "type"

```
{
        ...
        "op" : <string> "eq" | "gt" | "gte" | "like" | "lt" | "lte",
        "value" : <string>      ...
}
```

filterField is "type"

```
{
        ...
        "op" : <string> "eq" | "gt" | "gte" | "like" | "lt" | "lte",
        "value" : <string> "active" | "passive" | "lce" | "compliance" |
"custom"        ...
}
```

Filter Parameters

active - Only active Plugin Families will be returned. By default, both active and passive Plugin Families are returned.
passive - Only passive Plugin Families will be returned. By default, both active and passive Plugin Families are returned.

Example Response

Expand

```
{
        "type" : "regular",
        "response" : [
                {
                        "id" : "9",
```

```
                "name" : "AIX Local Security Checks"            },
        {
                "id" : "1000022",
                "name" : "Abuse"                },
        {
                "id" : "54",
                "name" : "Amazon Linux Local Security Checks"
        {
                "id" : "35",
                "name" : "Backdoors"            },
        {
                "id" : "1000001",
                "name" : "Backdoors"            },
        {
                "id" : "49",
                "name" : "Brute force attacks"          },
        {
                "id" : "1000002",
                "name" : "CGI"          },
        {
                "id" : "6",
                "name" : "CGI abuses"           },
        {
                "id" : "26",
                "name" : "CGI abuses  :  XSS"           },
        {
                "id" : "33",
                "name" : "CISCO"                },
        {
                "id" : "18",
                "name" : "CentOS Local Security Checks"         },
        {
                "id" : "1000031",
```

```
                "name" : "Cloud Services"               },
        {
                "id" : "37",
                "name" : "DNS"          },
        {
                "id" : "1000004",
                "name" : "DNS Servers"          },
        {
                "id" : "1000024",
                "name" : "Data Leakage"         },
        {
                "id" : "1000003",
                "name" : "Database"             },
        {
                "id" : "31",
                "name" : "Databases"            },
        {
                "id" : "3",
                "name" : "Debian Local Security Checks"         },
        {
                "id" : "25",
                "name" : "Default Unix Accounts"                },
        {
                "id" : "22",
                "name" : "Denial of Service"            },
        {
                "id" : "19",
                "name" : "FTP"          },
        {
                "id" : "1000027",
                "name" : "FTP Clients"          },
        {
                "id" : "1000006",
```

```
                "name" : "FTP Servers"          },
        {
                "id" : "5",
                "name" : "Fedora Local Security Checks"         },
        {
                "id" : "1000005",
                "name" : "Finger"               },
        {
                "id" : "44",
                "name" : "Finger abuses"                },
        {
                "id" : "34",
                "name" : "Firewalls"            },
        {
                "id" : "13",
                "name" : "FreeBSD Local Security Checks"
        {
                "id" : "40",
                "name" : "Gain a shell remotely"                },
        {
                "id" : "27",
                "name" : "Gain root remotely"           },
        {
                "id" : "30",
                "name" : "General"              },
        {
                "id" : "1000007",
                "name" : "Generic"              },
        {
                "id" : "7",
                "name" : "Gentoo Local Security Checks"         },
        {
                "id" : "2",
```

```
                "name" : "HP-UX Local Security Checks"          },
        {
                "id" : "1000008",
                "name" : "IMAP Servers"         },
        {
                "id" : "1000010",
                "name" : "IRC Clients"          },
        {
                "id" : "1000026",
                "name" : "IRC Servers"          },
        {
                "id" : "1000009",
                "name" : "Internet Messengers"          },
        {
                "id" : "1000028",
                "name" : "Internet Services"            },
        {
                "id" : "50",
                "name" : "Junos Local Security Checks"          },
        {
                "id" : "21",
                "name" : "MacOS X Local Security Checks"
        {
                "id" : "1000030",
                "name" : "Malware"              },
        {
                "id" : "16",
                "name" : "Mandrake Local Security Checks"
        {
                "id" : "47",
                "name" : "Mandriva Local Security Checks"
        {
                "id" : "23",
```

```
                "name" : "Misc."                },
        {
                "id" : "52",
                "name" : "Mobile Devices"               },
        {
                "id" : "1000029",
                "name" : "Mobile Devices"               },
        {
                "id" : "0",
                "name" : "N\/A"         },
        {
                "id" : "46",
                "name" : "NIS"          },
        {
                "id" : "43",
                "name" : "Netware"              },
        {
                "id" : "1000011",
                "name" : "Operating System Detection"           },
        {
                "id" : "53",
                "name" : "Oracle Linux Local Security Checks"
        {
                "id" : "1000013",
                "name" : "POP Server"           },
        {
                "id" : "55",
                "name" : "Palo Alto Local Security Checks"
        {
                "id" : "32",
                "name" : "Peer-To-Peer File Sharing"            },
        {
                "id" : "1000012",
```

```
                "name" : "Peer-To-Peer File Sharing"            },
        {
                "id" : "1000023",
                "name" : "Policy"               },
        {
                "id" : "39",
                "name" : "Policy Compliance"            },
        {
                "id" : "42",
                "name" : "Port scanners"                },
        {
                "id" : "28",
                "name" : "RPC"          },
        {
                "id" : "1000014",
                "name" : "RPC"          },
        {
                "id" : "1",
                "name" : "Red Hat Local Security Checks"
        {
                "id" : "17",
                "name" : "Remote file access"           },
        {
                "id" : "36",
                "name" : "SCADA"                },
        {
                "id" : "1000025",
                "name" : "SCADA"                },
        {
                "id" : "1000016",
                "name" : "SMTP Clients"         },
        {
                "id" : "1000017",
```

```
                "name" : "SMTP Servers"          },
        {
                "id" : "12",
                "name" : "SMTP problems"                 },
        {
                "id" : "45",
                "name" : "SNMP"          },
        {
                "id" : "1000018",
                "name" : "SNMP Traps"            },
        {
                "id" : "1000019",
                "name" : "SSH"           },
        {
                "id" : "1000015",
                "name" : "Samba"                 },
        {
                "id" : "51",
                "name" : "Scientific Linux Local Security Checks"
        {
                "id" : "24",
                "name" : "Service detection"             },
        {
                "id" : "41",
                "name" : "Settings"              },
        {
                "id" : "15",
                "name" : "Slackware Local Security Checks"
        {
                "id" : "4",
                "name" : "Solaris Local Security Checks"
        {
                "id" : "8",
```

```
                "name" : "SuSE Local Security Checks"           },
        {
                "id" : "14",
                "name" : "Ubuntu Local Security Checks"         },
        {
                "id" : "38",
                "name" : "Useless services"             },
        {
                "id" : "48",
                "name" : "VMware ESX Local Security Checks"
        {
                "id" : "1000020",
                "name" : "Web Clients"          },
        {
                "id" : "11",
                "name" : "Web Servers"          },
        {
                "id" : "1000021",
                "name" : "Web Servers"          },
        {
                "id" : "20",
                "name" : "Windows"              },
        {
                "id" : "10",
                "name" : "Windows  :  Microsoft Bulletins"
        {
                "id" : "29",
                "name" : "Windows  :  User management"          }
    ],
    "error_code" : 0,
    "error_msg" : "",
    "warnings" : [],
    "timestamp" : 1408728112
```

```
}
```

/pluginFamily/{id}

Methods

GET

Gets the Plugin Family associated with {id}.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
**name
type
count
plugins

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

red = field is a JSON object (e.g. "SCI" : {"id" : "2", "name" : "SCI Name", "description" : "Description"})

Request Parameters

None

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "id" : "1000030",
                "name" : "Malware",
                "type" : "passive",
                "plugins" : [],
                "count" : 0
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1408728549
}
```


/pluginFamily/{id}/plugins::GET

Methods

GET

Gets the Plugins associated with Family {id} matching the filters, if provided.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

*id
**name
**description
family
type
copyright
version
sourceFile
source

dependencies
requiredPorts
requiredUDPPorts
cpe
srcPort
dstPort
protocol
riskFactor
solution
seeAlso
synopsis
checkType
exploitEase
exploitAvailable
exploitFrameworks
cvssVector
cvssVectorBF
baseScore
temporalScore
cvssV3Vector
cvssV3VectorBF
cvssV3BaseScore
cvssV3TemporalScore
vprScore
vprContext
stigSeverity
pluginPubDate
pluginModDate
patchPubDate
patchModDate
vulnPubDate
modifiedTime
md5
xrefs

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

red = field is a JSON object (e.g. "SCI" : {"id" : "2", "name" : "SCI Name", "description" : "Description"})

Request Parameters

Expand

Parameters must be passed in as query string (as opposed to JSON) in the format of: /plugin?filterField=id&op=eq&value=1&...

NOTE #1: parameter "since" refers to plugins that have been modified since a given date.

NOTE #2: The <string> portion of the "xrefs:<string>" parameter is associated with a valid Xref field type. Valid Xref types at the time of this documentation are:

"ALAS" | "APPLE-SA" | "AUSCERT" | "BID" | "CERT" | "CERT-CC" | "CERT-FI" | "CERTA" | "CISCO-BUG-ID" | "CISCO-SA" | "CISCO-SR" | "CLSA" | "CONECTIVA" | "CVE" | "CWE" | "DSA" | "EDB-ID" | "FEDORA" | "FLSA" | "FreeBSD" | "GLSA" | "HP" | "HPSB" | "IAVA" | "IAVB" | "IAVT" | "ICS-ALERT" | "ICSA" | "MDKSA" | "MDVSA" | "MGASA" | "MSFT" | "MSVR" | "NSFOCUS" | "NessusID" | "OSVDB" | "OWASP" | "OpenPKG-SA" | "RHSA" | "SSA" | "Secunia" | "SuSE" | "TLSA" | "TSLSA" | "USN" | "VMSA" | "zone-h"

```
{
       "filterField" : <string>  "copyright" | "description" |
"exploitAvailable" | "family" | "id" | "name" | "patchPubDate" |
"patchModDate" | "pluginPubDate" | "pluginModDate" | "sourceFile" |
"type" | "version" | "vulnPubDate" | "xrefs" | "xrefs:<string>" (see
Note #2 above) OPTIONAL,
       "sortDirection" : <string> "ASC" | "DESC" DEFAULT "DESC",
       "sortField" : <string> "modifiedTime" | "id" | "name" | "family" |
"type" DEFAULT "modifiedTime",
       "type" : <string> "active" | "all" | "compliance" | "custom" |
"lce" | "notPassive" | "passive" DEFAULT "all",
       "startOffset" : <number> (positive integer) DEFAULT 0,
```

```
        "endOffset" : <number> (integer >= startOffset) DEFAULT 50,
        "since" : <number> (Epoch Seconds) DEFAULT 0,
        ...
}
```

filterField is specified and filterField is not "type"

```
{
        ...
        "op" : <string> "eq" | "gt" | "gte" | "like" | "lt" | "lte",
        "value" : <string>      ...
}
```

filterField is "type"

```
{
        ...
        "op" : <string> "eq" | "gt" | "gte" | "like" | "lt" | "lte",
        "value" : <string> "active" | "passive" | "lce" | "compliance" |
"custom"        ...
}
```

Example Response

Expand

```
{
        "type" : "regular",
        "response" : [
                {
                        "id" : "27063",
                        "name" : "HP-UX PHSS_36869 : HP System Management Home
for HP-UX, XSS (HPSBMA02274 SSRT071445 rev.3)",
                        "description" : "s700_800 11.11 HP System Management H
```

```
A.2.2.6.2 : \n\nPotential security vulnerabilities have been
identified with HP System\nManagement Homepage (SMH) for HP-UX.
These vulnerabilities could by\nexploited remotely to allow cross
site scripting (XSS)."          },
               {
                       "id" : "27064",
                       "name" : "HP-UX PHSS_36870 : HP System Management Home
for HP-UX, XSS (HPSBMA02274 SSRT071445 rev.3)",
                       "description" : "s700_800 11.23 HP System Management H
A.2.2.6.2 : \n\nPotential security vulnerabilities have been
identified with HP System\nManagement Homepage (SMH) for HP-UX.
These vulnerabilities could by\nexploited remotely to allow cross
site scripting (XSS)."          },
               {
                       "id" : "27065",
                       "name" : "HP-UX PHSS_36871  :  HP System Management Ho
(SMH) for HP-UX, XSS (HPSBMA02274 SSRT071445 rev.3)",
                       "description" : "s700_800 11.31 HP System Management H
A.2.2.6.2 : \n\nPotential security vulnerabilities have been
identified with HP System\nManagement Homepage (SMH) for HP-UX.
These vulnerabilities could by\nexploited remotely to allow cross
site scripting (XSS)."          }
       ],
       "error_code" : 0,"error_msg" : "",
       "warnings" : [],
       "timestamp" : 1411997624
}
```


Atlassian

Tenable Security Center API: Publishing Site

/pubSite

Methods

GET

Gets the list of Publishing Sites.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
**name
**description
type
uri
useProxy
authType
cert
username
password
verifyHost
maxChunkSize
createdTime
modifiedTime

Session user role "1" (Administrator)

organizations

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

Request Query Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
        "response" : [
                {
                        "id" : "2",
                        "name" : "test",
                        "description" : "desc",
                        "type" : "HTTP POST",
                        "uri" : "http:\/\/192.168.1.1\/test",
             "useProxy" : "false",
                        "authType" : "password",
                        "cert" : "",
                        "username" : "test",
                        "password" : "SET",
             "verifyHost" : "true",
                        "maxChunkSize" : "0",
                        "createdTime" : "1404245619",
                        "modifiedTime" : "1404245619"           }
        ],
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1404247733
}
```


POST

Adds a Publishing Site.

Request Parameters

Expand

```
{
       "name" : <string>,
       "description" : <string> DEFAULT "",
       "type" : <string> "HTTP POST" | "CMRS",
       "maxChunkSize" : <number> DEFAULT 0,
       "uri" : <string>,
    "useProxy" : <boolean> DEFAULT false,
       "authType" : <string> "certificate" | "password",
    "cert" : SET|NOT_SET,
    "username" : <string>,
    "password" : <string>,
    "verifyHost" : <boolean> DEFAULT true,
       "organizations" : [
               {
                       "id" : <number>                "uuid": <uuid>
       ]
...
}
```

authType "certificate"

```
...
       "cert" : <string>...
```

authType "password"

```
...
       "username" : <string>,
       "password" : <string>...
```

Example Response

Expand

```
{
        "type" : "regular",
        "response" : [
                {
                        "id" : "2",
                        "name" : "test",
                        "description" : "desc",
                        "type" : "HTTP POST",
                        "uri" : "http:\/\/192.168.1.1\/test",
            "useProxy" : "false",
                        "authType" : "password",
                        "cert" : "",
                        "username" : "test",
                        "password" : "SET",
            "verifyHost" : "true",
                        "maxChunkSize" : "0",
                        "createdTime" : "1404245619",
                        "modifiedTime" : "1404245619",
                        "organizations":[
                            {
                        "id": "1",
                        "name": "lab",
                        "description": "",
                        "uuid": "A21BF1F3-DAB2-4053-9E84-4EA2722C3851"
         }
                        ]
                },
        ],
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1404247733
}
```

/pubSite/{id}

Methods

GET

Gets the Publishing Site associated with {id}.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
**name
**description
type
uri
useProxy
authType
cert
username
password
verifyHost
maxChunkSize
createdTime
modifiedTime

Session user role "1" (Administrator)

organizations

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

Request Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
        "response" : {
                "id" : "2",
                "name" : "test",
                "description" : "desc",
                "type" : "HTTP POST",
                "uri" : "http:\/\/192.168.1.1\/test",
         "useProxy" : "false",
                "authType" : "password",
                "cert" : "",
                "username" : "test",
                "password" : "SET",
         "verifyHost" : "true",
                "maxChunkSize" : "0",
                "createdTime" : "1404245619",
                "modifiedTime" : "1404245619"   },      "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1404247733
}
```


PATCH

Edits the Publishing Site associated with {id}, changing only the passed in fields.

Request Parameters

(All fields are optional)

See /PubSite::POST for parameters.

Example Response

See /PubSite/{id}::GET for example response.

DELETE

Deletes the Publishing Site associated with {id}, depending on access and permissions.

Request Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
        "response" : {
                "id" : "2"      },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1401911117
}
```


Atlassian

Tenable Security Center API: Query

/query

Methods

GET

Gets the list of Queries.

Fields Parameter

Expand

NOTE: Currently, all fields come back on GET all, but the ** indicates fields which will be listed in a future release

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields type "vuln", sourceType "cumulative" | null

* id
** name
** description
creator
owner
ownerGroup
targetGroup
tool
type
tags
context
browseColumns
browseSortColumn
browseSortDirection
createdTime
modifiedTime
status
filters
canManage
canUse
groups

Legend

** = always comes back*
*** = comes back if fields list not specified on GET all*

Request Parameters

Expand

Parameters must be passed in as query string (as opposed to JSON) in the format of:
/query?type=lce

```
{
       "type" : <string> "alert" | "all" | "lce" | "mobile" | "ticket" |
"user" | "vuln" DEFAULT "all"}
```

Filter Parameters

usable - The response will be an object containing an array of usable Queries. By default, both usable and manageable objects are returned.
manageable - The response will be an object containing all manageable Queries. By default, both usable and manageable objects are returned.

Example Response

Expand

```
{
       "type" : "regular",
       "response" : {
              "usable" : [
                     {
                            "id" : "1",
                            "name" : "Name",
                            "description" : "Test for posting an alert que
                     {
                            "id" : "2",
                            "name" : "Post Copy Response Example",
                            "description" : ""                          },
                     {
                            "id" : "3",
                            "name" : "Post Copy Response Example2",
                            "description" : ""                          },
                     {
                            "id" : "1391",
```

```
                        "name" : "TEST",
                        "description" : ""                    },
                {
                        "id" : "1467",
                        "name" : "Test 1",
                        "description" : ""                    },
                {
                        "id" : "1468",
                        "name" : "Test 2",
                        "description" : ""                    },
                {
                        "id" : "1469",
                        "name" : "Test 3",
                        "description" : ""                    },
                {
                        "id" : "1470",
                        "name" : "Test 4",
                        "description" : ""                    },
                {
                        "id" : "1471",
                        "name" : "Test 5",
                        "description" : ""                    }
        ],
        "manageable" : [
                {
                        "id" : "1",
                        "name" : "Name",
                        "description" : "Test for posting an alert que
                {
                        "id" : "2",
                        "name" : "Post Copy Response Example",
                        "description" : ""                    },
                {
```

```
                        "id" : "3",
                        "name" : "Post Copy Response Example2",
                        "description" : ""                    },
                {
                        "id" : "1391",
                        "name" : "TEST",
                        "description" : ""                    },
                {
                        "id" : "1434",
                        "name" : "query1",
                        "description" : "Created with 'group1's shared
Asset 1'.\n\nThis asset will be unshared"                        },
                {
                        "id" : "1435",
                        "name" : "query2",
                        "description" : "Created with 'group1's shared
Asset 2'.\n\nThis asset will be deleted"                        },
                {
                        "id" : "1436",
                        "name" : "group1Query",
                        "description" : ""                    },
                {
                        "id" : "1467",
                        "name" : "Test 1",
                        "description" : ""                    },
                {
                        "id" : "1468",
                        "name" : "Test 2",
                        "description" : ""                    },
                {
                        "id" : "1469",
                        "name" : "Test 3",
                        "description" : ""                    },
```

```
                        {
                                "id" : "1470",
                                "name" : "Test 4",
                                "description" : ""                      },
                        {
                                "id" : "1471",
                                "name" : "Test 5",
                                "description" : ""                      }
                ]
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1427750981
}
```


POST

Adds a Query

Request Parameters

Expand


```
{
        "name" : <string>,
        "description" : <string> DEFAULT "",
        "ownerID" : <string> DEFAULT <Session User ID)
        "tags" : <string> DEFAULT "",
        "type" : <string> "alert" | "lce" | "mobile" | "ticket" | "user" |
"vuln",
        "context" : <string> DEFAULT "",
        "browseColumns" : <string> DEFAULT "",
        "browseSortColumn" : <string> DEFAULT "",
        "browseSortDirection" : <string> "ASC" | "DESC" DEFAULT "ASC",
```

```
        ...
}
```

Type: "alert" (Expand)

Alert Type

```
...
       "sortField" : <string> OPTIONAL (alphanumeric word(s) separated by
a space/dash),
       "sortDir" : <string> "ASC" | "DESC" OPTIONAL (sort is case
insensitive),
       "startOffset" : <number> OPTIONAL (integer; default "1" if not
specified and endOffset is specified),
       "endOffset" : <number> OPTIONAL (integer),
       "tool" : <string> "listalerts",
       "filters" : [
               {
                       "filterName" : <string> "alertName" | "createdEndTime"
"createdStartTime" | "createdTimeFrame" | "description" |
"didTriggerLastEvaluation" | "lastEvaluatedEndTime" |
"lastEvaluatedStartTime" | "lastEvaluatedTimeFrame" |
"lastTriggeredEndTime" | "lastTriggeredStartTime" |
"lastTriggeredTimeFrame" | "modifiedEndTime" | "modifiedStartTime" |
"modifiedTimeFrame",
                       "operator" : <string> "",
                       "value" : <string> | <number>          }...
       ] DEFAULT []
...
```

Type: "lce" (Expand)

LCE Type

NOTE #1: Filter operators are not validated, but the provided filters are the ones that will properly function.

NOTE #2: Filter "outputAssets" only applies to tool "sumasset".

```
...
       "sortField" : <string> OPTIONAL (alphanumeric word(s) separated by
a space/dash. Must accompany sortDir),
       "sortDir" : <string> "ASC" | "DESC" OPTIONAL (default "ASC" if not
specified and sortField is specified),
       "startOffset" : <number> OPTIONAL (integer; lower bound to returned
record set. default 0 if not specified),
       "endOffset" : <number> OPTIONAL (integer; upper bound to returned
record set. default 100 if not specified),
       "tool" : <string> "listdata" | "sumasset" | "sumclassa" |
"sumclassb" | "sumclassc" | "sumdate" | "sumevent" | "sumevent2" |
"sumip" | "sumport" | "sumprotocol" | "sumsensor" | "sumtime" |
"sumtype" | "sumuser" | "syslog" | "timedist",
       "filters" : [
               {
                       "filterName" : <string> "asset" | "assetID" |
"connectionDirection" | "correlated" | "date" | "destAsset" |
"destAssetID" | "destip" | "detailedEventName" | "dport" | "endtime"
| "eventName" | "ip" | "lce" | "lceIDs" | "numEvents" |
"outputAssets" | "port" | "protocol" | "repository" |
"repositoryIDs" | "sensor" | "silo" | "sourceAsset" |
"sourceAssetID" | "sourceip" | "sport" | "starttime" | "text" |
"timeframe" | "type" | "user",

                       filterName "asset" | "assetID" | "connectionDirection"
"correlated" | "date" | "destAsset" | "destAssetID" | "destip" |
"detailedEventName" | "endtime" | "eventName" | "ip" | "lce" |
"lceIDs" | "numEvents" | "outputAssets" | "protocol" | "repository"
| "repositoryIDs" | "sensor" | "silo" | "sourceAsset" |
"sourceAssetID" | "sourceip" | "starttime" | "text" | "timeframe" |
```

```
"type" | "user"                    ----------------------------------------
                        "operator" : <string> "=" | "!=",
                        "value" : (Format depends on filter's "filterName" pa

                        filterName "dport" | "port" | "sport"
------------------
                        "operator" :  <string> "=" | "!=" | "<=" | ">=",
                        "value" : (Format depends on filter's "filterName" pa

                }...
        ] DEFAULT []
...
```

sourceType "archive"

Note: sourceType will never be "archive." This is included for informational purposes only. Current functionality doesn't accept a "sourceType" parameter, and will always set it to default QUERY_NOT_TREND (null)

```
...
        "view" : <string>,
        "lce" : {
                "id" : <number> }
...
```

Type: "mobile" (Expand)

Mobile Type

NOTE: Filter operators are not validated, but the provided filters are the ones that will properly function.

```
...
        "sortField" : <string> OPTIONAL (alphanumeric; any valid field
returned in the results entry for the corresponding tool.  [Some
```

```
restrictions apply.]  Must accompany sortDir),
       "sortDir" : <string> "ASC" | "DESC" OPTIONAL (default "ASC" if not
specified and sortField is specified),
       "startOffset" : <number> OPTIONAL (integer; lower bound to returned
record set.  Must be explicitly supplied for tool "vulndetails"),
       "endOffset" : <number> OPTIONAL (integer; upper bound to returned
record set.  Must be explicitly supplied for tool "vulndetails"),
       "tool" : <string> "listvuln" | "sumdeviceid" | "summdmuser" |
"summodel" | "sumoscpe" | "sumpluginid" | "vulndetails",
       "filters" : [
              {
                     "filterName" : <string> "baseCVSSScore" | "cvssV3BaseS
"deviceID" | "deviceModel" | "deviceUser" | "deviceVersion" |
"exploitAvailable" | "family" | "familyID" | "lastMitigated" |
"lastSeen" | "mdmType" | "osCPE" | "patchPublished" | "pluginID" |
"pluginModified" | "pluginName" | "pluginOutput" | "pluginPublished"
| "port" | "protocol" | "repository" | "repositoryIDs" |
"serialNumber" | "severity" | "vulnPublished",

                     filterName "osCPE" | "baseCVSSScore" | "cvssV3BaseScor
|"pluginOutput" | "repository" | "repositoryIDs" | "deviceID" |
"deviceModel" | "deviceUser" | "pluginID"                          ----------
-----------------------------------
                     "operator" : "=" | "!=",
                     "value" : (Format depends on filter's "filterName" pa

                     filterName "mdmType" | "pluginName" | "lastMitigated"
"lastSeen" | "vulnPublished" | "pluginModified" | "patchPublished" |
"pluginPublished" | "acceptedRisk" | "daysMitigated" | "dnsName" |
"exploitAvailable" | "family" | "familyID" | "ip" | "lastMitigated"
| "mitigatedStatus" | "pluginText" | "port" | "protocol" |
"recastRisk" | "responsibleUser" | "severity" | "xref"                 -----
-------------------------------------------------------------------
```

```
-------------------------------------------------
                        "operator" : <string> "=" | "<=" | ">=" | "!=" | "betw
"outside" | "contains" | "excludes" | "in" | "!in",
                        "value" : (Format depends on filter's "filterName" pa

                },...
        ] DEFAULT []
...
```

Type: "ticket" (Expand)

Ticket Type

```
...
        "sortField" : <string> OPTIONAL (alphanumeric; must accompany
sortDir),
        "sortDir" : <string> "ASC" | "DESC" OPTIONAL (sort is case
insensitive; must accompany sortField),
        "startOffset" : <number> OPTIONAL (integer; default "0" if not
specified and endOffset is specified),
        "endOffset" : <number> OPTIONAL (integer),
        "tool" : <string> "listtickets" | "sumassignee" |
"sumclassification" | "sumcreator" | "sumstatus",
        "filters" : [
                {
                        "filterName" : <string> "assignedEndTime" | "assigned
"assignedTimeFrame" | "assignee" | "assigneeID" | "classification" |
"closedEndTime" | "closedStartTime" | "closedTimeFrame" |
"createdEndTime" | "createdStartTime" | "createdTimeFrame" |
"modifiedEndTime" | "modifiedStartTime" | "modifiedTimeFrame" |
"owner" | "ownerID" | "resolvedEndTime" | "resolvedStartTime" |
"resolvedTimeFrame" | "status",
                        "value" : (Format depends on filter's "filterName" pa
                },...
```

```
        ] DEFAULT []
...
```

Type: "user" (Expand)

User Type

```
...
        "sortField" : <string> OPTIONAL (alphanumeric; must accompany
sortDir.  username, roleID, and groupID will attempt to perform
case-insensitive sort on the text field in relation to the ID),
        "sortDir" : <string> "ASC" | "DESC" OPTIONAL (sort is case
insensitive; must accompany sortField),
        "startOffset" : <number> OPTIONAL (integer; default "1" if not
specified and endOffset is specified),
        "endOffset" : <number> OPTIONAL (integer),
        "tool" : <string> "listusers" | "sumgroup" | "sumrole",
        "filters" : [
                {
                        "filterName" : <string> "address" | "authType" | "cou
"email" | "fax" | "firstname" | "group" | "groupID" |
"lastLoginEndTime" | "lastLoginStartTime" | "lastLoginTimeFrame" |
"lastname" | "locked" | "phone" | "role" | "roleID" | "state" |
"title" | "username",
                        "operator" : <string>,
                        "value" : (Format depends on filter's "filterName" pa
                }...
        ]
...
```

Type: "vuln" (Expand)

Vuln Type

NOTE #1: Filter operators are not validated, but the provided filters are the ones that will properly function.

NOTE #2: Filter "outputAssets" only applies to tool "sumasset".

NOTE #3: Filter "solutionID" only applies to tools "sumremediation" and "remediationdetail". Moreover, tool "remediationdetail" must specify a "solutionID" filter.

```
...
      "sortField" : <string> OPTIONAL (alphanumeric; any valid field
returned in the results entry for the corresponding tool.  [Some
restrictions apply.]  Must accompany sortDir),
      "sortDir" : <string> "ASC" | "DESC" DEFAULT "ASC" (default "ASC" if
not specified and sortField is specified),
      "startOffset" : <number> OPTIONAL (integer; lower bound to returned
record set.  Must be explicitly supplied for tools "vulndetails" and
"listvuln"),
      "endOffset" : <number> OPTIONAL (integer; upper bound to returned
record set.  Must be explicitly supplied for tools "vulndetails" and
"listvuln"),
      "tool" : <string> "iplist" | "listmailclients" | "listos" |
"listservices" | "listsoftware" | "listsshservers" | "listvuln" |
"listwebclients" | "listwebservers" | "remediationdetail" |
"sumasset" | "sumcce" | "sumclassa" | "sumclassb" | "sumclassc" |
"sumcve" | "sumdnsname" | "sumfamily" | "sumiavm" | "sumid" |
"sumip" | "summsbulletin" | "sumport" | "sumprotocol" |
"sumremediation" | "sumseverity" | "sumuserresponsibility" |
"vulndetails" | "vulnipdetail" | "vulnipsummary",
      "filters" : [
            {
                  "filterName" : <string> "acceptRiskStatus" | "asset"
"assetCriticalityRating" | "assetID" | "auditFile" | "auditFileID" |
"baseCVSSScore" | "benchmarkName" | "cceID" | "cpe" | "cveID" |
"cvssV3BaseScore" | "cvssV3Vector" | "cvssVector" | "dataFormat" |
"daysMitigated" | "daysToMitigated" | "dnsName" | "exploitAvailable"
| "exploitFrameworks" | "family" | "familyID" | "firstSeen" |
"iavmID" | "ip" | "lastMitigated" | "lastSeen" | "mitigatedStatus" |
"msbulletinID" | "outputAssets" | "patchPublished" | "pluginID" |
```

```
"pluginModified" | "pluginName" | "pluginPublished" | "pluginText" |
"pluginType" | "policy" | "policyID" | "port" | "protocol" |
"recastRiskStatus" | "repository" | "repositoryIDs" |
"responsibleUser" | "responsibleUserIDs" | "severity" | "solutionID"
| "stigSeverity" | "tcpport" | "udpport" | "uuid" | "vprScore" |
"vulnPublished" | "xref",

                        filterName "acceptRiskStatus"                    -----
                        "operator" : <string> "=",
                        "value" : <string> "all" | "accepted" | "notAccepted"
                        NOTE: During evaluation on the Analysis page, or for v
objects, presenting
                              no "acceptRiskStatus" filter defaults to the "no
behavior.

                        filterName "asset"                          ----------
                        "operator": <string> "=" | "~" (combination expressior

                        filterName "asset", operator "="
--
                        "value" : [
                                {
                                        "id" : <number> (integer)
                                }...
                        ]

                        filterName "asset", operator "~"
--
                        "value" : <comboRecord> {
                                "operator": <string> "complement" | "intersect
"difference" | "union",
                                "operand1": <comboRecord> | <number> (integer)
                                        "id" : <number> (integer)
```

```
                                }

                                operator not "complement"
                                "operand2": <comboRecord> | <number> (integer)
                                        "id" : <number> (integer)
                                }
                        }

                        filterName "assetCriticalityRating"
                        "operator" : <string> "=",
                        "value" : <string> (inclusive, nonnegative, decimal ra
a dash ["-"] delimiter)

                        filterName "auditFile" | "policy" | "repository" |
"responsibleUser"                       ------------------------------------
--------------------
                        "operator": <string> "=",
                        "value" : {
                                "id" : <number> (integer)
                        }

                        filterName "baseCVSSScore"                          -----
                        "operator" : <string> "=",
                        "value" : <string> (inclusive, nonnegative, decimal ra
a dash ["-"] delimiter)

                        filterName "benchmarkName"                          -----
                        "operator" : <string> "=" (fuzzy-left, right-anchored
                        "value" : <string>

                        filterName "cceID" | "iavmID"                       -----
                        "operator" : <string> "=" (fuzzy match),
                        "value" : <string> (comma-separated list)
```

```
                        filterName "cpe"                              ----------
                        "operator": <string> "=" (i.e. explicit per entry) |
                                             "~=" (i.e. fuzzy match across ent
string) |
                                             "pcre" (i.e. Perl-compatible, reg
expression, across entire entries string),

                        filterName "cpe", operator "=" | "~="
------------
                        "value" : <string> (comma-separated or newline-separat

                        filterName "cpe", operator "pcre"
----
                        "value" : <string> (Perl-compatible, regular expressio

                        filterName "cveID" | "msbulletinID"
--------
                        "operator" : <string> "=" (fuzzy match),
                        "value" : <string> (comma-separated or newline-separat

                        filterName "cvssVector"                       ----------
                        "operator" : <string> "=",
                        "value" : <string> (comma-separated list of Simple or
CVSS vectors)

                                                                      Simple CVSS Ve
"AC:H" | "AC:M" | "AC:L" | "Au:N" | "Au:S" | "Au:M" | "C:N" | "C:P"
| "C:C" | "I:N" | "I:P" | "I:C" | "A:N" | "A:P" | "A:C" | "E:ND" |
"E:U" | "E:P" | "E:POC" | "E:F" | "E:H" | "RL:ND" | "RL:O" | "RL:OF"
| "RL:T" | "RL:TF" | "RL:W" | "RL:U" | "RC:ND" | "RC:UC" | "RC:UR" |
"RC:C"                                                          Complex CVSS
of Simple CVSS Vectors where all entries must match)
```

```
                        filterName "cvssV3BaseScore"                        ------
                        "operator" : <string> "=",
                        "value" : <string> (inclusive, nonnegative, decimal ra
a dash ["-"] delimiter)

                        filterName "cvssV3Vector"                           ------
                        "operator" : <string> "=",
                        "value" : <string> (comma-separated list of Simple or
CVSS vectors)

                                                                  Simple CVSS Ve
"AV:N" | "AC:H" | "AC:L" | "PR:H" | "PR:L" | "PR:N" | "PR:U" |
"UI:R" | "UI:N" | "S:C" | "S:U" | "C:N" | "C:L" | "C:H" | "I:N" |
"I:L" | "I:H" | "A:N" | "A:L" | "A:H" | "E:H" | "E:F" | "E:P" |
"E:U" | "E:X" | "RL:U" | "RL:W" | "RL:OF" | "RL:T" | "RL:O" | "RL:X"
| "RC:C" | "RC:R" | "RC:U" | "RC:X"
<string> (slash-separated list of Simple CVSS Vectors where all
entries must match)

                        filterName "daysMitigated" | "firstSeen" | "lastMitiga
"lastSeen" | "pluginModified" | "pluginPublished" | "vulnPublished"
                  ------------------------------------------------------------
------------------------------------------------------------------
-------------
                        "operator": <string> "=" (relative with custom format)
                        "value" : <string> "<minDaysBack>:<maxDaysBack>" (Both
minDaysBack and maxDaysBack are provided in the number of days ago.
[e.g. "0:90" is between now and 90 days ago].) | "<minDaysBack>:all"
(A value "all" indicates to return all results before minDaysBack) |
"currentMonth" | "lastMonth" | "currentQuarter" (i.e. the current
fiscal quarter) | "lastQuarter"                 filterName "dnsName"
---------
```

```
                        "operator" : <string> "=",
                        "value" : <string> (comma-separated or newline-separat
valid DNS names)

                        filterName "exploitAvailable"                    -----
                        "operator" : <string> "=",
                        "value" : <string> "true" | "false"
"exploitFrameworks"                     ------------------------------
                        "operator": <string> "=" (i.e. explicit for entire ent
string) |
                                                "~=" (i.e. fuzzy match across ent
string),
                        "value" : <string>                          filterName "fa
                        "operator": <string> "=" | "!=",
                        "value" : [
                                {
                                        "id" : <number> (integer)
                                }...
                        ]

                        filterName "ip"                  ---------------
                        "operator" : <string> "=" | "!=",
                        "value" : <string> (comma-separated or newline-separat
valid IPs and/or DNS names)

                        filterName "mitigatedStatus"                     -----
                        "operator": <string> "=",
                        "value" : <string> "previously" | "never"
                        filterName "outputAssets"                        -----
                        "operator": <string> "=",
                        "value" : <string> (comma-separated list of Integers)
                                {
                                        "id" : <number> (integer)
```

```
                              }...
                        ]
                        filterName "patchPublished"                          ------
                        "operator": <string> "=",
                        "value" : <string> "<endDay>:<startDay>" | "<endDay>:a
endDay and startDay are provided in the number of days ago. [e.g.
"0:90" is between now and 90 days ago]. A value of "all" for
startDay is interpreted as "0" [i.e. from "now", back endDay days
ago]) | "currentMonth" | "lastMonth" | "currentQuarter" (i.e. the
current fiscal quarter) | "lastQuarter" | "none" (i.e
vulnerabilities that cannot be resolved through a patch)

                        filterName "pluginID"                    -------------
                        "operator" : <string> "=" | "!=" | "<=" | ">=",

                        filterName "pluginID", operator "=" | "!="
----------------------
                        "value" : <number> (comma-separated or newline-separat
integers or inclusive integer ranges, using a dash ["-"] delimiter,
with each value between 0 and 8388607)

                        filterName "pluginID", operator "<=" | ">="
------------------------
                        "value" : <number> (integer, between 0 and 8388607)

                        filterName "pluginName"                  -------------
                        "operator": <string> "=" (i.e. fuzzy match) | "pcre"
compatible, regular expression),
                        "value" : <string>                       filterName "pl
-----
                        "operator": <string> "=" (i.e. fuzzy match, stripped t
[forced]) |
                                                "pcre" (i.e. Perl-compatible, reg
```

```
expression, stripped text [forced]),
                        "value" : <string>                          filterName "pl
-----
                        "operator": <string> "=",
                        "value" : <string> "passive" | "lce" | "active" | "con
(comma-separated)

                        filterName "port" | "tcpport" | "udpport"
--------------------
                        "operator" : <string> "=" | "!=" | "<=" | ">=",

                        filterName "port" | "tcpport" | "udpport", operator "=
-------------------------------------------------------------
                        "value" : <number> (comma-separated or newline-separat
integers or inclusive integer ranges, using a dash ["-"] delimiter,
with each value between 0 and 65535)

                        filterName "port" | "tcpport" | "udpport", operator "<
        ------------------------------------------------------------
                        "value" : <number> (integer, between 0 and 65535)

                        filterName "protocol"                       ----------
                        "operator": <string> "=" | "!=",
                        "value" : <string> (comma-separated or newline-separat
integers)

                        filterName "recastRiskStatus"                        -----
                        "operator" : <string> "=",
                        "value" : <string> "recast" | "notRecast"
                         --------------------
                        "operator": <string> "=" | "!=",
                        "value" : <string> (comma-separated or newline-separat
integers) | [
```

```
                                {
                                        "id" : <number> (integer)
                                }...
                        ]

                        filterName "solutionID"                 ----------
                        "operator" : <string> "="                       "value
(comma-separated or newline-separated list of integers; number is an
integer representing the Plugin ID of a solution)

                        filterName "stigSeverity"                       -----
                        "operator": <string> "=" | "!=",
                        "value" : <string> (comma-separated or newline-separat
Roman Numerals) | [
                                {
                                        "id" : <string> (valid Roman Numeral)
                                }...
                        ]

                        filterName "vprScore"                   ----------
                        "operator" : <string> "=",
                        "value" : <string> (inclusive, nonnegative, decimal ra
a dash ["-"] delimiter)

                        filterName "xref"                       ----------
                        "operator" : <string> "=" | "!=",
                        "value" : <string> (comma-separated list of XREF Expre
                                XREF Expression = <string> "<type>|<wildCard>"
Wildcard, pipe-delimited)
                                        XREF Type = <string>
matches a single occurrence of any character and "*" matches any
character, any number of times)
                }...
```

```
        ] DEFAULT []
...
```

sourceType "cumulative" | null

Note: sourceType will always be null. Current functionality doesn't accept a "sourceType" parameter, and will always set it to default QUERY_NOT_TREND (null)

```
...
       "tool" : <string> "cceipdetail" | "cveipdetail" | "iavmipdetail" |
"ipcount" | "iplist" | "listmailclients" | "listos" | "listservices"
| "listsoftware" | "listsshservers" | "listvuln" | "listwebclients"
| "listwebservers" | "popcount" | "sumasset" | "sumcce" |
"sumcceasr" | "sumclassa" | "sumclassb" | "sumclassc" | "sumcpe" |
"sumcve" | "sumdnsname" | "sumfamily" | "sumiavm" | "sumid" |
"sumip" | "summsbulletin" | "sumport" | "sumprotocol" |
"sumremediation" | "sumseverity" | "sumuserresponsibility" | "trend"
| "vulndetails" | "vulnipdetail" | "vulnipsummary"...
```

sourceType "individual"

Note: sourceType will never be "individual." This is included for informational purposes only. Current functionality doesn't accept a "sourceType" parameter, and will always set it to default QUERY_NOT_TREND (null)

```
...
       "tool" : <string> "cceipdetail" | "cveipdetail" | "iavmipdetail" |
"ipcount" | "iplist" | "listmailclients" | "listos" | "listservices"
| "listsoftware" | "listsshservers" | "listvuln" | "listwebclients"
| "listwebservers" | "popcount" | "sumasset" | "sumcce" |
"sumcceasr" | "sumclassa" | "sumclassb" | "sumclassc" | "sumcpe" |
"sumcve" | "sumdnsname" | "sumfamily" | "sumiavm" | "sumid" |
"sumip" | "summsbulletin" | "sumport" | "sumprotocol" |
"sumremediation" | "sumseverity" | "sumuserresponsibility" | "trend"
```

```
| "vulndetails" | "vulnipdetail" | "vulnipsummary",
        "scanID" : <number>...
```

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "id" : "12"             "name" : "Test Combo Filter 2",
                "description" : "",
                "tool" : "sumid",
                "type" : "vuln",
                "tags" : "",
                "context" : "",
                "browseColumns" : "",
                "browseSortColumn" : "",
                "browseSortDirection" : "ASC",
                "createdTime" : "1403620113",
                "modifiedTime" : "1403620113",
                "status" : "0",
                "ownerGID" : "0",
                "targetGID" : "-1",
                "filters" : [
                        {
                                "filterName" : "ip",
                                "operator" : "=",
                                "value" : "192.168.1.100"
                ],
                "canManage" : "true",
                "canUse" : "true",
                "creator" : {
                        "id" : "1"                      "username" : "JohnD",
```

```
                        "firstname" : "John",
                        "lastname" : "Doe",
                        "uuid" : "48F26F3B-6A79-4153-96DB-4C63D1BF3D46"
                "owner" : {
                        "id" : "1",
                        "username" : "JohnD",
                        "firstname" : "John",
                        "lastname" : "Doe",
                        "uuid" : "48F26F3B-6A79-4153-96DB-4C63D1BF3D46"
                "ownerGroup" : {
                        "id" : "0",
                        "name" : "Full Access",
                        "description" : "Full Access group"             },
                "targetGroup" : {
                        "id" : -1,
                        "name" : "",
                        "description" : ""              }
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1404224762
}
```


/query/{id}

Methods

GET

Gets the Query associated with {id}.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

* id
** name
** description
creator
owner
ownerGroup
targetGroup
tool
type
tags
context
browseColumns
browseSortColumn
browseSortDirection
createdTime
modifiedTime
status
filters
canManage
canUse
groups

Legend

** = always comes back*
*** = comes back if fields list not specified on GET all*

NOTE: *Currently, all fields come back on GET all, but the ** indicates fields which will be listed in a future release*

Example Response

Expand

```
{
	"type" : "regular",
	"response" : {
		"id" : "12"		"name" : "Test Combo Filter 2",
		"description" : "",
		"tool" : "sumid",
		"type" : "vuln",
		"tags" : "",
		"context" : "",
		"browseColumns" : "",
		"browseSortColumn" : "",
		"browseSortDirection" : "ASC",
		"createdTime" : "1403620113",
		"modifiedTime" : "1403620113",
		"status" : "0",
		"ownerGID" : "0",
		"targetGID" : "-1",
		"filters" : [
			{
				"filterName" : "ip",
				"operator" : "=",
				"value" : "192.168.1.100"
		],
		"canManage" : "true",
		"canUse" : "true",
		"creator" : {
			"id" : "1"			"username" : "JohnD",
			"firstname" : "John",
			"lastname" : "Doe",
			"uuid" : "48F26F3B-6A79-4153-96DB-4C63D1BF3D46"
		"owner" : {
			"id" : "1",
			"username" : "JohnD",
```

```
                        "firstname" : "John",
                        "lastname" : "Doe",
                        "uuid" : "48F26F3B-6A79-4153-96DB-4C63D1BF3D46"
                "ownerGroup" : {
                        "id" : "0",
                        "name" : "Full Access",
                        "description" : "Full Access group"            },
                "targetGroup" : {
                        "id" : -1,
                        "name" : "",
                        "description" : ""              }
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1404224762
}
```


PATCH

Edits the Query associated with {id} , changing only the passed in fields.

Request Parameters

(All fields are optional)

See /query::POST for parameters.

Example Response

See /query/{id}::GET

DELETE

Deletes the Query associated with {id} , depending on access and permissions.

Example Response

Expand

```
{
        "type" : "regular",
        "response" : "",
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1403100582
}
```

/query/{id}/share

Methods

POST

Shares the Query associated with {id}, depending on access and permissions

Request Parameters

Expand

```
{
        "groups" : [
                {
                        "id" : <number>          }...
        ]
}
```

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "id" : "3",
                "name" : "Post Copy Response Example2",
```

```
"description" : "",
"tool" : "sumid",
"type" : "vuln",
"tags" : "",
"context" : "",
"browseColumns" : "",
"browseSortColumn" : "",
"browseSortDirection" : "ASC",
"createdTime" : "1408380088",
"modifiedTime" : "1408380088",
"status" : "0",
"ownerGID" : "0",
"targetGID" : "-1",
"filters" : [
        {
                "filterName" : "ip",
                "operator" : "=",
                "value" : "192.168.1.100"
],
"creator" : {
        "id" : "1",
        "username" : "head",
        "firstname" : "Security Manager",
        "lastname" : "",
        "uuid" : "48F26F3B-6A79-4153-96DB-4C63D1BF3D46"
"owner" : {
        "id" : "1",
        "username" : "head",
        "firstname" : "Security Manager",
        "lastname" : "",
        "uuid" : "48F26F3B-6A79-4153-96DB-4C63D1BF3D46"
"ownerGroup" : {
        "id" : "0",
```

```
                        "name" : "Full Access",
                        "description" : "Full Access group"             },
                "targetGroup" : {
                        "id" : -1,
                        "name" : "",
                        "description" : ""              }
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1409087882
}
```


/query/tag

Methods

GET

Gets the full list of unique Query tags

Example Response

Expand


```
{
        "type" : "regular",
        "response" : [
                "Tag1",
                "Tag2",
                "Tag3"  ],
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1461093219
}
```

Tenable Security Center API: Recast Risk Rule

/recastRiskRule

Methods

GET

Gets the list of Recast Risk Rules across all reps, plugins, and orgs, unless filters are provided.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
****repository**
****organization**
****user**
****plugin**
**newSeverity
**hostType
**hostValue
**port
**protocol
**order
**status
**expires
comments
createdTime
modifiedTime

Legend

** = always comes back*
*** = comes back if fields list not specified on GET all*

Filters

Expand

```
repositoryIDs=<number>,... DEFAULT 0 (i.e. all Repositories)
pluginID=<number> | <string> "all" DEFAULT "all" (i.e. all Plugins)
port=<number> | <string> "all" DEFAULT "all" (i.e. all Ports)
```

Session User is role "1" (administrator)

```
organizationIDs=<number>,... | <string> "all" DEFAULT "all" (i.e.
all Organizations)
```

Session User is not role "1" (administrator)

```
organizationIDs=<number>,... | <string> "all" DEFAULT :sessionOrgID:
```

Paginated results:

By default, the result set encompasses all Recast Risk Rule

To obtain paginated results, a parameter value should be included in the request as follows:

?paginated=true

Additionally, for paginated results, the following parameters can be sent:

startOffset <number> (positive integer) DEFAULT 0,
endOffset <number> (integer >= startOffset) DEFAULT 50,
sortDirection <string> "ASC" | "DESC" DEFAULT "DESC",
sortField <string> "userID" | "pluginID" | "port" | "protocol" | "expires" | "createdTime",

Example Response

Expand

```
{
        "type" : "regular",
        "response" : [
```

```
{
        "id" : "1",
        "newSeverity" : "0",
        "hostType" : "all",
        "hostValue" : "",
        "port" : "any",
        "protocol" : "any",
        "order" : "1",
        "expires" : "-1",
        "status" : "0",
        "repository" : {
                "id" : "18",
                "name" : "New Rep 1",
                "description" : "",
                "type" : "Local",
                "uuid" : "51C9083D-3AF6-4557-9492-7B25FCF6BAE
        "organization" : {
                "id" : "8",
                "name" : "Org",
                "description" : "Testing for Policies with Ne
                "uuid" : "2E950182-08B6-4737-830B-4ACC8F6B92F
        "user" : {
                "id" : "1",
                "username" : "head",
                "firstname" : "Security Manager",
                "lastname" : "",
                "uuid" : "FF00F4D0-5B9F-4A26-998C-19430295284
        "plugin" : {
                "id" : "0",
                "name" : "Open Port",
                "description" : "",
                "type" : "active"                       }
}
```

```
        ],
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1410281615
}
```

POST

Adds a Recast Risk Rule to one repository.

Request Parameters

Expand

```
{
    "repositories" : [
        {
            "id" : <number>         }...
    ],
    "plugin" : {
        "id" : <number>     },
       "newSeverity" : {
              "id" : <number> "0" (info) | "1" (low) | "2" (medium) | "3" (h
| "4" (critical)
       },
       ...
```

hostType for Universal Repository type

```
        ...
       "hostType" : <string> "all" | "asset" | "ip" | "hostUUID",
       ...
```

hostType for Agent Repository type

```
        ...
       "hostType" : <string> "all" | "asset" | "uuid",
       ...
```

hostType for IPv4 or IPv6 Repository type

```
        ...
       "hostType" : <string> "all" | "asset" | "ip" ,
       ...
```

```
  "port" : <number:1..65535> | <string> "any" DEFAULT "any",
    "protocol" : <number:1..> | <string> "any" DEFAULT "any",
    "comments" : <string> DEFAULT "",
    "expires" : <number> (integer >= -1) DEFAULT -1 (not set)
    ...
}
```

hostType "asset"

The "hostValue" parameter should contain a usable, accessible Asset ID.

```
...
       "hostValue" : {
              "id" : <number> }
...
```

hostType "ip"

The "hostValue" parameter should contain a newline-separated and/or comma-separated list of IPs.

```
...
       "hostValue" : <string>...
```

hostType "uuid"

The "hostValue" parameter should contain a newline-separated and/or comma-separated list of UUIDs.

```
...
       "hostValue" : <string>...
```

hostType "hostUUID"

The "hostValue" parameter should contain a newline-separated and/or comma-separated list of UUIDs.

```
...
       "hostValue" : <string>...
```

Example Response

Expand

```
{
       "type" : "regular",
       "response" : [
              {
                     "id" : "1",
                     "newSeverity" : "0",
                     "hostType" : "all",
                     "hostValue" : "",
                     "port" : "any",
                     "protocol" : "any",
                     "comments" : "",
                     "order" : "1",
                     "status" : "0",
                     "expires" : "-1",
                     "createdTime" : "1410281580",
                     "modifiedTime" : "1410281580",
                     "repository" : {
```

```
                                "id" : "18",
                                "name" : "New Rep 1",
                                "description" : "",
                                "type" : "Local",
                                "uuid" : "51C9083D-3AF6-4557-9492-7B25FCF6BAE
                        "organization" : {
                                "id" : "8",
                                "name" : "Org",
                                "description" : "Testing for Policies with Ne
                                "uuid" : "2E950182-08B6-4737-830B-4ACC8F6B92F
                        "user" : {
                                "id" : "1",
                                "username" : "head",
                                "firstname" : "Security Manager",
                                "lastname" : "",
                                "uuid" : "FF00F4D0-5B9F-4A26-998C-19430295284
                        "plugin" : {
                                "id" : "0",
                                "name" : "Open Port",
                                "description" : "",
                                "type" : "active"                       }
                }
        ],
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1410281580
}
```


/recastRiskRule/{id}

Methods

GET

Gets the Recast Risk Rule associated with {id}.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
**repository
**organization
**user
**plugin
**newSeverity
**hostType
**hostValue
**port
**protocol
**order
**status
**expires
comments
createdTime
modifiedTime

Legend

** = always comes back*
*** = comes back if fields list not specified on GET all*

Request Query Parameters

None

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "id" : "1",
                "newSeverity" : "0",
                "hostType" : "all",
                "hostValue" : "",
                "port" : "any",
                "protocol" : "any",
                "comments" : "",
                "order" : "1",
                "status" : "0",
                "expires" : "-1",
                "createdTime" : "1410281580",
                "modifiedTime" : "1410281580",
                "repository" : {
                        "id" : "18",
                        "name" : "New Rep 1",
                        "description" : "",
                        "type" : "Local",
                        "uuid" : "51C9083D-3AF6-4557-9492-7B25FCF6BAEB"
                "organization" : {
                        "id" : "8",
                        "name" : "Org",
                        "description" : "Testing for Policies with New Schema"
                        "uuid" : "2E950182-08B6-4737-830B-4ACC8F6B92F9"
                "user" : {
                        "id" : "1",
                        "username" : "head",
                        "firstname" : "Security Manager",
                        "lastname" : "",
                        "uuid" : "FF00F4D0-5B9F-4A26-998C-19430295284A"
                "plugin" : {
```

```
                        "id" : "0",
                        "name" : "Open Port",
                        "description" : "",
                        "type" : "active"                }
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1410281625
}
```


DELETE

Deletes the Recast Risk Rule associated with {id}, depending on access and permissions.

Request Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
        "response" : "",
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1403100582
}
```


PATCH

Request Parameters

Expand

Allowed Fields

expires

Example Response

Expand

```
{
        "type" : "regular",
        "response" : "",
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1403100582
}
```

/recastRiskRule/apply

Methods

POST

Applies all rules for the given repository or all (id: 0)

Request Query Parameters

Expand

```
 {
        "repository" : {
                "id" : <number> }
}
```

Example Response

Expand

```
 {
        "type" : "regular",
```

```
        "response" : "",
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1410279161
}
```

Atlassian

Tenable Security Center API: Report

/report

Methods

GET

Gets the list of Reports

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
**name
**description
creator
owner
ownerGroup
reportDefinitionID
jobID
type
displayType
status
running

errorDetails
totalSteps
completedSteps
startTime
finishTime
pubSites
txLogs

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

Request Query Parameters

Expand

NOTE: The 'startTime' and 'endTime' parameters search against the 'createdTime' values. They do not consider or search against the 'finishTime' values.

```
{
    "owner" : <string> "",
    "status" : <string> "Completed" | "Error" | "Queued" | "Queuing"
| "Running" | "Resuming" | "Pausing" | "Paused" | "Stopping" |
"Stopped",
    "name" : <string> "",
    "startTime" : <number:epoch> DEFAULT {now-30 days},
       "endTime" : <number:epoch> DEFAULT {now}
    ...
}
```

Paginated results:

By default, the result set encompasses all Report Results.

To obtain paginated results, a parameter value should be included in the request as follows:

?paginated=true

Additionally, for paginated results, the following parameters can be sent:

startOffset <number> (positive integer) DEFAULT 0,
endOffset <number> (integer >= startOffset) DEFAULT 50,
sortDirection <string> "ASC" | "DESC" DEFAULT "DESC",
sortField <string> "name" | "type" | "ownerGroup" | "ownerID" | "finishTime" | "status",

Example Request Query Parameters

Expand

NOTE: The 'startTime' and 'endTime' parameters search against the 'createdTime' values. They do not consider or search against the 'finishTime' values.

For normal query param request

```
{
  "owner": "1,2",
  "status": "Running,Completed",
  "name": "Remediation",
  "startTime": 1700564860,
  "endTime": 1704884860
}
```

With Pagination query param

```
{
  "startOffset": 0,
  "endOffset": 50,
  "sortField": "name",
  "sortDirection": "ASC",
  "paginated": "true",
  "owner": "1,2",
  "status": "Running,Completed",
  "name": "Remediation",
  "startTime": 1700564860,
  "endTime": 1704884860
```

```
}
```

Filter Parameters

usable - The response will be an object containing an array of usable Reports. By default, both usable and manageable objects are returned.
manageable - The response will be an object containing all manageable Reports. By default, both usable and manageable objects are returned.
running - Only Reports that are currently running will be returned. This is compatible with usable and/or manageable filters. By default, both running and completed Reports are returned.
completed - Only Reports that have completed will be returned. This is compatible with usable and/or manageable filters. By default, both running and completed Reports are returned.

Example Response

Expand


```
{
	"type" : "regular",
	"response" : {
		"usable" : [
			{
				"id" : "1",
				"reportDefinitionID" : "-1",
				"jobID" : "1614",
				"name" : "Test Scan",
				"description" : "This report identifies instal
across a series of hosts, utilizing Nessus plugin 22869, Software
Enumeration (SSH). This plugin lists the software installed on the
remote host by calling the appropriate command (rpm -qa on RPM-based
Linux distributions, qpkg, dpkg, etc.).\nThis report is comprised of
a Table of Contents for each identified host. The Identified Hosts
Table lists the hosts by IP Address, NetBIOS Name, and DNS Name, and
is followed by a detailed look at each host individually.\n\nThis
area provides some host details in a header with IP Address, DNS
```

```
Name, NetBIOS Name, and Last Scan Date, and is followed by the host
Operating System and a list of installed software, and version (if
available).",
                                "type" : "pdf",
                                "status" : "Completed",
                                "running" : "false",
                                "errorDetails" : "Error removing components.\n
component #6.\nError deleting Data Source #10.\nError retrieving
owner of Query.\nUser #1 not found.\n",
                                "totalSteps" : "8",
                                "completedSteps" : "4",
                                "startTime" : "1403298387",
                                "finishTime" : "1403299387",
                                "ownerGID" : "0",
                                "displayType" : "pdf",
                                "pubSites" : [
                                        {
                                                "id" : "2",
                                                "name" : "test",
                                                "description" : "desc"
                                ],
                                "txLogs" : [],
                                "canUse" : "true",
                                "canManage" : "true",
                                "creator" : {
                                        "id" : "1",
                                        "username" : "head",
                                        "firstname" : "test",
                                        "lastname" : "User",
                        "uuid": "2E2B70F2-3471-428F-82AF-A6905090EAA9"
                },
                                "owner" : {
                                        "id" : "1",
```

```
                                        "username" : "head",
                                        "firstname" : "test",
                                        "lastname" : "User",
                        "uuid": "2E2B70F2-3471-428F-82AF-A6905090EAA9"
                 },
                                "ownerGroup" : {
                                        "id" : "0",
                                        "name" : "Full Access",
                                        "description" : "Full Access group"
                                },
                                ...
                        ]
                        "manageable" : [
                                {
                                        "id" : "1",
                                        "reportDefinitionID" : "-1",
                                        "jobID" : "1614",
                                        "name" : "Test Scan",
                                        "description" : "This report identifies instal
across a series of hosts, utilizing Nessus plugin 22869, Software
Enumeration (SSH). This plugin lists the software installed on the
remote host by calling the appropriate command (rpm -qa on RPM-based
Linux distributions, qpkg, dpkg, etc.).\nThis report is comprised of
a Table of Contents for each identified host. The Identified Hosts
Table lists the hosts by IP Address, NetBIOS Name, and DNS Name, and
is followed by a detailed look at each host individually.\n\nThis
area provides some host details in a header with IP Address, DNS
Name, NetBIOS Name, and Last Scan Date, and is followed by the host
Operating System and a list of installed software, and version (if
available).",
                                        "type" : "pdf",
                                        "status" : "Completed",
                                        "running" : "false",
```

```
                                "errorDetails" : "Error removing components.\n
component #6.\nError deleting Data Source #10.\nError retrieving
owner of Query.\nUser #1 not found.\n",
                                "totalSteps" : "8",
                                "completedSteps" : "4",
                                "startTime" : "1403298387",
                                "finishTime" : "1403299387",
                                "ownerGID" : "0",
                                "displayType" : "pdf",
                                "pubSites" : [
                                        {
                                                "id" : "2",
                                                "name" : "test",
                                                "description" : "desc"
                                ],
                                "txLogs" : [],
                                "canUse" : "true",
                                "canManage" : "true",
                                "creator" : {
                                        "id" : "1",
                                        "username" : "head",
                                        "firstname" : "test",
                                        "lastname" : "User",
                        "uuid": "2E2B70F2-3471-428F-82AF-A6905090EAA9"
                },
                                "owner" : {
                                        "id" : "1",
                                        "username" : "head",
                                        "firstname" : "test",
                                        "lastname" : "User",
                        "uuid": "2E2B70F2-3471-428F-82AF-A6905090EAA9"
                },
                                "ownerGroup" : {
```

```
                                        "id" : "0",
                                        "name" : "Full Access",
                                        "description" : "Full Access group"
                        },
                        ...
                ]
        }
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1404919744
}
```


Paginated response

Expand


```
{
    "type": "regular",
    "response": {
        "totalRecords": "1",
        "returnedRecords": 1,
        "startOffset": "0",
        "endOffset": "50",
        "usable": [
            {
                "name": "Critical and Exploitable Vulnerabilities
Report",
                "type": "pdf",
                "status": "Running",
                "startTime": "1704890653",
                "finishTime": "1704890749",
                "completedSteps": "24",
                "totalSteps": "24",
```

```
                "running": "false",
                "id": "4",
                "canUse": "true",
                "canManage": "true",
                "owner": {
                    "id": "1",
                    "username": "qahead",
                    "firstname": "Qa",
                    "lastname": "Head",
                    "uuid": "36DC8C6C-962A-4C65-AB6C-8C9986D40446"
             },
                "ownerGroup": {
                    "id": "0",
                    "name": "Full Access",
                    "description": "Full Access group"
 }
            }
        ],
        "manageable": [
            {
                "name": "Critical and Exploitable Vulnerabilities
Report",
                "type": "pdf",
                "status": "Running",
                "startTime": "1704890653",
                "finishTime": "1704890749",
                "completedSteps": "24",
                "totalSteps": "24",
                "running": "false",
                "id": "4",
                "canUse": "true",
                "canManage": "true",
                "owner": {
```

```
                    "id": "1",
                    "username": "qahead",
                    "firstname": "Qa",
                    "lastname": "Head",
                    "uuid": "36DC8C6C-962A-4C65-AB6C-8C9986D40446"
                },
                "ownerGroup": {
                    "id": "0",
                    "name": "Full Access",
                    "description": "Full Access group"
    }
            }
        ]
    },
    "error_code": 0,
    "error_msg": "",
    "warnings": [],
    "timestamp": 1704965474
}
```


/report/{id}

Methods

GET

Gets the Report associated with {id}.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
**name

**description
creator
owner
ownerGroup
reportDefinitionID
jobID
type
displayType
status
running
errorDetails
totalSteps
completedSteps
startTime
finishTime
pubSites
txLogs

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

Request Query Parameters

None

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "id" : "1",
                "reportDefinitionID" : "-1",
```

```
                "jobID" : "1614",
                "name" : "Test Scan",
                "description" : "This report identifies installed software ac
a series of hosts, utilizing Nessus plugin 22869, Software
Enumeration (SSH). This plugin lists the software installed on the
remote host by calling the appropriate command (rpm -qa on RPM-based
Linux distributions, qpkg, dpkg, etc.).\nThis report is comprised of
a Table of Contents for each identified host. The Identified Hosts
Table lists the hosts by IP Address, NetBIOS Name, and DNS Name, and
is followed by a detailed look at each host individually.\n\nThis
area provides some host details in a header with IP Address, DNS
Name, NetBIOS Name, and Last Scan Date, and is followed by the host
Operating System and a list of installed software, and version (if
available).",
                "type" : "pdf",
                "status" : "Completed",
                "running" : "false",
                "errorDetails" : "Error removing components.\nError removing
component #6.\nError deleting Data Source #10.\nError retrieving
owner of Query.\nUser #1 not found.\n",
                "totalSteps" : "8",
                "completedSteps" : "4",
                "startTime" : "1403298387",
                "finishTime" : "1403299387",
                "ownerGID" : "0",
                "pubSites" : [
                        {
                                "id" : "2",
                                "name" : "test",
                                "description" : "desc"                  }
                ],
                "creator" : {
                        "id" : "1",
```

```
                        "username" : "head",
                        "firstname" : "test",
                        "lastname" : "User",
              "uuid": "2E2B70F2-3471-428F-82AF-A6905090EAA9"              },
                 "owner" : {
                        "id" : "1",
                        "username" : "head",
                        "firstname" : "test",
                        "lastname" : "User",
              "uuid": "2E2B70F2-3471-428F-82AF-A6905090EAA9"              },
                 "ownerGroup" : {
                        "id" : "0",
                        "name" : "Full Access",
                        "description" : "Full Access group"              }
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1404920431
}
```


DELETE

Deletes the Report associated with {id}, depending on access and permissions.

Request Parameters

None

Example Response

Expand


```
{
    "type" : "regular",
    "response" : "",
```

```
    "error_code" : 0,
    "error_msg" : "",
    "warnings" : [],
    "timestamp" : 1403100582
}
```


/report/{id}/copy

Methods

POST

Copies the Report associated with {id}, depending on access and permissions.

Request Parameters

Expand

```
{
        "users" : [
                {
                        "id" : <number>          }...
        ]
}
```

Example Response

Expand


```
{
    "type" : "regular",
    "response" : {},
    "error_code" : 0,
    "error_msg" : "",
    "warnings" : [],
    "timestamp" : 1406924039
}
```

/report/{id}/email

Methods

POST

Emails the Report result associated with {id}, depending on access and permissions.

Request Parameters

Expand

```
{
        "email" : <string> (valid email list)
}
```

Example Response

Expand

```
{
    "type" : "regular",
    "response" : {},
    "error_code" : 0,
    "error_msg" : "",
    "warnings" : [],
    "timestamp" : 1406924039
}
```

/report/{id}/download

POST

Downloads the report associated with {id}.

Request Parameters

None

Example Response

None given. The response will be a PDF, RTF, CSV, ASR, ARF, or LASR file in binary or ascii format.

/report/{id}/stop

POST

Stops the Report associated with {id}.

Request Parameters

None

Example Response

Expand

```
{
    "type" : "regular",
    "response" : {},
    "error_code" : 0,
    "error_msg" : "",
    "warnings" : [],
    "timestamp" : 1404920650
}
```

/report/{id}/send

POST

Request Query Parameters

Expand

```
{
        "pubSites" : [
                <number>...
        ]
}
```

Example Response

Expand

```
{
        "type" : "regular",
        "response" : "",
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1407248107
}
```

Atlassian

Tenable Security Center API: Report Definition

/reportDefinition

Methods

GET

Gets the list of Report Definitions.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
**name
**description
**status
creator
owner
ownerGroup
type

dataSourceID
attributeSet
styleFamily
definition
xmldefinition
encryptionPassword
shareUsers
emailUsers
emailTargets
emailBCCTargets
createdTime
modifiedTime
pubSites
schedule
sources
scanResult
canManage
canUse
components
iterators
queryStatus

Legend

** = always comes back*
*** = comes back if fields list not specified on GET all*
***red** = field is a JSON object (**e.g.** "SCI" : {"id" : "2", "name" : "SCI Name", "description" : "Description"})*

Request Query Parameters

None

Filter Parameters

usable - The response will be an object containing an array of usable Report Definitions. By default, both usable and manageable objects are returned.

manageable - The response will be an object containing all manageable Report Definitions. By default, both usable and manageable objects are returned.

Example Response

Expand


```
{
	"type" : "regular",
	"response" : {
		"usable" : [
			{
				"id" : "3",
				"name" : "Test",
				"description" : "test",
				"type" : "lasr",
				"styleFamily" : "-1",
				"definition" : {
					"columns" : [
						{
							"name" : "all"
					],
					"dataSource" : {
						"queryID" : 2,
						"querySourceType" : "cumulati
						"querySourceID" : null,
						"querySourceView" : "all",
						"sortColumn" : null,
						"sortDirection" : null
					},
					"dataPoints" : 1.7976931348623e+308,
					"lasrInfo" : {
						"benchmarks" : [
							"Faked Data Benchmark
					}
```

```
                                },
                                "xmldefinition" : "a:4:{s:7:\"columns\";a:1:{i
{s:4:\"name\";s:3:\"all\";}}s:10:\"dataSource\";a:6:
{s:7:\"queryID\";i:2;s:15:\"querySourceType\";s:10:\"cumulative\";s:-
13:\"querySourceID\";N;s:15:\"querySourceView\";s:3:\"all\";s:10:\"s-
ortColumn\";N;s:13:\"sortDirection\";N;}s:10:\"dataPoints\";d:1.7976-
931348623157E+308;s:8:\"lasrInfo\";a:1:{s:10:\"benchmarks\";a:1:
{i:0;s:20:\"Faked Data Benchmark\";}}}",
                                "encryptionPassword" : "",
                                "status" : "0",
                                "shareUsers" : [],
                                "emailUsers" : [],
                                "emailTargets" : "",
                                "emailBCCTargets" : "",
                                "createdTime" : "1410369405",
                                "modifiedTime" : "1410369421",
                                "pubSites" : [],
                                "sources" : [
                                        {
                                                "id" : "3",
                                                "queryID" : "2",
                                                "querySourceType" : "cumulativ
                                                "querySourceID" : null,
                                                "querySourceView" : "all",
                                                "sortColumn" : null,
                                                "sortDirection" : null,
                                                "iteratorID" : "-1",
                                                "resultStyle" : "list",
                                                "dataPoints" : 1.797693134862
                                        }
                                ],
                                "scanResult" : [],
                                "components" : [
```

```
                {
                        "componentType" : "lasr",
                        "dataPoints" : 1.7976931348623
                        "columns" : "all"
        ],
        "iterators" : [],
        "schedule" : {
                "id" : "7",
                "type" : "template",
                "start" : "",
                "repeatRule" : "",
                "nextRun" : 0
        },
        "creator" : {
                "id" : "1",
                "username" : "head",
                "firstname" : "Security Manager",
                "lastname" : "",
                "uuid" : "96F2AD1B-1B83-462E-903A-84E
        "owner" : {
                "id" : "1",
                "username" : "head",
                "firstname" : "Security Manager",
                "lastname" : "",
                "uuid" : "96F2AD1B-1B83-462E-903A-84E
        "ownerGroup" : {
                "id" : "0",
                "name" : "Full Access",
                "description" : "Full Access group"
        "attributeSet" : {
                "id" : "5",
                "name" : "test",
                "description" : ""
```

```
                        },
                        {
                                "id" : "4",
                                "name" : "Test2",
                                "description" : "",
                                "type" : "lasr",
                                "styleFamily" : "-1",
                                "definition" : {
                                        "columns" : [
                                                {
                                                        "name" : "all"
                                        ],
                                        "dataSource" : {
                                                "queryID" : 12,
                                                "querySourceType" : "cumulativ
                                                "querySourceID" : null,
                                                "querySourceView" : "all",
                                                "sortColumn" : null,
                                                "sortDirection" : null
                                        },
                                        "dataPoints" : 1.7976931348623e+308,
                                        "lasrInfo" : {
                                                "benchmarks" : [
                                                        "Faked Data Benchmark"
                                        }
                                },
                                "xmldefinition" : "a:4:{s:7:\"columns\";a:1:{i
{s:4:\"name\";s:3:\"all\";}}s:10:\"dataSource\";a:6:
{s:7:\"queryID\";i:2;s:15:\"querySourceType\";s:10:\"cumulative\";s:-
13:\"querySourceID\";N;s:15:\"querySourceView\";s:3:\"all\";s:10:\"s-
ortColumn\";N;s:13:\"sortDirection\";N;}s:10:\"dataPoints\";d:1.7976-
931348623157E+308;s:8:\"lasrInfo\";a:1:{s:10:\"benchmarks\";a:1:
{i:0;s:20:\"Faked Data Benchmark\";}}}",
```

```
"encryptionPassword" : "",
"status" : "0",
"shareUsers" : [],
"emailUsers" : [],
"emailTargets" : "",
"emailTargetType" : "1",
"createdTime" : "1410369657",
"modifiedTime" : "1410369657",
"pubSites" : [],
"sources" : [
        {
                "id" : "4",
                "queryID" : "12",
                "querySourceType" : "cumulativ
                "querySourceID" : null,
                "querySourceView" : "all",
                "sortColumn" : null,
                "sortDirection" : null,
                "iteratorID" : "-1",
                "resultStyle" : "list",
                "dataPoints" : 1.7976931348623
        }
],
"scanResult" : [],
"components" : [
        {
                "componentType" : "lasr",
                "dataPoints" : 1.7976931348623
                "columns" : "all"
],
"iterators" : [],
"schedule" : {
        "id" : "8",
```

```
                        "type" : "template",
                        "start" : "",
                        "repeatRule" : "",
                        "nextRun" : 0
                },
                "creator" : {
                        "id" : "1",
                        "username" : "head",
                        "firstname" : "Security Manager",
                        "lastname" : "",
                        "uuid" : "96F2AD1B-1B83-462E-903A-84E
                "owner" : {
                        "id" : "1",
                        "username" : "head",
                        "firstname" : "Security Manager",
                        "lastname" : "",
                        "uuid" : "96F2AD1B-1B83-462E-903A-84E
                "ownerGroup" : {
                        "id" : "0",
                        "name" : "Full Access",
                        "description" : "Full Access group"
                "attributeSet" : {
                        "id" : "5",
                        "name" : "test",
                        "description" : ""
        }
],
"manageable" : [
        {
                "id" : "3",
                "name" : "Test",
                "description" : "test",
                "type" : "lasr",
```

```
                                "styleFamily" : "-1",
                                "definition" : {
                                        "columns" : [
                                                {
                                                        "name" : "all"
                                        ],
                                        "dataSource" : {
                                                "queryID" : 2,
                                                "querySourceType" : "cumulativ
                                                "querySourceID" : null,
                                                "querySourceView" : "all",
                                                "sortColumn" : null,
                                                "sortDirection" : null
                                        },
                                        "dataPoints" : 1.7976931348623e+308,
                                        "lasrInfo" : {
                                                "benchmarks" : [
                                                        "Faked Data Benchmark"
                                        }
                                },
                                "xmldefinition" : "a:4:{s:7:\"columns\";a:1:{i
{s:4:\"name\";s:3:\"all\";}}s:10:\"dataSource\";a:6:
{s:7:\"queryID\";i:2;s:15:\"querySourceType\";s:10:\"cumulative\";s:-
13:\"querySourceID\";N;s:15:\"querySourceView\";s:3:\"all\";s:10:\"s-
ortColumn\";N;s:13:\"sortDirection\";N;}s:10:\"dataPoints\";d:1.7976-
931348623157E+308;s:8:\"lasrInfo\";a:1:{s:10:\"benchmarks\";a:1:
{i:0;s:20:\"Faked Data Benchmark\";}}}",
                                "encryptionPassword" : "",
                                "status" : "0",
                                "shareUsers" : [],
                                "emailUsers" : [],
                                "emailTargets" : "",
                                "emailTargetType" : "1",
```

```
"createdTime" : "1410369405",
"modifiedTime" : "1410369421",
"pubSites" : [],
"sources" : [
        {
                "id" : "3",
                "queryID" : "2",
                "querySourceType" : "cumulativ
                "querySourceID" : null,
                "querySourceView" : "all",
                "sortColumn" : null,
                "sortDirection" : null,
                "iteratorID" : "-1",
                "resultStyle" : "list",
                "dataPoints" : 1.797693134862
        }
],
"scanResult" : [],
"components" : [
        {
                "componentType" : "lasr",
                "dataPoints" : 1.797693134862
                "columns" : "all"
],
"iterators" : [],
"schedule" : {
        "id" : "7",
        "type" : "template",
        "start" : "",
        "repeatRule" : "",
        "nextRun" : 0
},
"creator" : {
```

```
                        "id" : "1",
                        "username" : "head",
                        "firstname" : "Security Manager",
                        "lastname" : "",
                        "uuid" : "96F2AD1B-1B83-462E-903A-84E
                "owner" : {
                        "id" : "1",
                        "username" : "head",
                        "firstname" : "Security Manager",
                        "lastname" : "",
                        "uuid" : "96F2AD1B-1B83-462E-903A-84E
                "ownerGroup" : {
                        "id" : "0",
                        "name" : "Full Access",
                        "description" : "Full Access group"
                "attributeSet" : {
                        "id" : "5",
                        "name" : "test",
                        "description" : ""
        },
        {
                "id" : "4",
                "name" : "Test2",
                "description" : "",
                "type" : "lasr",
                "styleFamily" : "-1",
                "definition" : {
                        "columns" : [
                                {
                                        "name" : "all"
                        ],
                        "dataSource" : {
                                "queryID" : 12,
```

```
                                        "querySourceType" : "cumulativ
                                        "querySourceID" : null,
                                        "querySourceView" : "all",
                                        "sortColumn" : null,
                                        "sortDirection" : null
                                },
                                "dataPoints" : 1.7976931348623e+308,
                                "lasrInfo" : {
                                        "benchmarks" : [
                                                "Faked Data Benchmark"
                                }
                        },
                        "xmldefinition" : "a:4:{s:7:\"columns\";a:1:{i
{s:4:\"name\";s:3:\"all\";}}s:10:\"dataSource\";a:6:
{s:7:\"queryID\";i:2;s:15:\"querySourceType\";s:10:\"cumulative\";s:-
13:\"querySourceID\";N;s:15:\"querySourceView\";s:3:\"all\";s:10:\"s-
ortColumn\";N;s:13:\"sortDirection\";N;}s:10:\"dataPoints\";d:1.7976-
931348623157E+308;s:8:\"lasrInfo\";a:1:{s:10:\"benchmarks\";a:1:
{i:0;s:20:\"Faked Data Benchmark\";}}}",
                        "encryptionPassword" : "",
                        "status" : "0",
                        "shareUsers" : [],
                        "emailUsers" : [],
                        "emailTargets" : "",
                        "emailTargetType" : "1",
                        "createdTime" : "1410369657",
                        "modifiedTime" : "1410369657",
                        "pubSites" : [],
                        "sources" : [
                                {
                                        "id" : "4",
                                        "queryID" : "12",
                                        "querySourceType" : "cumulativ
```

```
                "querySourceID" : null,
                "querySourceView" : "all",
                "sortColumn" : null,
                "sortDirection" : null,
                "iteratorID" : "-1",
                "resultStyle" : "list",
                "dataPoints" : 1.7976931348623
        }
],
"scanResult" : [],
"components" : [
        {
                "componentType" : "lasr",
                "dataPoints" : 1.7976931348623
                "columns" : "all"
],
"iterators" : [],
"schedule" : {
        "id" : "8",
        "type" : "template",
        "start" : "",
        "repeatRule" : "",
        "nextRun" : 0
},
"creator" : {
        "id" : "1",
        "username" : "head",
        "firstname" : "Security Manager",
        "lastname" : "",
        "uuid" : "96F2AD1B-1B83-462E-903A-84E
"owner" : {
        "id" : "1",
        "username" : "head",
```

```
                                        "firstname" : "Security Manager",
                                        "lastname" : "",
                                        "uuid" : "96F2AD1B-1B83-462E-903A-84E
                                "ownerGroup" : {
                                        "id" : "0",
                                        "name" : "Full Access",
                                        "description" : "Full Access group"
                                "attributeSet" : {
                                        "id" : "5",
                                        "name" : "test",
                                        "description" : ""
                        }
                ]
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1413401160
}
```


POST

Adds a Report Definition

NOTE #1: For notes on the query object, see parameters for *[/query::POST](#)*.

NOTE #2: If a template ID is provided

- The template associated with the provided ID will be retrieved and used as the default values for the Report Definition.
- All Report Definition types are 'pdf'. These values can be overwritten.
- The 'name' will be handled by the back-end, and would default to the template name. If the template name already exists, it would default the name to the name plus the highest value used i.e. "templateName(2)"
- Templates do not include a schedule. A schedule must still be provided.

- Reports scheduled for a single occurrence are considered one-time reports. They run immediately and then are deleted. This includes schedules of type "now" or schedules of type "ical" and an empty "repeatRule" value

WARNING: If field *attributeSetID* is not numeric, it will pass validation. This check should be made more like the check for field *styleFamily*.

Request Parameters

Expand

```
{
       "name" : <string>,
       "template" : {
              "id" : <number> } OPTIONAL,
       "description" : <string> DEFAULT "",
       "type" : <string> "arf" | "asr" | "csv" | "lasr" | "pdf" | "rtf",
       "encryptionPassword" : <string> DEFAULT "",
       "pubSites" : [
              {
                     "id" : <number>         }...
       ] DEFAULT [],
       "schedule" : {
              "type" : <string> "ical" | "never" | "now" | "rollover" |
"template"      },
       "shareUsers" : [
              {
                     "id" : <number>         }...
       ] DEFAULT [],
       "emailUsers" : [
              {
                     "id" : <number>         }...
       ] DEFAULT [],
       "emailTargets" : <string> DEFAULT "" (comma-separated list of email
addresses),
       "emailBCCTargets" : <string> DEFAULT "" (comma-separated list of
```

```
email addresses),
...
}
```

schedule["type"] is "ical"

```
...
       "schedule" : {
              "start" : <string> (This value takes the iCal format),
              "repeatRule" : <string> (This value takes the repeat rule form
       },
...
```

Report definitions have many variations of structure and complexity. This information is intended to be used as a basic guideline and may not include every use-case.

type "csv",

```
...
       "definition" : {
              "dataSource" : {
                     "queryID" : <number> OPTIONAL
                     "querySourceType" : <string> "archive" | "cumulative"
"individual" | "lce" | "mobile"| "patched",
                     "querySourceID" : <number>,
                     "querySourceView" : <string> "" | "new" | "all" | "pat
                     "sortColumn" : <string>,
                     "sortDirection" : <string>,
                     "iteratorID" : <number> DEFAULT "-1" (not set)

                     queryID is not provided
                     ------------------------
                      "query" : <query object>,
              }
```

```
        }
...
```

type "pdf" | "rtf",

NOTE: ARC Objects may not be passed. ARCs must be created separately before added to a Report.

```
...
        "styleFamily" : <number>,
        "definition" : {
                "chapters" : [
                        {
                                "tag" : <string> "section" | "group" | "iterat
                                "name" : <string>,
                                "styleID" : <number> DEFAULT "-1" (not set),
                                "elements" : [
                                        {
                                                "tag" : <string> "arc" | "sect
"component"                                                      tag "arc"
                                                "id" : <number> DEFAULT -1,

                                                tag "section" | "group"
                                                "elements" : (see parent 'elem

                                                tag "iterator"
                                                "elements" : (see parent 'elem

                                                        elements parameter is
                                                        ---------------------
                                                        "styleID" : <number> D
                                                        "displayDataPoints" :
                                                        "columns" : [
                                                                {
                                                                        "name"
```

```
                                                                ] OPTIONAL?,

                                                                "definition" : {
                                                                        "dataSource"
                                                                                "query
                                                                                "query
"individual" | "lce" | "mobile"| "patched",                                     "query
                                                                                "query
"patched",
                                                                                "sortC
                                                                                "sortD
                                                                                "itera

                                                                                queryL
                                                                                ------
                                                                                "query
                                                                        }
                                                                }
                                                                "dataPoints" : <string
9223372036854775807) | <number>,

                                                        tag "component"
                                                        **see/dashboard/component::POS
                                                }...
                                        ]
                                }...
                ],
        }
...
```

type "asr"

```
...
       "definition" : {
              "asrInfo" : {
                     "includeARF" : <string> "false" | "true" (required)
                     "content" : <string> "benchmark" | ???? (required)

                     content "benchmark"                        ----------
                     "benchmarks" : []
              },
              "dataSource" : {
                     "queryID" : <number> OPTIONAL (if provided, must be as
with a vuln query),
                     "querySourceType" : <string> "archive" | "cumulative"
"individual" | "lce" | "mobile"| "patched",
                     "querySourceID" : <number>,
                     "querySourceView" : <string>,
                     "sortColumn" : <string>,
                     "sortDirection" : <string>,
                     "iteratorID" : <number> DEFAULT "-1" (not set)

                     queryID is not provided
                     ----------------------
                      "query" : <query object>,
              }
       },
       definition[asrInfo][includeARF] not "false"     -----------------
       "attributeSetID" : <number>...
```

type "arf" | "lasr"

```
...
       "attributeSetID" : <number>,
       "definition" : {
              "dataSource" : {
```

```
                        "queryID" : <number> OPTIONAL (if provided, must be as
with a vuln query),
                        "querySourceType" : <string> "archive" | "cumulative"
"individual" | "lce" | "mobile"| "patched",
                        "querySourceID" : <number>,
                        "querySourceView" : <string>,
                        "sortColumn" : <string>,
                        "sortDirection" : <string>,
                        "iteratorID" : <number> DEFAULT "-1" (not set)

                        queryID is not provided
                        -----------------------
                         "query" : <query object>,
                        },
                },
                "attributeSetID" : <number>     }
...
```

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "id" : "3",
                "name" : "Test",
                "description" : "test",
                "type" : "lasr",
                "styleFamily" : "-1",
                "definition" : {
                        "columns" : [
                                {
                                        "name" : "all"
```

```
                        ],
                        "dataSource" : {
                                "queryID" : 2,
                                "querySourceType" : "cumulative",
                                "querySourceID" : null,
                                "querySourceView" : "all",
                                "sortColumn" : null,
                                "sortDirection" : null
                        },
                        "dataPoints" : 1.7976931348623e+308,
                        "lasrInfo" : {
                                "benchmarks" : ["Faked Data Benchmark"]
                        }
                },
                "xmldefinition" : "a:4:{s:7:\"columns\";a:1:{i:0;a:1:
{s:4:\"name\";s:3:\"all\";}}s:10:\"dataSource\";a:6:
{s:7:\"queryID\";i:2;s:15:\"querySourceType\";s:10:\"cumulative\";s:-
13:\"querySourceID\";N;s:15:\"querySourceView\";s:3:\"all\";s:10:\"s-
ortColumn\";N;s:13:\"sortDirection\";N;}s:10:\"dataPoints\";d:1.7976-
931348623157E+308;s:8:\"lasrInfo\";a:1:{s:10:\"benchmarks\";a:1:
{i:0;s:20:\"Faked Data Benchmark\";}}}",
                "encryptionPassword" : "",
                "status" : "0",
                "shareUsers" : [],
                "emailUsers" : [],
                "emailTargets" : "",
                "emailBCCTargets" : "",
                "createdTime" : "1410369405",
                "modifiedTime" : "1410369421",
                "pubSites" : [],
                "sources" : [
                        {
                                "id" : "3",
```

```
                        "queryID" : "2",
                        "querySourceType" : "cumulative",
                        "querySourceID" : null,
                        "querySourceView" : "all",
                        "sortColumn" : null,
                        "sortDirection" : null,
                        "iteratorID" : "-1",
                        "resultStyle" : "list",
                        "dataPoints" : 1.7976931348623e+308
                }
        ],
        "scanResult" : [],
        "components" : [
                {
                        "componentType" : "lasr",
                        "dataPoints" : 1.7976931348623e+308,
                        "columns" : "all"                       }
        ],
        "iterators" : [],
        "schedule" : {
                "id" : "7",
                "type" : "template",
                "start" : "",
                "repeatRule" : "",
                "nextRun" : 0
        },
        "creator" : {
                "id" : "1",
                "username" : "head",
                "firstname" : "Security Manager",
                "lastname" : "",
                "uuid" : "96F2AD1B-1B83-462E-908A-84E6054F6B64"
        "owner" : {
```

```
                        "id" : "1",
                        "username" : "head",
                        "firstname" : "Security Manager",
                        "lastname" : "",
                        "uuid" : "96F2AD1B-1B83-462E-908A-84E6054F6B64"
                "ownerGroup" : {
                        "id" : "0",
                        "name" : "Full Access",
                        "description" : "Full Access group"             },
                "attributeSet" : {
                        "id" : "5",
                        "name" : "test",
                        "description" : ""              }
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1413401138
}
```


/reportDefinition/{id}

Methods

GET

Gets the Report Definition associated with {id}.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
**name

**description
**status
creator
owner
ownerGroup
type
dataSourceID
attributeSet
styleFamily
definition
xmldefinition
encryptionPassword
shareUsers
emailUsers
emailTargets
emailBCCTargets
createdTime
modifiedTime
pubSites
schedule
sources
scanResult
canManage
canUse
components
iterators
queryStatus

Legend

** = always comes back*
*** = comes back if fields list not specified on GET all*
***red** = field is a JSON object (**e.g.** "SCI" : {"id" : "2", "name" : "SCI Name", "description" : "Description"})*

Request Query Parameters

None

Example Response

Expand


```
{
	"type" : "regular",
	"response" : {
		"id" : "3",
		"name" : "Test",
		"description" : "test",
		"type" : "lasr",
		"styleFamily" : "-1",
		"definition" : {
			"columns" : [
				{
					"name" : "all"
			],
			"dataSource" : {
				"queryID" : 2,
				"querySourceType" : "cumulative",
				"querySourceID" : null,
				"querySourceView" : "all",
				"sortColumn" : null,
				"sortDirection" : null
			},
			"dataPoints" : 1.7976931348623e+308,
			"lasrInfo" : {
				"benchmarks" : ["Faked Data Benchmark"]
			}
		},
		"xmldefinition" : "a:4:{s:7:\"columns\";a:1:{i:0;a:1:
{s:4:\"name\";s:3:\"all\";}}s:10:\"dataSource\";a:6:
{s:7:\"queryID\";i:2;s:15:\"querySourceType\";s:10:\"cumulative\";s:-
13:\"querySourceID\";N;s:15:\"querySourceView\";s:3:\"all\";s:10:\"s-
```

```
ortColumn\";N;s:13:\"sortDirection\";N;}s:10:\"dataPoints\";d:1.7976-
931348623157E+308;s:8:\"lasrInfo\";a:1:{s:10:\"benchmarks\";a:1:
{i:0;s:20:\"Faked Data Benchmark\";}}}",
                "encryptionPassword" : "",
                "status" : "0",
                "shareUsers" : [],
                "emailUsers" : [],
                "emailTargets" : "",
                "emailBCCTargets" : "",
                "createdTime" : "1410369405",
                "modifiedTime" : "1410369421",
                "pubSites" : [],
                "sources" : [
                        {
                                "id" : "3",
                                "queryID" : "2",
                                "querySourceType" : "cumulative",
                                "querySourceID" : null,
                                "querySourceView" : "all",
                                "sortColumn" : null,
                                "sortDirection" : null,
                                "iteratorID" : "-1",
                                "resultStyle" : "list",
                                "dataPoints" : 1.7976931348623e+308
                        }
                ],
                "scanResult" : [],
                "components" : [
                        {
                                "componentType" : "lasr",
                                "dataPoints" : 1.7976931348623e+308,
                                "columns" : "all"                       }
                ],
```

```
"iterators" : [],
"schedule" : {
        "id" : "7",
        "type" : "template",
        "start" : "",
        "repeatRule" : "",
        "nextRun" : 0
},
"creator" : {
        "id" : "1",
        "username" : "head",
        "firstname" : "Security Manager",
        "lastname" : "",
        "uuid" : "96F2AD1B-1B83-462E-908A-84E6054F6B64"
"owner" : {
        "id" : "1",
        "username" : "head",
        "firstname" : "Security Manager",
        "lastname" : "",
        "uuid" : "96F2AD1B-1B83-462E-908A-84E6054F6B64"
"ownerGroup" : {
        "id" : "0",
        "name" : "Full Access",
        "description" : "Full Access group"            },
"attributeSet" : {
        "id" : "5",
        "name" : "test",
        "description" : ""            },
"queryStatus" : [
        {
                "id" : "1",
                "name" : "",
                "description" : """,
```

```
                                "status" : "0"                  }
                ]
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1413401138
}
```


PATCH

Edits the Report Definition associated with {id}, changing only the passed in fields.

Request Parameters

(All fields are optional)

See /reportDefinition::POST for parameters.

Example Response

See /reportDefinition/{id}::GET

DELETE

Deletes Reports associated with Report Definition {id}.

Request Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
        "response" : "",
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
```

```
        "timestamp" : 1405715741
}
```


/reportDefinition/{id}/launch

Methods

POST

Launches a Report Job specified from the Report Definition associated with {id}. To get the status of the Report Job, see API call */report::GET*.

Request Query Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
        "response" : {
                "reportDefinitionID" : "7",
                "reportResult" : {
                        "creatorID" : "2",
                        "ownerID" : "2",
                        "ownerGID" : "1",
                        "reportDefinitionID" : "7",
                        "jobID" : "113868",
                        "name" : "CS-4700 Iterator",
                        "description" : "",
                        "type" : "pdf",
                        "status" : "Queued",
                        "errorDetails" : "",
                        "totalSteps" : -1,
                        "completedSteps" : 0,
```

```
                        "startTime" : -1,
                        "finishTime" : 0,
                        "pubSites" : [],
                        "id" : "3"              }
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1434567869
}
```

/reportDefinition/{id}/copy

POST

Copies the Report Definition associated with {id}.

Request Query Parameters

Expand

```
{
        "name" : <string>,
        "targetUserID" : <number> DEFAULT (Session User's ID)
}
```

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "id" : "3",
                "name" : "Test",
                "description" : "test",
```

```
                "type" : "lasr",
                "styleFamily" : "-1",
                "definition" : {
                        "columns" : [
                                {
                                        "name" : "all"
                        ],
                        "dataSource" : {
                                "queryID" : 2,
                                "querySourceType" : "cumulative",
                                "querySourceID" : null,
                                "querySourceView" : "all",
                                "sortColumn" : null,
                                "sortDirection" : null
                        },
                        "dataPoints" : 1.7976931348623e+308,
                        "lasrInfo" : {
                                "benchmarks" : ["Faked Data Benchmark"]
                        }
                },
                "xmldefinition" : "a:4:{s:7:\"columns\";a:1:{i:0;a:1:
{s:4:\"name\";s:3:\"all\";}}s:10:\"dataSource\";a:6:
{s:7:\"queryID\";i:2;s:15:\"querySourceType\";s:10:\"cumulative\";s:-
13:\"querySourceID\";N;s:15:\"querySourceView\";s:3:\"all\";s:10:\"s-
ortColumn\";N;s:13:\"sortDirection\";N;}s:10:\"dataPoints\";d:1.7976-
931348623157E+308;s:8:\"lasrInfo\";a:1:{s:10:\"benchmarks\";a:1:
{i:0;s:20:\"Faked Data Benchmark\";}}}",
                "encryptionPassword" : "",
                "status" : "0",
                "shareUsers" : [],
                "emailUsers" : [],
                "emailTargets" : "",
                "emailBCCTargets" : "",
```

```
        "createdTime" : "1410369405",
        "modifiedTime" : "1410369421",
        "pubSites" : [],
        "sources" : [
                {
                        "id" : "3",
                        "queryID" : "2",
                        "querySourceType" : "cumulative",
                        "querySourceID" : null,
                        "querySourceView" : "all",
                        "sortColumn" : null,
                        "sortDirection" : null,
                        "iteratorID" : "-1",
                        "resultStyle" : "list",
                        "dataPoints" : 1.7976931348623e+308
                }
        ],
        "scanResult" : [],
        "components" : [
                {
                        "componentType" : "lasr",
                        "dataPoints" : 1.7976931348623e+308,
                        "columns" : "all"                       }
        ],
        "iterators" : [],
        "schedule" : {
                "id" : "7",
                "type" : "template",
                "start" : "",
                "repeatRule" : "",
                "nextRun" : 0
        },
        "creator" : {
```

```
                        "id" : "1",
                        "username" : "head",
                        "firstname" : "Security Manager",
                        "lastname" : "",
                        "uuid" : "96F2AD1B-1B83-462E-908A-84E6054F6B64"
                "owner" : {
                        "id" : "1",
                        "username" : "head",
                        "firstname" : "Security Manager",
                        "lastname" : "",
                        "uuid" : "96F2AD1B-1B83-462E-908A-84E6054F6B64"
                "ownerGroup" : {
                        "id" : "0",
                        "name" : "Full Access",
                        "description" : "Full Access group"             },
                "attributeSet" : {
                        "id" : "5",
                        "name" : "test",
                        "description" : ""              }
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1413401138
}
```


/reportDefinition/{id}/export

POST

Exports the Report Definition associated with {id}.

Request Query Parameters

Expand

```
{
        "exportType" : <string> "cleansed" | "full" | "placeholders"}
```

Example Response

None given. The response will be an xml file containing the Report Definition.

/reportDefinition/import

POST

Imports the report definition provided.

Request Query Parameters

Expand

```
 {
        "name" : <string>,
        "filename" : <string> (associated with valid reportDefinition file)
}
```

Example Response

Expand

```
 {
    "type" : "regular",
    "response" : "",
    "error_code" : 0,
    "error_msg" : "",
    "warnings" : [],
    "timestamp" : 1407248107
}
```

Atlassian

Tenable Security Center API: Report Image

/report/image

Methods

GET

Gets the list of Report Images

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
**name
**description
creator
type
filename
originalFilename
createdTime
modifiedTime
image

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

Request Query Parameters

None

Example Response

Expand

```
{
	"type" : "regular",
	"response" : [
		{
			"id" : "1",
			"name" : "Fake",
			"description" : "faked from SQLite Manager"
	],
	"error_code" : 0,
	"error_msg" : "",
	"warnings" : [],
	"timestamp" : 1418679112
}
```

POST

Adds an Report Image.

Request Parameters

Expand

NOTE: The 'image' field is for GET only. It cannot be added or modified directly

```
{
	"name" : <string>,
	"description" : <string> DEFAULT "",
	"type" : <string> "Logo" | "Watermark",
	"filename" : <string>,
	"originalFilename" : <string> DEFAULT (filename)
}
```

Example Response

Expand

```
{
	"type" : "regular",
	"response" : {
		"id" : "3",
		"name" : "reportImage",
		"description" : "Example for Documentation",
		"type" : "Logo",
		"filename" : "scfile_jtiiVb",
		"originalFilename" : "fake.png",
		"createdTime" : "1418746737",
		"modifiedTime" : "1418746737",
		"image" :
"iVBORw0KGgoAAAANSUhEUgAAAbQAAAEECAIAAADPnFZkAAAAAXNSR0IArs4c6QAAAAR-
nQU1BAACxjwv8YQUAAAAJcEhZcwAAEnQAABJ0Ad5mH3gAAAT8SURBVHhe7dndbeM4GED-
RqSsFTT2pZppJMVls1rJl6+rHhjErgOe8RSI\/6umCRn59A7AgjgBBHAGCOAIEcQQI4g-
gQxBEgiCNAEEeAII4AQRwBgjgCBHEECOIIEMQRIIgjQBBHgCCOEcOIIEMQRIIgjQBBHgCCOAEcAYI4AgRxBAjiCBDEESCII0AQR4AgjgBBHAGCOAIEcQQI4g-
gQxBEgiCNAEEeAII4AQRwBgjgCBHEECOIIEMQRIIgjQBBHgCCOAEcAYI4AgRxBAjiCBDEESCII0AQR4AgjgBBHAGCOAIEcQQI4ggQxBEgiCNAEEeAII4AQRwBgjgCBHEECOIIEMQRIIgjQBBHgCCOAEcAYI4AgRxBAjiCBDEESCII0AQR4AgjgBBHAGCOAIEcQQI4ggQxBEgiCNAEEeAII4AQRwBgjgCBHEECOIIEMQRIIgjQBBHgCCOAEcAYI4AgRxBAjiCBDEESCII0AQR4AgjgBBHAGCOAIEcQQI4ggQxBEgiCNAEEeAII4AQRwBgjgCBHEECOIIEMQRIIgjQBBHgCCOAEcAYI4AgRxBAjiCBDEESCII0AQR4AgjgBBHAGCOAIEcQQI4ggQxBEgiCNAEEeAII4AQRwBgjgO6evz49em338uK5f+/L6s2Vz1r2nlx+fX5cnc9Rvmr3c\/bGUY-
vJ04DmkWuLaevbut23XciuNtzN2M3Q8TR\/4WcRzSVra2PdRrs46rp9zuh4+vXv8weDN-
xHNLLDbps\/Pj8PDBh5ZRbGpdpFUdOQxyH9GqDrm38OjIil0wPe+OrHwZvJ45DerFBl2-
3\/7dqfsVyxdWn8IY6chjgO6aUGTWWbNu0OeVww\/b1xrDhyGuI4pFca9NjG\/Sl373c-
vjT\/EkdMQxyG90KApbvO0TWNWejc75ZrGnRPFkdMQxyE936Bq4+w6mHW8tvNq69L4Y7-
nlzu5+eBtxHNJOg5bN7Dbu1PGa4I\/Lov26iSOnIY5DejaO0\/plnLbqeI3j7Gf1Tt9m-
Wy5P4H8ijkN6skHrbdys490ptzxuHSqOnIY4Dum5Bk2rdyzq+HjKbc7q9VEcOQ1xHNJT-
DTrYxuW05Sm7eRRHTkMch\/RMg6a1q7e91XH1eOfXtThyGuI4pCcadKCNa\/P66WYexZ-
HTEMchHW7Qxr9b7uTAtVNueVyMFUdOQxyHdLRBR9vYEzdOmV49ThZHTkMch3SwQcfbOL-
sN3tZunnLLY\/V0w\/63wDuI45COxfGJNs4W32bunFI9vT1bJY78HeIIEMQRIIgjQBBH-
gCCOAEEcAYI4AgRxBAjiCBDEESCII0AQR4AgjgBBHAGCOAIEcQQI4ggQxBEgiCNAEEeA-
```

```
II4AQRwBgjgCBHEECOIIEMQRIIgjQBBHgCCOAEEcAYI4AgRxBAjiCBDEESCII0AQR4Ag-
jgBBHAGCOAIEcQQI4ggQxBEgiCNAEEeAII4AQRwBgjgCBHEECOIIEMQRIIgjQBBHgCCO-
AEEcAYI4AgRxBAjiCBDEESCII0AQR4AgjgBBHAGCOAIEcQQI4ggQxBEgiCNAEEeAII4A-
QRwBgjgCBHEECOIIEMQRIIgjQBBHgCCOAEEcAYI4AgRxBAjiCBDEESCII0AQR4AgjgBB-
HAGCOAIEcQQI4ggQxBEgiCNAEEeAII4AQRwBgjgCBHEECOIIEMQRIIgjQBBHgCCOAEEc-
AYI4AgRxBAjiCBDEESCII0AQR4AgjgBBHAGCOAIEcQQI4ggQxBEgiCNAEEeAII4AQRwB-
gjgCBHEECOIIEMQRIIgjQBBHgCCOAEEcAYI4AgRxBAjiCBDEESCII0AQR4CF7+9\/AL0-
1WNsOCEiAAAAAAElFTkSuQmCC",
                "creator" : {
                        "id" : "1",
                        "username" : "head",
                        "firstname" : "Security Manager",
                        "lastname" : "",
             "uuid": "2E2B70F2-3471-428F-82AF-A6905090EAA9"                }
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1418746737
}
```


/report/image/{id}

Methods

GET

Gets the Report Image associated with {id}.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
**name
**description
creator
type
filename
originalFilename
createdTime
modifiedTime
image

Legend

* = always comes back

** = comes back if fields list not specified on GET all

Request Query Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
        "response" : {
                "id" : "1",
                "name" : "Fake",
                "description" : "faked from SQLite Manager",
                "type" : "watermark",
                "filename" : "fake.png",
                "originalFilename" : "fake",
                "createdTime" : "1",
                "modifiedTime" : "1",
                "image" :
```

```
"iVBORw0KGgoAAAANSUhEUgAAAbQAAAEECAIAAADPnFZkAAAAAXNSR0IArs4c6QAAAAR-
nQU1BAACxjwv8YQUAAAAJcEhZcwAAEnQAABJ0Ad5mH3gAAAT8SURBVHhe7dndbeM4GED-
RqSsFTT2pZppJMVls1rJl6+rHhjErgOe8RSI\/6umCRn59A7AgjgBBHAGCOAIEcQQI4g-
gQxBEgiCNAEEeAII4AQRwBgjgCBHEECOIIEMQRIIgjQBBHgCCOAEcAYI4AgRxBAjiCB-
DEESCII0AQR4AgjgBBHAGCOAIEcQQI4ggQxBEgiCNAEEeAII4AQRwBgjgCBHEECOIIEM-
QRIIgjQBBHgCCOAEEcAYI4AgRxBAjiCBDEESCII0AQR4AgjgBBHAGCOAIEcQQI4ggQxB-
EgiCNAEEeAII4AQRwBgjgCBHEECOIIEMQRIIgjQBBHgCCOAEEcAYI4AgRxBAjiCBDEES-
CII0AQR4AgjgBBHAGCOAIEcQQI4ggQxBEgiCNAEEeAII4AQRwBgjgCBHEECOIIEMQRII-
gjQBBHgCCOAEEcAYI4AgRxBAjiCBDEESCII0AQR4AgjgBBHAGCOAIEcQQI4ggQxBEgiC-
NAEEeAII4AQRwBgjgO6evz49em338uK5f+\/L6s2Vz1r2nlx+fX5cnc9Rvmr3c\/bGUY-
vJ04DmkWuLaevbut23XciuNtzN2M3Q8TR\/4WcRzSVra2PdRrs46rp9zuh4+vXv8weDN-
xHNLLDbps\/Pj8PDBh5ZRbGpdpFUdOQxyH9GqDrm38OjIil0wPe+OrHwZvJ45DerFBl2-
3\/7dqfsVyxdWn8IY6chjgO6aUGTWWbNu0OeVww\/b1xrDhyGuI4pFca9NjG\/Sl373c-
vjT\/EkdMQxyG90KApbvO0TWNWejc75ZrGnRPFkdMQxyE936Bq4+w6mHW8tvNq69L4Y7-
nlzu5+eBtxHNJOg5bN7Dbu1PGa4I\/Lov26iSOnIY5DejaO0\/plnLbqeI3j7Gf1Tt9m-
Wy5P4H8ijkN6skHrbdys490ptzxuHSqOnIY4Dum5Bk2rdyzq+HjKbc7q9VEcOQ1xHNJT-
DTrYxuW05Sm7eRRHTkMch\/RMg6a1q7e91XH1eOfXtThyGuI4pCcadKCNa\/P66WYexZ-
HTEMchHW7Qxr9b7uTAtVNueVyMFUdOQxyHdLRBR9vYEzdOmV49ThZHTkMch3SwQcfbOL-
sN3tZunnLLY\/V0w\/63wDuI45COxfGJNs4W32bunFI9vT1bJY78HeIIEMQRIIgjQBBH-
gCCOAEEcAYI4AgRxBAjiCBDEESCII0AQR4AgjgBBHAGCOAIEcQQI4ggQxBEgiCNAEEeA-
II4AQRwBgjgCBHEECOIIEMQRIIgjQBBHgCCOAEcAYI4AgRxBAjiCBDEESCII0AQR4Ag-
jgBBHAGCOAIEcQQI4ggQxBEgiCNAEEeAII4AQRwBgjgCBHEECOIIEMQRIIgjQBBHgCCO-
AEEcAYI4AgRxBAjiCBDEESCII0AQR4AgjgBBHAGCOAIEcQQI4ggQxBEgiCNAEEeAII4A-
QRwBgjgCBHEECOIIEMQRIIgjQBBHgCCOAEcAYI4AgRxBAjiCBDEESCII0AQR4AgjgBB-
HAGCOAIEcQQI4ggQxBEgiCNAEEeAII4AQRwBgjgCBHEECOIIEMQRIIgjQBBHgCCOAEEc-
AYI4AgRxBAjiCBDEESCII0AQR4AgjgBBHAGCOAIEcQQI4ggQxBEgiCNAEEeAII4AQRwB-
gjgCBHEECOIIEMQRIIgjQBBHgCCOAEcAYI4AgRxBAjiCBDEESCII0AQR4CF7+9\/AL0-
1WNsOCEiAAAAAAElFTkSuQmCC",
                "creator" : {
                        "id" : "1",
                        "username" : "head",
                        "firstname" : "Security Manager",
                        "lastname" : "",
```

```
            "uuid": "2E2B70F2-3471-428F-82AF-A6905090EAA9"
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1418679161
}
```


PATCH

Edits the Report Image associated with {id}, changing only the passed in fields.

Request Parameters

(All fields are optional)

See /report/image::POST for parameters.

Example Response

See /report/image/{id}::GET

DELETE

Deletes the Report Image associated with {id}, depending on access and permissions.

Request Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
        "response" : "",
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1418744408
```

```
}
```

Atlassian

Tenable Security Center API: Report Template

/reportTemplate

Methods

GET

Gets the list of Report Templates.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
**name
**description
summary
category
definition
styleFamily
screenshotCount
enabled
minUpgradeVersion
templatePubTime
templateModTime
templateDefModTime
definitionModTime
createdTime
modifiedTime

tags
requirements

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

Request Query Parameters

Expand

NOTE #1: Pseudo Category "0" (recent) is currently not supported

NOTE #2: The *searchString* parameter takes in a space-separated set of keywords/phrases (in parenthesis) and builds a fuzzy match based on them. For excluding a keyword/phrase, is preceded by a '-'. Example:

```
"searchString" : "audit" -"SCAP" ..."
```

Parameters must be passed in as query string (as opposed to JSON) in the format of: /reportTemplate?categoryID="1"&...

```
{
	"categoryID" : <number> "1" (Threat Detection & Vulnerability
Assessments) | "2" (Monitoring) | "3" (Security Industry Trends) |
"4" (Executive) | "5" "Compliance & Configuration Assessment) | "6"
(Discovery & Detection) DEFAULT "" (All Categories),
	"searchString" : <string> (Search String Format. See NOTE#2)
DEFAULT "",
	"startOffset" : <number> (Positive Integer) DEFAULT "0",
	"endOffset" : <number> (Integer > startOffset) DEFAULT NOT_SET (all
results)
}
```

Example Response

Expand

```
{
        "type" : "regular",
        "response" : [
                {
                        "id" : "1",
                        "name" : "FakedDataTemplate",
                        "description" : "This is a faked data template for the
SC-19907"                 },
                {
                        "id" : "2",
                        "name" : "FakedDataTemplate2",
                        "description" : "This is a faked data template for the
SC-19907"                 }
        ],
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1412017247
}
```


/reportTemplate/{id}

Methods

GET

Gets the Report Template associated with {id}.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
**name

**description
summary
category
definition
styleFamily
screenshotCount
enabled
minUpgradeVersion
templatePubTime
templateModTime
templateDefModTime
definitionModTime
createdTime
modifiedTime
tags
requirements

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

Request Query Parameters

None

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "id" : "1",
                "name" : "FakedDataTemplate",
                "description" : "This is a faked data template for the testing
SC-19907",
```

```
                "summary" : null,
                "definition" : null,
                "styleFamily" : "1",
                "screenshotCount" : "2",
                "enabled" : "true",
                "minUpgradeVersion" : null,
                "templatePubTime" : null,
                "templateModTime" : null,
                "templateDefModTime" : null,
                "definitionModTime" : null,
                "createdTime" : null,
                "modifiedTime" : null,
                "tags" : [
                        "FakedTest1"            ],
                "requirements" : [
                        {
                                "requirement" : "fakedReq1",
                                "value" : "1"                   },
                        {
                                "requirement" : "fakedReq2",
                                "value" : null
                        }
                ],
                "category" : {
                        "id" : "1",
                        "name" : "Threat Detection & Vulnerability Assessments
                        "description" : "Aid with identifying vulnerabilities
potential threats."             }
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1412017433
```

```
}
```

/reportTemplate/{templateID}/image/{sequenceID}

Methods

GET

Gets the Report Template image associated with template {templateID} and image {sequenceID}.

NOTE: This endpoint is handled before token validation.

Request Query Parameters

None

Example Response

None given. The response will be a raw png file containing the requested Report Template image.

/reportTemplate/categories

Methods

GET

Gets the list of Report Template categories

Request Query Parameters

None

Example Response

Expand

```
{
        "type" : "regular",
        "response" : [
                {
                        "id" : "1",
```

```
                        "name" : "Threat Detection & Vulnerability Assessments
                        "description" : "Aid with identifying vulnerabilities
potential threats.",
                        "count" : "71"          },
                {
                        "id" : "2",
                        "name" : "Monitoring",
                        "description" : "Provide intrusion monitoring, alertin
analysis.",
                        "count" : "36"          },
                {
                        "id" : "3",
                        "name" : "Security Industry Trends",
                        "description" : "Influenced by trends, reports, and ar
industry leaders.",
                        "count" : "5"           },
                {
                        "id" : "4",
                        "name" : "Executive",
                        "description" : "Provide operational insight and metri
towards executives.",
                        "count" : "19"          },
                {
                        "id" : "5",
                        "name" : "Compliance & Configuration Assessment",
                        "description" : "Aid with configuration, change and co
management.",
                        "count" : "57"          },
                {
                        "id" : "6",
                        "name" : "Discovery & Detection",
                        "description" : "Aid in trust identification, rogue de
new device discovery.",
```

```
                        "count" : "23"          }
        ],
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1412091153
}
```


Atlassian

Tenable Security Center API: Repository

/repository

Methods

GET

Gets the list of Repositories.

NOTE: The field 'transfer' will only be returned if the type is "remote", running is "true", and the field is requested.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,.
```

NOTES:

- The fields related to data expiration (activeVulnsLifetime, passiveVulnsLifetime, lceVulnsLifetime, complianceVulnsLifetime, mitigatedVulnsLifetime) only apply to repositories of type "Local".
- 'typeFields' returns type-specific parameters inside of a 'typeFields." If requested, typeFields returns as follows:

dataFormat "agent": uuidCount, trendingDays, trendWithRaw, runningNessus, lastGenerateNessusTime, lastTrendUpdate, correlation, activeVulnsLifetime,

complianceVulnsLifetime,
mitigatedVulnsLifetime, percentCapacityCumulative, percentCapacityPatched
dataFormat "mobile": mobileSchedule, preferences, scanner, mdm, mdmType, deviceCount, status, errorDetails
dataFormat "IPv4": nessusSchedule, correlation, ipRange, ipCount, runningNessus, lastGenerateNessusTime, lastTrendUpdate, trendingDays, trendWithRaw, activeVulnsLifetime, passiveVulnsLifetime, lceVulnsLifetime, complianceVulnsLifetime,
mitigatedVulnsLifetime, percentCapacityCumulative, percentCapacityPatched
dataFormat "IPv6": nessusSchedule, correlation, ipRange, ipCount, runningNessus, lastGenerateNessusTime, lastTrendUpdate, trendingDays, trendWithRaw, activeVulnsLifetime, passiveVulnsLifetime, complianceVulnsLifetime,
mitigatedVulnsLifetime, percentCapacityCumulative, percentCapacityPatched
dataFormat "universal": nessusSchedule, correlation, ipRange, uuidCount, runningNessus, lastGenerateNessusTime, lastTrendUpdate, trendingDays, trendWithRaw, activeVulnsLifetime, passiveVulnsLifetime, complianceVulnsLifetime, mitigatedVulnsLifetime,
percentCapacityCumulative, percentCapacityPatched

Allowed Fields

*id
*uuid
**name
**description
type
dataFormat
vulnCount
remoteID
remoteIP
running
downloadFormat
lastSyncTime
lastVulnUpdate
createdTime
modifiedTime
luminFields
ipOverlaps
transfer

typeFields
remoteSchedule

Session User role "1" (Administrator)

organizations

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

Request Parameters

Expand

Parameters must be passed in as query string (as opposed to JSON) in the format of: /repository?type=All&...

```
{
        "type" : <string> "All" | "Local" | "Remote" | "Offline" DEFAULT
"All",
}
```

Expand Parameters

mdm (only applies to Mobile repositories. 'typeFields' must be requested)

Example Response

Expand

```
{
        "type" : "regular",
        "response" : [
                {
                        "id" : "37",
                        "name" : "ag repo1",
                        "description" : "Copied from QA",
```

```
                "dataFormat" : "agent",
                "uuid" : "A2FF7E13-2C0E-470E-A3C9-E077FE065A54"
        {
                "id" : "38",
                "name" : "jm ipv4",
                "description" : "copied from QA",
                "dataFormat" : "IPv4",
                "uuid" : "2E950182-08B6-4737-830B-4ACC8F6B92F9"
        {
                "id" : "39",
                "name" : "ipv6 rep",
                "description" : "Copied from QA (name changed)",
                "dataFormat" : "IPv6",
                "uuid" : "FF00F4D0-5B9F-4A26-998C-19430295284A"
        {
                "id" : "40",
                "name" : "universal rep",
                "description" : "first universal",
                "dataFormat" : "universal",
                "uuid" : "61606F1A-72CF-4A6D-A2B8-74787C6A8BEF"
        {
                "id" : "43",
                "name" : "Test Local mobile Repository",
                "description" : "DevForm test of mobile repository pos
                "dataFormat" : "mobile",
                "uuid" : "8DFA4F06-646A-4A63-A56D-08CCC9098682"
        {
                "id" : "44",
                "name" : "Test w\/pluginPrefs",
                "description" : "",
                "dataFormat" : "IPv4",
                "uuid" : "E33F8169-7C8B-4D1E-B69F-4C50B6347088"
    ],
```

```
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1423767348
}
```

POST

Adds a Repository.

NOTE: See Lumin for Lumin synchronization settings.

NOTE: The fields related to data expiration (activeVulnsLifetime, passiveVulnsLifetime, lceVulnsLifetime, complianceVulnsLifetime, mitigatedVulnsLifetime) only apply to repositories of type "Local".

Request Parameters

Expand

NOTE: The downloadFormat version number doesn't necessarily correlate directly to the version number for 'mobile' Repositories. As it is defaulted to the correct value, this parameter should not be passed.

```
{
        "name" : <string>,
        "description" : <string> DEFAULT "",
        "dataFormat" : <string> "agent" | "IPv4" | "IPv6" | "mobile" |
"universal",
        "type" : <string> "Local" | "Remote" | "Offline",
        "downloadFormat" : <string> "v2" DEFAULT "v2" (see Note),
        "organizations" : [
         {
             "id" : <number> OR "uuid" : <string>,
             "groupAssign" : <string> "all" | "fullAccess" |
"partial" | "" DEFAULT ""        }...
        ] OPTIONAL,
```

```
        ...
}
```

dataFormat "agent"

```
...
        "activeVulnsLifetime" : <number> DEFAULT 365 (Positive integer),
        "complianceVulnsLifetime" : <number> DEFAULT 365 (Positive
integer),
        "mitigatedVulnsLifetime" : <number> DEFAULT 365 (Positive integer),
        "trendingDays" : <number> (Positive integer no greater than "365"),
        "trendWithRaw" : <string> "false" | "true",
        "correlation" : [
                {
                        "id" : <number>         }...
        ],
...
```

dataFormat "IPv4"

```
...
        "ipRange" : <string> (valid IP format based on IP version),
        "activeVulnsLifetime" : <number> DEFAULT 365 (Positive integer),
        "passiveVulnsLifetime" : <number> DEFAULT 7 (Positive integer),
        "lceVulnsLifetime" : <number> DEFAULT 365 (Positive integer),
        "complianceVulnsLifetime" : <number> DEFAULT 365 (Positive
integer),
        "mitigatedVulnsLifetime" : <number> DEFAULT 365 (Positive integer),
        "trendingDays" : <number> (Positive integer no greater than "365"),
        "trendWithRaw" : <string> "false" | "true",
        "nessusSchedule" : {
                "type" : <string> "dependent" | "ical" | "never" | "rollover"
"template" DEFAULT "never"
                type "ical"             -----------
```

```
                "start" : <string> (This value takes the iCal format),
                "repeatRule" : <string> (This value takes the repeat rule form
        }
        type "Local"    ------------
        "correlation" : [
                {
                        "id" : <number>         }...
        ] DEFAULT [],
...
```

dataFormat "IPv6"

```
...
        "ipRange" : <string> (valid IP format based on IP version),
        "activeVulnsLifetime" : <number> DEFAULT 365 (Positive integer),
        "passiveVulnsLifetime" : <number> DEFAULT 7 (Positive integer),
        "complianceVulnsLifetime" : <number> DEFAULT 365 (Positive
integer),
        "mitigatedVulnsLifetime" : <number> DEFAULT 365 (Positive integer),
        "trendingDays" : <number> (Positive integer no greater than "365"),
        "trendWithRaw" : <string> "false" | "true",
        "nessusSchedule" : {
                "type" : <string> "dependent" | "ical" | "never" | "rollover"
"template" DEFAULT "never"
                type "ical"             -----------
                "start" : <string> (This value takes the iCal format),
                "repeatRule" : <string> (This value takes the repeat rule form
        }
        type "Local"    ------------
        "correlation" : [
                {
                        "id" : <number>         }...
        ] DEFAULT [],
...
```

dataFormat "universal"

```
...
       "ipRange" : <string> (valid IPv4 and/or IPv6 ranges),
       "activeVulnsLifetime" : <number> DEFAULT 365 (Positive integer),
       "passiveVulnsLifetime" : <number> DEFAULT 7 (Positive integer),
       "complianceVulnsLifetime" : <number> DEFAULT 365 (Positive
integer),
       "mitigatedVulnsLifetime" : <number> DEFAULT 365 (Positive integer),
       "trendingDays" : <number> (Positive integer no greater than "365"),
       "trendWithRaw" : <string> "false" | "true",
       "nessusSchedule" : {
              "type" : <string> "dependent" | "ical" | "never" | "rollover"
"template" DEFAULT "never"
              type "ical"             -----------
              "start" : <string> (This value takes the iCal format),
              "repeatRule" : <string> (This value takes the repeat rule forn
       }
       type "Local"    ------------
...
```

dataFormat "mobile"

NOTE #1: For Front-end, the valid preference names and types may be retrieved by looking at the editor block from */mdm/<id>::GET*. For Back-end, the idMapper.php file is utilized.
NOTE #2: 'preferences' are handled in the same manner as preferences for plugins. Particularly, if the preference name passed does not exist, the entry is ignored.

```
...
       "mdm" : {
              "id" : <string> }
       type "Local"    ------------
       "scanner" : {
```

```
                "id" : <number> },
        "mobileSchedule" : {
                "type" : "type" : <string> "dependent" | "ical" | "never" |
"rollover" | "template" DEFAULT "never"          type "ical"              ----
                "start" : <string> (This value takes the iCal format),
                "repeatRule" : <string> (This value takes the repeat rule form
        },
        "preferences" : [
                <string:name>:<string:value>...
        ] DEFAULT []
...
```

type "Remote"

```
...
        "remoteID" : <number>,
        "remoteIP" : <string> (valid remote SC IP),
        "remoteSchedule" : {
         "type" : "type" : <string> "dependent" | "ical" | "never" |
"rollover" | "template" DEFAULT "never"

         type "ical"        -----------
         "start" : <string> (This value takes the iCal format),
         "repeatRule" : <string> (This value takes the repeat rule
format)
        }
...
```

Example Response

Expand

```
{
        "type" : "regular",
```

```
"response" : {
        "id" : "37",
        "name" : "ag repo1",
        "description" : "Copied",
        "type" : "Local",
        "dataFormat" : "IPv4",
        "remoteID" : null,
        "remoteIP" : null,
        "running" : "false",
        "downloadFormat" : "v2",
        "lastSyncTime" : "0",
        "createdTime" : "1422396357",
        "modifiedTime" : "1422396357",
        "organizations" : [
                {
                        "id" : "8",
                        "groupAssign" : "fullAccess",
                        "name" : "Org",
                        "description" : "Testing for Policies with Nev
                        "uuid" : "F8F1B126-1B50-4A65-851A-1168F3283D7F
        ],
        "typeFields" : {
                "lastVulnUpdate" : 1423718403,
                "vulnCount" : 0,
                "nessusSchedule" : {
                        "type" : "never",
                        "start" : "",
                        "repeatRule" : ""                               },
                "correlation" : [],
                "ipRange" : "192.168.0.0\/24",
                "ipCount" : "0",
                "runningNessus" : "false",
                "lastGenerateNessusTime" : "0",
```

```
                        "activeVulnsLifetime" : "365",
                        "passiveVulnsLifetime" : "7",
                        "lceVulnsLifetime" : "365",
                        "complianceVulnsLifetime" : "365",
                        "mitigatedVulnsLifetime" : "365",
                        "trendingDays" : "0",
                        "trendWithRaw" : "true"192.168.1.145,
                },
                "luminFields" : {
                "enabled" : "false"             },
                "uuid" : "A2FF7E13-2C0E-470E-A3C9-E077FE065A54" },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],generateNessus
        "timestamp" : 1423767366
}
```


/repository/{id}

/repository/{uuid}

Methods

GET

Gets the Repository associated with {id} or {uuid}.

NOTE: The field 'transfer' will only be returned if the type is "remote", running is "true", and the field is requested.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

NOTES:

- The "ipOverlaps" field is not available at this endpoint.
- The fields related to data expiration (activeVulnsLifetime, passiveVulnsLifetime, lceVulnsLifetime, complianceVulnsLifetime, mitigatedVulnsLifetime) only apply to repositories of type "Local".
- 'typeFields' returns type-specific parameters inside of a 'typeFields." If requested, typeFields returns as follows:

dataFormat "agent": uuidCount, trendingDays, trendWithRaw, runningNessus, lastGenerateNessusTime, lastTrendUpdate, correlation, activeVulnsLifetime, complianceVulnsLifetime, mitigatedVulnsLifetime, percentCapacityCumulative, percentCapacityPatched
dataFormat "mobile": mobileSchedule, preferences, scanner, mdm, mdmType, deviceCount, status, errorDetails
dataFormat "IPv4": nessusSchedule, correlation, ipRange, ipCount, runningNessus, lastGenerateNessusTime, lastTrendUpdate, trendingDays, trendWithRaw, activeVulnsLifetime, passiveVulnsLifetime, lceVulnsLifetime, complianceVulnsLifetime, mitigatedVulnsLifetime, percentCapacityCumulative, percentCapacityPatched
dataFormat "IPv6": nessusSchedule, correlation, ipRange, ipCount, runningNessus, lastGenerateNessusTime, lastTrendUpdate, trendingDays, trendWithRaw, activeVulnsLifetime, passiveVulnsLifetime, complianceVulnsLifetime, mitigatedVulnsLifetime, percentCapacityCumulative, percentCapacityPatched
dataFormat "universal": nessusSchedule, correlation, ipRange, uuidCount, runningNessus, lastGenerateNessusTime, lastTrendUpdate, trendingDays, trendWithRaw, activeVulnsLifetime, passiveVulnsLifetime, complianceVulnsLifetime, mitigatedVulnsLifetime, percentCapacityCumulative, percentCapacityPatched

Allowed Fields

*id
*uuid
**name
**description
type
dataFormat
vulnCount
remoteID
remoteIP

running
downloadFormat
lastSyncTime
lastVulnUpdate
createdTime
modifiedTime
transfer
typeFields
luminFields
remoteSchedule

Session User role "1" (Administrator)

organizations

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

Request Parameters

None

Expand Parameters

mdm (only applies to Mobile repositories. 'typeFields' must be requested)

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "id" : "37",
                "name" : "ag repo1",
                "description" : "Copied",
```

```
"type" : "Local",
"dataFormat" : "IPv4",
"remoteID" : null,
"remoteIP" : null,
"running" : "false",
"downloadFormat" : "v2",
"lastSyncTime" : "0",
"createdTime" : "1422396357",
"modifiedTime" : "1422396357",
"organizations" : [
        {
                "id" : "8",
                "groupAssign" : "fullAccess",
                "name" : "Org",
                "description" : "Testing for Policies with Nev
                "uuid" : "FF00F4D0-5B9F-4A26-998C-19430295284A
],
"typeFields" : {
        "lastVulnUpdate" : 1423718403,
        "vulnCount" : 0,
        "nessusSchedule" : {
                "type" : "never",
                "start" : "",
                "repeatRule" : ""                                },
        "correlation" : [],
        "ipRange" : "192.168.0.0\/24",
        "ipCount" : "0",
        "runningNessus" : "false",
        "lastGenerateNessusTime" : "0",
        "activeVulnsLifetime" : "365",
        "passiveVulnsLifetime" : "7",
        "lceVulnsLifetime" : "365",
        "complianceVulnsLifetime" : "365",
```

```
                        "mitigatedVulnsLifetime" : "365",
                        "trendingDays" : "0",
                        "trendWithRaw" : "true",
                        "percentCapacityCumulative" : "71",
                        "percentCapacityPatched" " "62"         },
                "luminFields" : {
                        "firstSyncTime" : "1573594357",
                        "lastSyncSuccess" : "1573594357",
                        "lastSyncFailure" : "-1",
                        "details" : "details for LuminFields",
                        "enabled" : "true",
                        "ioNetworkUUID" : "990a9c09-222d-4771-b25a-1fa7a836432
                        "networkDeleted" : "false"
                },
                "uuid" : "A2FF7E13-2C0E-470E-A3C9-E077FE065A54" },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1423767366
}
```


PATCH

Edits the Repository associated with {id} or {uuid}, changing only the passed in fields.

NOTE: Parameters 'type', 'dataFormat', and 'mdm' may not be modified on PATCH.

Request Parameters

(All fields are optional)

See /repository::POST for parameters.

Example Response

See /repository/{id}::GET

DELETE

Deletes the Repository associated with {id} or {uuid}, depending on access and permissions.

Request Parameters

None

Example Response

Expand

```
{
        "type" : "regular",
        "response" : "",
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1401911117
}
```

/repository/{id}/acceptRiskRule

/repository/{uuid}/acceptRiskRule

Methods

GET

Gets the list of Accept Risk Rules in the Repository associated with {id} or {uuid}, unless filters are provided.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
**repository
**organization
**user

**plugin
**hostType
**hostValue
**port
**protocol
**expires
**status
comments
createdTime
modifiedTime

Legend

** = always comes back*
*** = comes back if fields list not specified on GET all*

Filters

Expand

```
pluginID=<number> | <string> "all" DEFAULT "all" (i.e. all Plugins)
port=<number> | <string> "all" DEFAULT "all" (i.e. all Ports)
```

Session User is role "1" (administrator)

```
organizationIDs=<number>,... | <string> "all" DEFAULT "all" (i.e.
all Organizations) OR organizationUUIDs=<string>,...
```

Session User is not role "1" (administrator)

```
organizationIDs=<number>,... | <string> "all" DEFAULT :sessionOrgID:
OR organizationUUIDs=<string>,...
```

Example Response

Expand

```
{
	"type" : "regular",
	"response" : [
		{
			"id" : "3",
			"hostType" : "all",
			"hostValue" : "",
			"port" : "any",
			"protocol" : "any",
			"expires" : "-1",
			"status" : "0",
			"repository" : {
				"id" : "17",
				"name" : "New Fields Repo",
				"description" : "",
				"type" : "Local",
				"uuid" : "A2FF7E13-2C0E-470E-A3C9-E077FE065A54
			"organization" : {
				"id" : "8",
				"name" : "Org",
				"description" : "Testing for Policies with New
				"uuid" : "FF00F4D0-5B9F-4A26-998C-19430295284A
			"user" : {
				"id" : "1",
				"username" : "head",
				"firstname" : "Security Manager",
				"lastname" : "",
				"uuid" : "96F2AD1B-1B83-462E-908A-84E6054F6B64
			"plugin" : {
				"id" : "0",
				"name" : "Open Port",
				"description" : "",
				"type" : "active"                    }
```

```
                }
        ],
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1410275054
}
```

/repository/{id}/recastRiskRule

/repository/{uuid}/recastRiskRule

POST

Downloads the report associated with {id}.

Request Parameters

None

Example Response

None given. The response will be a PDF, RTF, CSV, ASR, ARF, or LASR file in binary or ascii format.

/repository/{id}/recastRiskRule

/repository/{uuid}/recastRiskRule

Methods

GET

Gets the list of Recast Risk Rules in the Repository associated with {id} or {uuid}, unless filters are provided.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
**repository
**organization
**user
**plugin
**newSeverity
**hostType
**hostValue
**port
**protocol
**order
**status
comments
createdTime
modifiedTime

Legend

** = always comes back*
*** = comes back if fields list not specified on GET all*

Filters

Expand

```
pluginID=<number> | <string> "all" DEFAULT "all" (i.e. all Plugins)
port=<number> | <string> "all" DEFAULT "all" (i.e. all Ports)
```

Session User is role "1" (administrator)

```
organizationIDs=<number>,... | <string> "all" DEFAULT "all" (i.e.
all Organizations) OR organizationUUIDs=<string>,...
```

Session User is not role "1" (administrator)

```
organizationIDs=<number>,... | <string> "all" DEFAULT :sessionOrgID:
OR organizationUUIDs=<string>,...
```

Example Response

Expand


```
{
	"type" : "regular",
	"response" : [
		{
			"id" : "1",
			"newSeverity" : "0",
			"hostType" : "all",
			"hostValue" : "",
			"port" : "any",
			"protocol" : "any",
			"order" : "1",
			"status" : "0",
			"repository" : {
				"id" : "17",
				"name" : "New Fields Repo",
				"description" : "",
				"type" : "Local",
				"uuid" : "A2FF7E13-2C0E-470E-A3C9-E077FE065A54
			"organization" : {
				"id" : "8",
				"name" : "Org",
				"description" : "Testing for Policies with New
				"uuid" : "FF00F4D0-5B9F-4A26-998C-19430295284A
			"user" : {
				"id" : "1",
				"username" : "head",
				"firstname" : "Security Manager",
```

```
                                "lastname" : "",
                                "uuid" : "96F2AD1B-1B83-462E-908A-84E6054F6B64
                        "plugin" : {
                                "id" : "0",
                                "name" : "Open Port",
                                "description" : "",
                                "type" : "active"                               }
                }
        ],
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1410281615
}
```


/repository/{id}/assetIntersections

/repository/{uuid}/assetIntersections

GET

Gets the ip, uuid, or hostUUID intersections of an Asset.
NOTE: The number of assets should be limited. Intersecting large numbers of assets may be cause long delays, so pagination should be used in F/E
NOTE: The "uuid" json parameter corresponds to the Tenable UUID of the host, and it should not be confused with the UUID of the repository.
NOTE: The "hostUUID json parameter corresponds to the SC generated UUID of the host, and it should not be confused with the UUID of the repository or the Tenable UUID.

Request Parameters

Expand

Parameters must be passed in as query string (as opposed to JSON) in the format of: /assetIntersections?ip=1.1.1.1&dnsName=foo

Parameter "hostUUID" exists

```
{
       "hostUUID" : <string> (valid uuid)
}
```

Parameter "hostUUID" absent and parameter "uuid" exists

```
{
       "uuid" : <string> (valid uuid)
}
```

Parameters "uuid" and "hostUUID" absent

NOTE: If a uuid is not passed, an IP or an IP and a dnsName is required

```
{
       "ip" : <string> (valid ip address),
       "dnsName" : <string> OPTIONAL
}
```

Example Response

Expand

```
{
   "type":"regular",
   "response":{
      "assets":[
         {
            "id":"0",
            "name":"All Defined Ranges",
            "description":"All defining ranges of the Group in whose
context this Asset is being evaluated."         },
         {
            "id":"2",
```

```
            "name":"Systems that have been Scanned",
            "description":"This asset uses the Scan Summary plugin
to detect if a host has been scanned by Nessus. The Scan Summary
plugin contains the list of tests conducted during the most recent
scan."         },
         {
            "id":"23",
            "name":"SSL or TLS Servers",
            "description":"This asset list uses active and passive
plugins to detect servers running SSL and TLS."         },
         {
            "id":"35",
            "name":"Big Asset List",
            "description":""         },
         {
            "id":"38",
            "name":"Open Targets",
            "description":""         }
      ]
   },
   "error_code":0,
   "error_msg":"",
   "warnings":[],
   "timestamp":1522184799
}
```


/repository/{id}/import

/repository/{uuid}/import

The /repository/import resource.

POST

Starts an on-demand, import for the Repository associated with {id} or {uuid}. The data is specified by a previously uploaded, **gzip**ped tarball of Repository data obtained using */repository/{id}/export or*

/repository/{uuid}/export.

NOTE: The *file* field should contain the value of the same parameter passed back on **/file/upload::POST**.

Request Parameters

Expand

```
{
        "file" : <string>}
```

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "objectID" : "100",
                "objectType" : "importRepository",
                "type" : "now",
                "ownerID" : "1" },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1402950576
}
```

/repository/{id}/export

/repository/{uuid}/export

The /repository/export resource.

GET

Exports the Repository associated with {id} or {uuid} as a **gzip**ped tar file.

Request Parameters

None

Example Response

None given. The response will be a gzipped file containing a tarball of the Repository files.

The tarball will contain the following contents:

- A **Hostname.txt** file corresponding to the Tenable.sc from which the repository was exported. This value is populated by the *hostname* field from the SC License Configuration.
- The **license.key** file of the Tenable.sc from which the repository was exported.
- An **sc.version.txt** file with the version, data format, and mdm type on consecutive lines, respectively.
- The binary files corresponding to the Repository's current data.
- A VDB directory containing binary files for the Repository's trending data (if applicable).

/repository/{id}/sync

/repository/{uuid}/sync

The /repository/sync resource.

POST

Starts an on-demand synchronization of local data for the remote Repository associated with {id} or {uuid}.

Request Parameters

None

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
```

```
                "objectID" : "107",
                "objectType" : "repositorySynchronizationClient",
                "type" : "now",
                "definition" : {
                        "action" : "download",
                        "token" : "1039771703"          },
                "ownerID" : "1" },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1402947699
}
```


/repository/{id}/updateMobileData

/repository/{uuid}/updateMobileData

The /repository/updateMobileData resource.

POST

Starts an on-demand process to update the mobile data for the Repository associated with {id} or {uuid}. This is considered a mobile scan process by Tenable.sc.

Request Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
        "response" : {
                "id" : "156"    },
        "error_code" : 0,
```

```
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1402942558
}
```


/repository/{id}/deviceInfo

/repository/{uuid}/deviceInfo

GET

Gets the device information for the Repository associated with {id} or {uuid}, or {hostUUID}.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*ip
*uuid
*repositoryID
repository
score
total
severityInfo
severityLow
severityMedium
severityHigh
severityCritical
macAddress
policyName
pluginSet
netbiosName
dnsName
osCPE

biosGUID
tpmID
mcafeeGUID
lastAuthRun
lastUnauthRun
severityAll
os
hasPassive
hasCompliance
lastScan
links

Legend

** = always comes back*

Request Parameters

Expand

Parameters must be passed in as query string (as opposed to JSON) in the format of:
/repository/1/deviceInfo?uuid="123e4567-e89b-12d3-a456-426655440000" or
/repository/1/deviceInfo?ip="1.1.1.1"&dnsName="foo"

Parameter "hostUUID" exists

```
hostUUID=<string> (valid uuid)
```

Parameter "hostUUID" absent and parameter "uuid" exists

```
uuid=<string> (valid uuid)
```

Parameters "hostUUID" and "uuid" absent

```
ip=<string> (valid ip address)
&dnsName=<string> OPTIONAL
```

Parameter "sourceType" optimization

```
sourceType=<string> "cumulative" | "patched"
```

Example Response

Expand


```
{
	"type" : "regular",
	"response" : {
		"ip" : "192.168.0.1",
		"uuid" : "123e4567-e89b-12d3-a456-426655440000",
		"repositoryID" : "2",
		"score" : "2130",
		"total" : "322",
		"severityInfo" : "110",
		"severityLow" : "7",
		"severityMedium" : "41",
		"severityHigh" : "152",
		"severityCritical" : "12",
		"macAddress" : "00:00:00:00:00:00",
		"policyName" : "",
		"pluginSet" : "",
		"netbiosName" : "TARGET\\WIN7X64",
		"dnsName" : "target.domain.com",
		"osCPE" : "cpe:\/o:microsoft:windows_7: :gold:x64-ultimate",
		"biosGUID" : "",
		"tpmID" : "",
		"mcafeeGUID" : "",
		"lastAuthRun" : "",
		"lastUnauthRun" : "",
		"severityAll" : "12,152,41,7,110",
```

```
                "os" : "Microsoft Windows 7 Ultimate",
                "hasPassive" : "No",
                "hasCompliance" : "No",
                "lastScan" : "1408294249",
                "links" : [
                        {
                                "name" : "SANS",
                                "link" : "https : \/\/isc.sans.edu\/ipinfo.htm
                 },
                        {
                                "name" : "ARIN",
                                "link" : "http : \/\/whois.arin.net\/rest\/ip\
                ],
                "repository" : {
                        "id" : "2",
                        "name" : "Rep2",
                        "type" : "Local",
                        "description" : "",
                        "uuid" : "4F7DD1CD-EB1B-40D7-BCE1-2DB3E31F6F4C"
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1409855674
}
```


/repository/{id}/attachment/{attachmentID}

/repository/{uuid}/attachment/{attachmentID}

GET

Downloads the attachment with the given {attachmentID} from the provided repository.

Request Parameters

None

Example Response

None given. The response will be the downloaded file in binary or ascii format.

/repository/authorize

POST

Authorizes communication with the remote machine associated with the provided host ip.

Request Parameters

Expand

```
{
        "host" : <string>,
        "username" : <string>,
        "password" : <string>}
```

Example Response

Expand

```
{
        "type" : "regular",
        "response" : "",
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1402939540
}
```

/repository/fetchRemote

The /repository/download resource.

GET

Gets a list of Repositories at the specified location.

NOTE: The */sshKey/installRemoteKey* command may need to be used to gain access to the list of repositories at the remote host if it has not been done so previously. An error code of 63 (RESPONSE_DENIED) will indicate if such a request is required.

Request Parameters

Expand

Parameters must be passed in as query string (as opposed to JSON) in the format of: /repository/fetchRemote/?host=172.26.X.X

```
{
        "host" : <string>}
```

Example Response

Expand

```
{
        "type" : "regular",
        "response" : [
                {
                        "id" : "1",
                        "name" : "qarep_ipv4",
                        "description" : "",
                        "type" : "Local",
                        "dataFormat" : "IPv4",
                        "vulnCount" : 13352,
                        "remoteID" : null,
                        "remoteIP" : null,
                        "running" : "false",
                        "enableTrending" : "true",
                        "downloadFormat" : "v2",
                        "lastSyncTime" : "0",
                        "lastVulnUpdate" : 1402938930,
                        "createdTime" : "1357331461",
```

```
                        "modifiedTime" : "1357569012",
                        "organizations" : [
                                {
                                        "id" : "1",
                                        "groupAssign" : "all"
                                {
                                        "id" : "2",
                                        "groupAssign" : "all"
                        ],
                        "correlation" : [],
                        "ipRange" : "192.168.1.145\/22,192.168.1.145-
192.168.1.146,192.168.1.146\/22",
                        "ipCount" : "80",
                        "runningNessus" : "false",
                        "lastGenerateNessusTime" : "1402272018",
                        "size" : 41586909
                },
                {
                        "id" : "2",
                        "name" : "qarep_pvs_ipv4_3601",
                        "description" : "",
                        "type" : "Local",
                        "dataFormat" : "IPv4",
                        "vulnCount" : 0,
                        "remoteID" : null,
                        "remoteIP" : null,
                        "running" : "false",
                        "enableTrending" : "true",
                        "downloadFormat" : "v2",
                        "lastSyncTime" : "0",
                        "lastVulnUpdate" : 1402892411,
                        "createdTime" : "1357568971",
                        "modifiedTime" : "1357744461",
```

```
                "organizations" : [
                        {
                                "id" : "1",
                                "groupAssign" : "partial"
                ],
                "correlation" : [],
                "ipRange" : "192.168.0.0\/24",
                "ipCount" : "0",
                "runningNessus" : "false",
                "lastGenerateNessusTime" : "1402533002",
                "size" : 0
        },
        {
                "id" : "3",
                "name" : "qarep_pvs_ipv4",
                "description" : "",
                "type" : "Local",
                "dataFormat" : "IPv4",
                "vulnCount" : 0,
                "remoteID" : null,
                "remoteIP" : null,
                "running" : "false",
                "enableTrending" : "true",
                "downloadFormat" : "v2",
                "lastSyncTime" : "0",
                "lastVulnUpdate" : 1402938928,
                "createdTime" : "1357592482",
                "modifiedTime" : "1392317291",
                "organizations" : [
                        {
                                "id" : "1",
                                "groupAssign" : "all"
                        {
```

```
                        "id" : "2",
                        "groupAssign" : "all"
                ],
                "correlation" : [],
                "ipRange" : "192.168.0.0\/24",
                "ipCount" : "0",
                "runningNessus" : "false",
                "lastGenerateNessusTime" : "1402891203",
                "size" : 40
        },
        {
                "id" : "4",
                "name" : "qarep_lce",
                "description" : "",
                "type" : "Local",
                "dataFormat" : "IPv4",
                "vulnCount" : 4350,
                "remoteID" : null,
                "remoteIP" : null,
                "running" : "false",
                "enableTrending" : "false",
                "downloadFormat" : "v1",
                "lastSyncTime" : "0",
                "lastVulnUpdate" : 1402939008,
                "createdTime" : "1357744413",
                "modifiedTime" : "1357744413",
                "organizations" : [
                        {
                                "id" : "1",
                                "groupAssign" : "partial"
                        {
                                "id" : "2",
                                "groupAssign" : "all"
```

```
                        ],
                        "correlation" : [],
                        "ipRange" : "192.168.0.0\/24",
                        "ipCount" : "20",
                        "runningNessus" : "false",
                        "lastGenerateNessusTime" : "0",
                        "size" : 1413684
                }
        ],
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1402939540
}
```


Expand Items: details, shares

- details
    - Show specific details (such as vulnerability count, nessus schedule information, etc.)
- shares
    - Show the organizations granted access to the Repository.

Atlassian

Tenable Security Center API: Role

/role

/tes/role

/tes/role is only available in Tenable Enclave Security

Methods

GET

Gets the list of Roles

Fields Parameter

- The fields not under * or ** can be used only by Admin or users with manageRole permission enabled.
- Logged in user can use these fields to view details for self role only.
- Org users cannot view Admin role itself but can view any other roles created by admin.

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
**name
**description
creator
createdTime
modifiedTime
permManageApp
permManageGroups
permManageRoles
permManageImages
permManageGroupRelationships
permManageBlackoutWindows
permManageAttributeSets
permCreateTickets
permCreateAlerts
permCreateAuditFiles
permCreateLDAPAssets
permCreatePolicies
permPurgeTickets
permPurgeScanResults

permPurgeReportResults
permScan
permAgentsScan
permAgentsSync
permShareObjects
permUpdateFeeds
permUploadNessusResults
permViewOrgLogs
permManageAcceptRiskRules
permManageRecastRiskRules
permManageACR
permViewDomainInventoryAssets
permManageAttackSurfaceDomains
permManageVulnRoutingRules
permViewHostAssets
permManageRiskRules
organizationCounts

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

Request Parameters

None

Filter Parameters

subset - Removes subset roles from the return response.

Example Response

Expand

```
{
        "type" : "regular",
```

```
       "response" : [
                {
                        "id" : "0",
                        "name" : "No Role",
                        "description" : "This role is available as a catch-al
role gets deleted. It has virtually no permissions."
                },
                {
                        "id" : "2",
                        "name" : "Security Manager",
                        "description" : "The Security Manager role has full ac
actions at the organization level. A Security Manager has the
ability to create new groups and manage existing ones. A Security
Manager can also define how users interact with other groups.\n\nThe
ability to manage other users and their objects can be configured
using group permissions on the Access tab of User add/edit. This
includes viewing and stopping running scans and reports."
                },
                {
                        "id" : "3",
                        "name" : "Security Analyst",
                        "description" : "The Security Analyst role has the pe
perform all actions at the organizational level except managing
groups and users. A Security Analyst is most likely an advanced user
who can be trusted with some system related tasks such as setting
blackout windows or updating plugins."
                },
                {
                        "id" : "4",
                        "name" : "Vulnerability Analyst",
                        "description" : "The Vulnerability Analyst role can pe
tasks within the application. A Vulnerability Analyst is allowed to
look at security data, perform scans, share objects, view logs and
```

```
work with tickets."
                },
                {
                        "id" : "5",
                        "name" : "Executive",
                        "description" : "The Executive role is intended for us
interested in a high level overview of their security posture and
risk profile. Executives would most likely be browsing dashboards
and reviewing reports but would not be concerned with monitoring
running scans or managing users. Executives would also be able to
assign tasks to other users using the Ticketing interface."
                },
                {
                        "id" : "6",
                        "name" : "Credential Manager",
                        "description" : "The Credential Manager role can be us
specifically for handling credentials. A Credential Manager can
create and share credentials without revealing the contents of the
credential. This can be used by someone outside the security team to
keep scanning credentials up to date."
                },
                {
                        "id" : "7",
                        "name" : "Auditor",
                        "description" : "The Auditor role can access summary i
to perform 3rd party audits. An Auditor can view dashboards,
reports, and logs but cannot perform scans or create tickets.
Restricting access to vulnerability and event data can be achieved
by placing the user in an appropriately configured group."
                }
        ],
        "error_code" : 0,
        "error_msg" : "",
```

```
        "warnings" : [],
        "timestamp" : 1445013119
}
```

POST

Adds a Role

Request Parameters

Expand

Note: Roles cannot be created with permManageApp privilege.

```
{
        "name" : <string>,
        "description" : <string> DEFAULT "",
        "permManageGroups" : <string> "false" | "true" DEFAULT "false",
        "permManageRoles" : <string> "false" | "true" DEFAULT "false",
        "permManageImages" : <string> "false" | "true" DEFAULT "false",
        "permManageGroupRelationships" : <string> "false" | "true" DEFAULT
"false",
        "permManageBlackoutWindows" : <string> "false" | "true" DEFAULT
"false",
        "permManageAttributeSets" : <string> "false" | "true" DEFAULT
"false",
        "permCreateTickets" : <string> "false" | "true" DEFAULT "false",
        "permCreateAlerts" : <string> "false" | "true" DEFAULT "false",
        "permCreateAuditFiles" : <string> "false" | "true" DEFAULT "false",
        "permCreateLDAPAssets" : <string> "false" | "true" DEFAULT "false",
        "permCreatePolicies" : <string> "false" | "true" DEFAULT "false",
        "permPurgeTickets" : <string> "false" | "true" DEFAULT "false",
        "permPurgeScanResults" : <string> "false" | "true" DEFAULT "false",
        "permPurgeReportResults" : <string> "false" | "true" DEFAULT
"false",
```

```
        "permScan" : <string> "full" | "none" DEFAULT "none",
        "permAgentsScan" : <string> "false" | "true" DEFAULT "false",
        "permAgentsSync" : <string> "false" | "true" DEFAULT "false",
        "permShareObjects" : <string> "false" | "true" DEFAULT "false",
        "permUpdateFeeds" : <string> "false" | "true" DEFAULT "false",
        "permUploadNessusResults" : <string> "false" | "true" DEFAULT
"false",
        "permViewOrgLogs" : <string> "false" | "true" DEFAULT "false",
        "permManageAcceptRiskRules" : <string> "false" | "true" DEFAULT
"false",
        "permManageRecastRiskRules" <string> "false" | "true" DEFAULT
"false",
        "permManageACR" <string> "false" | "true" DEFAULT "false",
        "permViewDomainInventoryAssets" <string> "false" | "true" DEFAULT
"false",
        "permManageAttackSurfaceDomains" <string> "false" | "true" DEFAULT
"false",
        "permManageVulnRoutingRules" <string> "false" | "true" DEFAULT
"false",
        "permViewHostAssets" <string> "false" | "true" DEFAULT "false",
        "permManageRiskRules" <string> "false" | "true" DEFAULT "false"
}
```

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "id" : "1",
                "name" : "Administrator",
                "description" : "Role defining an administrator of the
application",
```

```
"createdTime" : "0",
"modifiedTime" : "0",
"permManageApp" : "true",
"permManageGroups" : "false",
"permManageRoles" : "true",
"permManageImages" : "false",
"permManageGroupRelationships" : "false",
"permManageBlackoutWindows" : "false",
"permManageAttributeSets" : "false",
"permCreateTickets" : "false",
"permCreateAlerts" : "false",
"permCreateAuditFiles" : "true",
"permCreateLDAPAssets" : "false",
"permCreatePolicies" : "true",
"permPurgeTickets" : "false",
"permPurgeScanResults" : "false",
"permPurgeReportResults" : "false",
"permScan" : "none",
"permAgentsScan" : "false",
"permAgentsSync": "false",
"permShareObjects" : "false",
"permUpdateFeeds" : "true",
"permUploadNessusResults" : "false",
"permViewOrgLogs" : "true",
"permManageAcceptRiskRules" : "true",
"permManageRecastRiskRules" : "true",
"permManageACR": "false",
"permViewDomainInventoryAssets": "false",
"permManageAttackSurfaceDomains": "false",
"permManageVulnRoutingRules": "false",
"permViewHostAssets": "false",
"permManageRiskRules": "false",
"organizationCounts" : [
```

```
                        {
                                "id" : "0",
                                "userCount" : "1"
                        },
                        {
                                "id" : "12",
                                "userCount" : "0"
                        }
                ],
                "creator" : {
                        "id" : "1",
                        "username" : "admin",
                        "firstname" : "Admin",
                        "lastname" : "User",
                        "uuid" : "96F2AD1B-1B83-462E-908A-84E6054F6B64"
                }
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1445013361
}
```


/role/{id}

/tes/role/{id}

/tes/role/{id} is only available in Tenable Enclave Security

Methods

GET

Gets the Role associated with {id}.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
**name
**description
creator
createdTime
modifiedTime
permManageApp
permManageGroups
permManageRoles
permManageImages
permManageGroupRelationships
permManageBlackoutWindows
permManageAttributeSets
permCreateTickets
permCreateAlerts
permCreateAuditFiles
permCreateLDAPAssets
permCreatePolicies
permPurgeTickets
permPurgeScanResults
permPurgeReportResults
permScan
permAgentsScan
permAgentsSync
permShareObjects
permUpdateFeeds
permUploadNessusResults
permViewOrgLogs
permManageAcceptRiskRules

permManageRecastRiskRules
permManageACR
permViewDomainInventoryAssets
permManageAttackSurfaceDomains
permManageVulnRoutingRules
permViewHostAssets
permManageRiskRules
organizationCounts

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

- The fields not under * or ** can be used only by Admin or users with manageRole permission enabled.
- Logged in user can use these fields to view details for self role only.
- Org users cannot view Admin role itself but can view any other roles created by admin.

Request Parameters

None

Example Response

Admin user

Expand


```
{
        "type" : "regular",
        "response" : {
                "id" : "1",
                "name" : "Administrator",
                "description" : "Role defining an administrator of the
application",
                "createdTime" : "0",
```

```
"modifiedTime" : "0",
"permManageApp" : "true",
"permManageGroups" : "false",
"permManageRoles" : "true",
"permManageImages" : "false",
"permManageGroupRelationships" : "false",
"permManageBlackoutWindows" : "false",
"permManageAttributeSets" : "false",
"permCreateTickets" : "false",
"permCreateAlerts" : "false",
"permCreateAuditFiles" : "true",
"permCreateLDAPAssets" : "false",
"permCreatePolicies" : "true",
"permPurgeTickets" : "false",
"permPurgeScanResults" : "false",
"permPurgeReportResults" : "false",
"permScan" : "none",
"permAgentsScan" : "false",
"permAgentsSync" : "false",
"permShareObjects" : "false",
"permUpdateFeeds" : "true",
"permUploadNessusResults" : "false",
"permViewOrgLogs" : "true",
"permManageAcceptRiskRules" : "true",
"permManageRecastRiskRules" : "true",
"permManageACR": "false",
"permViewDomainInventoryAssets": "false",
"permManageAttackSurfaceDomains": "false",
"permManageVulnRoutingRules": "false",
"permViewHostAssets": "false",
"permManageRiskRules": "false",
"organizationCounts" : [
        {
```

```
                                "id" : "0",
                                "userCount" : "1"
                        },
                        {
                                "id" : "12",
                                "userCount" : "0"
                        }
                ],
                "creator" : {
                        "id" : "1",
                        "username" : "admin",
                        "firstname" : "Admin",
                        "lastname" : "User",
                        "uuid" : "96F2AD1B-1B83-462E-908A-84E6054F6B64"
                }
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1445013361
}
```


Any user with manageRole permission enabled

Expand


```
{
        "type" : "regular",
        "response" : {
                "id" : "2",
                "name" : "Security Manager",
                "description" : "The Security Manager role has full access to
actions at the organization level. A Security Manager has the
ability to create new groups and manage existing ones. A Security
```

```
Manager can also define how users interact with other groups.\n\nThe
ability to manage other users and their objects can be configured
using group permissions on the Access tab of User add/edit. This
includes viewing and stopping running scans and reports.",
                "createdTime" : "0",
                "modifiedTime" : "0",
                "permManageApp" : "false",
                "permManageGroups" : "true",
                "permManageRoles" : "true",
                "permManageImages" : "true",
                "permManageGroupRelationships" : "true",
                "permManageBlackoutWindows" : "true",
                "permManageAttributeSets" : "true",
                "permCreateTickets" : "true",
                "permCreateAlerts" : "true",
                "permCreateAuditFiles" : "true",
                "permCreateLDAPAssets" : "true",
                "permCreatePolicies" : "true",
                "permPurgeTickets" : "true",
                "permPurgeScanResults" : "true",
                "permPurgeReportResults" : "true",
                "permScan" : "full",
                "permAgentsScan" : "true",
                "permAgentsSync" : "false",
                "permShareObjects" : "true",
                "permUpdateFeeds" : "true",
                "permUploadNessusResults" : "true",
                "permViewOrgLogs" : "true",
                "permManageAcceptRiskRules" : "true",
                "permManageRecastRiskRules" : "true",
                "permManageACR": "false",
                "permViewDomainInventoryAssets": "false",
                "permManageAttackSurfaceDomains": "false",
```

```
                "permManageVulnRoutingRules": "false",
                "permViewHostAssets": "false",
                "permManageRiskRules": "false",
                "organizationCounts" : [
                        {
                                "id" : "12",
                                "userCount" : "1"
                        }
                ],
                "creator" : {
                        "id" : "1",
                        "username" : "head",
                        "firstname" : "",
                        "lastname" : "",
                        "uuid" : "96F2AD1B-1B83-462E-908A-84E6054F6B64"
                }
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1445013361
}
```


Any user with manageRole permission disabled

Expand


```
{
        "type" : "regular",
        "response" : {
                "id" : "2",
                "name" : "Security Manager",
                "description" : "The Security Manager role has full access to
actions at the organization level. A Security Manager has the
```

```
ability to create new groups and manage existing ones. A Security
Manager can also define how users interact with other groups.\n\nThe
ability to manage other users and their objects can be configured
using group permissions on the Access tab of User add/edit. This
includes viewing and stopping running scans and reports."
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1445013361
}
```


Any user fetching self role

Expand


```
{
        "type" : "regular",
        "response" : {
                "id" : "8",
                "name" : "Self role",
                "description" : "Any role with manageRole permission disabled"
                "createdTime" : "0",
                "modifiedTime" : "0",
                "permManageApp" : "false",
                "permManageGroups" : "true",
                "permManageRoles" : "false",
                "permManageImages" : "true",
                "permManageGroupRelationships" : "true",
                "permManageBlackoutWindows" : "true",
                "permManageAttributeSets" : "true",
                "permCreateTickets" : "true",
                "permCreateAlerts" : "true",
                "permCreateAuditFiles" : "true",
```

```
"permCreateLDAPAssets" : "true",
"permCreatePolicies" : "true",
"permPurgeTickets" : "true",
"permPurgeScanResults" : "true",
"permPurgeReportResults" : "true",
"permScan" : "full",
"permAgentsScan" : "true",
"permAgentsSync" : "false",
"permShareObjects" : "true",
"permUpdateFeeds" : "true",
"permUploadNessusResults" : "true",
"permViewOrgLogs" : "true",
"permManageAcceptRiskRules" : "true",
"permManageRecastRiskRules" : "true",
"permManageACR": "false",
"permViewDomainInventoryAssets": "false",
"permManageAttackSurfaceDomains": "false",
"permManageVulnRoutingRules": "false",
"permViewHostAssets": "false",
"permManageRiskRules": "false",
"organizationCounts" : [
        {
                "id" : "12",
                "userCount" : "1"
        }
],
"creator" : {
        "id" : "1",
        "username" : "head",
        "firstname" : "",
        "lastname" : "",
        "uuid" : "96F2AD1B-1B83-462E-908A-84E6054F6B64"
}
```

```
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1445013361
}
```


PATCH

Edits the Role associated with {id}, changing only the passed in fields.

Request Parameters

(All fields are optional)

See /role::POST for parameters.

Example Response

See /role/{id}::GET

DELETE

Deletes the Role associated with {id}, depending on access and permissions.

Request Parameters

None

Example Response

Expand


```
{
    "type" : "regular",
    "response" : "",
    "error_code" : 0,
    "error_msg" : "",
    "warnings" : [],
```

```
    "timestamp" : 1403100582
}
```

Atlassian

Tenable Security Center API: SAML

This resource may only be used by administrators. Only 1 SAML association is currently supported (which will always be ID "1").

/saml

Methods

GET

Gets the list of SAML associations.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

**id
**name
**samlEnabled
*type
*entityID
*description
*idp
*usernameAttribute
*singleSignOnService
*singleLogoutService
*certData
*createdTime
*modifiedTime

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

Example Response

Expand


```
{
        "type" : "regular",
        "response": [
                {
                        "id" : "1",
                        "name" : "",
                        "description" : "SAML Association",
                        "entityID" : "http://www.samlprovider.com/str",
                        "idp" : "http://www.samlprovider.com/str",
                        "usernameAttribute" : "",
                        "singleSignOnService" : "https://dev-
x.y.com/app/tenabledev/str/sso/saml",
                        "singleLogoutService" : "https://dev-
x.y.com/app/tenabledev/str/sso/saml",
                        "certData" : "certdata",
                        "createdTime" : "1543852867",
                        "modifiedTime" : "1546641092",
                        "type" : "saml2",
                        "samlEnabled" : "true"          }
        ],
        "error_code": 0,
        "error_msg" : "",
        "warnings": [],
        "timestamp": 1546642280
}
```


/saml/{id}

Methods

GET

Gets the SAML associated with {id}.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

**id
**name
**samlEnabled
*type
*entityID
*description
*idp
*usernameAttribute
*singleSignOnService
*singleLogoutService
*certData
*createdTime
*modifiedTime

Legend

** = always comes back*
*** = comes back if fields list not specified on GET all*

Request Parameters

None

Example Response

Expand

```
{
        "type" : "regular",
        "response": {
                "id" : "1",
                "name" : "",
                "description" : "SAML Association",
                "entityID" : "http://www.samlprovider.com/str",
                "idp" : "http://www.samlprovider.com/str",
                "usernameAttribute" : "",
                "singleSignOnService" : "https://dev-
x.y.com/app/tenabledev/str/sso/saml",
                "singleLogoutService" : "https://dev-
x.y.com/app/tenabledev/str/sso/saml",
                "certData" : "certdata",
                "createdTime" : "1543852867",
                "modifiedTime" : "1546641092",
                "type" : "saml2",
                "samlEnabled" : "true"  },
        "error_code": 0,
        "error_msg" : "",
        "warnings": [],
        "timestamp": 1546642280
}
```


PATCH

Edits the SAML associated with {id} , changing only the passed in fields.

Request Parameters

(All fields are optional **EXCEPT** samlEnabled, which must be set to "true" or "false")

Expand

```
{
        "name" : <string>,
        "description" : <string>,
        "type" : <string> "saml2" | "shibboleth",
        "entityID" : <string>,
        "idp" : <string>,
        "usernameAttribute" : <string>,
        "singleSignOnService" : <string>,
        "singleLogoutService" : <string>,
        "certData" : <string>,
        "samlEnabled" : <string> "false" | "true"}
```

Example Response

See /saml/{id}::GET

/saml/getMetadata

Methods

GET

Gets the SC XML metadata file.

Example Response

Expand

```
{
        "type" : "regular",
        "response": {
                "filePath" : "saml/module.php/saml/sp/metadata.php/1"   },
        "error_code": 0,
        "error_msg" : "",
        "warnings": [],
        "timestamp": 1546642827
}
```

Tenable Security Center API: Scan

/scan

Methods

GET

Gets the list of Scans.

NOTE #1: Although a Scan's Schedule 'dependentID' is stored as the schedule ID of the object a scan is dependent upon in the database, it is sent from and returned to the user as the ID of the actual scan object.

NOTE #2 : The Unit of param inactivityTimeout is to be interpreted in seconds.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
*uuid
**name
**description
**status
ipList
type
plugin
repository
zone
dhcpTracking
classifyMitigatedAge
emailOnLaunch
emailOnFinish
timeoutAction

scanningVirtualHosts
rolloverType
createdTime
modifiedTime
ownerGroup
creator
owner
reports
assets
credentials
numDependents
schedule
policy
policyPrefs
maxScanTime
inactivityTimeout

Legend

** = always comes back*
*** = comes back if fields list not specified on GET all*
redFont = *field is a JSON object* (**e.g.** *"repository" :{* "id" : <id>,"name" : <name> })

Request Parameters

None

Expand Parameters

credentials

Filter Parameters

usable - The response will be an object containing an array of usable Scans. By default, both usable and manageable objects are returned.
manageable - The response will be an object containing all manageable Scans.. By default, both usable and manageable objects are returned.

Example Response

Expand


```
{
        "type" : "regular",
        "response" : {
                "usable" : [
                        {
                                "id" : "2",
                                "name" : "test",
                                "description" : null,
                                "status" : "0",
                                "uuid" : "2EAED2D2-DFC7-4CFE-9C94-25CF6481C515
                        {
                                "id" : "3",
                                "name" : "test2",
                                "description" : null,
                                "status" : "0",
                                "uuid" : "EC81E13E-B3B2-4A51-968D-E94D524B5254
                        {
                                "id" : "4",
                                "name" : "POSTtest",
                                "description" : "This is a test for POST",
                                "status" : "0",
                                "uuid" : "2EAED2D2-DFC7-4CFE-9C94-25CF6481C515
                ],
                "manageable" : [
                        {
                                "id" : "2",
                                "name" : "test",
                                "description" : null,
                                "status" : "0",
                                "uuid" : "2EAED2D2-DFC7-4CFE-9C94-25CF6481C515
                        {
                                "id" : "3",
```

```
                                "name" : "test2",
                                "description" : null,
                                "status" : "0",
                                "uuid" : "EC81E13E-B3B2-4A51-968D-E94D524B5254
                                "id" : "4",
                                "name" : "POSTtest",
                                "description" : "This is a test for POST",
                                "status" : "0",
                                "uuid" : "2EAED2D2-DFC7-4CFE-9C94-25CF6481C515
                ]
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1406828340
}
```


POST

Adds a Scan, depending on access and permissions.

NOTE #1: A Blackout Window must not be in effect

NOTE #2: Setting schedule type to "template" means that the scan will not run on a schedule.

NOTE #3: If the field *schedule frequency* is "dependent", the field *type* cannot be "template"

NOTE #4: Although a Scan's Schedule 'dependentID' is stored as the schedule ID of the object a scan is dependent upon in the database, it is sent from and returned to the user as the ID of the actual scan object.

NOTE #5: The Unit of param inactivityTimeout is seconds. And perceived only in intervals of 3600 [1hr]. If any other intermediate values are sent then it is ceiled to next valid step. Ex: 5432 is ceiled to 7200. This is done to keep consistency in the allowed values of dropdown in Frontend. The validation error messages in response too contain Unit in hours too keep it consistent with that shown in Frontend.

Request Parameters

Expand

```
{
        "name" : <string>,
        "type" : <string> DEFAULT "policy",
        "description" : <string> DEFAULT "",
        "repository" : {
                "id" : <number> },
        "zone" : {
                "id" : <number> DEFAULT "0" (All Zones)
        },
        "dhcpTracking" : <string> DEFAULT "false",
        "classifyMitigatedAge" : <number> DEFAULT "0",
        "schedule" : {
                "type" : "dependent" | "ical" | "never" | "rollover" | "templa
<string> DEFAULT "template"     },
        "reports" : [
                {
                        "id" : <number>,
                        "reportSource" : <string> "cumulative" | "patched" | "
| "lce" | "archive" | "mobile"          }...
        ] DEFAULT [],
        "assets" : [
                {
                        "id" : <number>         }...
        ] DEFAULT [],
        "credentials" : [
                {
                        "id" : <number>         }...
        ] DEFAULT [],
        "emailOnLaunch" : <string> "false" | "true" DEFAULT "false",
        "emailOnFinish" : <string> "false" | "true" DEFAULT "false",
        "timeoutAction" : <string> "discard" | "import" | "rollover"
DEFAULT "import",
```

```
        "scanningVirtualHosts" : <string> "false" | "true" DEFAULT "false",
        "rolloverType" : <string> "nextDay" | "template" DEFAULT
"template",
        "ipList" : <string> DEFAULT "" (valid IP),
        "maxScanTime" : <number> DEFAULT "3600",
        "inactivityTimeout" : <number> "3600" to "432000" STEP 3600 DEFAULT
"43200"}
```

schedule type is "ical"

NOTE: The "enabled" field can only be set to "false" for schedules of type "ical". For all other schedules types, "enabled" is set to "true".

```
...
        "schedule" : {
                "start" : <string> (This value takes the iCal format),
                "repeatRule" : <string> (This value takes the repeat rule form
                "enabled" : <string> "false" | "true" DEFAULT "true"    }
...
```

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "id" : "4",
                "name" : "POSTtest",
                "description" : "This is a test for POST",
                "ipList" : "100.100.100.100",
                "urlList" : "",
                "type" : "policy",
```

```
"policyID" : "1000002",
"pluginID" : "-1",
"zoneID" : "-1",
"dhcpTracking" : "false",
"classifyMitigatedAge" : "0",
"emailOnLaunch" : "false",
"emailOnFinish" : "false",
"timeoutAction" : "import",
"scanningVirtualHosts" : "false",
"rolloverType" : "template",
"status" : "0",
"createdTime" : "1406815242",
"modifiedTime" : "1406815242",
"maxScanTime" : "3600",
"inactivityTimeout" : "3600",
"ownerGID" : "0",
"reports" : [],
"assets" : [],
"credentials" : [],
"numDependents" : "0",
"schedule" : {
        "id" : "17",
        "dependentID" : "14",
        "objectType" : "scan",
        "type" : "dependent",
        "start" : "",
        "repeatRule" : "",
        "enabled" : "true",
        "nextRun" : 0,
        "dependent" : {
                "id" : "14",
                "name" : "Daily IP Scan",
                "description" : "",
```

```
                        "status" : "1024"                    }
                },
                "policy" : {
                        "id" : "1000002",
                        "name" : "POST TEST",
                        "description" : "Test of post for use with scan post t
                        "uuid" : "29F2B9E1-ADE9-4550-B63C-CEA1423E52FC"
                "pluginPrefs" : [],
                "creator" : {
                        "id" : "1",
                        "username" : "head3",
                        "firstname" : "",
                        "lastname" : "",
                        "uuid" : "96F2AD1B-1B83-462E-908A-84E6054F6B64"
        },
                "owner" : {
                        "id" : "1",
                        "username" : "head3",
                        "firstname" : "",
                        "lastname" : "",
                        "uuid" : "96F2AD1B-1B83-462E-908A-84E6054F6B64"
                "repository" : {
                        "id" : "2",
                        "name" : "test",
                        "description" : "test",
                        "type" : "Local",
                        "dataFormat" : "IPv4",
                        "uuid" : "A2FF7E13-2C0E-470E-A3C9-E077FE065A54"
                "canUse" : "true",
                "canManage" : "true",
                "ownerGroup" : {
                        "id" : "0",
                        "name" : "Full Access",
```

```
                        "description" : "Full Access group"             },
                "uuid" : "29F2B9E1-ADE9-4550-B63C-CEA1423E52FC" },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1406815242
}
```


/scan/{id}

/scan/{uuid}

Methods

GET

Gets the Scan associated with {id} or {uuid}.

NOTE #1: Although a Scan's Schedule 'dependentID' is stored as the schedule ID of the object a scan is dependent upon in the database, it is sent from and returned to the user as the ID of the actual scan object.

NOTE #2 : The Unit of param inactivityTimeout is to be interpreted in seconds.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
*uuid
**name
**description
**status
**ipList
**urlList

**type
****policy**
****plugin**
****repository**
**canUse
**canManage
****zone**
**dhcpTracking
**classifyMitigatedAge
**emailOnLaunch
**emailOnFinish
**timeoutAction
**scanningVirtualHosts
**rolloverType
**createdTime
**modifiedTime
****ownerGroup**
****creator**
****owner**
****reports**
****assets**
****credentials**
**numDependents
****schedule**
****policy**
****policyPrefs**
**maxScanTime
**inactivityTimeout

Legend

** = always comes back*

*** = comes back if fields list not specified on GET*

redFont = *field is a JSON object (**e.g.** "repository" :{ "id" : <id>, "name" : <name> })*

Request Parameters

None

Expand Parameters

credentials

Example Response

Expand


```
{
        "type" : "regular",
        "response" : {
                "id" : "4",
                "name" : "POSTtest",
                "description" : "This is a test for POST",
                "ipList" : "100.100.100.100",
                "urlList" : "",
                "type" : "policy",
                "dhcpTracking" : "false",
                "classifyMitigatedAge" : "0",
                "emailOnLaunch" : "false",
                "emailOnFinish" : "false",
                "timeoutAction" : "import",
                "scanningVirtualHosts" : "false",
                "rolloverType" : "template",
                "status" : "0",
                "createdTime" : "1406815242",
                "modifiedTime" : "1406815242",
                "reports" : [],
                "assets" : [],
                "numDependents" : "0",
                "schedule" : {
                        "id" : "17",
                        "dependentID" : "14",
                        "objectType" : "scan",
```

```
                "type" : "dependent",
                "start" : "",
                "repeatRule" : "",
                "enabled" : "true",
                "nextRun" : 0,
                "dependent" : {
                        "id" : "14",
                        "name" : "Daily IP Scan",
                        "description" : "",
                        "status" : "1024"                       }
        },
        "policy" : {
                "id" : "1000002",
                "name" : "POST TEST",
                "description" : "Test of post for use with scan post t
                "uuid" : "2E950182-08B6-4737-830B-4ACC8F6B92F9"
        "policyPrefs" : [],
        "repository" : {
                "id" : "2",
                "name" : "test",
                "description" : "test",
                "type" : "Local",
                "dataFormat" : "IPv4",
                "uuid" : "A2FF7E13-2C0E-470E-A3C9-E077FE065A54"
        "canUse" : "true",
        "canManage" : "true",
        "ownerGroup" : {
                "id" : "0",
                "name" : "Full Access",
                "description" : "Full Access group"            },
        "creator" : {
                "id" : "1",
                "username" : "head3",
```

```
                        "firstname" : "",
                        "lastname" : "",
                        "uuid" : "96F2AD1B-1B83-462E-908A-84E6054F6B64"
                "owner" : {
                        "id" : "1",
                        "username" : "head3",
                        "firstname" : "",
                        "lastname" : "",
                        "uuid" : "96F2AD1B-1B83-462E-908A-84E6054F6B64"
                "uuid" : "29F2B9E1-ADE9-4550-B63C-CEA1423E52FC" },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1406828664
}
```


PATCH

Edits the Scan associated with {id} or {uuid}, changing only the passed in fields.

NOTE: A Scan's 'type' parameter cannot be changed.

Request Parameters

(All fields are optional)

See /scan::POST for parameters.

Example Response

See /scan/{id}::GET

DELETE

Deletes the Scan associated with {id} or {uuid}, depending on access and permissions.

Request Parameters

None

Example Response

Expand

```
{
        "type" : "regular",
        "response" : "",
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1406732180
}
```

/scan/{id}/copy

/scan/{uuid}/copy

Methods

POST

Copies the Scan associated with {id} or {uuid}, depending on access and permissions.

Request Parameters

Expand

```
{
        "name" : <string>,
        "targetUser" : {
                "id" : <number> | "uuid" : <string>     }
}
```

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "scan" : {
```

```
"id" : "4",
"name" : "POSTtest",
"description" : "This is a test for POST",
"ipList" : "100.100.100.100",
"urlList" : "",
"type" : "policy",
"dhcpTracking" : "false",
"classifyMitigatedAge" : "0",
"emailOnLaunch" : "false",
"emailOnFinish" : "false",
"timeoutAction" : "import",
"scanningVirtualHosts" : "false",
"rolloverType" : "template",
"status" : "0",
"createdTime" : "1406815242",
"modifiedTime" : "1406815242",
"reports" : [],
"assets" : [],
"numDependents" : "0",
"schedule" : {
        "id" : "17",
        "dependentID" : "14",
        "objectType" : "scan",
        "type" : "dependent",
        "start" : "",
        "repeatRule" : "",
        "enabled" : "true",
        "nextRun" : 0,
        "dependent" : {
                "id" : "14",
                "name" : "Daily IP Scan",
                "description" : "",
                "status" : "1024"
```

```
        },
        "policy" : {
                "id" : "1000002",
                "name" : "POST TEST",
                "description" : "Test of post for use with sca
                "uuid" : "2E950182-08B6-4737-830B-4ACC8F6B92F9
        "policyPrefs" : [],
        "repository" : {
                "id" : "2",
                "name" : "test",
                "description" : "test",
                "type" : "Local",
                "dataFormat" : "IPv4",
                "uuid" : "A2FF7E13-2C0E-470E-A3C9-E077FE065A54
        "canUse" : "true",
        "canManage" : "true",
        "ownerGroup" : {
                "id" : "0",
                "name" : "Full Access",
                "description" : "Full Access group"
        "creator" : {
                "id" : "1",
                "username" : "head3",
                "firstname" : "",
                "lastname" : "",
                "uuid" : "96F2AD1B-1B83-462E-908A-84E6054F6B64
        "owner" : {
                "id" : "1",
                "username" : "head3",
                "firstname" : "",
                "lastname" : "",
                "uuid" : :"96F2AD1B-1B83-462E-908A-84E6054F6B6
        "uuid" : "29F2B9E1-ADE9-4550-B63C-CEA1423E52FC"
```

```
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1406750971
}
```


/scan/{id}/launch

/scan/{uuid}/launch

Methods

POST

Launches the Scan associated with {id} or {uuid}.

Request Parameters

NOTE: "diagnosticTarget" and "diagnosticPassword" are both optional, but must be provided together if present.

Expand


```
{
        "diagnosticTarget" : <string> (Valid IP/Hostname),
        "diagnosticPassword" : <string> (Non empty String)
}
```


Example Response

Expand


```
{
        "type" : "regular",
        "response" : {
                "scanID" : "2",
```

```
                "scanResult" : {
                        "initiatorID" : "1",
                        "ownerID" : "1",
                        "scanID" : "2",
                        "resultsSyncID" : -1,
                        "jobID" : "143301",
                        "repositoryID" : "1",
                        "name" : "test",
                        "description" : "",
                        "details" : "Plugin #",
                        "status" : "Queued",
                        "downloadFormat" : "v2",
                        "dataFormat" : "IPv4",
                        "resultType" : "active",
                        "id" : "3"              }
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1407510276
}
```


Atlassian

Tenable Security Center API: Scanner

Except for method *GET*, this endpoint may only be used by administrators.

/scanner

Methods

GET

Gets the list of Scanners.

NOTE: This call will return all Scanners for an Administrator. For an Organization User, it will only return agent-capable Scanners associated with that User's Organization.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields (Admin User)

*id
**name
**description
**agentCapable
**wasCapable
**status
**statusMessage
ip
port
useProxy
enabled
verifyHost
managePlugins
authType
cert
username
password
version
webVersion
admin
msp
numScans
numHosts
numSessions
numTCPSessions
loadAvg
uptime
pluginSet
loadedPluginSet

serverUUID
createdTime
modifiedTime
accessKey
secretKey
zones
nessusManagerOrgs

Allowed Fields (Org User)

*id
**name
**description
**status
agentCapable

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

***red** = field is a JSON object (**e.g.** "SCI" : {"id" : "2", "name" : "SCI Name", "description" : "Description"})*

Request Query Parameters

None

Example Response

Expand

```
{
        "type" : "regular",
        "response" : [
                {
                        "id" : "12",
                        "name" : "Scanner 1",
```

```
                "description" : "Copied from QA",
                "agentCapable" : "true",
                "wasCapable" : "false",
                "status" : "1",
                "statusMessage" : ""            },
        {
                "id" : "14",
                "name" : "Scanner using Safe Scan Range",
                "description" : "",
                "agentCapable" : "true",
                "wasCapable" : "false",
                "status" : "16",
                "statusMessage" : ""            },
        {
                "id" : "15",
                "name" : "mp zone 1 scanner",
                "description" : "Copied from QA",
                "agentCapable" : "true",
                "wasCapable" : "false",
                "status" : "1",
                "statusMessage" : ""            },
        {
                "id" : "16",
                "name" : "NessusTest",
                "description" : "Copied From QA",
                "agentCapable" : "false",
                "wasCapable" : "true",
                "status" : "32",
                "statusMessage" : ""            },
        {
                "id" : "17",
                "name" : "sc",
                "description" : "",
```

```
                        "agentCapable" : "false",
                        "wasCapable" : "true",
                        "status" : "2",
                        "statusMessage" : ""            }
        ],
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1426878501
}
```

POST

Adds a Scanner.

Request Parameters

Expand

```
{
        "name" : <string>,
        "description" : <string> DEFAULT "",
        "authType" : <string> "certificate" | "apiKeys" | "password"
DEFAULT "password",
        "ip" : <string>,
        "port" : <number>,
        "useProxy" : <string> "true" | "false" DEFAULT "false",
        "verifyHost" : <string> "true" | "false" DEFAULT "true",
        "enabled" : <string> "true" | "false" DEFAULT "true",
        "managePlugins" : <string> "true" | "false" DEFAULT "false",
        "agentCapable" : <string> "true" | "false" DEFAULT "false",
        "wasCapable" : <string> "true" | "false" DEFAULT "false",
        "zones" : [
                {
                        "id" : <number>         }...
```

```
        ] DEFAULT [],
        "nessusManagerOrgs" : [
                {
                        "id" : <number>          }...
        ] DEFAULT [],
        "accessKey" : <string> DEFAULT "",
        "secretKey" : <string> DEFAULT ""...
}
```

authType "certificate"

```
...
        "cert" : <string>,
        "password" : <string> DEFAULT "",
...
```

authType "password"

```
...
        "username" : <string>,
        "password" : <string>...
```

authType "apiKeys"

```
...
        "accessKey" : <string> DEFAULT "",
        "secretKey" : <string> DEFAULT "",
...
```

- Details
    - Zones are not used
    - Agent Capable should be set to "true"

Example Response

Expand


```
{
	"type" : "regular",
	"response" : {
		"id" : "5",
		"name" : "My Active Scanner",
		"description" : "",
		"ip" : "192.168.1.1",
		"port" : "443",
		"useProxy" : "false",
		"enabled" : "true",
		"verifyHost" : "true",
		"managePlugins" : "false",
		"authType" : "password",
		"accessKey" : "SET",
		"secretKey" : "SET",
		"agentCapable" : "true",
		"wasCapable" : "false",
		"cert" : null,
		"username" : "nonadmin",
		"password" : "SET",
		"version" : null,
		"webVersion" : null,
		"admin" : "false",
		"msp" : "false",
		"numScans" : "0",
		"numHosts" : "0",
		"numSessions" : "0",
		"numTCPSessions" : "0",
		"loadAvg" : "0.0",
		"uptime" : -1,
		"status" : "8192",
		"statusMessage" : null,
```

```
                "pluginSet" : null,
                "loadedPluginSet" : null,
                "serverUUID" : null,
                "createdTime" : "1402435586",
                "modifiedTime" : "1402435586",
                "zones" : [
                        {
                                "id" : "1",
                                "name" : "Big Zone",
                                "description" : "",
                                "uuid" : "4F7DD1CD-EB1B-40D7-BCE1-2DB3E31F6F4
                ],
                "nessusManagerOrgs" : [
                        {
                                "id" : "1",
                                "name" : "Big Org",
                                "description" : "",
                                "uuid" : "FF00F4D0-5B9F-4A26-998C-19430295284
                ]
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1402435586
}
```


/scanner/{id}

Methods

GET

Gets the Scanner associated with {id}.

NOTE: This call will return all Scanners for an Administrator. For an Organization User, it will only return agent-capable Scanners associated with that User's Organization.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields (Admin User)

*id
**name
**description
**status
**ip
**port
**useProxy
**enabled
**verifyHost
**managePlugins
**authType
**nessusType
**cert
**username
**password
**agentCapable
**wasCapable
**version
**webVersion
**admin
**msp
**numScans
**numHosts
**numSessions
**numTCPSessions
**loadAvg
**uptime
**statusMessage
**pluginSet

**loadedPluginSet
**serverUUID
**createdTime
**modifiedTime
**accessKey
**secretKey
****zones**
****nessusManagerOrgs**

Allowed Fields (Org User)

*id
**name
**description
**status
agentCapable

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

***red** = field is a JSON object (**e.g.** "SCI" : {"id" : "2", "name" : "SCI Name", "description" : "Description"})*

Request Query Parameters

None

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "id" : "5",
                "name" : "My Active Scanner",
```

```
"description" : "",
"ip" : "192.168.1.1",
"port" : "443",
"useProxy" : "false",
"enabled" : "true",
"verifyHost" : "true",
"managePlugins" : "false",
"authType" : "password",
"nessusType" : "Nessus Manager",
"cert" : null,
"username" : "nonadmin",
"password" : "SET",
"agentCapable" : "true",
"wasCapable" : "false",
"accessKey" : null,
"secretKey". : null,
"version" : null,
"webVersion" : null,
"admin" : "false",
"msp" : "false",
"numScans" : "0",
"numHosts" : "0",
"numSessions" : "0",
"numTCPSessions" : "0",
"loadAvg" : "0.0",
"uptime" : -1,
"status" : "8192",
"statusMessage" : null,
"pluginSet" : null,
"loadedPluginSet" : null,
"serverUUID" : null,
"createdTime" : "1402435586",
"modifiedTime" : "1402435586",
```

```
                "zones" : [
                        {
                                "id" : "1",
                                "name" : "Big Zone",
                                "description" : "",
                                "uuid" : "4F7DD1CD-EB1B-40D7-BCE1-2DB3E31F6F4
                ],
                "nessusManagerOrgs" : [
                        {
                                "id" : "1",
                                "name" : "Big Org",
                                "description" : "",
                                "uuid" : "FF00F4D0-5B9F-4A26-998C-19430295284
                ]
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1402435871
}
```


PATCH

Edits the Scanner associated with {id}, changing only the passed in fields.

Request Parameters

(All fields are optional)

See /scanner::POST for parameters.

Example Response

See /scanner/{id}::GET

DELETE

Deletes the Scanner associated with {id}, depending on access and permissions.

Request Parameters

None

Example Response

Expand

```
{
        "type" : "regular",
        "response" : "",
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1402436001
}
```

/scanner/{id}/testScansQuery

POST

Tests the Scans glob against the API of the Scanner associated with {id}.

Request Parameters

Expand

```
{
        "scansGlob" : <string>  "resultsSync" : {
                "id" : <number> } OPTIONAL
}
```

Example Response

Expand

```
{
        "type" : "regular",
        "response" : [
                {
```

```
                        "name" : "basic agent scan all agents",
                        "numResults" : 5
                },
                {
                        "name" : "C agent policy compliance scan",
                        "numResults" : 4
                },
                {
                        "name" : "mp advanced agent scan all plugins plus mult
contents compliance audits",
                        "numResults" : 2
                },
                {
                        "name" : "windows agent malware scan",
                        "numResults" : 3
                }
        ],
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1442351168
}
```


/scanner/{id}/bug-report

POST

Downloads the bug report logs by querying the Nessus API endpoint for the Scanner associated with {id}.

Request Parameters

Expand


```
{
        "scrub_mode" : <string> "0" | "1" DEFAULT "0",
```

```
        "full_mode" : <string> "0" | "1" DEFAULT "0",
}
```

Example Response

Expand

None given.

1. The response will be an inline file representing the bug report requested from Nessus.
2. Any errors will be returned as JSON using the customary response envelope involved with standard calls.

/scanner/{id}/health

GET

Retrieve scanner health statistics by querying the Nessus API endpoint for the Scanner associated with {id}.

NOTE: The "count" field represents the number of data points to retrieve over the last 24 hours, with the default of "1" retrieving statistics for the current request.

Field Parameters

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax i.e. /scanner/{id}/health?count={count}

```
    ?fields=<field>,...
```

Allowed Fields (Admin User)

*count

Request Query Paramaters

None

```
{
        "count" : <integer> DEFAULT "1",
}
```

Legend

** = always comes back*

Example Response

Expand

```
{
        "type" : "regular",
        "response" : (Object)
                "perf_stats_history" : (Array)(Object)
                        "kbytes_received" : 3
                        "kbytes_sent" : 12
                        "avg_dns_lookup_time" : 0
                        "num_dns_lookups" : 0
                        "avg_rdns_lookup_time" : 0
                        "num_rdns_lookups" : 0
                        "cpu_load_avg" : 2
                        "nessus_log_disk_free" : 42681
                        "nessus_log_disk_total" : 51175
                        "nessus_data_disk_free" : 42681
                        "nessus_data_disk_total" : 51175
                        "temp_disk_free" : 42681
                        "temp_disk_total" : 51175
                        "num_tcp_sessions" : 0
                        "nessus_vmem" : 1290
                        "nessus_mem" : 243
                        "sys_ram_used" : null
                        "sys_ram" : 7727
                        "sys_cores" : 2
```

```
                        "num_hosts" : 0
                        "num_scans" : 0
                        "timestamp" : 1567631211
                "perf_stats_current" : (Object)
                        "kbytes_received" : 0
                        "kbytes_sent" : 0
                        "avg_dns_lookup_time" : 0
                        "num_dns_lookups" : 0
                        "avg_rdns_lookup_time" : 0
                        "num_rdns_lookups" : 0
                        "cpu_load_avg" : 0
                        "nessus_log_disk_free" : 42672
                        "nessus_log_disk_total" : 51175
                        "nessus_data_disk_free" : 42672
                        "nessus_data_disk_total" : 51175
                        "temp_disk_free" : 42672
                        "temp_disk_total" : 51175
                        "num_tcp_sessions" : 0
                        "nessus_vmem" : 1290
                        "nessus_mem" : 195
                        "sys_ram_used" : null
                        "sys_ram" : 7727
                        "sys_cores" : 2
                        "num_hosts" : 0
                        "num_scans" : 0
                        "timestamp" : 1567631211,
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1402435958
}
```


/scanner/updateStatus

The /scanner/updateStatus resource.

POST

Starts an on-demand Scanner status update.

Request Parameters

None.

Example Response

Expand


```
{
        "type" : "regular",
        "response" : [
                {
                        "id" : "5",
                        "name" : "My Active Scanner",
                        "description" : "",
                        "status" : "8200"               }
        ],
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1402435958
}
```


Expand Items:

- details

  Show type specific details (such as certificate information, etc.)

Atlassian

Tenable Security Center API: Scan Policy

/policy

Methods

GET

Gets the list of Policies.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
*uuid
**name
**description
**status
policyTemplate
policyProfileName
creator
tags
type
createdTime
modifiedTime
context
generateXCCDFResults
auditFiles
preferences
targetGroup

Session user role "1" (Administrator)

owner
ownerGroup

Session user role not "1" (Administrator)

status
groups

Template ID "1" (Advanced Scan Template) or "25" (Advanced Agent Scan Template) families

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

***red** = field is a JSON object (**e.g.** "SCI" : {"id" : "2", "name" : "SCI Name", "description" : "Description"})*

Request Parameters

Expand

NOTE: The owner ID for admin is always -100

```
{
    "name" : <string> "",
    "owner" : <string> "",
    "policyTemplate" : <string> "",
    "groupID" : <string> "",
       "tags" : <string> ""    ...
}
```

Paginated results:

By default, the result set encompasses all Policy.

To obtain paginated results, a parameter value should be included in the request as follows:

?paginated=true

Additionally, for paginated results, the following parameters can be sent:

startOffset <number> (positive integer) DEFAULT 0,
endOffset <number> (integer >= startOffset) DEFAULT 50,
sortDirection <string> "ASC" | "DESC" DEFAULT "DESC",

sortField <string> "name" | "tags" | "policyTemplateID" | "ownerID" | "ownerGID" | "modifiedTime",

Example Request Query Parameters

Expand

For normal query param request

```
{
  "policyTemplate": "3,1,7",
  "tags": "BASIC-NETWORK-SCAN",
  "owner": "-100,1",
  "groupID": "0,1",
  "name": "SCAN-875"}
```

With Pagination query param

```
{
  "startOffset": 0,
  "endOffset": 50,
  "sortField": "name",
  "sortDirection": "ASC",
  "paginated": "true",
  "policyTemplate": "3,1,7",
  "tags": "BASIC-NETWORK-SCAN",
  "owner": "-100,1",
  "groupID": "0,1",
  "name": "SCAN-875"}
```

Filter Parameters

usable - The response will be an object containing an array of usable Policies. By default, both usable and manageable objects are returned.
manageable - The response will be an object containing all manageable Policies. By default, both usable and manageable objects are returned.

Example Response

Expand


```
{
        "type" : "regular",
        "response" : {
                "usable" : [
                        {
                                "id" : "1",
                                "name" : "test",
                                "description" : "desc",
                                "status" : "0",
                                "uuid" : "2E950182-08B6-4737-830B-4ACC8F6B92F
                        {
                                "id" : "2",
                                "name" : "test2",
                                "description" : "desc",
                                "status" : "0",
                                "uuid" : "929EF9DD-8A81-4864-AFD2-F87845224F6
                        {
                                "id" : "3",
                                "name" : "test3",
                                "description" : "desc",
                                "status" : "0",
                                "uuid" : "F4B2DE11-F6A1-4058-AFF6-F7D49C23866
                        {
                                "id" : "4",
                                "name" : "test4",
                                "description" : "test desc",
                                "status" : "0",
                                "uuid" : "F4B2DE11-F6A1-4058-AFF6-F7D49C23866
                        {
                                "id" : "1000001",
                                "name" : "nesus upload - ibm credentials",
```

```
            "description" : "",
            "status" : "0",
            "uuid" : "BC2DC4A1-298F-4CC3-A7D4-ABED7248E40
        {
            "id" : "1000002",
            "name" : "nesus upload - ibm credentials - up
            "description" : "Nessus Policy exported from
            "status" : "0",
            "uuid" : "058E06E5-2E30-4E6C-8D27-20FBE45CED2
        {
            "id" : "1000003",
            "name" : "IBM iSeries Credentials Name",
            "description" : "Imported Nessus Policy",
            "status" : "0",
            "uuid" : "970AF7B9-1DE2-43DF-BA29-A282FACE693
        {
            "id" : "1000004",
            "name" : "Nessus Upload 2",
            "description" : "Imported Nessus Policy",
            "status" : "0",
            "uuid" : "893A5150-FB99-4405-AEA1-F88E720686C
        {
            "id" : "1000005",
            "name" : "Nessus Upload 3",
            "description" : "Imported Nessus Policy",
            "status" : "0",
            "uuid" : "308027F4-77F9-4444-A5CE-E57B3928078
        {
            "id" : "1000016",
            "name" : "Tom Test",
            "description" : "Imported Nessus Policy",
            "status" : "0",
            "uuid" : "2278CBB5-F927-4C8F-AEC1-EEF76DEB175
```

```
                {
                        "id" : "1000017",
                        "name" : "Nessus Upload 4",
                        "description" : "Imported Nessus Policy",
                        "status" : "0",
                        "uuid" : "4CF267BB-0A5C-47AB-BAC3-E77E6270EBC5
                {
                        "id" : "1000018",
                        "name" : "Tom Test 2",
                        "description" : "Imported Nessus Policy",
                        "status" : "0",
                        "uuid" : "E8F73EF3-9D8D-4FCA-A3F4-2B4D176767B9
                {
                        "id" : "1000019",
                        "name" : "DOCtest",
                        "description" : "desc",
                        "status" : "0",
                        "uuid" : "178C9E5F-E768-40D4-951C-5A76E7DC6BDA
                {
                        "id" : "1000020",
                        "name" : "test5",
                        "description" : "test desc",
                        "status" : "0",
                        "uuid" : "A4C62370-91ED-42DA-927B-3FE24397456
        ],
        "manageable" : [
                {
                        "id" : "1000001",
                        "name" : "nesus upload - ibm credentials",
                        "description" : "",
                        "status" : "0",
                        "uuid" : "BC2DC4A1-298F-4CC3-A7D4-ABED7248E40
                {
```

```
                "id" : "1000002",
                "name" : "nesus upload - ibm credentials - upl
                "description" : "Nessus Policy exported from T
                "status" : "0",
                "uuid" : "058E06E5-2E30-4E6C-8D27-20FBE45CED2F
        {
                "id" : "1000003",
                "name" : "IBM iSeries Credentials Name",
                "description" : "Imported Nessus Policy",
                "status" : "0",
                "uuid" : "970AF7B9-1DE2-43DF-BA29-A282FACE693F
        {
                "id" : "1000004",
                "name" : "Nessus Upload 2",
                "description" : "Imported Nessus Policy",
                "status" : "0",
                "uuid" : "893A5150-FB99-4405-AEA1-F88E720686C8
        {
                "id" : "1000005",
                "name" : "Nessus Upload 3",
                "description" : "Imported Nessus Policy",
                "status" : "0",
                "uuid" : "308027F4-77F9-4444-A5CE-E57B3928078F
        {
                "id" : "1000016",
                "name" : "Tom Test",
                "description" : "Imported Nessus Policy",
                "status" : "0",
                "uuid" : "2278CBB5-F927-4C8F-AEC1-EEF76DEB175F
        {
                "id" : "1000017",
                "name" : "Nessus Upload 4",
                "description" : "Imported Nessus Policy",
```

```
                                "status" : "0",
                                "uuid" : "4CF267BB-0A5C-47AB-BAC3-E77E6270EBC5
                        {
                                "id" : "1000018",
                                "name" : "Tom Test 2",
                                "description" : "Imported Nessus Policy",
                                "status" : "0",
                                "uuid" : "E8F73EF3-9D8D-4FCA-A3F4-2B4D176767B9
                        {
                                "id" : "1000019",
                                "name" : "DOCtest",
                                "description" : "desc",
                                "status" : "0",
                                "uuid" : "178C9E5F-E768-40D4-951C-5A76E7DC6BDA
                        {
                                "id" : "1000020",
                                "name" : "test5",
                                "description" : "test desc",
                                "status" : "0",
                                "uuid" : "A4C62370-91ED-42DA-927B-3FE243974563
                ]
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1406233675
}
```


Paginated response

Expand


```
{
    "type": "regular",
```

```
    "response": {
        "totalRecords": "1",
        "returnedRecords": 1,
        "startOffset": "0",
        "endOffset": "50",
        "usable": [
            {
                "name": "Basic network Scan",
                "description": "",
                "tags": "BASIC-NETWORK-SCAN",
                "createdTime": "1704867262",
                "modifiedTime": "1704867262",
                "status": "0",
                "id": "1000002",
                "groups": [],
                "canUse": "true",
                "canManage": "true",
                "ownerGroup": {
                    "id": "0",
                    "name": "Full Access",
                    "description": "Full Access group"
},
                "owner": {
                    "id": "1",
                    "username": "qahead",
                    "firstname": "Qa",
                    "lastname": "Head",
                    "uuid": "36DC8C6C-962A-4C65-AB6C-8C9986D40446"
            },
                "policyTemplate": {
                    "id": "3",
                    "name": "Basic Network Scan",
                    "description": "A full system scan suitable for
```

```
any host.",
                    "agent": "false",
                    "isWas": "false"                },
                "uuid": "8DCCD0D1-BA3F-47A6-8197-F85C86381FF8"
    },
            {
                "name": "ADMIN - Policy Compliance Auditing",
                "description": "",
                "tags": "admin",
                "createdTime": "1704876775",
                "modifiedTime": "1704876775",
                "status": "0",
                "id": "1",
                "canUse": "true",
                "canManage": "false",
                "policyTemplate": {
                    "id": "7",
                    "name": "Policy Compliance Auditing",
                    "description": "Audit system configurations
against a known baseline.",
                    "agent": "false",
                    "isWas": "false"                },
                "uuid": "E26BE33B-E25F-483B-901D-093692E1686B"
    }
       ],
       "manageable": [
            {
                "name": "Basic network Scan",
                "description": "",
                "tags": "BASIC-NETWORK-SCAN",
                "createdTime": "1704867262",
                "modifiedTime": "1704867262",
                "status": "0",
```

```
                "id": "1000002",
                "groups": [],
                "canUse": "true",
                "canManage": "true",
                "ownerGroup": {
                    "id": "0",
                    "name": "Full Access",
                    "description": "Full Access group"
 },
                "owner": {
                    "id": "1",
                    "username": "qahead",
                    "firstname": "Qa",
                    "lastname": "Head",
                    "uuid": "36DC8C6C-962A-4C65-AB6C-8C9986D40446"
            },
                "policyTemplate": {
                    "id": "3",
                    "name": "Basic Network Scan",
                    "description": "A full system scan suitable for
any host.",
                    "agent": "false",
                    "isWas": "false"                },
                "uuid": "8DCCD0D1-BA3F-47A6-8197-F85C86381FF8"
     }
        ]
    },
    "error_code": 0,
    "error_msg": "",
    "warnings": [],
    "timestamp": 1704968196
}
```


POST

Adds a Policy at the Admin or Organizational level.

NOTE #1: To specify a *mixed* Plugin Family, the *plugins* field must be present; otherwise, the family type defaults to *enabled*.
NOTE #2: When a policy is not context "" (empty), a new name will be generated. The 'name' parameter, if passed, will be overwritten.

Request Parameters

Expand

```
{
       "context" : <string> "" | "scan" DEFAULT ""     "description" :
<string> DEFAULT "",
       "tags" : <string> DEFAULT "",
       "preferences" : [
              <string:name> : <string:value>...
       ] DEFAULT [],
       "auditFiles" : [
              {
                     "id" : <number>         }...
       ] DEFAULT [],
       "policyTemplate" : {
              "id" : <number> },
       "policyProfileName" : <string> OPTIONAL,
       "generateXCCDFResults" : <string> "false" | "true" DEFAULT "false"
        context "" (empty)
       ------------------
       "name" : <string>}
```

policyTemplate ID "1" (Advanced Scan Template) or "25" (Advanced Agent Scan Template)

```
...
       "families" : [
              {
                     "id" : <number>,
           "plugins" : [
```

```
                                {
                                        "id" : <number>                 },
                ....
            ] OPTIONAL (must be specified to effect a "mixed" Plugin
Family type),

            Family "enabled"            ----------------
            "state" : <string> "unlocked" DEFAULT "unlocked"
            Family "mixed"            --------------
            "state" : <string> "unlocked" | "locked" DEFAULT
"locked"                }...
       ] DEFAULT []
...
```

Session User is not an administrator

```
{
       "ownerID" : <number> DEFAULT {creatorID},  (
}
```

Example Response

Expand

```
{
       "type" : "regular",
       "response" : [
               {
                       "id" : "1000019",
                       "name" : "DOCtest",
                       "description" : "desc",
                       "policyTemplate" : {
                               "id" : "1",
                               "name" : "Advanced Scan",
```

```
                                "description" : "Configure a scan without usi
recommendations.",
                                "agent" : "false",
                                "isWas" : "false"                               },
                        "policyProfileName" : "",
                        "generateXCCDFResults" : "false",
                        "creatorID" : "1",
                        "ownerID" : "1",
                        "context" : "",
                        "tags" : "",
                        "createdTime" : "1406224504",
                        "modifiedTime" : "1406224504",
                        "ownerGID" : "0",
                        "targetGID" : "-1",
                        "auditFiles" : [],
                        "preferences" : [],
                        "families" : [
                                {
                                        "id" : "9",
                                        "type" : "mixed",
                                        "state" : "unlocked",
                    "name" : "AIX Local Security Checks",
                                        "count" : "11164"
                                {
                                        "id" : "54",
                                        "type" : "mixed",
                                        "state" : "locked",
                    "name" : "Amazon Linux Local Security Checks",
                                        "count" : "502"
                                {
                                        "id" : "35",
                                        "type" : "enabled",
                                        "state" : "unlocked",
```

```
                "name" : "Backdoors",
                                "count" : "102"
                        {
                                "id" : "18",
                                "type" : "enabled",
                                "state" : "unlocked",
                "name" : "CentOS Local Security Checks",
                                "count" : "1890"
                        {
                                "id" : "6",
                                "type" : "enabled",
                                "state" : "unlocked",
                "name" : "CGI abuses",
                                "count" : "3235"
                        {
                                "id" : "26",
                                "type" : "enabled",
                                "state" : "unlocked",
                "name" : "CGI abuses  :  XSS",
                                "count" : "600"
                        {
                                "id" : "33",
                                "type" : "enabled",
                                "state" : "unlocked",
                "name" : "CISCO",
                                "count" : "576"
                        {
                                "id" : "31",
                                "type" : "enabled",
                                "state" : "unlocked",
                "name" : "Databases",
                                "count" : "372"
                        {
```

```
            "id" : "3",
            "type" : "enabled",
            "state" : "unlocked",
            "name" : "Debian Local Security Checks
            "count" : "3179"
        {
            "id" : "25",
            "type" : "enabled",
            "state" : "unlocked",
            "name" : "Default Unix Accounts",
            "count" : "101"
        {
            "id" : "22",
            "type" : "enabled",
            "state" : "unlocked",
            "name" : "Denial of Service",
            "count" : "107"
        {
            "id" : "37",
            "type" : "enabled",
            "state" : "unlocked",
            "name" : "DNS",
            "count" : "110"
        {
            "id" : "57",
            "type" : "enabled",
            "state" : "unlocked",
            "name" : "F5 Networks Local Security C
            "count" : "154"
        {
            "id" : "5",
            "type" : "enabled",
            "state" : "unlocked",
```

```
            "name" : "Fedora Local Security Checks
            "count" : "8067"
        {
            "id" : "34",
            "type" : "enabled",
            "state" : "unlocked",
            "name" : "Firewalls",
            "count" : "139"
        {
            "id" : "13",
            "type" : "enabled",
            "state" : "unlocked",
            "name" : "FreeBSD Local Security Chec
            "count" : "2616"
        {
            "id" : "19",
            "type" : "enabled",
            "state" : "unlocked",
            "name" : "FTP",
            "count" : "244"
        {
            "id" : "40",
            "type" : "enabled",
            "state" : "unlocked",
            "name" : "Gain a shell remotely",
            "count" : "274"
        {
            "id" : "30",
            "type" : "enabled",
            "state" : "unlocked",
            "name" : "General",
            "count" : "198"
        {
```

```
        "id" : "7",
        "type" : "enabled",
        "state" : "unlocked",
        "name" : "Gentoo Local Security Checks
        "count" : "2071"
{
        "id" : "2",
        "type" : "enabled",
        "state" : "unlocked",
        "name" : "HP-UX Local Security Checks"
        "count" : "1974"
{
        "id" : "56",
        "type" : "enabled",
        "state" : "unlocked",
        "name" : "Huawei Local Security Checks
        "count" : "14"
{
        "id" : "50",
        "type" : "enabled",
        "state" : "unlocked",
        "name" : "Junos Local Security Checks"
        "count" : "107"
{
        "id" : "21",
        "type" : "enabled",
        "state" : "unlocked",
        "name" : "MacOS X Local Security Checl
        "count" : "717"
{
        "id" : "47",
        "type" : "enabled",
        "state" : "unlocked",
```

```
            "name" : "Mandriva Local Security Chec
            "count" : "2970"
        {
            "id" : "23",
            "type" : "enabled",
            "state" : "unlocked",
            "name" : "Misc.",
            "count" : "972"
        {
            "id" : "52",
            "type" : "enabled",
            "state" : "unlocked",
            "name" : "Mobile Devices",
            "count" : "43"
        {
            "id" : "43",
            "type" : "enabled",
            "state" : "unlocked",
            "name" : "Netware",
            "count" : "14"
        {
            "id" : "53",
            "type" : "enabled",
            "state" : "unlocked",
            "name" : "Oracle Linux Local Security
            "count" : "1912"
        {
            "id" : "55",
            "type" : "enabled",
            "state" : "unlocked",
            "name" : "Palo Alto Local Security Che
            "count" : "20"
        {
```

```
                        "id" : "32",
                        "type" : "enabled",
                        "state" :"unlocked",
                        "name" : "Peer-To-Peer File Sharing",
                        "count" : "72"
                {
                        "id" : "39",
                        "type" : "enabled",
                        "state" :"unlocked",
                        "name" : "Policy Compliance",
                        "count" : "38"
                {
                        "id" : "42",
                        "type" : "enabled",
                        "state" :"unlocked",
        "name" : "Port scanners",
                        "count" : "8"
                {
                        "id" : "1",
                        "type" : "enabled",
                        "state" :"unlocked",
                        "name" : "Red Hat Local Security Chec
                        "count" : "3424"
                {
                        "id" : "28",
                        "type" : "enabled",
                        "state" : "unlocked",
                        "name" : "RPC",
                        "count" : "36"
                {
                        "id" : "36",
                        "type" : "enabled",
                        "state" : "unlocked",
```

```
            "name" : "SCADA",
            "count" : "198"
        {
            "id" : "51",
            "type" : "enabled",
            "state" : "unlocked",
            "name" : "Scientific Linux Local Secu
            "count" : "1760"
        {
            "id" : "24",
            "type" : "enabled",
            "state" : "unlocked",
            "name" : "Service detection",
            "count" : "408"
        {
            "id" : "41",
            "type" : "enabled",
            "state" : "unlocked",
            "name" : "Settings",
            "count" : "66"
        {
            "id" : "15",
            "type" : "enabled",
            "state" : "unlocked",
            "name" : "Slackware Local Security Che
            "count" : "757"
        {
            "id" : "12",
            "type" : "enabled",
            "state" : "unlocked",
            "name" : "SMTP problems",
            "count" : "135"
        {
```

```
        "id" : "45",
        "type" : "enabled",
        "state" : "unlocked",
        "name" : "SNMP",
        "count" : "33"
{
        "id" : "4",
        "type" : "enabled",
        "state" : "unlocked",
        "name" : "Solaris Local Security Chec
        "count" : "3798"
{
        "id" : "8",
        "type" : "enabled",
        "state" : "unlocked",
        "name" : "SuSE Local Security Checks",
        "count" : "7355"
{
        "id" : "14",
        "type" : "enabled",
        "state" : "unlocked",
        "name" : "Ubuntu Local Security Checks
        "count" : "2767"
{
        "id" : "48",
        "type" : "enabled",
        "state" : "unlocked",
        "name" : "VMware ESX Local Security Ch
        "count" : "94"
{
        "id" : "11",
        "type" : "enabled",
        "state" : "unlocked",
```

```
                                "name" : "Web Servers",
                                "count" : "876"
                        {
                                "id" : "20",
                                "type" : "enabled",
                                "state" : "unlocked",
                "name" : "Windows",
                                "count" : "3113"
                        {
                                "id" : "10",
                                "type" : "enabled",
                                "state" : "unlocked",
                                "name" : "Windows  :  Microsoft Bullet
                                "count" : "986"
                        {
                                "id" : "29",
                                "type" : "enabled",
                                "state" : "unlocked",
                                "name" : "Windows  :  User management'
                                "count" : "28"
                ],
                "status" : "0",
                "creator" : {
                        "id" : "1",
                        "username" : "head",
                        "firstname" : "test",
                        "lastname" : "User",
                        "uuid" : "96F2AD1B-1B83-462E-908A-84E6054F6B64
                "canUse" : "true",
                "canManage" : "true",
                "groups" : [],
                "uuid" : "2E950182-08B6-4737-830B-4ACC8F6B92F9"
        ],
```

```
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1406224504
}
```

/policy/{id}

/policy/{uuid}

Methods

GET

Gets the Policy associated with {id} or {uuid}.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
*uuid
**name
**description
**status
policyTemplateType
policyTemplate
policyProfileName
creator
tags
type
status
createdTime
modifiedTime

context
generateXCCDFResults
auditFiles
preferences
targetGroup

Session user role "1" (Administrator)

owner
ownerGroup

Session user role not "1" (Administrator)

groups

Template ID "1" (Advanced Scan Template) or "25" (Advanced Agent Scan Template)

families

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

***red** = field is a JSON object (**e.g.** "SCI" : {"id" : "2", "name" : "SCI Name", "description" : "Description"})*

Request Parameters

None

Example Response

Expand

```
{
        "type" : "regular",
        "response" : [
```

```
                {
                        "id" : "1",
                        "generateXCCDFResults" : "false",
                        "context" : "",
                        "policyTemplate" : {
                                "id" : "1",
                                "name" : "Advanced Scan",
                                "description" : "Configure a scan without usi
recommendations.",
                                "agent" : "false",
                                "isWas" : "false"                       },
                        "policyProfileName" : "",
                        "name" : "test",
                        "description" : "desc",
                        "tags" : "",
                        "createdTime" : "1406148027",
                        "modifiedTime" : "1406148027",
                        "status" : "0",
                        "auditFiles" : [],
                        "preferences" : {
                                "preference1" : "value1",
                                "preference2" : "value2"
                        "families" : [
                                {
                                        "id" : "9",
                                        "type" : "enabled",
                                        "state" : "unlocked",
                                        "name" : "AIX Local Security Checks",
                                        "count" : "11164"
                                {
                                        "id" : "54",
                                        "type" : "mixed",
                                        "state" : "unlocked",
```

```
            "name" : "Amazon Linux Local Security
            "count" : "502"
        {
            "id" : "35",
            "type" : "mixed",
            "state" : "locked",
            "name" : "Backdoors",
            "count" : "102"
        {
            "id" : "18",
            "type" : "mixed",
            "state" : "unlocked",
            "name" : "CentOS Local Security Checks
            "count" : "1890"
        {
            "id" : "6",
            "type" : "mixed",
            "state" : "locked",
            "name" : "CGI abuses",
            "count" : "3235"
        {
            "id" : "26",
            "type" : "enabled",
            "state" : "unlocked",
            "name" : "CGI abuses  :  XSS",
            "count" : "600"
        {
            "id" : "33",
            "type" : "enabled",
            "state" : "unlocked",
            "name" : "CISCO",
            "count" : "576"
        {
```

```
            "id" : "31",
            "type" : "enabled",
            "state" : "unlocked",
            "name" : "Databases",
            "count" : "372"
        {
            "id" : "3",
            "type" : "enabled",
            "state" : "unlocked",
            "name" : "Debian Local Security Checks
            "count" : "3179"
        {
            "id" : "25",
            "type" : "enabled",
            "state" : "unlocked",
            "name" : "Default Unix Accounts",
            "count" : "101"
        {
            "id" : "22",
            "type" : "enabled",
            "state" : "unlocked",
            "name" : "Denial of Service",
            "count" : "107"
        {
            "id" : "37",
            "type" : "enabled",
            "state" : "unlocked",
            "name" : "DNS",
            "count" : "110"
        {
            "id" : "57",
            "type" : "enabled",
            "state" : "unlocked",
```

```
            "name" : "F5 Networks Local Security C
            "count" : "154"
        {
            "id" : "5",
            "type" : "enabled",
            "state" : "unlocked",
            "name" : "Fedora Local Security Checks
            "count" : "8067"
        {
            "id" : "34",
            "type" : "enabled",
            "state" : "unlocked",
            "name" : "Firewalls",
            "count" : "139"
        {
            "id" : "13",
            "type" : "enabled",
            "state" : "unlocked",
            "name" : "FreeBSD Local Security Checl
            "count" : "2616"
        {
            "id" : "19",
            "type" : "enabled",
            "state" : "unlocked",
            "name" : "FTP",
            "count" : "244"
        {
            "id" : "40",
            "type" : "enabled",
            "state" : "unlocked",
            "name" : "Gain a shell remotely",
            "count" : "274"
        {
```

```
            "id" : "30",
            "type" : "enabled",
            "state" : "unlocked",
            "name" : "General",
            "count" : "198"
        {
            "id" : "7",
            "type" : "enabled",
            "state" : "unlocked",
            "name" : "Gentoo Local Security Checks
            "count" : "2071"
        {
            "id" : "2",
            "type" : "enabled",
            "state" : "unlocked",
            "name" : "HP-UX Local Security Checks"
            "count" : "1974"
        {
            "id" : "56",
            "type" : "enabled",
            "state" : "unlocked",

            "name" : "Huawei Local Security Checks
            "count" : "14"
        {
            "id" : "50",
            "type" : "enabled",
            "state" : "unlocked",
            "name" : "Junos Local Security Checks"
            "count" : "107"
        {
            "id" : "21",
            "type" : "enabled",
```

```
            "state" : "unlocked",
            "name" : "MacOS X Local Security Check
            "count" : "717"
        {
            "id" : "47",
            "type" : "enabled",
            "state" : "unlocked",
            "name" : "Mandriva Local Security Chec
            "count" : "2970"
        {
            "id" : "23",
            "type" : "enabled",
            "state" : "unlocked",
            "name" : "Misc.",
            "count" : "972"
        {
            "id" : "52",
            "type" : "enabled",
            "state" : "unlocked",
            "name" : "Mobile Devices",
            "count" : "43"
        {
            "id" : "43",
            "type" : "enabled",
            "state" : "unlocked",
            "name" : "Netware",
            "count" : "14"
        {
            "id" : "53",
            "type" : "enabled",
            "state" : "unlocked",
            "name" : "Oracle Linux Local Security
            "count" : "1912"
```

```
{
        "id" : "55",
        "type" : "enabled",
        "state" : "unlocked",
        "name" : "Palo Alto Local Security Che
        "count" : "20"
{
        "id" : "32",
        "type" : "enabled",
        "state" : "unlocked",
        "name" : "Peer-To-Peer File Sharing",
        "count" : "72"
{
        "id" : "39",
        "type" : "enabled",
        "state" : "unlocked",
        "name" : "Policy Compliance",
        "count" : "38"
{
        "id" : "42",
        "type" : "enabled",
        "state" : "unlocked",
        "name" : "Port scanners",
        "count" : "8"
{
        "id" : "1",
        "type" : "enabled",
        "state" : "unlocked",
        "name" : "Red Hat Local Security Checl
        "count" : "3424"
{
        "id" : "28",
        "type" : "enabled",
```

```
            "state" : "unlocked",
            "name" : "RPC",
            "count" : "36"
        {
            "id" : "36",
            "type" : "enabled",
            "state" : "unlocked",
            "name" : "SCADA",
            "count" : "198"
        {
            "id" : "51",
            "type" : "enabled",
            "state" : "unlocked",
            "name" : "Scientific Linux Local Secu
            "count" : "1760"
        {
            "id" : "24",
            "type" : "enabled",
            "state" : "unlocked",
            "name" : "Service detection",
            "count" : "408"
        {
            "id" : "41",
            "type" : "enabled",
            "state" : "unlocked",
            "name" : "Settings",
            "count" : "66"
        {
            "id" : "15",
            "type" : "enabled",
            "state" : "unlocked",
            "name" : "Slackware Local Security Che
            "count" : "757"
```

```
{
        "id" : "12",
        "type" : "enabled",
        "state" : "unlocked",
        "name" : "SMTP problems",
        "count" : "135"
{
        "id" : "45",
        "type" : "enabled",
        "state" : "unlocked",
        "name" : "SNMP",
        "count" : "33"
{
        "id" : "4",
        "type" : "enabled",
        "state" : "unlocked",
        "name" : "Solaris Local Security Chec
        "count" : "3798"
{
        "id" : "8",
        "type" : "enabled",
        "state" : "unlocked",
        "name" : "SuSE Local Security Checks",
        "count" : "7355"
{
        "id" : "14",
        "type" : "enabled",
        "state" : "unlocked",
        "name" : "Ubuntu Local Security Checks
        "count" : "2767"
{
        "id" : "48",
        "type" : "enabled",
```

```
                        "state" : "unlocked",
                        "name" : "VMware ESX Local Security Ch
                        "count" : "94"
                {
                        "id" : "11",
                        "type" : "enabled",
                        "state" : "unlocked",
                        "name" : "Web Servers",
                        "count" : "876"
                {
                        "id" : "20",
                        "type" : "enabled",
                        "state" : "unlocked",
                        "name" : "Windows",
                        "count" : "3113"
                {
                        "id" : "10",
                        "type" : "enabled",
                        "state" : "unlocked",
                        "name" : "Windows  :  Microsoft Bullet
                        "count" : "986"
                {
                        "id" : "29",
                        "type" : "mixed",
                        "state" : "locked",
                        "name" : "Windows  :  User management'
                        "count" : "28"
        ],
        "creator" : {
                "id" : "1",
                "username" : "head",
                "firstname" : "test",
                "lastname" : "User",
```

```
                                "uuid" : "96F2AD1B-1B83-462E-908A-84E6054F6B64"
                        "canUse" : "true",
                        "canManage" : "false",
                        "uuid" : "2E950182-08B6-4737-830B-4ACC8F6B92F9"
        ],
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1406223313
}
```

PATCH

Edits the Policy associated with {id} or {uuid}, changing only the passed in fields.

NOTE #1: A policy's context may not be modified. When a policy is not context "" (empty), a new name will be generated. If the 'name' parameter is passed, it will be overwritten.
NOTE #2: In addition to the root object level (as usual), preferences and auth preference levels are defaulted. To maintain passwords on policy preferences, the policy preference object must contain the 'id' associated with that preference.

Request Parameters

All fields are optional

See /policy::POST for parameters.

Expand

In addition, the following may be used to completely remove a preference:

NOTE: Not sending a preference will cause it to remain unchanged. Sending a preference as null, false, blank, or empty will just simply set the respective preference to that value. The only way to remove a preference is to include it in the removePrefs.

```
{
        ...
        "removePrefs" : [
```

```
                <string:name>...
        ] DEFAULT []
}
```

Example Response

See /policy/{id}::GET

DELETE

Deletes the Policy associated with {id} or {uuid}, depending on access and permissions.

Request Parameters

Expand

NOTE: If the parameter targetGID is specified, this will delete the specified policy share to the provided targetGID. Otherwise, it will delete the specified policy.

```
{
        "targetGID" : <number> DEFAULT -1 (not set)
}
```

Example Response

Expand

```
{
    "type" : "regular",
    "response" : "",
    "error_code" : 0,
    "error_msg" : "",
    "warnings" : [],
    "timestamp" : 1403100582
}
```

/policy/{id}/copy

/policy/{uuid}/copy

POST

Copies the Policy associated with {id} or {uuid}, depending on access and permissions.

NOTE: The policy that is associated with {id} or {uuid} must contain context "" (empty).

Request Parameters

Expand

```
{
        "name" : <string> DEFAULT -1 (not set)
}
```

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "id" : "4",
                "name" : "testCopy2",
                "description" : "test",
                "policyTemplate" : {
                        "id" : "1",
                        "name" : "Advanced Scan",
                        "description" : "Configure a scan without using any
recommendations.",
                        "agent" : "false",
                        "isWas" : "false"               },
                "policyProfileName" : "",
                "generateXCCDFResults" : "false",
                "creatorID" : "1",
                "context" : null,
                "tags" : "",
                "status" : "0",
```

```
                "createdTime" : "1410976021",
                "modifiedTime" : "1410976021",
                "auditFiles" : [],
                "preferences" : [],
                "families" : [],
                "creator" : {
                        "id" : "1",
                        "username" : "head",
                        "firstname" : "test",
                        "lastname" : "User",
                        "uuid" : "96F2AD1B-1B83-462E-908A-84E6054F6B64"
                "canUse" : "true",
                "canManage" : "false",
                "uuid" : "71E25154-8888-458C-9B66-F6905CA217EB" },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1410976021
}
```


/policy/{id}/export

/policy/{uuid}/export

Methods

POST

Exports the Policy associated with {id} or {uuid}, depending on access and permissions.

Request Parameters

None

Example Response

None given. The response will be an xml file containing the Scan Policy.

/policy/{id}/share

/policy/{uuid}/share

Methods

POST

Shares the Policy associated with {id} or {uuid}, depending on access and permissions

Request Parameters

Expand

```
{
        "groups" : [
                {
                        "id" : <number>          }...
        ]
}
```

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "id" : "1000002",
                "name" : "POST TEST",
                "description" : "Test of post for use with scan post test",
                "policyProfileName" : null,
                "generateXCCDFResults" : "false",
                "creatorID" : "1",
                "ownerID" : "1",
                "context" : "",
                "tags" : "",
```

```
"createdTime" : "1406815230",
"modifiedTime" : "1406831623",
"ownerGID" : "0",
"targetGID" : "-1",
"auditFiles" : [
        {
                "id" : "5",
                "name" : "Admin - Top 25 extended File Listene
                "description" : "",
                "type" : "windowsfiles",
                "uuid" : "F8F1B126-1B50-4A65-851A-1168F3283D7F
        {
                "id" : "6",
                "name" : "Admin - Top 25 lite",
                "description" : "",
                "type" : "windowsfiles",
                "uuid" : "8C255497-411D-4C7C-B44B-602EBA251B9F
        {
                "id" : "1000030",
                "name" : "Basic Audit File",
                "description" : "",
                "type" : "windowsfiles",
                "uuid" : "5EC6E35C-5B2C-435F-A5CB-C99EDBA5BA01
        {
                "id" : "1000047",
                "ownerID" : "1",
                "name" : "With Scap",
                "description" : "",
                "type" : "windowsfiles",
                "uuid" : "BAFE2113-DF13-4C7C-8837-B6C8DF2D04DF
        {
                "id" : "1000048",
                "ownerID" : "1",
```

```
                                "name" : "test12122",
                                "description" : "",
                                "type" : "scapWindows",
                                "uuid" : "20E94166-BCF8-46D1-B2C2-B331154A0D18
                        {
                                "id" : "1000049",
                                "ownerID" : "1",
                                "name" : "Test",
                                "description" : "",
                                "type" : "scapWindows",
                                "uuid" : "5EC6E35C-5B2C-435F-A5CB-C99ED3A5BA01
                ],
                "preferences" : [],
                "families" : [],
                "status" : "0",
                "policyTemplate" : {
                        "id" : "1",
                        "name" : "Advanced",
                        "description" : "Configure a policy without using any
or recommendations.",
                        "agent" : "false",
                        "isWas" : "false"               },
                "creator" : {
                        "id" : "1",
                        "username" : "head",
                        "firstname" : "Security Manager",
                        "lastname" : "",
                        "uuid" : "96F2AD1B-1B83-462E-908A-84E6054F6B64"
                "owner" : {
                        "id" : "1",
                        "username" : "head",
                        "firstname" : "Security Manager",
                        "lastname" : "",
```

```
                        "uuid" : "96F2AD1B-1B83-462E-908A-84E6054F6B64"
                "ownerGroup" : {
                        "id" : "0",
                        "name" : "Full Access",
                        "description" : "Full Access group"            },
                "targetGroup" : {
                        "id" : -1,
                        "name" : "",
                        "description" : ""              },
                "uuid" : "2E950182-08B6-4737-830B-4ACC8F6B92F9" },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1409087451
}
```


/policy/import

Methods

POST

Request Parameters

Expand

```
{
        "name" : <string>,
        "filename" : <string>,
        "description" : <string> DEFAULT "",
        "tags" : <string> OPTIONAL
}
```

Example Response

Expand

```
{
    "type" : "regular",
    "response" :  "",
    "error_code" : 0,
    "error_msg" : "",
    "warnings" : [],
    "timestamp" : 1407340545
}
```


/policy/tag

Methods

GET

Gets the full list of unique Policy tags

Note: Organization user responses will contain both organization and admin policy tags. Admin user responses will contain only admin policy tags.

Request Parameters

none

Example Response

Expand


```
{
       "type" : "regular",
       "response" : [
              "Tag1",
              "Tag2",
              "Tag3"  ],
       "error_code" : 0,
       "error_msg" : "",
       "warnings" : [],
```

```
        "timestamp" : 1461093219
}
```

Atlassian

Tenable Security Center API: Scan Policy Templates

/policyTemplate

Methods

GET

Gets the list of Policy Templates.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
**name
**description
**status
editor
detailedEditor
createdTime
modifiedTime
templatePubTime
templateModTime
templateDefModTime
agent
isWas

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

Request Parameters

None

Example Response

Expand


```
{
       "type" : "regular",
       "response" : [
                {
                        "id" : "2",
                        "name" : "Host Discovery",
                        "description" : "A simple scan to discover live hosts
ports."          },
                {
                        "id" : "3",
                        "name" : "Basic Network Scan",
                        "description" : "A full system scan suitable for any h
                {
                        "id" : "4",
                        "name" : "Credentialed Patch Audit",
                        "description" : "Authenticate to hosts and enumerate m
updates."                },
                {
                        "id" : "5",
                        "name" : "Web Application Tests",
                        "description" : "Scan for published and unknown web
vulnerabilities."                },
                {
                        "id" : "6",
```

```
                        "name" : "Windows Malware Scan",
                        "description" : "Scan for malware on Windows systems."
                {
                        "id" : "7",
                        "name" : "Policy Compliance Auditing",
                        "description" : "Audit system configurations against a
baseline."                },
                {
                        "id" : "8",
                        "name" : "Internal PCI Network Scan",
                        "description" : "Perform an internal PCI DSS (11.2.1)
vulnerability scan."                },
                {
                        "id" : "9",
                        "name" : "SCAP Compliance Audit",
                        "description" : "Audit systems by using SCAP content."
                {
                        "id" : "10",
                        "name" : "Bash Shellshock Detection",
                        "description" : "Remote and local checks for CVE-2014-
CVE-2014-7169."         },
                {
                        "id" : "11",
                        "name" : "GHOST (glibc) Detection",
                        "description" : "Local checks for CVE-2015-0235."
                {
                        "id" : "12",
                        "name" : "Advanced Scan",
                        "description" : "Configure a scan without using any
recommendations."                }
        ],
        "error_code" : 0,
        "error_msg" : "",
```

```
        "warnings" : [],
        "timestamp" : 1424979243
}
```

/policyTemplate/{id}

Methods

GET

Gets the Policy Template associated with {id}.

NOTE:

- Field *settings* represents left hand navigation in UI.
- Field *regex* represents a regular expression. Values INT_REGEX and PORT_REGEX are defined constants.
- Field *values* is required for the radio group input type.
- See the name/value pairs in "options" for naming attributes inside field *conditionalSettings*.
- Field *name* under *conditionalSettings* forms the name of a sub-section below the current section. If omitted, items are added to the current section.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
**name
**description
editor
createdTime
modifiedTime
templatePubTime
templateModTime

templateDefModTime
agent
isWas

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

Request Parameters

None

Example Response

Expand


```
{
       "type" : "regular",
       "response" : {
              "id" : "2",
              "name" : "Host Discovery",
              "description" : "A simple scan to discover live hosts and oper
ports.",
              "editor" : "{\"sections\":
[{\"name\":\"Setup\",\"id\":\"setup\",\"subsections\":
[{\"id\":\"setup_general\",\"name\":\"General\",\"inputs\":
[{\"id\":\"name\",\"type\":\"entry\",\"name\":\"Name\",\"required\":-
\"true\"},
{\"id\":\"description\",\"type\":\"textarea\",\"name\":\"Descriptio-
n\"}]},{\"id\":\"setup_
modes\",\"name\":\"Configuration\",\"inputs\":
[{\"type\":\"dropdown\",\"id\":\"MODE|discovery\",\"name\":\"Discove-
ry\",\"default\":\"host_enumeration\",\"options\":[{\"name\":\"Host
enumeration\",\"id\":\"host_enumeration\",\"hint\":\"<ul><li>General
Settings:<ul><li>Always test the local Nessus host<\\\/li><li>Use
```

```
fast network discovery<\\\/li><\\\/ul><li>Ping hosts
using:<ul><li>TCP<\\\/li><li>ARP<\\\/li><li>ICMP (2
retries)<\\\/li><\\\/ul><\\\/li><li>Scan all devices,
including:<ul><li>Printers<\\\/li><li>Novell Netware
hosts<\\\/li><\\\/ul><\\\/li><\\\/ul>\"},{\"name\":\"Port scan
(common ports)\",\"id\":\"portscan_
common\",\"hint\":\"<ul><li>General Settings:<ul><li>Always test the
local Nessus host<\\\/li><li>Use fast network
discovery<\\\/li><\\\/ul><\\\/li><li>Port Scanner
Settings:<ul><li>Scan common ports<\\\/li><li>Use netstat if
credentials are provided<\\\/li><li>Use SYN scanner if
necessary<\\\/li><\\\/ul><\\\/li><li>Ping hosts
using:<ul><li>TCP<\\\/li><li>ARP<\\\/li><li>ICMP (2
retries)<\\\/li><\\\/ul><\\\/li><li>Scan all devices,
including:<ul><li>Printers<\\\/li><li>Novell Netware
hosts<\\\/li><\\\/ul><\\\/li><\\\/ul>\"},{\"name\":\"Port scan (all
ports)\",\"id\":\"portscan_all\",\"hint\":\"<ul><li>General
Settings:<ul><li>Always test the local Nessus host<\\\/li><li>Use
fast network discovery<\\\/li><\\\/ul><\\\/li><li>Port Scanner
Settings:<ul><li>Scan all ports (1-65535)<\\\/li><li>Use netstat if
credentials are provided<\\\/li><li>Use SYN scanner if
necessary<\\\/li><\\\/ul><\\\/li><li>Ping hosts
using:<ul><li>TCP<\\\/li><li>ARP<\\\/li><li>ICMP (2
retries)<\\\/li><\\\/ul><\\\/li><li>Scan all devices,
including:<ul><li>Printers<\\\/li><li>Novell Netware
hosts<\\\/li><\\\/ul><\\\/li><\\\/ul>\"},
{\"name\":\"Custom\",\"id\":\"custom\",\"custom\":\"true\",\"hint\":-
\"<ul><li>Choose your own discovery settings.<\\\/li><\\\/ul>\"}]},
{\"type\":\"dropdown\",\"id\":\"MODE|report\",\"name\":\"Report\",\"-
default\":\"default_output\",\"options\":
[{\"name\":\"Default\",\"id\":\"default_
output\",\"hint\":\"<ul><li>Report output:<ul><li>Allow users to
edit scan results<\\\/li><\\\/ul><\\\/li><\\\/ul>\"},
```

{\"name\":\"Custom\",\"id\":\"custom\",\"custom\":\"true\",\"hint\":-
\"
Choose your own report
settings.<\\\/li><\\\/ul>\"}]}]}],\"section\":\"setup\"},
{\"name\":\"Host Discovery\",\"inputs\":[{\"id\":\"ping_the_remote_
host\",\"type\":\"checkbox\",\"name\":\"Ping the remote
host\",\"default\":\"yes\",\"conditionalSettings\":{\"yes\":
{\"subsections\":[{\"name\":\"General settings\",\"inputs\":
[{\"id\":\"test_local_nessus_
host\",\"type\":\"checkbox\",\"name\":\"Test the local Nessus
host\",\"default\":\"yes\",\"hint\":\"This setting specifies whether
the local Nessus host should be scanned when it falls within the
target range specified for the scan.\"},{\"id\":\"fast_network_
discovery\",\"type\":\"checkbox\",\"name\":\"Use fast network
discovery\",\"hint\":\"If a host responds to ping, Nessus attempts
to avoid false positives, performing additional tests to verify the
response did not come from a proxy or load balancer. Fast network
discovery bypasses those additional
tests.\",\"default\":\"no\"}],\"id\":\"ping_the_remote_host_
general\"},{\"name\":\"Ping Methods\",\"inputs\":[{\"id\":\"arp_
ping\",\"type\":\"checkbox\",\"name\":\"ARP\",\"default\":\"yes\"},
{\"id\":\"tcp_
ping\",\"type\":\"checkbox\",\"name\":\"TCP\",\"default\":\"yes\",\"-
conditionalSettings\":{\"yes\":{\"inputs\":[{\"id\":\"tcp_ping_dest_
ports\",\"type\":\"medium-entry\",\"name\":\"Destination
ports\",\"default\":\"built-in\"}]}}},{\"id\":\"icmp_
ping\",\"type\":\"checkbox\",\"name\":\"ICMP\",\"default\":\"yes\",\-
"conditionalSettings\":{\"yes\":{\"inputs\":[{\"id\":\"icmp_unreach_
means_host_down\",\"type\":\"checkbox\",\"name\":\"Assume ICMP
unreachable from the gateway means the host is
down\",\"default\":\"no\"},{\"id\":\"icmp_ping_
retries\",\"type\":\"medium-entry\",\"name\":\"Maximum number of
retries\",\"default\":\"2\",\"regex\":\"^\\\\d+$\"}]}}},
{\"id\":\"udp_

```
ping\",\"type\":\"checkbox\",\"name\":\"UDP\",\"default\":\"no\"}],\-
"id\":\"ping_the_remote_host_protocols\"}]}}}],\"subsections\":
[{\"name\":\"Fragile Devices\",\"inputs\":[{\"id\":\"scan_network_
printers\",\"type\":\"checkbox\",\"name\":\"Scan Network
Printers\",\"default\":\"no\"},{\"id\":\"scan_netware_
hosts\",\"type\":\"checkbox\",\"name\":\"Scan Novell Netware
hosts\",\"default\":\"no\"}],\"id\":\"discovery_host_discovery_
fragile_devices\"},{\"name\":\"Wake-on-LAN\",\"inputs\":
[{\"id\":\"wol_mac_addresses\",\"type\":\"file\",\"name\":\"List of
MAC addresses\"},{\"id\":\"wol_wait_time\",\"type\":\"medium-
entry\",\"name\":\"Boot time wait (in
minutes)\",\"default\":\"5\",\"regex\":\"^\\\\d+$\"}],\"id\":\"disco-
very_host_discovery_wol\"},{\"name\":\"Network Type\",\"inputs\":
[{\"id\":\"network_type\",\"type\":\"dropdown\",\"name\":\"Network
Type\",\"options\":[\"Mixed (use RFC 1918)\",\"Private
LAN\",\"Public WAN (Internet)\"],\"default\":\"Mixed (use RFC
1918)\"}],\"id\":\"discovery_host_discovery_network_
type\"}],\"id\":\"discovery_host_
discovery\",\"section\":\"discovery\"},{\"id\":\"discovery_network_
discovery\",\"subsections\":[{\"name\":\"Ports\",\"inputs\":
[{\"id\":\"unscanned_
closed\",\"type\":\"checkbox\",\"name\":\"Consider unscanned ports
as closed\",\"default\":\"no\"},{\"id\":\"portscan_
range\",\"type\":\"medium-entry\",\"name\":\"Port scan
range:\",\"default\":\"default\"}],\"id\":\"discovery_network_
discovery_ports\",\"section\":\"discovery_network_discovery\"},
{\"name\":\"Network Port Scanners\",\"inputs\":[{\"id\":\"tcp_
scanner\",\"type\":\"checkbox\",\"name\":\"TCP\",\"default\":\"no\",-
\"conditionalSettings\":{\"yes\":{\"inputs\":[{\"id\":\"tcp_
firewall_detection\",\"type\":\"dropdown\",\"name\":\"Override
automatic firewall detection\",\"default\":\"Automatic
(normal)\",\"options\":[{\"name\":\"Automatic
(normal)\",\"hint\":\"\"},{\"name\":\"Do not detect RST rate
```

limitation (soft)\",\"hint\":\"Use soft detection\"},
{\"name\":\"Ignore closed ports (aggressive)\",\"hint\":\"Use
aggressive detection\"},{\"name\":\"Disabled
(softer)\",\"hint\":\"Disable detection\"}]}]}}},{\"id\":\"syn_
scanner\",\"type\":\"checkbox\",\"name\":\"SYN\",\"default\":\"yes\"-
,\"conditionalSettings\":{\"yes\":{\"inputs\":[{\"id\":\"syn_
firewall_detection\",\"type\":\"dropdown\",\"name\":\"Override
automatic firewall detection\",\"default\":\"Automatic
(normal)\",\"options\":[{\"name\":\"Automatic
(normal)\",\"hint\":\"\"},{\"name\":\"Do not detect RST rate
limitation (soft)\",\"hint\":\"Use soft detection\"},
{\"name\":\"Ignore closed ports (aggressive)\",\"hint\":\"Use
aggressive detection\"},{\"name\":\"Disabled
(softer)\",\"hint\":\"Disable detection\"}]}]}}},{\"id\":\"udp_
scanner\",\"type\":\"checkbox\",\"name\":\"UDP\",\"default\":\"no\",-
\"hint\":\"Due to the nature of the protocol, it is generally not
possible for a port scanner to tell the difference between open and
filtered UDP ports. Enabling the UDP port scanner may dramatically
increase the scan time and produce unreliable results. Consider
using the netstat or SNMP port enumeration options instead if
possible.\"}],\"id\":\"discovery_network_discovery_network_
scanners\",\"section\":\"discovery_network_discovery\"}]},
{\"name\":\"Report\",\"subsections\":[{\"name\":\"Report
output\",\"inputs\":[{\"id\":\"allow_post_scan_
editing\",\"type\":\"checkbox\",\"name\":\"Allow users to edit scan
results\",\"default\":\"yes\"},{\"id\":\"reverse_
lookup\",\"type\":\"checkbox\",\"name\":\"Designate hosts by their
DNS name\",\"default\":\"no\"},{\"id\":\"log_live_
hosts\",\"type\":\"checkbox\",\"name\":\"Display hosts that respond
to ping\",\"default\":\"no\"},{\"id\":\"display_unreachable_
hosts\",\"type\":\"checkbox\",\"name\":\"Display unreachable
hosts\",\"default\":\"no\"}],\"id\":\"report_report_

```
output\",\"section\":\"report\"}],\"id\":\"report\",\"section\":\"re-
port\"}]}",
                "createdTime" : "1423297810",
                "modifiedTime" : "1424507404",
                "templateModTime" : "1424474588",
                "templatePubTime" : "1406151204",
                "templateDefModTime" : "1424470185",
                "agent" : "false",
                "isWas" : "false"       },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1424979089
}
```


Atlassian

Tenable Security Center API: Scan Result

/scanResult

Methods

GET

Gets the list of Scan Results.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
**name
**description
**status

initiator
owner
ownerGroup
repository
scan
job
details
importStatus
importStart
importFinish
importDuration
downloadAvailable
downloadFormat
dataFormat
resultType
resultSource
running
errorDetails
importErrorDetails
totalIPs
scannedIPs
startTime
finishTime
scanDuration
completedIPs
completedChecks
totalChecks
agentScanUUID
agentScanContainerUUID
timeCompareField

Note: field "progress" not allowed. To get this field, you must specify a specific scanResult (id).

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

Request Parameters

Expand

NOTE: The 'startTime' and 'endTime' parameters search against the 'createdTime' values. They do not consider or search against the 'finishTime' values.

```
{
        "startTime" : <number:epoch> DEFAULT {now-30 days},
        "endTime" : <number:epoch> DEFAULT {now}
}
```

Filter Parameters

usable - The response will be an object containing an array of usable Scan Results. By default, both usable and manageable objects are returned.
manageable - The response will be an object containing all manageable Scan Results. By default, both usable and manageable objects are returned.
running - Only Scan Results that are currently running will be returned. This is compatible with usable and/or manageable filters. By default, both running and completed Scan Results are returned.
completed - Only Scan Results that have completed will be returned. This is compatible with usable and/or manageable filters. By default, both running and completed Scan Results are returned.
optimizeCompletedScans- Skip retrieval of progress fields (completedIPs, completedChecks, totalChecks) for scans that are no longer in progress to optimize speed.
timeCompareField - Only support finishTime and createdTime

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "usable" : [
                        {
                                "id" : "1",
```

```
                                "name" : "Test Scan",
                                "description" : "",
                                "status" : "Completed"                  }
                ],
                "manageable" : [
                        {
                                "id" : "1",
                                "name" : "Test Scan",
                                "description" : "",
                                "status" : "Completed"                  }
                ]
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1407249641
}
```


/scanResult/{id}

Methods

GET

Gets the Scan Result associated with {id}.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
**name
**description
**status

initiator
owner
ownerGroup
repository
scan
job
details
importStatus
importStart
importFinish

importDuration?downloadAvailable

downloadFormat
dataFormat
resultType
resultSource
running
errorDetails
importErrorDetails
totalIPs
scannedIPs
startTime
finishTime

scanDuration?completedIPs

completedChecks
totalChecks

agentScanUUID
agentScanContainerUUID
progress

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

redFont = *field is a JSON object (**e.g.** "repository" :{ "id" : <id>, "name" : <name> })*

Request Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
        "response" : {
                "id" : "11",
                "name" : "Weekly Scan",
                "description" : "",
                "details" : "Policy 'Basic 1'",
                "status" : "Completed",
                "importStatus" : "Error",
                "importStart" : "1424815361",
                "importFinish" : "-1",
                "importDuration" : -1,
                "downloadAvailable" : "false",
                "downloadFormat" : "v2",
                "dataFormat" : "IPv4",
                "resultType" : "active",
                "resultSource" : "internal",
                "running" : "false",
                "errorDetails" : "",
                "importErrorDetails" : "Scan import error (code #139).",
                "totalIPs" : "200",
                "scannedIPs" : "200",
                "startTime" : "1424815208",
```

```
"finishTime" : "1424815360",
"scanDuration" : 152,
"completedIPs" : "200",
"completedChecks" : "10600",
"totalChecks" : "10600",
"agentScanUUID" : "",
"agentScanContainerUUID" : "",
"progress" : {
        "completedIPs" : "200",
        "completedChecks" : "10600",
        "totalChecks" : "10600",
        "checksPerHost" : "53",
        "totalIPs" : "200",
        "runState" : "Stopped",
        "scanningIPs" : "",
        "scanningSize" : 0,
        "scannedIPs" : "192.168.0.0",
        "scannedSize" : 29,
        "awaitingDownloadIPs" : "",
        "awaitingDownloadSize" : 0,
        "distributedSize" : 200,
        "status" : "Completed",
        "deadHostSize" : 171,
        "deadHostIPs" : "192.168.0.0",
        "scanners" : [
                {
                        "id" : "12",
                        "loadAvg" : "0.0",
                        "chunkCompleted" : "120",
                        "completedChecks" : "6360",
                        "chunks" : [
                                {
                                        "id" : "1",
```

```
                                                    "name" : "fc136656-2dc
1.",
                                                    "ips" : "192.168.0.0",
                                                    "size" : "1",
                                                    "completedHosts" : "0"
                                                    "completedChecks" : "1
                                                    "scanningIPs" : "192.1
                                                    "canningSize" : "1",
                                                    "scannedIPs" : "",
                                                    "scannedSize" : "0",
                                                    "status" : "Running",
                                                    "startTime" : "145573
                                                    "endTime" : "145573682
                                                    "deadHostIPs" : "",
                                                    "deadHostSize" : 0
                                            }
                                    ],
                                    "scannedSize" : 11,
                                    "scannedIPs" : "192.168.0.0",
                                    "scanningSize" : 0,
                                    "scanningIPs" : "",
                                    "awaitingDownloadSize" : 0,
                                    "awaitingDownloadIPs" : "",
                                    "deadHostSize" : 109,
                                    "deadHostIPs" : "192.168.0.0",
                                    "distributedSize" : 120
                            },
                            {
                                    "id" : "15",
                                    "loadAvg" : "0.0",
                                    "chunkCompleted" : "80",
                                    "completedChecks" : "4240",
                                    "chunks" : [],
```

```
                                "scannedSize" : 18,
                                "scannedIPs" : "192.168.0.0",
                                "scanningSize" : 0,
                                "scanningIPs" : "",
                                "awaitingDownloadSize" : 0,
                                "awaitingDownloadIPs" : "",
                                "deadHostSize" : 62,
                                "deadHostIPs" : "192.168.0.0",
                                "distributedSize" : 80
                        }
                ]
        },
        "initiator" : {
                "id" : "1",
                "username" : "head",
                "firstname" : "Security Manager",
                "lastname" : "",
                "uuid" : "96F2AD1B-1B83-462E-908A-84E6054F6B64"
        "owner" : {
                "id" : "1",
                "username" : "head",
                "firstname" : "Security Manager",
                "lastname" : "",
                "uuid" : "96F2AD1B-1B83-462E-908A-84E6054F6B64"
        "ownerGroup" : {
                "id" : "0",
                "name" : "Full Access",
                "description" : "Full Access group"             },
        "scan" : {
                "id" : -1,
                "name" : "",
                "description" : "",
                "type" : ""             },
```

```
                "repository" : {
                        "id" : "38",
                        "name" : "jm ipv4",
                        "description" : "copied from 97",
                        "type" : "Local",
                        "dataFormat" : "IPv4",
                        "uuid" : "A2FF7E13-2C0E-470E-A3C9-E077FE065A54"
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1426878968
}
```


DELETE

Deletes the Scan Result associated with {id}, depending on access and permissions.

Request Parameters

None

Example Response

Expand


```
{
    "type" : "regular",
    "response" : "",
    "error_code" : 0,
    "error_msg" : "",
    "warnings" : [],
    "timestamp" : 1403100582
}
```


/scanResult/{id}/copy

Methods

POST

Copies the Scan Result associated with {id}, depending on access and permissions.

Request Parameters

Expand

```
{
        "users" : [
                {
                        "id" : <number>          }...
        ]
}
```

Example Response

Expand

```
{
    "type" : "regular",
    "response" : {},
    "error_code" : 0,
    "error_msg" : "",
    "warnings" : [],
    "timestamp" : 1406924039
}
```

/scanResult/{id}/email

Methods

POST

Emails the Scan Result associated with {id}, depending on access and permissions.

Request Parameters

Expand

```
{
        "email" : <string> (valid email list)
}
```

Example Response

Expand

```
{
    "type" : "regular",
    "response" : {},
    "error_code" : 0,
    "error_msg" : "",
    "warnings" : [],
    "timestamp" : 1406924039
}
```

/scanResult/import

Methods

POST

Imports the Scan Result associated with the uploaded file, identified by *filename*.

Request Parameters

Expand

```
{
        "filename" : <string>,
        "repository" : {
                "id" : <number> },
        "classifyMitigatedAge" : <number> DEFAULT "0",
        "dhcpTracking" : <string> "false" | "true" DEFAULT "false",
        "scanningVirtualHosts" : <string> "false" | "true" DEFAULT "false"}
```

Example Response

Expand

```
{
        "type" : "regular",
        "response" : "",
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1407268778
}
```

/scanResult/{id}/import

Methods

POST

Re-imports the Scan Result associated with {id}.

Request Parameters

Expand

```
{
        "classifyMitigatedAge" : <number> DEFAULT "0",
        "dhcpTracking" : <string> "false" | "true" DEFAULT "false",
        "scanningVirtualHosts" : <string> "false" | "true" DEFAULT "false"}
```

Example Response

Expand

```
{
        "type" : "regular",
        "response" : "",
        "error_code" : 0,
        "error_msg" : "",
```

```
        "warnings" : [],
        "timestamp" : 1407268778
}
```


/scanResult/{id}/stop

Methods

POST

Stops the Scan Result associated with {id}.

NOTE: This endpoint is not applicable for Agent Sync Results, and it is disabled as such.

Request Parameters

None

Example Response

Expand


```
{
    "type" : "regular",
       "response" : {
              "id" : "86",
              "resultsSyncID" : "-1",
              "agentScanID" : "-1",
              "jobID" : "180641",
              "name" : "test scan",
              "description" : "",
              "details" : "BNS",
              "status" : "Running",
              "importStatus" : "No Results",
              "importStart" : "-1",
              "importFinish" : "-1",
              "diagnosticAvailable" : "false",
```

```
"downloadAvailable" : "false",
"downloadFormat" : "v2",
"dataFormat" : "IPv4",
"resultType" : "active",
"resultSource" : "internal",
"running" : "true",
"errorDetails" : "",
"importErrorDetails" : "",
"totalIPs" : "256",
"scannedIPs" : "0",
"startTime" : "1554407208",
"finishTime" : "-1",
"createdTime" : "1554407202",
"scanDuration" : "1008",
"importDuration" : "-1",
"completedIPs" : "20",
"completedChecks" : "2008",
"totalChecks" : "25600",
"agentScanUUID" : "xxxx-xxxx-xxxx-xxxx",
"agentScanContainerUUID" : "yyyy-yyyy-yyyy-yyyy",
"canUse" : "true",
"canManage" : "true",
"initiator" : {
    "id" : "1",
    "username" : "test user",
    "firstname" : "",
    "lastname" : "",
        "uuid" : "96F2AD1B-1B83-462E-908A-84E6054F6B64"
"owner":{
    "id" : "1",
    "username" : "test user",
    "firstname" : "",
    "lastname" : "",
```

```
                        "uuid" : "96F2AD1B-1B83-462E-908A-84E6054F6B64"
                "scan" : {
                    "id" : "18",
                    "name" : "test scan",
                    "description" : "",
                        "type" : "policy"                },
                "repository":{
                    "id" : "516",
                    "name" : "repo1",
                        "description" : "",
                        "type" : "Local",
                        "dataFormat" : "IPv4",
                        "uuid" : "A2FF7E13-2C0E-470E-A3C9-E077FE065A54"
                "ownerGroup":{
                        "id" : "0",
                        "name" : "Full Access",
                        "description" : "Full Access group"             }
        },
    "error_code" : 0,
    "error_msg" : "",
    "warnings" : [],
    "timestamp" : 1406918252
}
```


/scanResult/{id}/pause

Methods

POST

Pauses the Scan Result associated with {id}.

NOTE: This endpoint is not applicable for Agent Results, and it is disabled as such.

Request Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
        "response" : {
                "id" : "86",
                "resultsSyncID" : "-1",
                "agentScanID" : "-1",
                "jobID" : "180641",
                "name" : "test scan",
                "description" : "",
                "details" : "BNS",
                "status" : "Running",
                "importStatus" : "No Results",
                "importStart" : "-1",
                "importFinish" : "-1",
                "diagnosticAvailable" : "false",
                "downloadAvailable" : "false",
                "downloadFormat" : "v2",
                "dataFormat" : "IPv4",
                "resultType" : "active",
                "resultSource" : "internal",
                "running" : "true",
                "errorDetails" : "",
                "importErrorDetails" : "",
                "totalIPs" : "256",
                "scannedIPs" : "0",
                "startTime" : "1554407208",
                "finishTime" : "-1",
                "createdTime" : "1554407202",
                "scanDuration" : "794",
                "importDuration" : "-1",
                "completedIPs" : "0",
```

```
"completedChecks" : "0",
"totalChecks" : "25600",
"agentScanUUID" : "",
"agentScanContainerUUID" : "",
"canUse" : "true",
"canManage" : "true",
"initiator" : {
    "id" : "1",
    "username" : "test user",
    "firstname" : "",
    "lastname" : "",
        "uuid" : "96F2AD1B-1B83-462E-908A-84E6054F6B64"
"owner" : {
    "id" : "1",
    "username" : "test user",
    "firstname" : "",
    "lastname" : "",
        "uuid" : "96F2AD1B-1B83-462E-908A-84E6054F6B64"
"scan" : {
    "id" : "18",
    "name" : "test scan",
    "description" : "",
        "type" : "policy"               },
"repository" : {
    "id" : "516",
    "name" : "repo1",
    "description" : "",
        "type" : "Local",
        "dataFormat" : "IPv4",
        "uuid" : "A2FF7E13-2C0E-470E-A3C9-E077FE065A54"
"ownerGroup" : {
    "id" : "0",
        "name" : "Full Access",
```

```
                        "description" : "Full Access group"             }
    },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1406917515
}
```


/scanResult/{id}/resume

Methods

POST

Resumes the Scan Result associated with {id}.

NOTE: This endpoint is not applicable for Agent Results, and it is disabled as such.

Request Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
        "response" : {
                "id" : "86",
                "resultsSyncID" : "-1",
                "agentScanID" : "-1",
                "jobID" : "180641",
                "name" : "test scan",
                "description" : "",
                "details" : "BNS",
                "status" : "Paused",
```

```
"importStatus" : "No Results",
"importStart" : "-1",
"importFinish" : "-1",
"diagnosticAvailable" : "false",
"downloadAvailable" : "false",
"downloadFormat" : "v2",
"dataFormat" : "IPv4",
"resultType" : "active",
"resultSource" : "internal",
"running" : "true",
"errorDetails" : "",
"importErrorDetails" : "",
"totalIPs" : "256",
"scannedIPs" : "0",
"startTime" : "1554407208",
"finishTime" : "-1",
"createdTime" : "1554407202",
"scanDuration" : "794",
"importDuration" : "-1",
"completedIPs" : "0",
"completedChecks" : "0",
"totalChecks" : "25600",
"agentScanUUID" : "",
"agentScanContainerUUID" : ""           "canUse" : "true",
"canManage" : "true",
"initiator" : {
    "id" : "1",
    "username" : "test user",
    "firstname" : "",
    "lastname" : "",
        "uuid" : "96F2AD1B-1B83-462E-908A-84E6054F6B64"
"owner" : {
    "id" : "1",
```

```
                    "username" : "test user",
                    "firstname" : "",
                    "lastname" : "",
                        "uuid" : "96F2AD1B-1B83-462E-908A-84E6054F6B64"
                "scan" : {
                    "id" : "18",
                    "name" : "test scan",
                    "description" : "",
                        "type" : "policy"                },
                "repository" : {
                    "id" : "516",
                    "name" : "repo1",
                    "description" : "",
                        "type" : "Local",
                        "dataFormat" : "IPv4",
                        "uuid" : "A2FF7E13-2C0E-470E-A3C9-E077FE065A54"
                "ownerGroup" : {
                    "id" : "0",
                        "name" : "Full Access",
                        "description" : "Full Access group"             }
    },
       "error_code" : 0,
       "error_msg" : "",
       "warnings" : [],
       "timestamp" : 1406917515
}
```


/scanResult/{id}/download

Methods

POST

Downloads the Scan Result associated with {id}.

NOTE: A Scan Result of the requested downloadType must exist for the target Scan Result. For most Scans, only the v2 downloadType applies..

Request Parameters

Expand

```
{
       "downloadType" : <string> "diagnostic" | "oval" | "scap1_2" | "v2"
DEFAULT "v2"}
```

Example Response

None. The response is a downloaded file for the requested type.

- For type "v2", the file is a Nessus file or a zip file containing a Nessus file.
- For types "oval" and "scap1_2", the file is a zip file containing the oval or scap results.
- For type "diagnostic", the file is a diagnostic database file.

/scanResult/{id}/attachment/{attachmentID}

GET

Downloads the attachment with the given {attachmentID} for the provided scan result.

Request Parameters

None

Example Response

None given. The response will be the downloaded file in binary or ascii format.

Atlassian

Tenable Security Center API: Sensor Proxy

These endpoints may only be used by administrators.

/sensor-proxy

GET

Methods

Gets the list of Sensor Proxies.

NOTE: This call will return all Sensor Proxies for an Administrator.

Fields Parameter

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields (Admin User)

*id

**uuid
**name
**description
**enabled

**status
**version

platform

distro
lastLinkedOn
lastCheckinTime
createdTime
modifiedTime

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

Request Query Parameters

None

Example Response


```
{
        "type": "regular",
        "response": [
                {
                 "name": "Sensor Proxy Two",
                 "status": "2",
                 "version": "1.0.10",
                 "platform": "linux",
                 "distro": "Oracle Linux Server 8.8",
                 "proxy_build": "2024.1021.51949.11",
                 "linkedOn": "1231654654",
                 "modifiedTime": "1231654685",
                 "id": "2",
                 "uuid": "xxxxxxxx-xxxx-xxxx-873c-c6b15e2cf0c3"
             },
             {
                 "name": "Sidecar 3",
                 "status": "2",
                 "version": "1.0.10",
                 "platform": "linux",
                 "distro": "Oracle Linux Server 8.8",
                 "proxy_build": "2024.1021.51949.11",
                 "linkedOn": "1729708556",
                 "modifiedTime": "1730304651",
                 "id": "5",
                 "uuid": "xxxxxx-916b-11ef-8db5-02420a050005"
             }
        ],
        "error_code": 0,
        "error_msg": "",
```

```
        "warnings": [],
        "timestamp": 1727369687
}
```

/sensor-proxy/search

POST

Methods

Gets the list of specified Sensor Proxies.

Fields Parameter

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

The *limit* parameter should be an integer greater than 0

```
?limit=<number>,...
```

The *startOffset* parameter should be an integer greater than 0

```
?startOffset=<number>,...
```

The *endOffset* parameter should be an integer greater than 0

```
?endOffset=<number>,...
```

The *pagination* parameter should a boolean

```
?pagination=<boolean>,...
```

Allowed Fields

*id

**uuid
**name
**description
**enabled

**status
**version

platform

distro
lastLinkedOn
lastCheckinTime
createdTime
modifiedTime

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

Example Request

```
{
    "filters": {
        "and": [
            {
                "property": "linkedOn",
                "operator": "between",
                "value": "all"
            },
            {
                "property": "modifiedTime",
                "operator": "between",
                "value": "all"
            }
```

```
        ]
    }
}
```

Example Response

```
{
    "type": "regular",
    "response": {
        "totalRecords": "3",
        "returnedRecords": 3,
        "startOffset": "0",
        "results": [
            {
                "name": "Sensor Proxy Two",
                "status": "2",
                "version": "1.0.10",
                "platform": "linux",
                "distro": "Oracle Linux Server 8.8",
                "proxy_build": "2024.1021.51949.11",
                "linkedOn": "1231654654",
                "modifiedTime": "1231654685",
                "id": "2",
                "uuid": "xxxxxxxx-8a53-416d-873c-c6b15e2cf0c3"
            },
            {
                "name": "Sidecar3",
                "status": "2",
                "version": "1.0.10",
                "platform": "linux",
                "distro": "Oracle Linux Server 8.8",
                "proxy_build": "2024.1021.51949.11",
```

```
                "linkedOn": "1729708556",
                "modifiedTime": "1730304651",
                "id": "5",
                "uuid": "xxxxxxxxx-916b-11ef-8db5-02420a050005"
            },
            {
                "name": "Sensor Proxy One",
                "status": "2",
                "version": "2.1.1",
                "platform": "platform1",
                "distro": "distro 1",
                "proxy_build": "build 1",
                "linkedOn": "1231654654",
                "modifiedTime": "1231654655",
                "id": "1",
                "uuid": "aaaa-bbbb-cccc-dddd"
            }
        ]
    },
    "error_code": 0,
    "error_msg": "",
    "warnings": [],
    "timestamp": 1730474777
}
```


/sensor-proxy/{id}

GET

Methods

Gets the Sensor Proxy associated with {id}.

NOTE: This call will return Sensor Proxy associated with {id} for an Administrator.

Fields Parameter

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields (Admin User)

*id

**uuid
**name
**description
**enabled

**status
**version

platform

distro
lastLinkedOn
lastCheckinTime
createdTime
modifiedTime

Legend

- *= always comes back*

*** = comes back if fields list not specified on GET all***

Request Query Parameters

None

Example Response

```
{
        "type": "regular",
```

```
        "response": {
         "name": "Sensor Proxy Two",
         "status": "2",
         "version": "1.0.10",
         "platform": "linux",
         "distro": "Oracle Linux Server 8.8",
         "proxy_build": "2024.1021.51949.11",
         "linkedOn": "1231654654",
         "modifiedTime": "1231654685",
         "id": "2",
         "uuid": "xxxxxxxx-xxxx-xxxx-873c-c6b15e2cf0c3"
    },
        "error_code": 0,
        "error_msg": "",
        "warnings": [],
        "timestamp": 1727369700
}
```


PATCH

Edits the Sensor Proxy associated with {id}, changing only the passed in fields.

Request Parameters


```
{
        "name": "Sensor Proxy update",
        "description": "description update",
        "enabled": "true" // false
}
```


Example Response

See /sensor-proxy/{id}::GET

DELETE

Deletes the Sensor Proxy associated with {id}.

Request Parameters

None

Example Response

```
{
        "type" : "regular",
        "response" : "",
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1402436001
}
```

Attachments:

macro?definition=e2FuY2hvcjp3YXNTY2FubmVyR0VUMX0&locale=en_US&version=2

(image/png)
macro?definition=e2FuY2hvcjp3YXNTY2FubmVyUEFUQ0h9&locale=en_US&version=2

(image/png)
macro?definition=e2FuY2hvcjp3YXNTY2FubmVyREVMRVRFfQ&locale=en_US&version=2

(image/png)
Atlassian

Tenable Security Center API: Software Update

/softwareUpdate

Methods

GET

Gets the list of Software Updates.

Request Parameters

None

Example Response

Expand


```
{
    "type" : "regular",
    "response" : [
        {
            "id": "SC-202308.1-6.2.0-rh7-64",
            "description": "(EL7) Updates Apache to V2.4.56.",
            "lastPatchSuccess": "-1",
            "staged": "false",
            "installed": "false",
            "lastPatchFailure": "-1",
            "manualUpdateOnly": "false",
                      "details": ""        },
        {
            "id": "SC-202308.2-6.2.0",
            "description": "Normalizes agent UUIDs in Asset Lists
synchronized to Tenable One.",
            "lastPatchSuccess": "-1",
            "staged": "false",
            "installed": "false",
            "lastPatchFailure": "-1",
            "manualUpdateOnly": "false",
                      "details": ""        }
    ],
    "error_code" : 0,
    "error_msg" : "",
    "warnings" : {},
    "timestamp" : 1423499298
}
```


PATCH

For all Software Update IDs provided, updates the status so that they ready to install. The Software Updates are installed during the next system restart.

Request Parameters

```
{
    "updateIDsToInstall" : [
        <string>,  (Software Update ID (e.g. "SC-202308.2-6.2.0"))
        <string>,
        ...
       ]
}
```

Example Response

Expand


```
{
    "type" : "regular",
    "response" : [
        {
            "id": "SC-202308.1-6.2.0-rh7-64",
            "description": "(EL7) Updates Apache to V2.4.56.",
            "lastPatchSuccess": "-1",
            "staged": "true",
            "installed": "false",
            "lastPatchFailure": "-1",
            "manualUpdateOnly": "false",
                      "details": ""        },
        {
            "id": "SC-202308.2-6.2.0",
            "description": "Normalizes agent UUIDs in Asset Lists
synchronized to Tenable One.",
            "lastPatchSuccess": "-1",
            "staged": "true",
```

```
            "installed": "false",
            "lastPatchFailure": "-1",
            "manualUpdateOnly": "false",
                      "details": ""        }
    ],
    "error_code" : 0,
    "error_msg" : "",
    "warnings" : {},
    "timestamp" : 1423499298
}
```


Atlassian

Tenable Security Center API: Solutions

The Solutions is experimental and can be changed, altered, or deleted after any release.

/solutions

Methods

POST

Process a query for Solutions.

NOTE: For notes on the query object, see parameters for */query::POST*.

Request Parameters

Expand

```
{
       "query": <query object>}
```

Example Response

Expand

```
{
        "type" : "regular",
        "response": {
         "totalRecords": "50",
         "returnedRecords": 50,
         "startOffset": "0",
         "endOffset": "50",
         "results": [
             {
                 "pluginID": "94017",
                 "solution": "Apply MS16-120: Security Update for
Microsoft Graphics Component (3192884)",
                 "total": "13",
                 "totalPctg": "0.37%",
                 "hostTotal": "12",
                 "vprScore": "0.0",
                 "cvssV3BaseScore": "10"            }
         ]
     }
        "error_code": 0,
        "error_msg" : "",
        "warnings": [],
        "timestamp": 1546642280
}
```


/solutions/{pluginID}

Methods

POST

Process a query for Solutions associated with {pluginID}.

NOTE: For notes on the query object, see parameters for */query::POST*.

Request Paramaters

Expand

```
{
        "query": <query object>}
```

Example Response

Expand


```
{
        "type" : "regular",
        "response": {
                {
                "results": {
                        "solution": "Apply MS16-120: Security Update for Micr
Graphics Component (3192884)",
                        "cveTotal": 3,
                        "total": "13",
                        "hostTotal": "12",
                        "vprScore": "0.0",
                        "cvssV3BaseScore": "10"                 }
                }
        },
        "error_code": 0,
        "error_msg" : "",
        "warnings": [],
        "timestamp": 1546642280
}
```


/solutions/{pluginID}/vuln

POST

Process a query for Solutions that collects vulnerabilities associated with {pluginID}.

NOTE : For notes on the query object, see parameters for */query::POST*.

Request Parameters

Expand

```
{
        "query": <query object>}
```

Example Response

Expand

```
{
        "type" : "regular",
        "response": {
                {
                "results": {
                        "pluginID": "49950",
                "pluginName": "MS10-073: Vulnerabilities in Windows
Kernel-Mode Drivers Could Allow Elevation of Privilege (981957)",
                "cvssV3BaseScore": "7.2",
                "hostTotal": "2",
                "vprScore": "7.4"               }
                }
        },
        "error_code": 0,
        "error_msg" : "",
        "warnings": [],
        "timestamp": 1546642280
}
```

/solutions/{pluginID}/asset

POST

Process a query for Solutions that collects assets associated with {pluginID}.

NOTE : For notes on the query object, see parameters for ***/query::POST***.

Request Parameters

Expand

```
{
        "query": <query object>}
```

Example Response

Expand

```
{
        "type" : "regular",
        "response": {
                {
                "results": {
                 "ip": "xx.xx.xx.xx",
                 "netbiosName": "TARGET\\SQL2016",
                 "macAddres": "",
                 "dnsName": "",
                 "osCPE": "cpe:/o:microsoft:windows_server_2016",
                 "repository": {
                     "id": "1",
                     "name": "Repo",
                     "description": "",
                     "dataFormat": "IPv4"                }
             }
                }
        },
        "error_code": 0,
        "error_msg" : "",
        "warnings": [],
        "timestamp": 1546642280
}
```

Atlassian

Tenable Security Center API: SSHKey

This endpoint may only be used by administrators.

/sshKey

The /sshKey resource.

Methods

GET

Gets a list of SSH keys from the tns user's 'authorized_hosts' file

Request Query Parameters

None

Example Response

Expand


```
[
        {
                "hash" : "1fab2df0da66974356208fc695de",
                "type" : "dsa",
                "comment" : "tns@scautotest",
                "key" :
"AAA346sfqmF+ICrDHGyl1354RkqiEEYk\/Xb6Gsd8PTVn1dKIjEV645sPXBnqXhAoQB-
LmLgm\/diXQ=="  },
        {
                "hash" : "694a87b1fa16asvwe062d66be1110",
                "type" : "dsa",
                "comment" : "tns@scbuild1",
                "key" :
"AAAAB\/fogTEadsfURiLQj0mH11gp+x\/E9R57wBYl7oDEjjz123523uEWgwaevawUr-
crPEmyxVye6Jo\/JfH"     }
]
```


POST

Adds an SSH key (in the correct format) to the tns user's 'authorized_hosts' file. Optionally, assign/override the 'comment' portion of the entry.

Request Parameters

Expand

NOTE: The key is a string separated by spaces, containing a type, key, and comment. The "type" inside of the key string must be one of: "ssh-dss" | "ssh-rsa". The "comment" inside the key string is optional but we require the "comment" parameter. If it is empty, we default to the session user's username plus the date.

```
{
        "key" : <string:"type key comment">,
        "comment" : <string:"some comment">}
```

Example Response

Expand

```
{
        "type":"regular",
        "response": {
                "hash" : "63c84acew353verdfdcb39ed",
                "comment" : "tns@scautotest3",
                "key" :
"AAAAaIwRkqiEEYk\/Xb6Gsd8PTVn1dKIjEVD0LKqLt5sPXBnqXhAoQBLmLgm\/diXQ=-
=",
                "type" : "ssh-dss"      },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1426796233
}
```

DELETE

Deletes the SSH Key associated with {hash}, depending on access and permissions.

Request Parameters

Expand

```
{
        "hash" : "63c8caew435cdcb39ed"}
```

Example Response

Expand

```
{
    "type" : "regular",
    "response" : "",
    "error_code" : 0,
    "error_msg" : "",
    "warnings" : [],
    "timestamp" : 1403100582
}
```

/sshKey/download

Methods

GET

Downloads Tenable.sc's RSA public key.

Request Parameters

None

Example Response

Expand

ssh-rsa AAAABURLhAMUqUpGu4rrl5e7sdfU4Yc7FCLO+GZSePYouoQ5ntoay0VCzBL2Uvuy7SLUaCjgXGPjUZhCTdBC0g/I7t4Lk7/YEH+ZU0xsdlq3KdJLZ1WO4pKF4P1fKwG1o8/ym4IcY9Q/yWN9vw== tns@johndoe

/sshKey/installRemoteKey

Methods

POST

Installs the Public SSH key for Tenable.sc on to the specified, remote host.

Request Parameters

Expand

```
{
        "host" : <string>,
        "username" : <string>,
        "password" : <string>}
```

Example Response

Expand


```
{
       "type" : "regular",
       "response" : {
              "comment" : "tns@John-Dev",
              "key" :
"AAAAB3NzaC154629gho\/5K8Dawv4398dtmz2kiCAQdiZwtJnXv9KYKKrzVqGCNQD43cv34
eEcV\/cgRMAGAKFEsTk3\/X7hYbNSnF4UA7Y=",
              "type" : "ssh-dss"      },
       "error_code" : 0,
       "error_msg" : "",
       "warnings" : [],
       "timestamp" : 1403011994
}
```


Atlassian

Tenable Security Center API: Status

/status

Methods

GET

Gets a collection of status information, including license.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

jobd
licenseStatus
migrationStatus
PluginSubscriptionStatus
LCEPluginSubscriptionStatus
PassivePluginSubscriptionStatus
pluginUpdates
feedUpdates
activeIPs
licensedIPs
zoneStatus
noLCEs
noReps
lastDbBackupStatus
lastDbBackupSuccess
lastDbBackupFailure

Note: There is no <id> GET with status. All fields are returned, by default, here.

Request Parameters

None

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "jobd" : "Running",
                "licenseStatus" : "Valid",
                "migrationStatus" : null,
                "PluginSubscriptionStatus" : "Unconfigured",
                "LCEPluginSubscriptionStatus" : "Unconfigured",
                "PassivePluginSubscriptionStatus" : null,
                "pluginUpdates" : {
                        "active" : {
                                "updateTime" : "1373297148",
                                "stale" : "true",
                                "pluginCurrentSet" : "201307080915"
                        "passive" : {
                                "updateTime" : "1373297113",
                                "stale" : "true"                        },
                        "industrial" : {
                                "stale" : "true"                        },
                        "lce" : {
                                "updateTime" : "0",
                                "stale" : "true"                        }
                },
                "feedUpdates" : {
                        "updateTime" : "1400514960",
                        "stale" : "true"                },
                "activeIPs" : "0",
                "licensedIPs" : "1000",
                "noLCEs" : "true",
                "noReps" : "true",
                "lastDbBackupStatus" : "0",
                "lastDbBackupSuccess" : "1615491750",
                "lastDbBackupFailure" : "-1",
```

```
                "zones" : {
                        "id" : "1"                      "name" : "Default Scan
"status" : "Working"                    "uuid" : "4F7DD1CD-EB1B-40D7-BCE1-
2DB3E31F6F4C"           }
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1405023348
}
```


Atlassian

Tenable Security Center API: Style

/style

Methods

GET

Gets all the Styles available to the current user

Request Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
        "response" :    [
                {
                        "id" : "27","name" : "tenable-default-1","description"
report style","type" : "text"           },
                ...
```

```
        ],
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1421273343
}
```


/style/{id}

Methods

GET

Gets the Style associated with {id}.

Request Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
        "response" :  {
                "id" : "1",
                "name" : "Letter",
                "description" : "",
                "type" : "paper",
                "attributes" : []
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1421273493
}
```

Tenable Security Center API: StyleFamily

/styleFamily

Methods

GET

Gets all the Style Families available to the current user

Request Parameters

None

Example Response

Expand


```
{
        "type":"regular",
        "response": [
                {
                        "id":"1",
                        "name":"Tenable, Letter",
                        "description":"Default Tenable style, letter",
                        "enabled":"true"                },
                ...
        ],
        "error_code":0,
        "error_msg":"",
        "warnings":[],
        "timestamp":1421273628
}
```


/styleFamily/{id}

Methods

GET

Gets the Style Familiy associated with {id}.

Request Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
        "response" :  {
                "id" : "1",
                "name" : "Tenable, Letter",
                "description" : "Default Tenable style, letter",
                "enabled" : "true",
                "mappings" :  [
                        {
                                "styleFamilyID" : "1",
                                "styleType" : "default",
                                "styleID" : "27",
                                "styleName" : "tenable-default-1"
                        ...
                ]
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1421273720
}
```


Atlassian

Tenable Security Center API: Tenable.sc Instance

This API resource is only usable in Tenable.sc Director.

/sci

Methods

GET

Gets the list of linked Tenable.sc Instances.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
*workingScanners
*totalScanners
*status
*scanners
**name
**description
ip
version
lastSyncTime

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

Example Response

Administrator

Expand

```
{
        "type" : "regular",
        "response" : [
                {
                        "name" : "Invalid SC",
                        "ip" : "0.0.0.0",
                        "version" : "Unknown",
                        "status" : "8194",
                        "lastSyncTime" : "1574443980",
                        "id" : "1",
                        "scanners" : [],
                        "workingScanners" : 0,
                        "totalScanners" : 0
                },
                {
                        "name" : "My SC",
                        "ip" : "172.26.100.123",
                        "version" : "5.13.0",
                        "status" : "1",
                        "lastSyncTime" : "1574707501",
                        "id" : "2",
                        "scanners" : [
                                {
                                        "id" : "4064",
                                        "name" : "ScannerA",
                                        "description" : "This is a descriptio
                                {
                                        "id" : "4065",
                                        "name" : "ScannerB",
                                        "description" : ""
                                {
                                        "id" : "4066",
                                        "name" : "Broken Scanner",
```

```
                                        "description" : ""
                        ],
                        "workingScanners" : 2,
                        "totalScanners" : 3
                },
        ],
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1574707627
}
```


Organization User

None

POST

Adds a linked Tenable.sc Instance.

Request Parameters

Expand


```
{
        "name" : <string>,
        "description" : <string> DEFAULT "",
        "context" : <string> DEFAULT "",
        "status" : <number> DEFAULT "-1",
        "createdTime" : <number> DEFAULT "0",
        "modifiedTime" : <number> DEFAULT "0",
        "ip" : <string>,
        "port" : <number>,
        "useProxy" : <boolean> DEFAULT "false",
        "verifyHost" : <boolean> DEFAULT "false",
        "accessKey" : <string>,
```

```
        "secretKey" : <string>,
        "lastCommunicationTime" : <number> DEFAULT "0",
        "lastSyncTime" : <number> DEFAULT "0"}
```

Example Response

Expand

```
{
    "type" : "regular",
    "response" : {
        "id" : "22",
        "name" : "Temp Box",
        "description" : "",
        "ip" : "1.2.3.4",
        "port" : "123",
        "useProxy" : "false",
        "verifyHost" : "false",
        "accessKey" : "3124ffd6ca5a4f4ba20557da5b829b2a",
        "secretKey" : "SET",
        "version" : "Unknown",
        "status" : "8192",
              "scanners" : [
              {
                      "id": "24",
               "name": "ScannerA",
               "description": "123"           },
           {
               "id": "25",
               "name": "ScannerB",
               "description": "abc"           },
           {
               "id": "26",
               "name": "ScannerC",
```

```
                "description": ""            }
        ],
        "lastCommunicationTime" : "-1",
        "lastSyncTime" : "-1",
        "createdTime" : "1574782552",
        "modifiedTime" : "1574782552",
        "workingScanners" : 0,
        "totalScanners" : 0
    },
    "error_code" : 0,
    "error_msg" : "",
    "warnings" : [],
    "timestamp" : 1574782552
}
```


/sci/{id}

Methods

GET

Gets the Tenable.sc Instance associated with {id}.

NOTE: Does not return any scanner information except number of scanners and number of operational scanners

Example Response

Administrator

Expand


```
{
       "type" : "regular",
       "response" : {
              "id" : "2",
              "name" : "My SC",
```

```
                "description" : "This is my SC",
                "ip" : "1.2.3.4",
                "port" : "123",
                "useProxy" : "false",
                "verifyHost" : "false",
                "accessKey" : "8bb3a64f6fb0483ba0769d20779d289c",
                "secretKey" : "SET",
                "version" : "5.13.0",
                "status" : "1",
                "lastCommunicationTime" : "1574785801",
                "lastSyncTime" : "1574785801",
                "createdTime" : "1574107088",
                "modifiedTime" : "1574190265",
                "workingScanners" : 2,
                "totalScanners" : 4
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1574786283
}
```


Organization User

None

PATCH

Edits the linked Tenable.sc Instance information associated with {id}, changing only the passed in fields.

NOTES:

- This does not currently edit the actual Tenable.sc, only to the local information associated to that linked Tenable.sc Instance
- This will start a "SCI Status Refresh" job to update the local SCI with the remote information

Request Parameters

Expand

name
port
ip
description
accessKey
secretKey
verifyHost
useProxy

(All fields are optional)

See /sci::GET for parameters.

Example Request Payload

Expand

```
{
        "name" : "Example Name",
        "description" : "Example Description"}
```

Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "id" : "42",
                "name" : "Example Name",
                "description" : "Example Description",
                "ip" : "1.2.3.4",
                "port" : "123",
                "useProxy" : "false",
```

```
                "verifyHost" : "false",
                "accessKey" : "3124ffd6ca5a4f4ba20557da5b829b2a",
                "secretKey" : "SET",
                "version" : "5.13.0",
                "status" : "8193",
                "lastCommunicationTime" : "1574783102",
                "lastSyncTime" : "1574783102",
                "createdTime" : "1574782552",
                "modifiedTime" : "1574783434",
                "workingScanners" : 1,
                "totalScanners" : 1
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1574783433
}
```


DELETE

Deletes the link to the Tenable.sc Instance associated with {id}.

NOTE: This does not delete the actual Tenable.sc, only the local information associated to that linked Tenable.sc Instance

Example Response

Expand


```
{
        "type" : "regular",
        "response" : "",
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1574785744
```

```
}
```

Atlassian

Tenable Security Center API: TES Admin Roles

/tes/role/admin

/tes/role/admin is only available in Tenable Enclave Security

Methods

GET

Get information about the roles an admin user can create

Fields Parameter

Expand

No Allowed Fields

Example Response

Expand

```
{
    "type": "regular",
    "response": [
        {
            "id": "1",
            "name": "Administrator",
            "description": "Role defining an administrator of the
application"
        },
        {
```

```
            "id": "2",
            "name": "Security Manager",
            "description": "The Security Manager role has full
access to all actions at the organization level. A Security Manager
has the ability to create new groups and manage existing ones. A
Security Manager can also define how users interact with other
groups.\n\nThe ability to manage other users and their objects can
be configured using group permissions on the Access tab of User
add\/edit. This includes viewing and stopping running scans and
reports."
        },
        {
            "id": "9",
            "name": "Container Security Administrator",
            "description": "Administration access to the Container
Security Blade."
        }
    ],
    "error_code": 0,
    "error_msg": "",
    "warnings": [],
    "timestamp": 1723574754
}
```


Atlassian

Tenable Security Center API: TES User Permissions

/tes/userPermissions

Methods

GET

Get information about the current user including, user details, role, group, and org.

Fields Parameter

Expand

No Allowed Fields

Example Response (Admin role)

Expand


```
{
    "type": "regular",
    "response": {
        "user": {
            "id": "1",
            "status": "0",
            "username": "admin",
            "firstname": "admin",
            "lastname": "admin",
            "title": "Application Administrator",
            "email": "",
            "address": "",
            "city": "",
            "state": "",
            "country": "",
            "phone": "",
            "fax": "",
            "createdTime": "1721707018",
            "modifiedTime": "1721827979",
            "lastLogin": "1721919082",
            "lastLoginIP": "10.253.129.137",
            "mustChangePassword": "false",
            "passwordExpires": "false",
            "passwordExpiration": null,
            "passwordExpirationOverride": "false",
```

```
            "passwordSetDate": "1721713971",
            "locked": "false",
            "failedLogins": "0",
            "authType": "tns",
            "fingerprint": null,
            "password": "SET",
            "ldapUsername": "",
            "managedUsersGroups": [],
            "managedObjectsGroups": [],
            "preferences": [
                {
                    "name": "edg.admin_users.admin1",
                    "value": "{\"activeColumns\":
[{\"field\":\"username\",\"visible\":true,\"width\":259,\"sortDir\":-
\"none\"},
{\"field\":\"name\",\"visible\":true,\"width\":259,\"sortDir\":\"non-
e\"},
{\"field\":\"authType\",\"visible\":true,\"width\":259,\"sortDir\":\-
"none\"},
{\"field\":\"role\",\"visible\":true,\"width\":259,\"sortDir\":\"non-
e\"},
{\"field\":\"title\",\"visible\":true,\"width\":259,\"sortDir\":\"no-
ne\"},
{\"field\":\"lastLogin\",\"visible\":true,\"width\":264,\"sortDir\":-
\"none\"}]}",
                    "tag": "application"
                },
                {
                    "name": "timezone",
                    "value": "America/New_York",
                    "tag": "system"
                }
            ],
```

```
            "linkedUsers": [],
            "apiKeys": [],
            "canUse": true,
            "canManage": true,
            "uuid": "480087C9-678B-46DC-A401-3C714506AACA",
            "role": {
                "id": "1",
                "name": "Administrator",
                "description": "Role defining an administrator of
the application"
            },
            "ldap": {
                "id": -1,
                "name": "",
                "description": ""
            },
            "group": {
                "id": -1,
                "name": "",
                "description": ""
            }
        },
        "role": {
            "id": "1",
            "name": "Administrator",
            "description": "Role defining an administrator of the
application",
            "createdTime": "0",
            "modifiedTime": "0",
            "permManageApp": "true",
            "permManageGroups": "false",
            "permManageRoles": "false",
            "permManageImages": "false",
```

```
"permManageGroupRelationships": "false",
"permManageBlackoutWindows": "true",
"permManageAttributeSets": "false",
"permCreateTickets": "false",
"permCreateAlerts": "false",
"permCreateAuditFiles": "false",
"permCreateLDAPAssets": "false",
"permCreatePolicies": "false",
"permPurgeTickets": "false",
"permPurgeScanResults": "false",
"permPurgeReportResults": "false",
"permScan": "none",
"permAgentsScan": "false",
"permAgentsSync": "false",
"permShareObjects": "false",
"permUpdateFeeds": "true",
"permUploadNessusResults": "false",
"permViewOrgLogs": "true",
"permManageAcceptRiskRules": "true",
"permManageRecastRiskRules": "true",
"permManageACR": "true",
"permViewDomainInventoryAssets": "false",
"permManageAttackSurfaceDomains": "false",
"permManageVulnRoutingRules": "false",
"permViewHostAssets": "true",
"permManageRiskRules": "true",
"permTPCAdmin": "true",
"permConSecUserManagement": "true",
"permConSecManageScanners": "false",
"permConSecScheduleScan": "false",
"permConSecExportData": "false",
"permConSecRunReport": "false",
"permConSecViewApp": "false",
```

```
            "permConSecManagePolicy": "false",
            "permConSecViewLogs": "true",
            "permSCViewApp": "true",
            "organizationCounts": [
                {
                    "id": 0,
                    "userCount": "2"
                },
                {
                    "id": "1",
                    "userCount": "0"
                }
            ],
            "creator": {
                "id": "1",
                "username": "admin",
                "firstname": "admin",
                "lastname": "admin",
                "uuid": "480087C9-678B-46DC-A401-3C714506AACA"
            }
        }
    },
    "error_code": 0,
    "error_msg": "",
    "warnings": [],
    "timestamp": 1721919231
}
```


Example Response (Org user)

Expand

```
{
    "type": "regular",
    "response": {
        "user": {
            "id": "1",
            "status": "0",
            "username": "qa",
            "firstname": "",
            "lastname": "",
            "title": "",
            "email": "",
            "address": "",
            "city": "",
            "state": "",
            "country": "",
            "phone": "",
            "fax": "",
            "createdTime": "1721713973",
            "modifiedTime": "1721775662",
            "lastLogin": "1722022750",
            "lastLoginIP": "10.253.129.137",
            "mustChangePassword": "false",
            "passwordExpires": "false",
            "passwordExpiration": null,
            "passwordExpirationOverride": "false",
            "passwordSetDate": "1721713973",
            "locked": "false",
            "failedLogins": "0",
            "authType": "tns",
            "fingerprint": null,
            "password": "SET",
            "ldapUsername": "",
            "managedUsersGroups": [
```

```
                {
                    "id": "-1",
                    "name": "All Groups",
                    "description": "All Groups"
                }
            ],
            "managedObjectsGroups": [
                {
                    "id": "-1",
                    "name": "All Groups",
                    "description": "All Groups"
                }
            ],
            "preferences": [
                {
                    "name":
"edg.groupPermission.orgundefined.userundefined",
                    "value": "{\"activeColumns\":
[{\"field\":\"groupName\",\"visible\":true,\"width\":320,\"sortDir\"-
:\"asc\"},
{\"field\":\"userPermission\",\"visible\":true,\"width\":320,\"sortD-
ir\":\"none\"},
{\"field\":\"objectPermission\",\"visible\":true,\"width\":320,\"sor-
tDir\":\"none\"}]}",
                    "tag": "application"
                },
                {
                    "name": "edg.policies.user1.org1",
                    "value": "{\"activeColumns\":
[{\"field\":\"name\",\"visible\":true,\"width\":261,\"sortDir\":\"as-
c\"},
{\"field\":\"tag\",\"visible\":true,\"width\":261,\"sortDir\":\"non-
e\"},
```

```
{\"field\":\"policyTemplate\",\"visible\":true,\"width\":261,\"sortD-
ir\":\"none\"},
{\"field\":\"ownerGroup\",\"visible\":true,\"width\":261,\"sortDir\"-
:\"none\"},
{\"field\":\"owner\",\"visible\":true,\"width\":261,\"sortDir\":\"no-
ne\"},
{\"field\":\"modifiedTime\",\"visible\":true,\"width\":265,\"sortDir-
\":\"none\"}]}",
                    "tag": "application"
                },
                {
                    "name": "edg.users.user1.org1",
                    "value": "{\"activeColumns\":
[{\"field\":\"username\",\"visible\":true,\"width\":222,\"sortDir\":-
\"none\"},
{\"field\":\"name\",\"visible\":true,\"width\":222,\"sortDir\":\"non-
e\"},
{\"field\":\"group\",\"visible\":true,\"width\":222,\"sortDir\":\"no-
ne\"},
{\"field\":\"authType\",\"visible\":true,\"width\":222,\"sortDir\":\-
"none\"},
{\"field\":\"role\",\"visible\":true,\"width\":222,\"sortDir\":\"non-
e\"},
{\"field\":\"title\",\"visible\":true,\"width\":222,\"sortDir\":\"no-
ne\"},
{\"field\":\"lastLogin\",\"visible\":true,\"width\":227,\"sortDir\":-
\"none\"}]}",
                    "tag": "application"
                },
                {
                    "name": "darkMode",
                    "value": "false",
                    "tag": "system"
```

```
                },
                {
                    "name": "timezone",
                    "value": "America/New_York",
                    "tag": "system"
                }
            ],
            "apiKeys": [],
            "canUse": true,
            "canManage": true,
            "uuid": "4F70F71A-B892-419B-B8D0-51803AAF76C9",
            "role": {
                "id": "2",
                "name": "Security Manager",
                "description": "The Security Manager role has full
access to all actions at the organization level. A Security Manager
has the ability to create new groups and manage existing ones. A
Security Manager can also define how users interact with other
groups.\n\nThe ability to manage other users and their objects can
be configured using group permissions on the Access tab of User
add/edit. This includes viewing and stopping running scans and
reports."
            },
            "responsibleAsset": {
                "id": -1,
                "name": "",
                "description": ""
            },
            "group": {
                "id": "0",
                "name": "Full Access",
                "description": "Full Access group"
            },
```

```
            "ldap": {
                "id": -1,
                "name": "",
                "description": ""
            }
        },
        "role": {
            "id": "2",
            "name": "Security Manager",
            "description": "The Security Manager role has full
access to all actions at the organization level. A Security Manager
has the ability to create new groups and manage existing ones. A
Security Manager can also define how users interact with other
groups.\n\nThe ability to manage other users and their objects can
be configured using group permissions on the Access tab of User
add/edit. This includes viewing and stopping running scans and
reports.",
            "createdTime": "0",
            "modifiedTime": "0",
            "permManageApp": "false",
            "permManageGroups": "true",
            "permManageRoles": "true",
            "permManageImages": "true",
            "permManageGroupRelationships": "true",
            "permManageBlackoutWindows": "true",
            "permManageAttributeSets": "true",
            "permCreateTickets": "true",
            "permCreateAlerts": "true",
            "permCreateAuditFiles": "true",
            "permCreateLDAPAssets": "true",
            "permCreatePolicies": "true",
            "permPurgeTickets": "false",
            "permPurgeScanResults": "false",
```

```
"permPurgeReportResults": "false",
"permScan": "full",
"permAgentsScan": "true",
"permAgentsSync": "true",
"permShareObjects": "true",
"permUpdateFeeds": "true",
"permUploadNessusResults": "true",
"permViewOrgLogs": "true",
"permManageAcceptRiskRules": "true",
"permManageRecastRiskRules": "true",
"permManageACR": "true",
"permViewDomainInventoryAssets": "true",
"permManageAttackSurfaceDomains": "true",
"permManageVulnRoutingRules": "true",
"permViewHostAssets": "true",
"permManageRiskRules": "true",
"permTPCAdmin": "false",
"permConSecUserManagement": "true",
"permConSecManageScanners": "true",
"permConSecScheduleScan": "true",
"permConSecExportData": "true",
"permConSecRunReport": "true",
"permConSecViewApp": "true",
"permConSecManagePolicy": "true",
"permConSecViewLogs": "true",
"permSCViewApp": "true",
"organizationCounts": [
    {
        "id": 1,
        "userCount": "1"
    }
],
"creator": {
```

```
            "id": "1",
            "username": "qa",
            "firstname": "",
            "lastname": "",
            "uuid": "4F70F71A-B892-419B-B8D0-51803AAF76C9"
        }
    },
    "group": {
        "id": "0",
        "name": "Full Access",
        "description": "Full Access group",
        "createdTime": "1721713971",
        "modifiedTime": "1721713971",
        "createDefaultObjects": "true",
        "lces": [],
        "repositories": [
            {
                "id": "1",
                "name": "universal",
                "description": "",
                "sciID": "1",
                "lastVulnUpdate": "0",
                "type": "Local",
                "dataFormat": "universal",
                "uuid": "361FEC46-5532-4F14-8EA2-D7D22F3AD338"
            }
        ],
        "definingAssets": [
            {
                "id": "0",
                "name": "All Defined Ranges",
                "description": "",
                "uuid": null
```

```
                },
                {
                    "id": "0",
                    "name": "All Defined Ranges",
                    "description": "All defining ranges of the Group
in whose context this Asset is being evaluated.",
                    "uuid": null
                }
            ],
            "userCount": 4,
            "users": [
                {
                    "id": "1",
                    "username": "qa",
                    "firstname": "",
                    "lastname": "",
                    "uuid": "4F70F71A-B892-419B-B8D0-51803AAF76C9"
                },
                {
                    "id": "2",
                    "username": "consecadmin",
                    "firstname": "",
                    "lastname": "",
                    "uuid": "20EBC47C-AE83-4B59-814A-6CE2F425C57C"
                }
            ],
            "consecRBACResources": [],
            "assets": [],
            "policies": [],
            "queries": [],
            "credentials": [],
            "dashboardTabs": [],
            "auditFiles": [],
```

```
            "arcs": []
        },
        "organization": {
            "id": "1",
            "name": "TES",
            "description": "",
            "email": "",
            "address": "",
            "city": "",
            "state": "",
            "country": "",
            "phone": "",
            "fax": "",
            "ipInfoLinks": [
                {
                    "name": "SANS",
                    "link":
"https://isc.sans.edu/ipinfo.html?ip=%IP%"
                },
                {
                    "name": "ARIN",
                    "link": "https://whois.arin.net/rest/ip/%IP%"
                }
            ],
            "zoneSelection": "selectable+auto",
            "restrictedIPs": "",
            "vulnScoreLow": "1",
            "vulnScoreMedium": "3",
            "vulnScoreHigh": "10",
            "vulnScoreCritical": "40",
            "vulnScoringSystem": "CVSSv3",
            "createdTime": "1721713971",
            "modifiedTime": "1721715001",
```

```
            "passwordExpires": "false",
            "passwordExpiration": null,
            "userCount": "4",
            "lces": [],
            "repositories": [
                {
                    "id": "1",
                    "name": "universal",
                    "description": "",
                    "type": "Local",
                    "dataFormat": "universal",
                    "groupAssign": "all",
                    "uuid": "361FEC46-5532-4F14-8EA2-D7D22F3AD338"
                }
            ],
            "zones": [
                {
                    "id": "1",
                    "name": "Default Scan Zone",
                    "description": "",
                    "uuid": "0B4C4207-F981-409C-8BC3-4B4E379455F4"
                }
            ],
            "nessusManagers": [],
            "pubSites": [],
            "ldaps": [],
            "scannerKeyExpiration": "90",
            "consecRBACResources": [],
            "uuid": "85E04564-EAA9-4E8E-A645-0AD45931609C"
        }
    },
    "error_code": 0,
    "error_msg": "",
```

```
    "warnings": [],
    "timestamp": 1722022770
}
```


Atlassian

Tenable Security Center API: Ticket

Admins do not have access to this endpoint.

/ticket

Methods

GET

Gets the list of Tickets.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
**name
**description
creator
owner
assignee
ownerGroup
assigneeGroup
queries
classification
status
notes
assignedTime

resolvedTime
closedTime
createdTime
modifiedTime
canUse
canManage
canRespond

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*
redFont = *field is a JSON object (* ***e.g.*** *"repository" :{ "id" : <id>, "name" : <name> })*

Request Parameters

None

Filter Parameters

usable - The response will be an object containing an array of usable Tickets. By default, both usable and manageable objects are returned.
manageable - The response will be an object containing all manageable Tickets. By default, both usable and manageable objects are returned.

Example Response

Expand

```
{
    "type" : "regular",
    "response" : {
        "usable" : [
            {
                "id" : "1",
                "name" : "TestTicket",
                "description" : ""            }
        ],
```

```
        "manageable" : [
            {
                "id" : "1",
                "name" : "TestTicket",
                "description" : ""            }
        ]
    },
    "error_code" : 0,
    "error_msg" : "",
    "warnings" : {},
    "timestamp" : 1423499298
}
```


POST

Adds a Ticket.

Request Parameters

Expand


```
{
    "name": <string>,
    "assignee": {
                "id" : <number> },
    "status": <string> (Optional; always "assigned" on add),
    "classification": <string> (Optional; default: "Information";
"Information" | "Configuration" | "Patch" | "Disable" | "Firewall" |
"Schedule" | "IDS" | "Other" | "Accept Risk" | "Recast Risk" | "Re-
scan Request" | "False Positive" | "System Probe" | "External Probe"
| "Investigation Needed" | "Compromised System" | "Virus Incident" |
"Bad Credentials" | "Unauthorized Software" | "Unauthorized System"
| "Unauthorized User" ),
    "description": <string> (Optional),
    "notes": <string> (Optional),
```

```
    "queries": [
        {<query ID Record>}...
    ] (Optional),
    "query": <query Object> (Optional)
}
```

Example Response

Expand

```
{
       "type" : "regular",
       "response" : {
              "id" : "1",
              "name" : "test",
              "description" : "Test",
              "classification" : "Unauthorized System",
              "status" : "assigned",
              "notes" : "Created for testing of alerts",
              "assignedTime" : "1424810461",
              "resolvedTime" : "-1",
              "closedTime" : "-1",
              "createdTime" : "1424810461",
              "modifiedTime" : "1424810461",
              "queries" : [],
        "canUse" : "true",
        "canManage" : "true",
        "canRespond" : "true",
              "creator" : {
                     "id" : "1",
                     "username" : "head",
                     "firstname" : "Security Manager",
                     "lastname" : "",
                     "uuid" : "96F2AD1B-1B83-462E-908A-84E6054F6B64"
```

```
                "owner" : {
                        "id" : "1",
                        "username" : "head",
                        "firstname" : "Security Manager",
                        "lastname" : "",
                        "uuid" : "96F2AD1B-1B83-462E-908A-84E6054F6B64"
                "assignee" : {
                        "id" : "1",
                        "username" : "head",
                        "firstname" : "Security Manager",
                        "lastname" : "",
                        "uuid" : "96F2AD1B-1B83-462E-908A-84E6054F6B64"
                "ownerGroup" : {
                        "id" : "0",
                        "name" : "Full Access",
                        "description" : "Full Access group"             },
                "assigneeGroup" : {
                        "id" : "0",
                        "name" : "Full Access",
                        "description" : "Full Access group"             }
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1426879889
}
```


/ticket/{id}

Methods

GET

Gets the Ticket associated with {id}.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
**name
**description
creator
owner
assignee
ownerGroup
assigneeGroup
queries
classification
status
notes
assignedTime
resolvedTime
closedTime
createdTime
modifiedTime
canUse
canManage
canRespond

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*
redFont = *field is a JSON object (**e.g.** "repository" :{ "id" : <id>, "name" : <name> })*

Request Parameters

None

Example Response

Expand

```
{
    "type" : "regular",
    "response" : {
        "id" : "6",
        "name" : "TestTicket",
        "description" : "",
        "classification" : "Information",
        "status" : "assigned",
        "notes" : "",
        "assignedTime" : "1423501383",
        "resolvedTime" : "-1",
        "closedTime" : "-1",
        "createdTime" : "1423501383",
        "modifiedTime" : "1423501383",
        "canUse" : "true",
        "canManage" : "true",
        "canRespond" : "true",
        "creator" : {
            "id" : "1",
            "username" : "head",
            "firstname" : "hi",
            "lastname" : "User",
                        "uuid" : "96F2AD1B-1B83-462E-908A-84E6054F6B64"
        "owner" : {
            "id" : "1",
            "username" : "head",
            "firstname" : "hi",
            "lastname" : "User",
                        "uuid" : "96F2AD1B-1B83-462E-908A-84E6054F6B64"
        "assignee" : {
            "id" : "1",
            "username" : "head",
            "firstname" : "hi",
```

```
            "lastname" : "User",
                       "uuid" : "96F2AD1B-1B83-462E-908A-84E6054F6B64"
        "ownerGroup" : {
            "id" : "0",
            "name" : "Full Access",
            "description" : "Full Access group"                },
        "assigneeGroup" : {
            "id" : "0",
            "name" : "Full Access",
            "description" : "Full Access group"                }
       },
    "error_code" : 0,
    "error_msg" : "",
    "warnings" : {},
    "timestamp" : 1423501383
}
```


PATCH

Edits the Ticket associated with {id}, changing only the passed in fields.

NOTE: When a ticket status is changed to "closed", all queries associated with the ticket are deleted.

Request Parameters

(All fields are optional)

See /ticket::POST for parameters.

Example Response

See /ticket/{id}::GET

Atlassian

Tenable Security Center API: Token

/token

Methods

POST

Logs the specified User into Tenable.sc and establishes a token for subsequent requests.

NOTE #1: Subsequent requests up to and including */token::DELETE* should set the token as the value of the "X-SecurityCenter" HTTP header field

NOTE #2: The value for unassociatedCert will be "true" if a certificate is present and not associated with any user. You may then associate the certificate with the current user.

NOTE #3: On response if releaseSession returns "true", the user has reached its maximum login limit.

NOTE #4: For information on logging in with a client certificate, see */system::GET*.

Request Parameters

Expand

```
{
        "username" : <string>,
        "password" : <string>,
        "releaseSession" : <boolean> DEFAULT false
}
```

Example Response - Available session for user to login

Expand

```
{
        "type" : "regular",
        "response" : {
                "failedLoginIP": "255.255.255.255"              "failedLogins"
"lastFailedLogin": "1452889027"         "lastLogin": "1452884944"
"lastLoginIP": "255.255.255.255"                "token" : 123456789,
                "unassociatedCert" : "false"    },
        "error_code" : 0,
```

```
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1403115433

}
```


Example Response - No sessions available for user to login

Expand


```
 {
   "type":"regular",
   "response":{
      "releaseSession":true
   },
   "error_code":0,
   "error_msg":"",
   "warnings":[

   ],
   "timestamp":1453406894
}
```


DELETE

Deletes the token associated with the logged in User.

Request Parameters

None

Example Response

Expand


```
{
        "type" : "regular",
```

```
        "response" : "",
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1403116505
}
```

Atlassian

Tenable Security Center API: User

/user

/tes/user

/tes/user is only available in Tenable Enclave Security

Methods

GET

Gets the list of Users. Depending on your role, this resource will return the following:

- A list of all Administrators (by default if the session user has the Administrator Role) or a list of all Users (if the session user is an Administrator and the optional field orgID is provided) in the provided organization.
    - NOTE: If the orgID field is provided, the Fields parameter is not supported. See the example response for the static list of fields that are returned.
- A list of all Users within the Organization's context if the session user is not an Administrator, depending on access and permissions.

Fields Parameter

The fields not under * or ** can be used only by users with enough permissions which includes:

- Admin role
- Security Manager
- Users with 'Manage Users' enabled for any Group [The fields will however be visible only for the users of the groups they can manage]
- Logged in user can use these fields to view details for self only.

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
*uuid
**username
**firstname
**lastname
**status
**email
role
title
address
city
state
country
phone
fax
createdTime
modifiedTime
lastLogin
lastLoginIP
mustChangePassword
passwordExpires
passwordExpiration
passwordExpirationOverride

passwordSetDate
locked
failedLogins
authType
fingerprint
password
apiKeys
canUse
canManage
preferences
ldap
ldapUsername
linkedUsers
parent

Session user is not role "1" (Administrator)

managedUsersGroups
managedObjectsGroups
responsibleAsset
group

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

redFont = *field is a JSON object (* ***e.g.*** *"repository" :{ "id" : <id>, "name" : <name> })*

Request User Parameters

Expand

Session user is an Administrator

To see a list of all SecurityManagers the *orgID* parameter should be specified along the query string, and it takes the syntax

```
?orgID=<number>
```

Session user is not an Administrator

None

Paginated results:

By default the results set contain all admin users or for the requested org.

To get paginated results a param value should be sent in the request as below

```
?paginated=true
```

Additionally for paginated results we can send the offsets

```
startOffset <string> [DEFAULT 0]
```

and

```
endOffset <string> [DEFAULT 50]
```

Filtering params:

Filtering of the results is allowed for below fields:

- `firstname <string> [Partial match]`
- `lastname <string> [Partial match]`
- `username <string> [Partial match]`
- `lastLoginTimeFrame <string> [15m | 20m | 30m | h | 2h | 4h | 6h | 12h | 24h | 48h | 72h | 5d | 7d | 15d | 25d | 30d | 50d | 60d | 90d | 120d | 180d | 365d]`
- `lastLoginStartTime <string> [unixtimestamp]`
- `lastLoginEndTime <string> [unixtimestamp]`
- `locked <string> [ true | false ]`
- `groupID <string> [comma separated group IDs]`
- `authType <string> [ ldap | tns | cert | saml | linked | linked_non_admin ]`

- roleID <string> [comma separated role IDs]
- title <string> [Partial match]
- email <string> [Partial match]
- address <string> [Partial match]
- state <string> [Partial match]
- country <string> [Partial match]
- phone <string> [Partial match]
- fax <string> [Partial match]
- name <string> [Partial match] [matches firstname or lastname]

Example Request Query Parameters

Expand

For request with filter param [json object]

```
?filters=[{"filterName":"roleID","value":"0,2"},
{"filterName":"firstname","value":"a"}]
```

Example Response

Administrator

Expand


```
{
        "type" : "regular",
        "response" : [
                {
                        "id" : "1",
                        "status" : "0",
```

```
"username" : "admin",
"ldapUsername" : "",
"firstname" : "Admin",
"lastname" : "User",
"title" : "Application Administrator",
"email" : "",
"address" : "",
"city" : "",
"state" : "",
"country" : "",
"phone" : "",
"fax" : "",
"createdTime" : "1432921843",
"modifiedTime" : "1453473716",
"lastLogin" : "1454350174",
"lastLoginIP" : "172.20.0.0",
"mustChangePassword" : "false",
"passwordExpires": "true",
"passwordExpiration": "90",
"passwordExpirationOverride": "false",
"passwordSetDate": "1432921843",
"locked" : "false",
"failedLogins" : "0",
"authType" : "tns",
"fingerprint" : null,
"password" : "SET",
"preferences" : [
        {
                "name" : "timezone",
                "value" : "America/New_York",
                "tag" : ""
        }
],
```

```
                        "apiKeys" : [],
                        "canUse" : true,
                        "canManage" : true,
                        "role" : {
                                "id" : "1",
                                "name" : "Administrator",
                                "description" : "Role defining an administrato
application"
                        },
                        "ldap" : {
                                "id" : "-1",
                                "name" : "",
                                "description" : ""
                        },
                        "linkedUsers" : [
                                {
                                        "user" {
                                                "id" : "2",
                                                "username" : "head",
                                                "firstname" : "John",
                                                "lastname" : "Doe",
                                                "uuid" : "96F2AD1B-1B83-462E-9
                                        },
                                        "organization" : {
                                                "id" : "1",
                                                "name" : "Org1",
                                                "description" : "",
                                                "uuid" : "FF00F4D0-5B9F-4A26-9
                                        }
                                }
                        ],
                        "uuid" : "18C16668-F942-407D-B7E0-4EEB8523F429"
                }
```

```
        ],
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1454350178
}
```


Administrator (with orgID field provided)

Expand


```
{
        "type" : "regular",
        "response" : [
                {
                        "id" : "1",
                        "username" : "head",
                        "firstname" : "",
                        "lastname" : "",
                        "apiKeys". : [],
                        "canUse" : true,
                        "canManage" : true,
                        "uuid" : "18C16668-F942-407D-B7E0-4EEB8523F429"
                }
        ],
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1454350178
}
```


Organization User (Security Manager or User with ManageUser permission of any group)

Expand

```
{
        "type" : "regular",
        "response" : [
                {
                        "id" : "1",
                        "status" : "0",
                        "username" : "head",
                        "ldapUsername" : "",
                        "firstname" : "Organization",
                        "lastname" : "User",
                        "title" : "",
                        "email" : "",
                        "address" : "",
                        "city" : "",
                        "state" : "",
                        "country" : "",
                        "phone" : "",
                        "fax" : "",
                        "createdTime" : "1432921843",
                        "modifiedTime" : "1453473716",
             "managedUsersGroups" : [
                 {
                     "id": "-1",
                     "name": "All Groups",
                     "description": "All Groups"
                 }
             ],
             "managedObjectsGroups" : [
                 {
                     "id": "-1",
                     "name": "All Groups",
                     "description": "All Groups"
                 }
```

```
            ],
                        "lastLogin" : "1454350174",
                        "lastLoginIP" : "172.20.0.0",
                        "mustChangePassword" : "false",
                        "passwordExpires": "true",
                        "passwordExpiration": "90",
                        "passwordExpirationOverride": "false",
                        "passwordSetDate": "1432921843",
                        "locked" : "false",
                        "failedLogins" : "0",
                        "authType" : "tns",
                        "fingerprint" : null,
                        "password" : "SET",
                        "preferences" : [
                                {
                                        "name" : "timezone",
                                        "value" : "America/New_York",
                                        "tag" : ""
                                }
                        ],
                        "apiKeys" : [],
                        "canUse" : true,
                        "canManage" : true,
                        "role" : {
                                "id" : "2",
                                "name" : "Security Manager",
                                "description" : "The Security Manager role has
all actions at the organization level. A Security Manager has the
ability to create new groups and manage existing ones. A Security
Manager can also define how users interact with other groups.\n\nThe
ability to manage other users and their objects can be configured
using group permissions on the Access tab of User add/edit. This
includes viewing and stopping running scans and reports."
```

```
                        },
                        "ldap" : {
                                "id" : "-1",
                                "name" : "",
                                "description" : ""
                        },
            "responsibleAsset" : {
                "id": -1,
                "name": "",
                "description": ""
            },
            "group": {
                "id": "0",
                "name": "Full Access",
                "description": "Full Access group"
            },
                        "uuid" : "18C16668-F942-407D-B7E0-4EEB8523F429"
               }
    ],
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1454348491
}
```


Organization User (without ManageUsers in any Group permissions)

Expand


```
{
        "type" : "regular",
        "response" : [
                {
                        "id" : "1",
```

```
                "username" : "head",
                "firstname" : "",
                "lastname" : "",
                "status" : 0,
                "email" : "",
                "authType" : "ldap",
                "uuid" : "18C16668-F942-407D-B7E0-4EEB8523F429"
        },
        {
                "id" : "2",
                "username" : "User 2",
                "firstname" : "",
                "lastname" : "",
                "status" : 0,
                "email" : "",
                "authType" : "tns",
                "uuid" : "18C16668-F942-407D-B7E0-4EEB8523F429"
        },
        {
                "id" : "3",
                "status" : "0",
                "username" : "self",
                "ldapUsername" : "",
                "firstname" : "Organization",
                "lastname" : "Self",
                "title" : "",
                "email" : "",
                "address" : "",
                "city" : "",
                "state" : "",
                "country" : "",
                "phone" : "",
                "fax" : "",
```

```
            "createdTime" : "1432921843",
            "modifiedTime" : "1453473716",
        "managedUsersGroups" : [
        ],
        "managedObjectsGroups" : [
            {
                "id": "-1",
                "name": "All Groups",
                "description": "All Groups"
            }
        ],
            "lastLogin" : "1454350174",
            "lastLoginIP" : "172.20.0.0",
            "mustChangePassword" : "false",
            "passwordExpires": "true",
            "passwordExpiration": "90",
            "passwordExpirationOverride": "false",
            "passwordSetDate": "1432921843",
            "locked" : "false",
            "failedLogins" : "0",
            "authType" : "tns",
            "fingerprint" : null,
            "password" : "SET",
            "preferences" : [
                    {
                            "name" : "timezone",
                            "value" : "America/New_York",
                            "tag" : ""
                    }
            ],
            "apiKeys" : [],
            "canUse" : true,
            "canManage" : true,
```

```
                        "role" : {
                                "id" : "2",
                                "name" : "Any role",
                                "description" : "Any role with any permission
                        },
                        "ldap" : {
                                "id" : "-1",
                                "name" : "",
                                "description" : ""
                        },
            "responsibleAsset" : {
                "id": -1,
                "name": "",
                "description": ""
            },
            "group": {
                "id": "0",
                "name": "Restricted group",
                "description": "Some group with restricted
permissions"
            },
                        "uuid" : "18C16668-F942-407D-B7E0-4EEB8523F429"
                }
        ],
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1454350178
}
```


Paginated response

Expand

```
{
        "type" : "regular",
        "response" :
        {
                "totalRecords" => 123,
                "returnedRecords" => 50,
                "startOffset" => 0,
                "endOffset" => 50,
                "results" => [
                        {
                                "id" : "1",
                                "username" : "head",
                                "firstname" : "",
                                "lastname" : "",
                                "status" : 0,
                                "email" : "",
                                "authType" : "ldap",
                                "uuid" : "18C16668-F942-407D-B7E0-4EEB8523F42
                        },
                        {
                                "id" : "2",
                                "username" : "User 2",
                                "firstname" : "",
                                "lastname" : "",
                                "status" : 0,
                                "email" : "",
                                "authType" : "tns",
                                "uuid" : "18C16668-F942-407D-B7E0-4EEB8523F42
                        },
                        {
                                "id" : "3",
                                "status" : "0",
                                "username" : "self",
```

```
                "ldapUsername" : "",
                "firstname" : "Organization",
                "lastname" : "Self",
                "title" : "",
                "email" : "",
                "address" : "",
                "city" : "",
                "state" : "",
                "country" : "",
                "phone" : "",
                "fax" : "",
                "createdTime" : "1432921843",
                "modifiedTime" : "1453473716",
                "managedUsersGroups" : [
                ],
                "managedObjectsGroups" : [
                        {
                                "id": "-1",
                                "name": "All Groups",
                                "description": "All Groups"
                        }
        ],
                "lastLogin" : "1454350174",
                "lastLoginIP" : "172.20.0.0",
                "mustChangePassword" : "false",
                "passwordExpires": "true",
                "passwordExpiration": "90",
                "passwordExpirationOverride": "false",
                "passwordSetDate": "1432921843",
                "locked" : "false",
                "failedLogins" : "0",
                "authType" : "tns",
                "fingerprint" : null,
```

```
                        "password" : "SET",
                        "preferences" : [
                                {
                                        "name" : "timezone",
                                        "value" : "America/New_York",
                                        "tag" : ""
                                }
                        ],
                        "apiKeys" : [],
                        "canUse" : true,
                        "canManage" : true,
                        "role" : {
                                "id" : "2",
                                "name" : "Any role",
                                "description" : "Any role with any pe
                        },
                        "ldap" : {
                                "id" : "-1",
                                "name" : "",
                                "description" : ""
                        },
            "responsibleAsset" : {
                                "id": -1,
                    "name": "",
                "description": ""
                },
              "group": {
                    "id": "0",
                    "name": "Restricted group",
                    "description": "Some group with restricted
permissions"
                        },
                        "uuid" : "18C16668-F942-407D-B7E0-4EEB8523F42
```

```
                        }
                ],
        }
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1454350178
}
```

POST

Adds a User. Depending on your role, this resource will add the following:

- An Administrator (by default if the session user has the Administrator Role) or a SecurityManager (if the session user is an Administrator and the optional field orgID is provided) into the provided organization.
- A User within the Organization's context if the session user is not an Administrator and has permission to manage users in group.

Request Parameters

Expand

The *passwordExpirationOverride* parameter does not apply to Administrator users.

```
{
        "status" : <number> DEFAULT "0",
        "roleID" : <number>,
        "username" : <string>,
        "firstname" : <string> DEFAULT "",
        "lastname" : <string> DEFAULT "",
        "title" : <string> DEFAULT "",
        "email" : <string> DEFAULT "" (required to be present and valid if
emailNotice is not empty and is not "none"),
        "address" : <string> DEFAULT "",
```

```
        "city" : <string> DEFAULT "",
        "state" : <string> DEFAULT "",
        "country" : <string> DEFAULT "",
        "phone" : <string> DEFAULT "",
        "fax" : <string> DEFAULT "",
        "locked" : <string> "false" | "true" DEFAULT "false",
        "authType" : <string> "ldap" | "legacy" | "linked" | "saml" |
"tns",
        "fingerprint" : <string> DEFAULT null,
        "emailNotice" :  <string> "both" | "id" | "none" | "password"
DEFAULT "",
        "preferences" : [
                {
                        "name" : <string>,
                        "tag" : <string> DEFAULT "",
                        "value" : <string>
                }...
        ] DEFAULT [
                {
                        "name" : "timezone",
                        "tag" : "system",
                        "value" : <string> (default timezone)
                }
        ]
}
```

authType "ldap"

Note: The "ldapUsername" attribute will be set to mirror the "username" attribute.

```
...
        "mustChangePassword" : <string> "false" DEFAULT "false",
        "ldap" : {
                "id" : <string>
```

```
        }
...
```

authType "saml"

```
...
        "mustChangePassword" : <string> "false" DEFAULT "false"
...
```

authType not "ldap" or "saml"

```
...
        "password" : <string> (must meet the requirements for configuration
setting, "PasswordMinLength"),
        "mustChangePassword" : <string> "false" | "true" DEFAULT "false"
    "passwordExpires" : <string> "false" | "true" DEFAULT "false",
    "passwordExpiration" : <number> (a number between 1 and 365)
DEFAULT 90,
    "passwordExpirationOverride" : <string> "false" | "true" DEFAULT
"false",
 ...
```

authType "linked"

Note: Only Administrators can create linked users and linked users cannot be Administrators.

```
...
        "parent" : {
                "id" : <number> DEFAULT "-1"
        }
...
```

Session user's role can manage group relationships or Session user role "1" (Administrator)

```
...
       "managedUsersGroups" : [
                {
                        "id" : <number>
                }...
       ],
       "managedObjectsGroups" : [
                {
                        "id" : <number>
                }...
       ]
...
```

Session user role "1" (Administrator)

```
...
       "orgID" : <number> DEFAULT "0" (adding another admin),
...
```

Session user role not "1" (Administrator)

```
...
       "groupID" : <number> (required to be a valid group ID whose users
you can manage),
       "responsibleAssetID" : "-1" (NOT SET) | "0" (ALL ASSETS ACCESS) |
<number> (number is required to be the id of a valid, usable,
accessible asset)
...
```

roleID not "1" (Administrator)

WARNING: The parameters in this section have been DEPRECATED as of Tenable.sc 5.11.0. Relying on their usageis highly discouraged. See /group::POST (createDefaultObjects parameter).

```
...
       "importReports" : <string> "false" | "true" DEFAULT <Target Group's
createDefaultObjects setting> ,
       "importDashboards" : <string> "false" | "true" DEFAULT <Target
Group's createDefaultObjects setting>,
       "importARCs" : <string> "false" | "true" DEFAULT <Target Group's
createDefaultObjects setting>,
       "importDashboards" is "true"
       ---------------------------
       "dashboardTemplate" : <string> (File path to template) DEFAULT
<Default filepath>,
       "importARCs" is "true"
       ----------------------
       "arcTemplate" : <string> (File path to template) DEFAULT <Default
filepath>,
...
```

Example Response

Expand

```
{
       "type" : "regular",
       "response" : {
              "id" : "1",
              "status" : "0",
              "username" : "head",
              "ldapUsername" : "",
              "firstname" : "",
              "lastname" : "",
              "title" : "",
              "email" : "",
              "address" : "",
              "city" : "",
```

```
        "state" : "",
        "country" : "",
        "phone" : "",
        "fax" : "",
        "createdTime" : "1433519288",
        "modifiedTime" : "1453477493",
        "lastLogin" : "1454349916",
        "lastLoginIP" : "172.20.0.0",
        "mustChangePassword" : "false",
    "passwordExpires": "true",
    "passwordExpiration": "90",
    "passwordExpirationOverride": "false",
    "passwordSetDate": "1433519288",
       "locked" : "false",
        "failedLogins" : "0",
        "authType" : "tns",
        "fingerprint" : null,
        "password" : "SET",
        "managedUsersGroups" : [
                {
                        "id" : "-1",
                        "name" : "All Groups",
                        "description" : "All Groups"
                }
        ],
        "managedObjectsGroups" : [
                {
                        "id" : "-1",
                        "name" : "All Groups",
                        "description" : "All Groups"
                }
        ],
        "preferences" : [
```

```
                        {
                                "name" : "timezone",
                                "value" : "America/Nome",
                                "tag" : "system"
                        }
                ],
                "canUse" : true,
                "canManage" : true,
                "role" : {
                        "id" : "2",
                        "name" : "Security Manager",
                        "description" : "The Security Manager role has full ac
actions at the organization level. A Security Manager has the
ability to create new groups and manage existing ones. A Security
Manager can also define how users interact with other groups.\n\nThe
ability to manage other users and their objects can be configured
using group permissions on the Access tab of User add/edit. This
includes viewing and stopping running scans and reports."
                },
                "responsibleAsset" : {
                        "id" : "19",
                        "name" : "Windows Hosts",
                        "description" : "The operating system detected has Wi
installed.\n\nThis will be helpful for those getting started with
Tenable.sc.",
                        "uuid" : "2DF066B8-F310-44BB-B6BE-BC6D5BDEE0AB"
                },
                "group" : {
                        "id" : "0",
                        "name" : "Full Access",
                        "description" : "Full Access group"
                },
                "ldap" : {
```

```
                        "id" : -1,
                        "name" : "",
                        "description" : ""
                },
                "parent" : {
                        "user" {
                                "id" : "0",
                                "username" : "admin",
                                "firstname" : "Jane",
                                "lastname" : "Doe",
                                "uuid" : "18C16668-F942-407D-B7E0-4EEB8523F42
                        }
                        "organization" : {
                                "id" : "0",
                                "name" : "Tenable.sc Administration",
                                "description" : "",
                                "uuid" : "FF00F4D0-5B9F-4A26-998C-19430295284
                        }
                },
                "uuid" : "96F2AD1B-1B83-462E-908A-84E6054F6B64"
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1454350250
}
```


/user/{id}

/user/{uuid}

/tes/user/{id}

/tes/user/{uuid}

/tes/user/{uuid} and /tes/user/{id} are only available in Tenable Enclave Security

Methods

GET

Gets the User associated with {id} or {uuid}. Depending on your role, this resource will return the following:

- An Administrator (by default if the session user has the Administrator Role) or a SecurityManager (if the session user is an Administrator and the optional field orgID is provided) in the provided organization.
- A User within the Organization's context if the session user is not an Administrator, depending on access and permissions.

Fields Parameter

The fields not under * or ** can be used only by users with enough permissions which includes:

- Admin role
- Security Manager
- Users with 'Manage Users' enabled for any Group [The fields will however be visible only for the users of the groups they can manage]
- Logged in user can use these fields to view details for self only.

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
*uuid
**username
**firstname
**lastname
**status
**email

**role
title
address
city
state
country
phone
fax
createdTime
modifiedTime
lastLogin
lastLoginIP
mustChangePassword
passwordExpires
passwordExpiration
passwordExpirationOverride
passwordSetDate
locked
failedLogins
authType
fingerprint
password
apiKeys
**canUse
**canManage
managedUsersGroups
managedObjectsGroups
preferences
ldapUsername
ldap
linkedUsers
parent
linkedUserRole

Session user is not role "1" (Administrator)

responsibleAsset
****group**

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

***redFont =** field is a JSON object (**e.g.** "repository" :{ "id" : <id>, "name" : <name> })*

Request User Parameters

Expand

Session user is an Administrator

To see a list of all SecurityManagers the *orgID* parameter should be specified along the query string, and it takes the syntax

```
?orgID=<number>
```

Session user is not an Administrator

None

Example Response

Administrator

Expand


```
{
        "type" : "regular",
        "response" : {
                "id" : "1",
                "status" : "0",
                "username" : "admin",
                "ldapUsername" : "",
                "firstname" : "Admin",
                "lastname" : "User",
```

```
            "title" : "Application Administrator",
            "email" : "",
            "address" : "",
            "city" : "",
            "state" : "",
            "country" : "",
            "phone" : "",
            "fax" : "",
            "createdTime" : "1432921843",
            "modifiedTime" : "1453473716",
            "lastLogin" : "1454350174",
            "lastLoginIP" : "172.20.0.0",
            "mustChangePassword" : "false",
      "passwordExpires": "true",
      "passwordExpiration": "90",
      "passwordExpirationOverride": "false",
      "passwordSetDate": "1432921843",
            "locked" : "false",
            "failedLogins" : "0",
            "authType" : "tns",
            "fingerprint" : null,
            "password" : "SET",
            "managedUsersGroups" : [],
            "managedObjectsGroups" : [],
            "preferences" : [
                  {
                        "name" : "timezone",
                        "value" : "America/New_York",
                        "tag" : ""
                  }
            ],
            "apiKeys" : [],
            "canUse" : true,
```

```
                "canManage" : true,
                "role" : {
                        "id" : "1",
                        "name" : "Administrator",
                        "description" : "Role defining an administrator of the
application"
                },
                "group" : {
                        "id" : -1,
                        "name" : "",
                        "description" : ""
                },
                "ldapUsername" : "",
                "ldap" : {
                        "id" : -1,
                        "name" : "",
                        "description" : ""
                },
                linkedUsers : [
                        {
                                "user" {
                                        "id" : "2",
                                        "username" : "head",
                                        "firstname" : "John",
                                        "lastname" : "Doe",
                                        "uuid" : "96F2AD1B-1B83-462E-903A-84E
                                },
                                "organization" : {
                                        "id" : "1",
                                        "name" : "Org1",
                                        "description" : "",
                                        "uuid" : "C61339EA-680C-4946-8131-8A4
                                }
```

```
                        }
                ],
                "linkedUserRole" : {
                "id" : "11",
                "name" : "SM-Linked",
                "description" : "Role description"
        },
                "uuid" : "18C16668-F942-407D-B7E0-4EEB8523F429"
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1454350376
}
```


Organization User (Security Manager or User with ManageUser permission of any group)

NOTE: The *parent* object is only returned when viewing an Organization User as an Administrator.

Expand


```
{
        "type" : "regular",
        "response" : {
                "id" : "2",
                "status" : "0",
                "username" : "head",
                "ldapUsername" : "",
                "firstname" : "",
                "lastname" : "",
                "title" : "",
                "email" : "",
                "address" : "",
                "city" : "",
```

```
        "state" : "",
        "country" : "",
        "phone" : "",
        "fax" : "",
        "createdTime" : "1433519288",
        "modifiedTime" : "1453477493",
        "lastLogin" : "1454349916",
        "lastLoginIP" : "172.20.0.0",
        "mustChangePassword" : "false",
    "passwordExpires": "true",
    "passwordExpiration": "90",
    "passwordExpirationOverride": "false",
    "passwordSetDate": "1433519288",
        "locked" : "false",
        "failedLogins" : "0",
        "authType" : "tns",
        "fingerprint" : null,
        "password" : "SET",
        "managedUsersGroups" : [
                {
                        "id" : "-1",
                        "name" : "All Groups",
                        "description" : "All Groups"
                }
        ],
        "managedObjectsGroups" : [
                {
                        "id" : "-1",
                        "name" : "All Groups",
                        "description" : "All Groups"
                }
        ],
        "preferences" : [
```

```
                        {
                                "name" : "timezone",
                                "value" : "America/Nome",
                                "tag" : "system"
                        }
                ],
                "apiKeys" : [],
                "canUse" : true,
                "canManage" : true,
                "role" : {
                        "id" : "2",
                        "name" : "Security Manager",
                        "description" : "The Security Manager role has full ac
actions at the organization level. A Security Manager has the
ability to create new groups and manage existing ones. A Security
Manager can also define how users interact with other groups.\n\nThe
ability to manage other users and their objects can be configured
using group permissions on the Access tab of User add/edit. This
includes viewing and stopping running scans and reports."
                },
                "responsibleAsset" : {
                        "id" : "19",
                        "name" : "Windows Hosts",
                        "description" : "The operating system detected has Wi
installed.\n\nThis will be helpful for those getting started with
Tenable.sc.",
                        "uuid" : "2DF066B8-F310-44BB-B6BE-BC6D5BDEE0AB"
                },
                "group" : {
                        "id" : "0",
                        "name" : "Full Access",
                        "description" : "Full Access group"
                },
```

```
                "ldapUserName" : "",
                "ldap" : {
                        "id" : -1,
                        "name" : "",
                        "description" : ""
                },
                "parent" : {
                        "user" : {
                                "id" : "0",
                                "username" : "admin",
                                "firstname" : "Jane",
                                "lastname" : "Doe",
                                "uuid" : "C61339EA-680C-4946-8181-8A4A8C0EF05A
                        },
                        "organization" : {
                                "id" : "0",
                                "name" : "Tenable.sc Administration",
                                "description" : "",
                                "uuid" : "FF00F4D0-5B9F-4A26-998C-19430295284A
                        }
                },
                "linkedUserRole" : {
                "id" : "11",
                "name" : "SM-Linked",
                "description" : "Role description"
        },
                "uuid" : "96F2AD1B-1B83-462E-908A-84E6054F6B64"
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1454350250
}
```


Organization User (without ManageUsers in any Group permissions)

Expand


```
{
        "type" : "regular",
        "response" : {
                "id" : "2",
                "username" : "User 2",
                "firstname" : "",
                "lastname" : "",
                "status" : 0,
                "email" : "",
                "uuid" : "18C16668-F942-407D-B7E0-4EEB8523F429"
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1454350178
}
```


Any User (fetching details of self)

Expand


```
{
        "type" : "regular",
        "response" : {
                "id" : "3",
                "status" : "0",
                "username" : "self",
                "ldapUsername" : "",
                "firstname" : "Organization",
                "lastname" : "Self",
                "title" : "",
                "email" : "",
                "address" : "",
```

```
            "city" : "",
            "state" : "",
            "country" : "",
            "phone" : "",
            "fax" : "",
            "createdTime" : "1432921843",
            "modifiedTime" : "1453473716",
        "managedUsersGroups" : [
        ],
        "managedObjectsGroups" : [
            {
                "id": "-1",
                "name": "All Groups",
                "description": "All Groups"
            }
        ],
            "lastLogin" : "1454350174",
            "lastLoginIP" : "172.20.0.0",
            "mustChangePassword" : "false",
            "passwordExpires": "true",
            "passwordExpiration": "90",
            "passwordExpirationOverride": "false",
            "passwordSetDate": "1432921843",
            "locked" : "false",
            "failedLogins" : "0",
            "authType" : "tns",
            "fingerprint" : null,
            "password" : "SET",
            "preferences" : [
                    {
                            "name" : "timezone",
                            "value" : "America/New_York",
                            "tag" : ""
```

```
                        }
                ],
                "apiKeys" : [],
                "canUse" : true,
                "canManage" : true,
                "role" : {
                        "id" : "2",
                        "name" : "Any role",
                        "description" : "Any role with any permission."
                },
                "ldap" : {
                        "id" : "-1",
                        "name" : "",
                        "description" : ""
                },
         "responsibleAsset" : {
             "id": -1,
             "name": "",
             "description": ""
         },
         "group": {
             "id": "0",
             "name": "Restricted group",
             "description": "Some group with restricted permissions"
         },
                "uuid" : "18C16668-F942-407D-B7E0-4EEB8523F429"
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1454350178
}
```


PATCH

Edits the User associated with {id} or (uuid), changing only the passed in fields. Depending on your role, this resource allow you to edit the following:

- An Administrator (by default if the session user has the Administrator Role) or a SecurityManager (if the session user is an Administrator and the optional field orgID is provided) in the provided organization.
- A User within the Organization's context if the session user is not an Administrator, depending on access and permissions.

You cannot edit the current user using this endpoint.

If you are locking an Administrator, and that Administrator has linked users (organization users whose *authType* = "linked" and whose parent matches the Administrator being locked), those linked users are locked as well.

Only Administrators can edit linked users (organization users whose *authType* = "linked"), and the following fields cannot be edited: *roleID, groupID, authType , parent, password, mustChangePassword.*

The *passwordExpirationOverride* parameter does not apply to Administrator users.

Request Parameters

If the 'password' is included in the PATCH parameters, a valid 'currentPassword' is required in the same request payload. Otherwise all other parameters are optional and identical to /user::POST

Expand

```
{
        "password" : <string> "NEW_PASSWORD",
        "currentPassword" : <string> "OLD_PASSWORD"
}
```

Example Response

See /user/{id}::GET

DELETE

Deletes the User associated with {id} or {uuid}, depending on access and permissions. Depending on your role, this resource allows you to delete the following:

- An Administrator (by default if the session user has the Administrator Role) or a SecurityManager (if the session user is an Administrator and the optional field orgID is provided) in the provided organization.
- A User within the Organization's context if the session user is not an Administrator, depending on access and permissions.

The objects owned by the user being deleted can be migrated to another user by passing in the optional *migrateUserID* parameter. Depending on your role, this resource allows you to migrate based on the following conditions:

- If the session user has the Administrator Role, the Migrate User must be an Organization Security Manager in the Full Access Group and in the same Organization as the user being deleted.
- If the session user does not have the Administrator Role, you must be able to manage the objects of the Migrate User's group.

If an Administrator has linked users (organization users whose *authType* = "linked" and whose parent is the Administrator being deleted), that Administrator cannot be deleted without deleting the linked users first. Additionally, linked users can only be deleted by an Administrator.

Request Parameters

Expand

Session user is an Administrator

```
{
       "orgID" : <number> (org ID) OR "orgUUID" : <string> (org UUID)
OPTIONAL,
       "migrateUserID": <number> (user ID) OR "migrateUserUUID" : <string>
(user UUID) OPTIONAL
}
```

Session user is not an Administrator

```
{
        "migrateUserID": <number> (user ID) OR "migrateUserUUID" : <string>
(user UUID) OPTIONAL
}
```

Example Response

Expand

```
{
        "type" : "regular",
        "response" : "",
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1402436001
}
```

Atlassian

Tenable Security Center API: WAS Scan

/wasScan

Methods

GET

Gets the list of WAS Scans.

NOTE: Although a Scan's Schedule 'dependentID' is stored as the schedule ID of the object a scan is dependent upon in the database, it is sent from and returned to the user as the ID of the actual scan object.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
*uuid
**name
**description
**status
ipList
urlList
type
plugin
repository
zone
dhcpTracking
classifyMitigatedAge
emailOnLaunch
emailOnFinish
timeoutAction
scanningVirtualHosts
rolloverType
createdTime
modifiedTime
ownerGroup
creator
owner
reports
assets
credentials
numDependents
schedule
policy
policyPrefs
maxScanTime

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

redFont = *field is a JSON object* (**e.g.** *"repository"* :{ "id" : <id>,"name" : <name> })

Request Parameters

None

Expand Parameters

credentials

Filter Parameters

usable - The response will be an object containing an array of usable WAS Scans. By default, both usable and manageable objects are returned.
manageable - The response will be an object containing all manageable WAS Scans.. By default, both usable and manageable objects are returned.

Example Response

Expand


```
{
        "type" : "regular",
        "response" : {
                "usable" : [
                        {
                                "id" : "2",
                                "name" : "test",
                                "description" : null,
                                "status" : "0",
                                "uuid" : "2EAED2D2-DFC7-4CFE-9C94-25CF6481C515
                        {
                                "id" : "3",
                                "name" : "test2",
                                "description" : null,
                                "status" : "0",
```

```
                                "uuid" : "EC81E13E-B3B2-4A51-968D-E94D524B5254
                        {
                                "id" : "4",
                                "name" : "POSTtest",
                                "description" : "This is a test for POST",
                                "status" : "0",
                                "uuid" : "2EAED2D2-DFC7-4CFE-9C94-25CF6481C515
                ],
                "manageable" : [
                        {
                                "id" : "2",
                                "name" : "test",
                                "description" : null,
                                "status" : "0",
                                "uuid" : "2EAED2D2-DFC7-4CFE-9C94-25CF6481C515
                        {
                                "id" : "3",
                                "name" : "test2",
                                "description" : null,
                                "status" : "0",
                                "uuid" : "EC81E13E-B3B2-4A51-968D-E94D524B5254
                                "id" : "4",
                                "name" : "POSTtest",
                                "description" : "This is a test for POST",
                                "status" : "0",
                                "uuid" : "2EAED2D2-DFC7-4CFE-9C94-25CF6481C515
                ]
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1406828340
}
```


POST

Adds a WAS Scan, depending on access and permissions.

NOTE #1: A Blackout Window must not be in effect

NOTE #2: Setting schedule type to "template" means that the scan will not run on a schedule.

NOTE #3: If the field *schedule frequency* is "dependent", the field *type* cannot be "template"

NOTE #4: Although a Scan's Schedule 'dependentID' is stored as the schedule ID of the object a scan is dependent upon in the database, it is sent from and returned to the user as the ID of the actual scan object.

Request Parameters

Expand

```
{
       "name" : <string>,
       "type" : <string> DEFAULT "policy",
       "description" : <string> DEFAULT "",
       "repository" : {
              "id" : <number> },
       "zone" : {
              "id" : <number> DEFAULT "0" (All Zones)
       },
       "dhcpTracking" : <string> DEFAULT "false",
       "classifyMitigatedAge" : <number> DEFAULT "0",
       "schedule" : {
              "type" : "dependent" | "ical" | "never" | "rollover" | "templa
<string> DEFAULT "template"     },
       "reports" : [
              {
                     "id" : <number>,
                     "reportSource" : <string> "cumulative" | "patched" | "
| "lce" | "archive" | "mobile"          }...
       ] DEFAULT [],
       "assets" : [
```

```
                {
                        "id" : <number>         }...
        ] DEFAULT [],
        "credentials" : [
                {
                        "id" : <number>         }...
        ] DEFAULT [],
        "emailOnLaunch" : <string> "false" | "true" DEFAULT "false",
        "emailOnFinish" : <string> "false" | "true" DEFAULT "false",
        "timeoutAction" : <string> "discard" | "import" | "rollover"
DEFAULT "import",
        "scanningVirtualHosts" : <string> "false" | "true" DEFAULT "false",
        "rolloverType" : <string> "nextDay" | "template" DEFAULT
"template",
        "urlList" : <string> DEFAULT "" (valid URL),
        "maxScanTime" : <number> DEFAULT "3600"}
```

schedule type is "ical"

NOTE: The "enabled" field can only be set to "false" for schedules of type "ical". For all other schedules types, "enabled" is set to "true".

```
...
        "schedule" : {
                "start" : <string> (This value takes the iCal format),
                "repeatRule" : <string> (This value takes the repeat rule form
                "enabled" : <string> "false" | "true" DEFAULT "true"    }
...
```

Example Response

Expand

```
{
	"type" : "regular",
	"response" : {
		"id" : "4",
		"name" : "POSTtest",
		"description" : "This is a test for POST",
		"ipList" : "",
		"urlList" : "http://example.com",
		"type" : "policy",
		"policyID" : "1000002",
		"pluginID" : "-1",
		"zoneID" : "-1",
		"dhcpTracking" : "false",
		"classifyMitigatedAge" : "0",
		"emailOnLaunch" : "false",
		"emailOnFinish" : "false",
		"timeoutAction" : "import",
		"scanningVirtualHosts" : "false",
		"rolloverType" : "template",
		"status" : "0",
		"createdTime" : "1406815242",
		"modifiedTime" : "1406815242",
		"maxScanTime" : "3600",
		"ownerGID" : "0",
		"reports" : [],
		"assets" : [],
		"credentials" : [],
		"numDependents" : "0",
		"schedule" : {
			"id" : "17",
			"dependentID" : "14",
			"objectType" : "scan",
			"type" : "dependent",
```

```
                "start" : "",
                "repeatRule" : "",
                "enabled" : "true",
                "nextRun" : 0,
                "dependent" : {
                        "id" : "14",
                        "name" : "Daily IP Scan",
                        "description" : "",
                        "status" : "1024"                                    }
        },
        "policy" : {
                "id" : "1000002",
                "name" : "POST TEST",
                "description" : "Test of post for use with scan post t
                "uuid" : "29F2B9E1-ADE9-4550-B63C-CEA1423E52FC"
        "pluginPrefs" : [],
        "creator" : {
                "id" : "1",
                "username" : "head3",
                "firstname" : "",
                "lastname" : "",
                "uuid" : "96F2AD1B-1B83-462E-908A-84E6054F6B64"
    },
        "owner" : {
                "id" : "1",
                "username" : "head3",
                "firstname" : "",
                "lastname" : "",
                "uuid" : "96F2AD1B-1B83-462E-908A-84E6054F6B64"
        "repository" : {
                "id" : "2",
                "name" : "test",
                "description" : "test",
```

```
                        "type" : "Local",
                        "dataFormat" : "IPv4",
                        "uuid" : "A2FF7E13-2C0E-470E-A3C9-E077FE065A54"
                "canUse" : "true",
                "canManage" : "true",
                "ownerGroup" : {
                        "id" : "0",
                        "name" : "Full Access",
                        "description" : "Full Access group"             },
                "uuid" : "29F2B9E1-ADE9-4550-B63C-CEA1423E52FC" },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1406815242
}
```


/wasScan/{id}

/wasScan/{uuid}

Methods

GET

Gets the WAS Scan associated with {id} or {uuid}.

NOTE: Although a Scan's Schedule 'dependentID' is stored as the schedule ID of the object a scan is dependent upon in the database, it is sent from and returned to the user as the ID of the actual scan object.

Fields Parameter

Expand

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields

*id
*uuid
**name
**description
**status
**ipList
**urlList
**type
****policy**
****plugin**
****repository**
**canUse
**canManage
****zone**
**dhcpTracking
**classifyMitigatedAge
**emailOnLaunch
**emailOnFinish
**timeoutAction
**scanningVirtualHosts
**rolloverType
**createdTime
**modifiedTime
****ownerGroup**
****creator**
****owner**
****reports**
****assets**
****credentials**
**numDependents
****schedule**
****policy**
****policyPrefs**
**maxScanTime

Legend

** = always comes back*

*** = comes back if fields list not specified on GET*

redFont = *field is a JSON object (**e.g.** "repository" :{ "id" : <id>, "name" : <name> })*

Request Parameters

None

Expand Parameters

credentials

Example Response

Expand


```
{
        "type" : "regular",
        "response" : {
                "id" : "4",
                "name" : "POSTtest",
                "description" : "This is a test for POST",
                "ipList" : "",
                "urlList" : "http://example.com",
                "type" : "policy",
                "dhcpTracking" : "false",
                "classifyMitigatedAge" : "0",
                "emailOnLaunch" : "false",
                "emailOnFinish" : "false",
                "timeoutAction" : "import",
                "scanningVirtualHosts" : "false",
                "rolloverType" : "template",
                "status" : "0",
                "createdTime" : "1406815242",
                "modifiedTime" : "1406815242",
                "reports" : [],
```

```
"assets" : [],
"numDependents" : "0",
"schedule" : {
        "id" : "17",
        "dependentID" : "14",
        "objectType" : "scan",
        "type" : "dependent",
        "start" : "",
        "repeatRule" : "",
        "enabled" : "true",
        "nextRun" : 0,
        "dependent" : {
                "id" : "14",
                "name" : "Daily IP Scan",
                "description" : "",
                "status" : "1024"                    }
},
"policy" : {
        "id" : "1000002",
        "name" : "POST TEST",
        "description" : "Test of post for use with scan post t
        "uuid" : "2E950182-08B6-4737-830B-4ACC8F6B92F9"
"policyPrefs" : [],
"repository" : {
        "id" : "2",
        "name" : "test",
        "description" : "test",
        "type" : "Local",
        "dataFormat" : "IPv4",
        "uuid" : "A2FF7E13-2C0E-470E-A3C9-E077FE065A54"
"canUse" : "true",
"canManage" : "true",
"ownerGroup" : {
```

```
                        "id" : "0",
                        "name" : "Full Access",
                        "description" : "Full Access group"             },
                "creator" : {
                        "id" : "1",
                        "username" : "head3",
                        "firstname" : "",
                        "lastname" : "",
                        "uuid" : "96F2AD1B-1B83-462E-908A-84E6054F6B64"
                "owner" : {
                        "id" : "1",
                        "username" : "head3",
                        "firstname" : "",
                        "lastname" : "",
                        "uuid" : "96F2AD1B-1B83-462E-908A-84E6054F6B64"
                "uuid" : "29F2B9E1-ADE9-4550-B63C-CEA1423E52FC" },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1406828664
}
```


PATCH

Edits the WAS Scan associated with {id} or {uuid}, changing only the passed in fields.

NOTE: A WAS Scan's 'type' parameter cannot be changed.

Request Parameters

(All fields are optional)

See /wasScan::POST for parameters.

Example Response

See /wasScan/{id}::GET

DELETE

Deletes the WAS Scan associated with {id} or {uuid}, depending on access and permissions.

Request Parameters

None

Example Response

Expand

```
{
        "type" : "regular",
        "response" : "",
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1406732180
}
```

/wasScan/{id}/copy

/wasScan/{uuid}/copy

Methods

POST

Copies the WAS Scan associated with {id} or {uuid}, depending on access and permissions.

Request Parameters

Expand

```
{
        "name" : <string>,
        "targetUser" : {
                "id" : <number> | "uuid" : <string>     }
}
```

Example Response

Expand

```
{
	"type" : "regular",
	"response" : {
		"scan" : {
			"id" : "4",
			"name" : "POSTtest",
			"description" : "This is a test for POST",
			"ipList" : "",
			"urlList" : "http://example.com",
			"type" : "policy",
			"dhcpTracking" : "false",
			"classifyMitigatedAge" : "0",
			"emailOnLaunch" : "false",
			"emailOnFinish" : "false",
			"timeoutAction" : "import",
			"scanningVirtualHosts" : "false",
			"rolloverType" : "template",
			"status" : "0",
			"createdTime" : "1406815242",
			"modifiedTime" : "1406815242",
			"reports" : [],
			"assets" : [],
			"numDependents" : "0",
			"schedule" : {
				"id" : "17",
				"dependentID" : "14",
				"objectType" : "scan",
				"type" : "dependent",
				"start" : "",
				"repeatRule" : "",
				"enabled" : "true",
				"nextRun" : 0,
				"dependent" : {
```

```
                        "id" : "14",
                        "name" : "Daily IP Scan",
                        "description" : "",
                        "status" : "1024"
                },
                "policy" : {
                        "id" : "1000002",
                        "name" : "POST TEST",
                        "description" : "Test of post for use with sca
                        "uuid" : "2E950182-08B6-4737-830B-4ACC8F6B92F9
                "policyPrefs" : [],
                "repository" : {
                        "id" : "2",
                        "name" : "test",
                        "description" : "test",
                        "type" : "Local",
                        "dataFormat" : "IPv4",
                        "uuid" : "A2FF7E13-2C0E-470E-A3C9-E077FE065A54
                "canUse" : "true",
                "canManage" : "true",
                "ownerGroup" : {
                        "id" : "0",
                        "name" : "Full Access",
                        "description" : "Full Access group"
                "creator" : {
                        "id" : "1",
                        "username" : "head3",
                        "firstname" : "",
                        "lastname" : "",
                        "uuid" : "96F2AD1B-1B83-462E-908A-84E6054F6B64
                "owner" : {
                        "id" : "1",
                        "username" : "head3",
```

```
                                "firstname" : "",
                                "lastname" : "",
                                "uuid" : :"96F2AD1B-1B83-462E-908A-84E6054F6B
                        "uuid" : "29F2B9E1-ADE9-4550-B63C-CEA1423E52FC"
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1406750971
}
```


/wasScan/{id}/launch

/wasScan/{uuid}/launch

Methods

POST

Launches the WAS Scan associated with {id} or {uuid}.

Request Parameters

NOTE: "diagnosticTarget" and "diagnosticPassword" are both optional, but must be provided together if present.

Expand


```
{
        "diagnosticTarget" : <string> (Valid IP/Hostname),
        "diagnosticPassword" : <string> (Non empty String)
}
```


Example Response

Expand

```
{
        "type" : "regular",
        "response" : {
                "scanID" : "2",
                "scanResult" : {
                        "initiatorID" : "1",
                        "ownerID" : "1",
                        "scanID" : "2",
                        "resultsSyncID" : -1,
                        "jobID" : "143301",
                        "repositoryID" : "1",
                        "name" : "test",
                        "description" : "",
                        "details" : "Plugin #",
                        "status" : "Queued",
                        "downloadFormat" : "v2",
                        "dataFormat" : "IPv4",
                        "resultType" : "active",
                        "id" : "3"              }
        },
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1407510276
}
```


Atlassian

Tenable Security Center API: WAS Scanner

These endpoints may only be used by administrators.

/wasScanner

Methods

GET

Gets the list of WAS Scanners.

NOTE: This call will return all WAS Scanners for an Administrator.

Fields Parameter

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields (Admin User)

*id
**name
**description
**enabled

**status
**version
**ips
lastLinkedOn
lastCheckinTime
createdTime
modifiedTime

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

Request Query Parameters

None

Example Response

```
{
        "type": "regular",
```

```
        "response": [
                {
                        "id": "1",
                        "name": "WAS Scanner",
                        "description": "Description of WAS Scanner",
                        "status": "0",
                        "version": "1.0.1",
                        "ips": "10.0.0.0"
                },
                {
                        "id": "2",
                        "name": "New WAS Scanner",
                        "description": "Updated WAS Scanner",
                        "status": "1",
                        "version": "1.2.3",
                        "ips": "10.0.0.1,10.0.0.2"
                }
        ],
        "error_code": 0,
        "error_msg": "",
        "warnings": [],
        "timestamp": 1727369687
}
```


/wasScanner/{id}

Methods

GET

Gets the WAS Scanner associated with {id}.

NOTE: This call will return WAS Scanner associated with {id} for an Administrator.

Fields Parameter

The *fields* parameter should be specified along the query string, and it takes the syntax

```
?fields=<field>,...
```

Allowed Fields (Admin User)

*id
**name
**description
**enabled

**status
**version
**ips
lastLinkedOn
lastCheckinTime
createdTime
modifiedTime

Legend

** = always comes back*

*** = comes back if fields list not specified on GET all*

Request Query Parameters

None

Example Response

```
{
        "type": "regular",
        "response": {
                "id": "7",
                "name": "WAS Scanner 7 Updated",
                "description": "description update",
                "enabled": "true",
```

```
                "version": null,
                "pluginSet": null,
                "status": "0",
                "linkedOn": "1726683642",
                "lastCheckinTime": "1726683642",
                "ips": "10.1.1.1,10.1.1.2,10.1.1.3",
                "createdTime": "1726683642",
                "modifiedTime": "1727100479"
        },
        "error_code": 0,
        "error_msg": "",
        "warnings": [],
        "timestamp": 1727369700
}
```


PATCH

Edits the WAS Scanner associated with {id}, changing only the passed in fields.

Request Parameters

```
{
        "name": "Was Scanner update",
        "description": "description update",
        "enabled": "true" // false
}
```

Example Response

See /wasScanner/{id}::GET

DELETE

Deletes the WAS Scanner associated with {id}.

Request Parameters

None

Example Response

```
{
        "type" : "regular",
        "response" : "",
        "error_code" : 0,
        "error_msg" : "",
        "warnings" : [],
        "timestamp" : 1402436001
}
```

Atlassian