## Contents

**Tenable.sc API: Overview**  
- Getting Started .................................................. 13  
- Structure of the REST URIs ................................... 13  
- Authentication .................................................... 14

**Changelog**  
- Version 5.19.x .................................................. 14  
- Version 5.18.x .................................................. 16  
- Version 5.17.x .................................................. 18  
- Version 5.16.x .................................................. 20  
- Version 5.15.x .................................................. 21  
- Version 5.14.x .................................................. 21  
- Version 5.13.x .................................................. 22  
- Version 5.12.x .................................................. 23  
- Version 5.11.x .................................................. 25  
- Version 5.10.x .................................................. 25

**Accept Risk Rule**  
- `/acceptRiskRule` ............................................... 27  
- `/acceptRiskRule/{id}` ......................................... 32  
- `/acceptRiskRule/apply` ....................................... 35

**Agent Results Sync**  
- `/agentResultsSync` .............................................. 36  
- `/agentResultsSync/{id}` ...................................... 41  
- `/agentResultsSync/{id}/copy` ............................... 45  
- `/agentResultsSync/{id}/launch` ............................ 48
Alert
/alert ........................................ 50
/alert/{id} ................................ 59
/alert/{id}/execute .................. 66

Analysis
/analysis .................................. 72
/analysis/download .................. 79

ARC
/arc ......................................... 83
/arc/{id} .................................. 91
/arc/import .............................. 96
/arc/{id}/export ...................... 96
/arc/{id}/copy ......................... 97
/arc/{id}/refresh .................... 98
/arc/{id}/share ....................... 98

ARC Template
/arctemplate ................................ 100
/arctemplate/{id} .................. 102
/arctemplate/{templateID}/image 105
/arctemplate/categories ........ 105

Asset
/asset ........................................ 107
/asset/{id} ................................ 124
/asset/import .......................... 132
/asset/{id}/export .................. 134
/asset/{id}/refresh ................ 135
/asset/testLDAPQuery .............. 136
/asset/{id}/share .................... 137
/asset/tag .............................. 139

Asset Template
/assetTemplate ....................... 141
Configuration Section
/configSection ........................................ 250
/configSection/{id} .................................... 252

Credential
/credential ............................................. 254
/credential/{id} ........................................ 273
/credential/{id}/share ............................... 278
/credential/tag ....................................... 280

Current Organization
/currentOrganization ............................... 282

Current User
/currentUser ........................................ 284
/currentUser/associateCert ....................... 292
/currentUser/preferences ......................... 292
/currentUser/switch .................................. 295

Custom Plugins
/customPlugins ....................................... 297
/customPlugins/{type}/process .................... 298

Dashboard Component
/dashboard/{dID}/component ....................... 300
/dashboard/{dID}/component/{cID} .................. 310
/dashboard/{dID}/component/{cID}/copy .......... 314
/dashboard/{dID}/component/{cID}/refresh ...... 317

Dashboard Tab
/dashboard ............................................ 321
/dashboard/{id} ....................................... 327
/dashboard/{id}/copy .................................. 331
/dashboard/import ..................................... 334
/dashboard/{id}/export ........................... 337
/dashboard/{id}/share ............................... 340
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dashboard Template</td>
<td>343</td>
</tr>
<tr>
<td>/dashboardTemplate</td>
<td>343</td>
</tr>
<tr>
<td>/dashboardTemplate/{id}</td>
<td>356</td>
</tr>
<tr>
<td>/dashboardTemplate/{templateID}/image</td>
<td>362</td>
</tr>
<tr>
<td>/dashboardTemplate/categories</td>
<td>362</td>
</tr>
<tr>
<td>Device Information</td>
<td>365</td>
</tr>
<tr>
<td>/deviceInfo</td>
<td>365</td>
</tr>
<tr>
<td>Director Insights</td>
<td>369</td>
</tr>
<tr>
<td>/mgmt/insights</td>
<td>369</td>
</tr>
<tr>
<td>Director Organization</td>
<td>373</td>
</tr>
<tr>
<td>/mgmt/organization</td>
<td>373</td>
</tr>
<tr>
<td>/mgmt/organization/{id}</td>
<td>379</td>
</tr>
<tr>
<td>Director Scan Result</td>
<td>385</td>
</tr>
<tr>
<td>/mgmt/scanResult</td>
<td>385</td>
</tr>
<tr>
<td>/mgmt/scanResult/{id}</td>
<td>390</td>
</tr>
<tr>
<td>/mgmt/scanResult/{id}/email</td>
<td>394</td>
</tr>
<tr>
<td>/mgmt/scanResult/{id}/stop</td>
<td>394</td>
</tr>
<tr>
<td>/mgmt/scanResult/{id}/pause</td>
<td>397</td>
</tr>
<tr>
<td>/mgmt/scanResult/{id}/resume</td>
<td>399</td>
</tr>
<tr>
<td>/mgmt/scanResult/{id}/retrieve</td>
<td>402</td>
</tr>
<tr>
<td>/mgmt/scanResult/{id}/download</td>
<td>404</td>
</tr>
<tr>
<td>Director Scan Zone</td>
<td>405</td>
</tr>
<tr>
<td>/mgmt/zone</td>
<td>405</td>
</tr>
<tr>
<td>/mgmt/zone/{id}</td>
<td>408</td>
</tr>
<tr>
<td>Director Scanner</td>
<td>412</td>
</tr>
<tr>
<td>/mgmt/scanner</td>
<td>412</td>
</tr>
<tr>
<td>/mgmt/scanner/{id}</td>
<td>418</td>
</tr>
<tr>
<td>Director System</td>
<td>423</td>
</tr>
<tr>
<td>/mgmt/system/logFiles</td>
<td>423</td>
</tr>
<tr>
<td>/mgmt/system/logs</td>
<td>425</td>
</tr>
<tr>
<td>Section</td>
<td>Path</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------------------------------</td>
</tr>
<tr>
<td>Feed</td>
<td>/feed</td>
</tr>
<tr>
<td></td>
<td>/feed/{type}</td>
</tr>
<tr>
<td></td>
<td>/feed/{type}/update</td>
</tr>
<tr>
<td></td>
<td>/feed/{type}/process</td>
</tr>
<tr>
<td>File</td>
<td>/file/upload</td>
</tr>
<tr>
<td></td>
<td>/file/clear</td>
</tr>
<tr>
<td>Freeze Window</td>
<td>/freeze</td>
</tr>
<tr>
<td></td>
<td>/freeze/{id}</td>
</tr>
<tr>
<td>Group</td>
<td>/group</td>
</tr>
<tr>
<td></td>
<td>/group/{id}</td>
</tr>
<tr>
<td>Job</td>
<td>/job</td>
</tr>
<tr>
<td></td>
<td>/job/{id}</td>
</tr>
<tr>
<td></td>
<td>/job/{id}/kill</td>
</tr>
<tr>
<td>LCE</td>
<td>/lce</td>
</tr>
<tr>
<td></td>
<td>/lce/authorize</td>
</tr>
<tr>
<td></td>
<td>/lce/{id}</td>
</tr>
<tr>
<td></td>
<td>/lce/{id}/authorize</td>
</tr>
<tr>
<td></td>
<td>/lce/eventTypes</td>
</tr>
<tr>
<td>LCE Client</td>
<td>/lce/{id}/client</td>
</tr>
<tr>
<td></td>
<td>/lce/{id}/client/types</td>
</tr>
<tr>
<td></td>
<td>/lce/{id}/client/osTypes</td>
</tr>
<tr>
<td></td>
<td>/lce/{serverID}/client/{clientID}</td>
</tr>
<tr>
<td></td>
<td>/lce/{serverID}/client/{clientID}/authorize</td>
</tr>
<tr>
<td></td>
<td>/lce/{serverID}/client/{clientID}/revoke</td>
</tr>
</tbody>
</table>
LCE Policy 491
/lce/{id}/policy ......................................................... 491

LDAP 500
/ldap ................................................................. 500
/ldap/{id} ............................................................ 504
/ldap/{id}/query .................................................... 507
/ldap/test ............................................................. 508
/ldap/{id}/test ........................................................ 509

Lumin 511
/lumin/repositories ................................................ 511
/lumin/assets ........................................................ 513
/lumin/assets/schedule ........................................... 514
/lumin/metrics ...................................................... 515
/lumin/test ............................................................ 516

MDM 517
/mdm ................................................................. 517
/mdm/{id} ............................................................. 519

Notification 521
/notification .......................................................... 521
/notification/{id} .................................................... 523

Organization 525
/organization ........................................................ 525
/organization/{id} .................................................. 535
/organization/{id}/acceptRiskRule .............................. 540
/organization/{id}/recastRiskRule .............................. 543

Organization Security Manager 546
/organization/{orgID}/securityManager ....................... 546
/organization/{orgID}/securityManager/{id} .................. 555

Organization User 561
/organization/{orgID}/user ........................................ 561
<table>
<thead>
<tr>
<th>Path</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>/organization/{orgID}/user/{id}</td>
<td>563</td>
</tr>
<tr>
<td><strong>Passive Scanner (NNM)</strong></td>
<td>568</td>
</tr>
<tr>
<td>/passivescanner</td>
<td>568</td>
</tr>
<tr>
<td>/passivescanner/{id}</td>
<td>573</td>
</tr>
<tr>
<td>/passivescanner/updateStatus</td>
<td>576</td>
</tr>
<tr>
<td><strong>Plugin</strong></td>
<td>578</td>
</tr>
<tr>
<td>/plugin</td>
<td>578</td>
</tr>
<tr>
<td>/plugin/{id}</td>
<td>581</td>
</tr>
<tr>
<td><strong>Plugin Family</strong></td>
<td>588</td>
</tr>
<tr>
<td>/pluginFamily</td>
<td>588</td>
</tr>
<tr>
<td>/pluginFamily/{id}</td>
<td>600</td>
</tr>
<tr>
<td>/pluginFamily/{id}/plugins::GET</td>
<td>601</td>
</tr>
<tr>
<td><strong>Publishing Site</strong></td>
<td>606</td>
</tr>
<tr>
<td>/pubSite</td>
<td>606</td>
</tr>
<tr>
<td>/pubSite/{id}</td>
<td>609</td>
</tr>
<tr>
<td><strong>Query</strong></td>
<td>613</td>
</tr>
<tr>
<td>/query</td>
<td>613</td>
</tr>
<tr>
<td>/query/{id}</td>
<td>632</td>
</tr>
<tr>
<td>/query/{id}/share</td>
<td>636</td>
</tr>
<tr>
<td>/query/tag</td>
<td>638</td>
</tr>
<tr>
<td><strong>Recast Risk Rule</strong></td>
<td>639</td>
</tr>
<tr>
<td>/recastRiskRule</td>
<td>639</td>
</tr>
<tr>
<td>/recastRiskRule/{id}</td>
<td>644</td>
</tr>
<tr>
<td>/recastRiskRule/apply</td>
<td>647</td>
</tr>
<tr>
<td><strong>Report</strong></td>
<td>649</td>
</tr>
<tr>
<td>/report</td>
<td>649</td>
</tr>
<tr>
<td>/report/{id}</td>
<td>654</td>
</tr>
<tr>
<td>/report/{id}/copy</td>
<td>657</td>
</tr>
<tr>
<td>/report/{id}/email</td>
<td>658</td>
</tr>
<tr>
<td>/report/{id}/stop</td>
<td>659</td>
</tr>
</tbody>
</table>
/report/[id]/send ................................................. 659

**Report Definition** 661
/reportDefinition ............................................. 661
/reportDefinition/[id] ........................................ 681
/reportDefinition/[id]/launch ................................ 687
/reportDefinition/[id]/copy .................................. 688
/reportDefinition/[id]/export ............................... 691
/reportDefinition/import .................................... 692

**Report Image** 693
/report/image ................................................ 693
/report/image/[id] ........................................... 695

**Report Template** 699
/reportTemplate .............................................. 699
/reportTemplate/[id] ......................................... 701
/reportTemplate/[templateID]/image/[sequenceID] .... 703
/reportTemplate/categories ................................ 704

**Repository** 706
/repository ..................................................... 706
/repository/[id] .............................................. 714
/repository/[id]/acceptRiskRule ......................... 719
/repository/[id]/recastRiskRule ......................... 722
/repository/[id]/assetIntersections ..................... 724
/repository/[id]/import .................................... 726
/repository/[id]/export .................................... 727
/repository/[id]/sync ...................................... 728
/repository/[id]/updateMobileData ....................... 729
/repository/[id]/deviceInfo ............................... 730
/repository/authorize ..................................... 733
/repository/authorize ..................................... 734

**Role** 740
/role .......................................................... 740
/role/{id} ................................................................. 753

SAML 758
/saml ........................................................................ 758
/saml/{id} .................................................................. 759
/saml/getMetadata ..................................................... 762

Scan 763
(scan ........................................................................ 763
/scan/{id} .................................................................. 770
/scan/{id}/copy .......................................................... 775
/scan/{id}/launch ......................................................... 778

Scanner 780
/scanner ..................................................................... 780
/scanner/{id} ................................................................ 786
/scanner/{id}/testScansQuery ..................................... 790
/scanner/{id}/bug-report ............................................. 791
/scanner/{id}/health .................................................... 792
/scanner/updateStatus ................................................. 794

Scan Policy 796
/policy ........................................................................ 796
/policy/{id} ................................................................ 812
/policy/{id}/copy ......................................................... 823
/policy/{id}/export ....................................................... 824
/policy/{id}/share ........................................................ 824
/policy/import ............................................................. 831
/policy/tag ................................................................ 832

Scan Policy Templates 833
/policyTemplate .......................................................... 833
/policyTemplate/{id} .................................................... 835

Scan Result 838
/scanResult .................................................................. 838
/scanResult/{id} .......................................................... 841
/scanResult/{id}/copy .................................................. 847
/scanResult/{id}/email ............................................... 848
/scanResult/import .................................................. 848
/scanResult/{id}/import ........................................... 849
/scanResult/{id}/stop ............................................... 850
/scanResult/{id}/pause ............................................. 853
/scanResult/{id}/resume ........................................... 855
/scanResult/{id}/download ........................................ 857

Scan Zone 859
/zone ................................................................. 859
/zone/{id} .......................................................... 862

Solutions 866
/solutions ......................................................... 866
/solutions/{pluginID} ............................................. 867
/solutions/{pluginID}/vuln ........................................ 868
/solutions/{pluginID}/asset ....................................... 869

SSHKey 871
/sshKey ............................................................ 871
/sshKey/download .................................................. 873
/sshKey/installRemoteKey ........................................ 874

Status 875
/status ............................................................... 875

Style 878
/style ............................................................... 878
/style/{id} .......................................................... 878

StyleFamily 880
/styleFamily ...................................................... 880
/styleFamily/{id} .................................................. 880

System 882
/system .............................................................. 882
Tenable.sc API: Overview

This is the reference document for the REST API and resources provided by Tenable.sc (formerly SecurityCenter). The REST APIs are for developers who want to integrate Tenable.sc with other standalone or web applications, and administrators who want to script interactions with the Tenable.sc server. For more information about a particular endpoint, click on its name in the navigation bar. You’ll be taken to the endpoint’s documentation page, which includes what query parameters the endpoint will accept, what the JSON object’s parameters will be in the response, and an example query/response.

Please note that whenever Tenable extends the protocol or implementation, we may not be able to maintain backward compatibility; consequently, some APIs will change in either structure or functionality. Therefore,
this document comes with NO GUARANTEE OF FUTURE COMPATIBILITY. Additionally, since these APIs are used for customizations, Tenable cannot support customers with their specific implementations. If you require assistance with design or implementation, please contact your account manager for information on how Tenable Professional Services can provide assistance.

If you are interested in using the API to provide a joint solution for customers, please consider becoming a Tenable Alliance Partner; you can find details at www.tenable.com/partners.

**Getting Started**

Because the REST API is based on open standards, you can use any web development language to access the API.

**Structure of the REST URIs**

Tenable.sc REST APIs provide access to resources (data entities) via URI paths. To use a REST API, your application will make an HTTP request and parse the response. The Tenable.sc REST API uses JSON as its communication format, and the standard HTTP methods like GET, PUT, POST and DELETE (see API descriptions below for which methods are available for each resource).

URIs for SecurityCenter's REST API resource have the following structure:

```
http://host:port/rest/resource-name
```

Return all available objects of type resource. **All** non-expansion fields are included:

```
/resource
```

Return object with ID. **All** non-expansion fields are included:

```
/resource/{id}
```

Appended to GET requests, reply should only include the listed fields:

```
?fields=field1,field2,...
```

Return all **editable** fields for requested object:

```
?editable
```

Appended to GET requests, reply should include requested expansion data, in addition to normally returned data:
Possible expansion data includes shares for shareable objects, IP data for assets, i.e. data that is not normally needed.

**Authentication**

Most Tenable.sc API REST calls require authentication via a unique set of API keys. The ‘x-apikey’ header element is used to pass your API keys in HTTP request messages.

The ‘x-apikey’ header element has the following format, where the ‘ACCESS_KEY’ and ‘SECRET_KEY’ parameters correspond to the API keys that Tenable.sc generates for each system user:

```
x-apikey: accesskey=ACCESS_KEY; secretkey=SECRET_KEY;
```

For more information about API key authorization, see API Key Authorization in the *Tenable.sc API Best Practices Guide*.

**Changelog**

**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` parameter is 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.
- **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) ldapUser-Sync, 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 “sum-remediation” 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, IceVulnsLifetime, 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, IceVulnsLifetime, 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 Databases.
  - Added support for a new Credential type, Apache Cassandra, available for Databases.
  - 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, /scanner: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.sc:

• 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.sc:

• IP Information
  - The /iplInfo::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/iplInfo::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
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*

*
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:

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" : ""
      },
      "organization" : {
        "id" : "8",
        "name" : "Org",
        "description" : "Testing for Policies with New Schema"  
    }
  ]
}
POST

Adds an Accept Risk Rule to one repository.

Request Parameters

Expand

{"repositories": [
  {
    "id": <number>
  },
  ...
],
"plugin": {
  "id": <number>
},
"user": {
  "id": "1",
  "username": "head",
  "firstname": "Security Manager",
  "lastname": ""
},
"plugin": {
  "id": "0",
  "name": "Open Port",
  "description": ""
}
},
"error_code": 0,
"error_msg": ",
"warnings": [],
"timestamp": 1410275054
}
"hostType" : <string> "all" | "asset" | "ip" | "uuid",
"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>
...  

**Example Response**

Expand

{  
  "type" : "regular",
  "response" : [

{
    "id" : "3",
    "repID" : "17",
    "orgID" : "8",
    "userID" : "1",
    "pluginID" : "0",
    "hostType" : "all",
    "hostValue" : "",
    "port" : "any",
    "protocol" : "any",
    "comments" : "",
    "expires" : "-1",
    "status" : "0",
    "createdTime" : "1410275013",
    "modifiedTime" : "1410275013",
    "repository" : {
        "id" : "17",
        "name" : "New Fields Repo",
        "description" : ""
    },
    "organization" : {
        "id" : "8",
        "name" : "Org",
        "description" : "Testing for Policies with New Schema"
    },
    "user" : {
        "id" : "1",
        "username" : "head",
        "firstname" : "Security Manager",
        "lastname" : ""
    },
    "plugin" : {
        "id" : "0",
        "name" : "Open Port",
        "description" : ""
    }
}
/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**

**Request Query Parameters**
None

**Example Response**
Expand

```json
{
    "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": ""
        },
        "organization": {
            "id": "8",
            "name": "",
            "description": ""
        }
    }
}
```
"name" : "Org",
"description" : "Testing for Policies with New Schema"
},
"user" : {
"id" : "1",
"username" : "head",
"firstname" : "Security Manager",
"lastname" : ""
},
"plugin" : {
"id" : "0",
"name" : "Open Port",
"description" : ""
}
"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
}
Agent Results Sync

/agentResultsSync

Methods

GET

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
eemailOnLaunch
eemailOnFinish
createdTime
modifiedTime
ownerGroup
creator
owner
reports
numDependents
schedule
lastDownloadSuccess
downloadResultsAfter
Legend

* = always comes back

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

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

```json
{
    "type" : "regular",
    "response" : {
        "usable" : [
            {
                "id" : "2",
                "name" : "test",
                "description" : ""
            },
            {
                "id" : "3",
                "name" : "test2",
                "description" : ""
            }
        ]
    }
}
```
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 synchroniz-
ing results from agents. Any results before that timestamp will not be imported. The field is ONLY accepted during POST (Not PATCH).

**Request Parameters**

Expand

```json
{
    "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" | "individual" | "lce" | "archive" | "mobile"
        }...
    ],
    "emailOnLaunch" : <string> "false" | "true" DEFAULT "false",
    "emailOnFinish" : <string> "false" | "true" DEFAULT "false"
}
```

schedule type is "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" : "4",
        "creatorID" : "1",
        "ownerID" : "1",
        "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",
        }
    }
}
{"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

**Request Parameters**

None

**Expand Parameters**

credentials

**Example Response**

Expand

```json
{
    "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"
},
"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 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

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

Example Response
Expand

```json
{
  "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, please do not enable zone",
},
"repository" : {
  "id" : "14",
  "name" : "John's Test IPv4 Rep",
  "description" : ""
},
"ownerGroup" : {
  "id" : "0",
  "name" : "Full Access",
  "description" : "Full Access group"
},
"creator" : {
  "id" : "1",
  "username" : "sm",
  "firstname" : "Security",
  "lastname" : "Manager"
},
"owner" : {
  "id" : "2",
  "username" : "qahead",
  "firstname" : ",",
  "lastname" : ""
}
},
"error_code" : 0,
"error_msg" : "",
"warnings" : []}
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
}
Alert

>alert

Methods

GET

GETs the list of Alerts.

Fields Parameter

Expand

The \texttt{fields} parameter should be specified along the query string, and it takes the syntax

\texttt{?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**

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" : "Manageable Alert 1",
                "description" : "Manageable alerts description",
                "status" : "1"
            }
        ]
    }
}
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"
    type "ical"
    -----------
    "start" : <string> (This value takes the iCal format),
    "repeatRule" : <string> (This value takes the repeat rule format)
},
"action" : [
    {
        "type" : <string> "email" | "notification" | "report" | "scan" | "syslog"
        type "email"
        -----------
        "subject" : <string>,
        "message" : <string> DEFAULT "",
        "addresses" : <string> (valid email addresses separated by ' \n') DEFAULT "",
        "users" : [
            {
                "id" : <number>
            }...
        ] DEFAULT [],
        "includeResults" : <string> "false" | "true" DEFAULT "true"
        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" | "Warning"

type "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" : "Security Manager",
          "lastname" : ""
        }
      ],
      "includeResults" : "true"
    },
    "objectId" : "-1",
    "status" : "0",
    "users" : [
      {
        "id" : "1",
        "username" : "head",
        "firstname" : "Security Manager",
        "lastname" : ""
      }
    ]
  }
]
"firstname": "Security Manager",
"lastname": ""
}
]
],
{
"id": "62",
"type": "notification",
"definition": {
"message": "Test Notification Action",
"users": [
{
"id": "1",
"username": "head",
"firstname": "Security Manager",
"lastname": ""
}
]
},
"objectID": "-1",
"status": "0",
"users": [
{
"id": "1",
"username": "head",
"firstname": "Security Manager",
"lastname": ""
}
]
],
"id": "63",
"type": "report",
"definition": {
"reportID": "11",
"users": [
{
"id": "1",
"username": "head",
"firstname": "Security Manager",
"lastname": ""
}
]
"report" : {
    "id" : -1,
    "name" : "",
    "description" : ""
}
",
"objectID" : "11",
"status" : "0",
"users" : []
},
{
  "id" : "64",
  "type" : "scan",
  "definition" : {
    "scanID" : "60",
    "scan" : {
      "id" : "60",
      "name" : "Test Scan",
      "description" : "Used for Alert - needs to be default template"
    }
  }
},
"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" : "",

],
"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" : ""
},
"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
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**

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": "Security Manager",              "lastname": ""            }          ],          "includeResults": "true"        },        "objectId": "-1"      }    ]  }}
"status": "0",
"users": [
  {
    "id": "1",
    "username": "head",
    "firstname": "Security Manager",
    "lastname": ""
  }
]
],
{
"id": "62",
"type": "notification",
"definition": {
  "message": "Test Notification Action",
  "users": [
    {
      "id": "1",
      "username": "head",
      "firstname": "Security Manager",
      "lastname": ""
    }
  ]
},
"objectId": "-1",
"status": "0",
"users": [
  {
    "id": "1",
    "username": "head",
    "firstname": "Security Manager",
    "lastname": ""
  }
]
},
}
{  
    "id" : "63",
    "type" : "report",
    "definition" : {  
        "reportID" : "11",
        "report" : {  
            "id" : -1,
            "name" : ",",
            "description" : ","
        }
    },
    "objectID" : "11",
    "status" : "0",
    "users" : []
},
{  
    "id" : "64",
    "type" : "scan",
    "definition" : {  
        "scanID" : "60",
        "scan" : {  
            "id" : "60",
            "name" : "Test Scan",
            "description" : "Used for Alert - needs to be default template"
        }
    },
    "objectID" : "60",
    "status" : "0",
    "users" : []
},
{  
    "id" : "65",
    "type" : "syslog",
    "definition" : {  
        "host" : "127.0.0.1",
        "port" : "514",
        "protocol" : "udp",
        "formatter" : "default"
    }
}
"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 Manager",
            "lastname" : ","
        }
    },
    "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" : ""
},
"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"
            }
          ],
          "includeResults": "true"
        },
        "objectID": "-1",
      }
    ]
  }
}
"status" : "0",
"subject" : "Test Email Action",
"message" : "",
"addresses" : "",
"users" : [
    {
        "id" : "1"
    }
],
"includeResults" : "true"
],
"id" : "2",
"type" : "notification",
"definition" : {
    "message" : "Test Notification Action",
    "users" : [
        {
            "id" : "1"
        }
    ]
},
"objectID" : "-1",
"status" : "0",
"message" : "Test Notification Action",
"users" : [
    {
        "id" : "1"
    }
],
"id" : "3",
"type" : "report",
"definition" : {

null
"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"
      },
      "name": "",
      "description": "",
      "notes": ""
   },
   "objectId": "-1",
   "status": "0",
   "assignee": {
      "id": "1"
   },
   "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" : ""
},
"ownerGroup" : {
    "id" : "0",
    "name" : "Full Access",
    "description" : "Full Access group"
}
},
"error_code" : 0,
"error_msg" : "",
"warnings" : [],
"timestamp" : 1424975475}
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:

```json
{
    "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**

```json
{
    "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)
}
```

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

```json
{
    "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)
}
```

**Source Type**

```json
"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),
"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" : "keywords",
        "operator" : ""
      }
    ]
  }
}
"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**
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 Maturity",
    "value" : "Unproven",
    "type" : "string"
},
{
    "id" : "predicted_impactScore",
    "name" : "Predicted Impact Score",
    "value" : false,
    "type" : "boolean"
},
{
    "id" : "product_coverage",
    "name" : "Product Coverage",
    "value" : "Low",
    "type" : "string"
},
{
    "id" : "threat_intensity_last_28",
    "name" : "Threat Intensity",
    "value" : "Low",
    "type" : "string"
},
{
    "id" : "threat_recency",
    "value" : "Low",
    "type" : "string"
"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 / 2.154 Multiple Vulnerabilities",
"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 / 2.150.1 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>
}
When the `sourceType` is “individual”, `scanID` and `view` must be provided in the root of the request object:

```json
{
    "type": "vuln",
    "query": {
        "id": <number> | (valid query)
    },
    "sourceType": "individual",
    "sortDir": "ASC" | "DESC" OPTIONAL,
    "sortField": (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**

```json
{
    "type": "event",
    "query": {
```
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.
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
ownergroups
ownerGrouptargetGroup
lastUpdateTime
lastCompletedUpdateTime
lastComplianceUpdateTime
createdTIme
modifiedTIme
focusFiltersschedule
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**

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

```json
{
    "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" : ""
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" | "records",
      "conditionalOperator" : <string> "Any" | "No" | "All" | "">
      "<" | "\>
      "displayType" : <string> "percentage" | "ratio" | "state",
      "baseFilters" : [
      
      ]
   ]
}
"filterName": <string> (valid Query filterName based on queryType),
"value": (Format depends on filter's "filterName" parameter),
"operator": <string> (Options depend on filter's "filterName" parameter)
] DEFAULT [],
"compliantFilters": [
{
  "filterName": <string> (valid Query filterName based on queryType),
  "value": (Format depends on filter's "filterName" parameter),
  "operator": <string> (Options depend on filter's "filterName" parameter)
},
"drilldownFilters": [
{
  "filterName": <string> (valid Query filterName based on queryType),
  "value": (Format depends on filter's "filterName" parameter),
  "operator": <string> (Options depend on filter's "filterName" parameter)
}
],
"conditionalOperator" is ">" | "<" | ">=" | ">="
------------------------------------------------
"conditionalValue": <number>
,...
],
"focusFilters": [
{
  "operator": <string> ">" | "<" | ">=" | ">=" | ">=",
  "filterName": <string> "asset" | "repository" | "ip",

"filterName" is "asset" and "operator" is ">~"
------------------------------------------------
"value": {

"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" : "",
...
"lastUpdateTime" : "-1",
"lastCompletedUpdateTime" : "-1",
"lastComplianceUpdateTime" : "-1",
"createdTime" : "1413315326",
"modifiedTime" : "1413315326",
"running" : "false",
"focusFilters" : [
  {
    "filterName" : "ip",
    "operator" : "=",
    "value" : "172.26.20.0"
  }
],
"order" : "1",
"groups" : [],
"policyStatements" : [
  {
    "id" : "1",
    "arcID" : "1",
    "label" : "label",
    "baseFilters" : "a:1:{i:0;a:3:{s:8:"operator";s:1:"=";s:10:"filterName";s:2:"ip";s:5:"value";s:7:"172.26.20.0";}}",
    "compliantFilters" : "a:1:{i:0;a:3:{s:8:"operator";s:1:"<";s:10:"filterName";s:13:"repositoryIDs";s:5:"value";s:2:"17";}}",
    "drilldownFilters" : "a:1:{i:0;a:3:{s:8:"operator";s:1:"=";s:10:"filterName";s:7:"assetID";s:5:"value";s:1:"1";}}",
    "baseStatus" : "0",
    "compliantStatus" : "0",
    "drilldownStatus" : "0",
    "conditionalName" : "records",
    "conditionalOperator" : "<=",
    "conditionalValue" : "1",
    "displayType" : "state",
    "result" : ""
  }
],
"baseQuery" : {
  "id" : "15"}
"compliantQuery" : {
  "id" : "16"
},
"drilldownQuery" : {
  "id" : "17"
}
],
"result" : "fail",
"status" : 0,
"schedule" : {
  "id" : "68",
  "type" : "template",
  "start" : "",
  "repeatRule" : "",
  "nextRun" : 0
},
"activated" : "true",
"canUse" : "true",
"canManage" : "true",
"creator" : {
  "id" : "1",
  "username" : "head",
  "firstname" : "Security Manager",
  "lastname" : ""
},
"owner" : {
  "id" : "1",
  "username" : "head",
  "firstname" : "Security Manager",
  "lastname" : ""
},
"ownerGroup" : {
  "id" : "0",
  "name" : "Full Access",
  "90"
"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
ownergroups
ownerGrouptargetGroup
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  

**Request Parameters**  

None  

**Example Response**  

Expand  

{
    "type" : "regular",
    "response" : {
        "id" : "1",
        "name" : "POST TEST",
        "running" : "false",
        "description" : "",
        "lastUpdateTime" : "-1",
        "lastCompletedUpdateTime" : "-1",
        "lastComplianceUpdateTime" : "-1",
        "createdTime" : "1413315326",
        "modifiedTime" : "1413315326",
    
```
"focusFilters" : [
    {
        "filterName" : "ip",
        "operator" : "+",
        "value" : "172.26.20.0"
    }
],
"order" : "1",
"groups" : [],
"policyStatements" : [
    {
        "id" : "1",
        "arcID" : "1",
        "label" : "label",
        "baseFilters" : "a:1:{i:0;a:3:{s:8:"operator";s:1:"=";s:10:"filterName";s:2:"ip";s:5:"value";s:7:"172.26.20.0";}}",
        "compliantFilters" : "a:1:{i:0;a:3:{s:8:"operator";s:1:"<";s:10:"filterName";s:13:"repositoryIDs";s:5:"value";s:2:"17";}}",
        "drilldownFilters" : "a:1:{i:0;a:3:{s:8:"operator";s:1:"=";s:10:"filterName";s:7:"assetID";s:5:"value";s:1:"1";}}",
        "baseStatus" : "0",
        "compliantStatus" : "0",
        "drilldownStatus" : "0",
        "conditionalName" : "records",
        "conditionalOperator" : "<=",
        "conditionalValue" : "1",
        "displayType" : "state",
        "result" : "",
        "resultOutput" : "{}",
        "baseQuery" : {
            "id" : "15"
        },
        "compliantQuery" : {
            "id" : "16"
        },
        "drilldownQuery" : {
            "id" : "17"
        }
    }
]


```json
}
],
"result": "fail",
"status": 0,
"schedule": {
  "id": "68",
  "type": "template",
  "start": "",
  "repeatRule": "",
  "nextRun": 0
},
"activated": "true",
"canUse": "true",
"canManage": "true",
"creator": {
  "id": "1",
  "username": "head",
  "firstname": "Security Manager",
  "lastname": ""
},
"owner": {
  "id": "1",
  "username": "head",
  "firstname": "Security Manager",
  "lastname": ""
},
"ownerGroup": {
  "id": "0",
  "name": "Full Access",
  "description": "Full Access group"
}

"error_code": 0,
"error_msg": "",
"warnings": []
```
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>YToxOntpOjA7YTozOntzOjEwOiJmaWx0ZXJ0aW5nIjtzOjc6ImFzc2V0SWQiO3M6ODoib3BlcmFuZDEiO3M6MTA6Ii0xOlVua25vd24iO3M6ODoib3BlcmFuZDIiO3M6MTA6Ii0xOlVua25v...</focusFilters>
    <policyStatements>
        <policyStatement>
            <label>PS</label>
            <displayType>state</displayType>
            <definition>YTo2OntzOjExOiJiYXNlRmlsdGVycyI7YToxOntpOjA7YTozOntzOjEwOiJmaWx0ZXJOYW1lIjtzOjI6ImlwIjtzOjg6Im9wZXJhdG9yIjtzOjE6Ij0iO3M6NToiaG9zdHMiO3M6MzoiQWxsIjtzOjE2OiJjb25kaXRpb25hbFZhbHVlIjtzOjA6IiI7fQ==</definition>
        </policyStatement>
    </policyStatements>
    <schedule>FREQ=DAILY;INTERVAL=1</schedule>
</arcTemplate>
Copies an existing ARC associated with {id}, depending on access and permissions.

**Request Parameters**

Expand

```json
{
    "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`
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
policyStatementstagsrequirementscategory
minUpgradeVersion
templatePubTime
templateModTime
definitionModTime
createdTime
modifiedTime

Legend*

*

* = always comes back

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

```json
{
   "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

```json
{
   "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

Request Query Parameters
Example Response

```
{
  "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" : "",
"displayText" : "state",
"result" : "",
"resultOutput" : "{}",
"queryType" : "vuln"
"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
}
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
**name
**description
type
ownerGroup

Session user not role “1” (Administrator

**status
creator
owner
targetGroup
groupstemplatetypeFields
type
tags
context
createdTime
modifiedTime
repositories
ipCount
assetDataFields
viewableIPs (requesting this field for all assets may result in slow processing)

Session user not role “1” (Administrator

**organization
luminFields

Legend*
*

* = always comes back

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

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": "",
         "organization": {
            "id": "1",
            "name": "org1",
            "description": "",
         },
      },
      {
         "id": "28",
         "name": "Test 1",
         "description": "",
         "organization": {
            "id": "1",
            "name": "org1",
            "description": "",
         },
      },
      {
         "id": "29",
         "name": "Test 2",
         "description": "",
         "organization": {
            "id": "1",
            "name": "org1",
            "description": "",
         },
      }
   ]
}
"name": "org1",
"description": "",
},
],
[
"id": "30",
"name": "Test 3",
"description": "",
"organization": {
"id": "1",
"name": "org1",
"description": "",
}
],
[
"id": "31",
"name": "10287 TEST",
"description": "",
"organization": {
"id": "1",
"name": "org1",
"description": "",
}
],
[
"id": "32",
"name": "TEST",
"description": "",
"organization": {
"id": "1",
"name": "org1",
"description": "",
}
],
[}
"id" : "33",
"name" : "test",
"description" : "",
"organization" : {
   "id" : "1"
   "name" : "org1",
   "description" : "",
},
},
{
   "id" : "1",
   "name" : "dnsnameTestPost",
   "description" : "",
   "organization" : {
      "id" : "1"
      "name" : "org1",
      "description" : "",
   },
},
{
   "id" : "26",
   "name" : "Test",
   "description" : "",
   "organization" : {
      "id" : "1"
      "name" : "org1",
      "description" : "",
   },
},
{
   "id" : "27",
   "name" : "Test2",
   "description" : "",
   "organization" : {
      "id" : "1"


```

"name" : "org1",
"description" : "",
},
},
{
"id" : "28",
"name" : "Test 1",
"description" : "",
"organization" : {
  "id" :  "1"
  "name" : "org1",
  "description" : "",
}
},
},
{
"id" : "29",
"name" : "Test 2",
"description" : "",
"organization" : {
  "id" :  "1"
  "name" : "org1",
  "description" : "",
}
},
},
{
"id" : "30",
"name" : "Test 3",
"description" : "",
"organization" : {
  "id" :  "1"
  "name" : "org1",
  "description" : "",
}
},

```


"id" : "31",
"name" : "10287 TEST",
"description" : "",
"organization" : {
   "id" : "1"
   "name" : "org1",
   "description" : "",
},
},
{
"id" : "32",
"name" : "TEST",
"description" : "",
"organization" : {
   "id" : "1"
   "name" : "org1",
   "description" : "",
},
},
{
"id" : "33",
"name" : "test",
"description" : "",
"organization" : {
   "id" : "1"
   "name" : "org1",
   "description" : "",
},
}
]
"error_code" : 0,
"error_msg" : "",
"warnings" : [],
"timestamp" : 1412273607
Organization User

Expand

{
  "type": "regular",
  "response": {
    "usable": [
      {
        "id": "1",
        "name": "dnsnameTestPost",
        "description": "",
        "status": "0"
      },
      {
        "id": "28",
        "name": "Test 1",
        "description": "",
        "status": "0"
      },
      {
        "id": "29",
        "name": "Test 2",
        "description": "",
        "status": "0"
      },
      {
        "id": "30",
        "name": "Test 3",
        "description": "",
        "status": "0"
      },
      {
        "id": "31",
        "name": "",
        "description": "",
        "status": "0"
      }
    ]
  }
}
"name" : "10287 TEST",
"description" : "",
"status" : "0"
],
{
 "id" : "32",
 "name" : "TEST",
 "description" : "",
 "status" : "0"
},
{
 "id" : "33",
 "name" : "test",
 "description" : "",
 "status" : "0"
}
],
"manageable" : [
{
 "id" : "1",
 "name" : "dnsnameTestPost",
 "description" : "",
 "status" : "0"
},
{
 "id" : "26",
 "name" : "Test",
 "description" : "",
 "status" : "0"
},
{
 "id" : "27",
 "name" : "Test2",
 "description" : "",
 "status" : "0"
{ "id": "28",
"name": "Test 1",
"description": ":",
"status": "0"
},
{ "id": "29",
"name": "Test 2",
"description": ":",
"status": "0"
},
{ "id": "30",
"name": "Test 3",
"description": ":",
"status": "0"
},
{ "id": "31",
"name": "10287 TEST",
"description": ":",
"status": "0"
},
{ "id": "32",
"name": "TEST",
"description": ":",
"status": "0"
},
{ "id": "33",
"name": "test",
"description": ":",
"status": "0"}
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 empty),
    "fieldValue" : <string> DEFAULT "" (if fieldName not empty)
  }...
] 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" | "intersection" | "union",
  "operand1" : {
    "id" : <number> (asset ID)
  } | <combinationRecord>,

  **operator not "complement"**
  -------------------------

  operand2 : {
    "id" : <number> (asset ID)
  } | <combinationRecord>

}...
type "dynamic"

... 
"rules": { 
  "operator" : <string> "all" | "any",
  "children" : [
  {
    "type" : <string> "clause" | "group",

child type "clause"

"operator" : <string> "contains" | "eq" | "lt" | "lte" | "ne" "gt"
"filterName" : <string> "dns" | "exploitAvailable" | "exploitFrameworks"
"pluginIDConstraint" : <string> (integer or comma-separated range)

filterName "pluginid" | "severity"

"value" : {
  "id" : <number>
},

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" : "2",
"creatorID" : "1",
"ownerID" : "1",
"name" : "test asset",
"type" : "dynamic",
"description" : "description",
"tags" : "",
"context" : "",
"status" : "0",
"templateID" : "35",
"createdTime" : "1401903765",
"modifiedTime" : "1401903765",
"ownerGID" : "0",
"targetGID" : "-1",
"typeFields" : {
"rules" : {
"operator" : "any",
"children" : [
{
"filterName" : "severity",
"operator" : "eq",
"value" : "1",
"pluginIDConstraint" : "-1",
"type" : "clause"
}
],
"type" : "group"
}
},
"ipCount":[
{

122


"repositoryID":"2",
"ipCount":"0",
"ips":[
  "192.168.1.0-192.168.1.255"
],
"repository":{
  "id":"2",
  "name":"QA Range",
  "description":""
}
],

"assetDataFields":[]
"groups" : [],
"canUse" : "true",
"canManage" : "true",
"creator" : {
  "id" : "1",
  "username" : "orghead",
  "firstname" : "test",
  "lastname" : "User"
},
"owner" : {
  "id" : "1",
  "username" : "orghead",
  "firstname" : "test",
  "lastname" : "User"
},
"ownerGroup" : {
  "id" : "0",
  "name" : "Full Access",
  "description" : "Full Access group"
},
"targetGroup" : {
/asset/{id}

Methods

GET

GETs the Asset 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
type
ownerGroup
Session user not role “1” (Administrator)
creator
owner
ownerGroup
targetGroup
groupstemplatetypeFieldsviewableIPs
tags
context
createdTime
modifiedTime
repositories
ipCount
assetDataFields
Session user role “1” (Administrator)
luminFieldsorganization

Legend*
*

*= always comes back

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

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}

{
    "orgID" : <string>
}

Organization User

None
Example Response

Administrator

Expand

{
    "type" : "regular",
    "response" : {
        "id" : "33",
        "name" : "test",
        "type" : "combination",
        "description" : "",
        "organization" : {
            "id" : "1",
            "name" : "org1",
            "description" : "",
        }
        "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
}
null
"id" : "17",
"name" : "New Fields Repo",
"description" : ""
}
},
{
"ipCount" : "0",
"repository" : {
    "id" : "18",
    "name" : "New Rep 1",
    "description" : ""
}
},
{
"ipCount" : "0",
"repository" : {
    "id" : "19",
    "name" : "New Rep 2",
    "description" : ""
}
},
{
"ipCount" : "0",
"repository" : {
    "id" : "20",
    "name" : "New Rep 3",
    "description" : ""
}
},
{
"ipCount" : "0",
"repository" : {
    "id" : "21",
    "name" : "New Rep 4",
    "description" : ""
}


},
{
    "ipCount": "0",
    "repository": {
        "id": "22",
        "name": "New Rep 5",
        "description": ""
    }
},
{
    "ipCount": "0",
    "repository": {
        "id": "23",
        "name": "New Rep 6",
        "description": ""
    }
},
{
    "ipCount": "0",
    "repository": {
        "id": "24",
        "name": "New Rep 7",
        "description": ""
    }
}
],
"ipCount": 0,
"groups": [],
"assetDataFields": [],
"viewableIPs": [
{
    "repository": {
        "id": "37",
        "name": "ag repo1"


},
"ipList" : "192.168.1.1\n",
"ipCount" : "1"
},

{
    "repository" : {
        "id" : "38",
        "name" : "jm ipv4"
    },
    "ipList" : "192.168.1.1\n",
    "ipCount" : "1"
},

{
    "repository" : {
        "id" : "39",
        "name" : "ipv6 rep"
    },
    "ipList" : "",
    "ipCount" : "0"
}
],
"creator" : {
    "id" : "1",
    "username" : "head",
    "firstname" : "Security Manager",
    "lastname" : ""
},
"owner" : {
    "id" : "1",
    "username" : "head",
    "firstname" : "Security Manager",
    "lastname" : ""
},
"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}, changing only the passed in fields.

**Request Parameters**
(All fields are optional)
See /asset::POST for parameters.

**Example Response**
See /asset/{id}::GET

**DELETE**
Deletes the Asset associated with {id}, 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",
            "creatorID" : "1",
            "ownerID" : "1",
            "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=tenablesecurity,DC=com",
                    "searchString" : "(objectclass=Computer)"
                }
            },
            "ipCount" : "",
            "groups" : [],
            "assetDataFields" : [],
            "canUse" : "true",
            "canManage" : "true",
            "creator" : {
                "id" : "1",
                "username" : "testorg",
            }
        }
    ]
}
"firstname" : "first",
"lastname" : "last"
},
"owner" : {
  "id" : "1",
  "username" : "testorg",
  "firstname" : "first",
  "lastname" : "last"
},
"ownerGroup" : {
  "id" : "0",
  "name" : "Full Access",
  "description" : "Full Access group"
},
"targetGroup" : {
  "id" : -1,
  "name" : "",
  "description" : ""
}
],
"error_code" : 0,
"error_msg" : "",
"warnings" : [],
"timestamp" : 1402582394
}

/asset/{id}/export

**GET**

Exports the Asset associated with [id] as plain text XML.

**Request Parameters**

None
Example Response

Expand

```xml
<?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>YT0yOntz0jU6InJ1bGVzIjthOjM6e3M6ODoib3BlcmlzOi03M6MzoiYW55I7czoyOiItMSI7czo0OiJ0eXBlIjtzOjY6ImNsYXVzZSI7fX1zOjQ6InR5cGUiO3M6NToiZ3JvdXAiO31zOjE1OiJhc3NldERhdGFGaWVsZHI=
  </asset>
</assets>
```

/asset/{id}/refresh

POST

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

NOTE: This can only be called by Administrators.

Request Parameters

Expand

```json
{
  "orgID" : <number>,
  "repIDs" : [
    {
      "id" : <number>
    },
    ...
  ]
}
```
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" : {

Example Response

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

/asset/{id}/share

Methods

POST

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

Request Parameters

Expand

```
{  
    "groups" : [  
```
Example Response

Expand

{  "type": "regular",  "response": {
    "id": "1",
    "creatorID": "1",
    "ownerID": "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"}
"last_name" : ""
},
"owner" : {
    "id" : "1",
    "username" : "head",
    "first_name" : "Security Manager",
    "last_name" : ""
},
"owner_group" : {
    "id" : "0",
    "name" : "Full Access",
    "description" : "Full Access group"
},
"target_group" : {
    "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
}


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

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" ... | "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 of the most common

},
{
"id" : "421",
"name" : "Networking Equipment",
"description" : "This asset collection contains many of the assets related to networking, operating systems, collected data, and various enterprise applications."
},
{
"id" : "22",
"name" : "Linux/Unix Operating Systems",
"description" : "Asset lists used to group different distribution of Linux/Unix operating systems. This will be helpful for those getting started with Tenable.sc.

},
{
"id" : "20",
"name" : "Windows Collection",
"description" : "Asset lists used to group windows and related related vulnerabilities. This 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

**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 has been given SMB credentials to log into the remote host, however these credentials do not have administrative privileges. 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. This will be helpful for those getting started with Tenable.sc."
   },
   "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 system configuration data such as patch level and user credentials."
}
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 mechanisms to identify common operating systems.",
         "count":"124",
         "status":""
      },
      {
         "id":"2",
         "name":"Client Applications",
         "description":"Identify systems with client centric applications installed.",
         "count":null,
         "status":""
      }
   ]
}
"count":"48",
"status":""
},

{
"id":"3",
"name":"Server Applications",
"description":"Identify systems with server centric applications such as database services, email services, and directory services.
"count":"31",
"status":""
},

{
"id":"4",
"name":"Virtual Technology",
"description":"Identify systems with virtualization technology or virtual management applications installed.
"count":"9",
"status":""
},

{
"id":"5",
"name":"Infrastructure Technology",
"description":"Identify systems that are used for network communications infrastructure such as routers, switches, and access points.
"count":"42",
"status":""
},

{
"id":"6",
"name":"Vulnerabilities",
"description":"Identify devices or applications based on the presence of a specified severity and/or vulnerability.
"count":"9",
"status":""
},

{
"id":"7",
"name":"Compliance",
"description":"Identify devices that have been checked for compliance against a specific audit file.
"count":"",
"status":""
}
"count":"25",
"status":""
},
{
"id":"8",
"name":"Device Behavior",
"description":"Identify devices that share common traffic patterns and/or open ports.",
"count":"31",
"status":""
},
{
"id":"9",
"name":"Collected Data",
"description":"Identify devices that have collected system configuration data such as patch level and user credentials.",
"count":"111",
"status":""
}
],
"error_code":0,
"error_msg":"",
"warnings":[]
"timestamp":1416249497
}
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**

Request Attribute Set Parameters

None
Example Response

Expand

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

\[\text{?fields=<field>,...}\]

**Allowed Fields**

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

**Legend**

* = always comes back

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

**Example Response**

Expand
{  
  "type" : "regular",
  "response" : {
    "id" : "1",
    "type" : "arf",
    "name" : "name",
    "description" : "description",
    "creatorID" : "1",
    "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

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",
                "155"
            ]
        }
    }
}
"administration_poc\full_name\first_name",
"administration_poc\full_name\last_name",
"administration_poc\full_name\middle_initial",
"administration_poc\full_name\generational_qualifier",
"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
}
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
**name
**description
**type
**statusgroups
creator
version
context
filename
originalFilename
createdTime
modifiedTime
lastRefreshedTime
canUse
canManage
Session User role not “1” (Administrator)

ownerGroup

targetGroup

owner

Legend*
*

* = always comes back

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

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

{/n
"type" : "regular",
"response" : {
"usable" : [
{
"id" : "5",
"name" : "Admin - Top 25 extended File Listener",
}]]}
"description": ",
"type": "windowsfiles",
"status": "0"
},
{
   "id": "6",
   "name": "Admin - Top 25 lite",
   "description": ",
   "type": "windowsfiles",
   "status": "0"
},
{
   "id": "1000030",
   "name": "Basic Audit File",
   "description": ",
   "type": "windowsfiles",
   "status": "0"
},
{
   "id": "1000047",
   "name": "With Scap",
   "description": ",
   "type": "windowsfiles",
   "status": "0"
},
{
   "id": "1000048",
   "name": "test12122",
   "description": ",
   "type": "scapWindows",
   "status": "0"
},
{
   "id": "1000049",
   "name": "Test",
   "description": ",
   "status": "0"
"description": "",
"type": "scapWindows",
"status": "0"
}
],
"manageable": [
{
"id": "1000030",
"name": "Basic Audit File",
"description": "",
"type": "windowsfiles",
"status": "0"
},
{
"id": "1000047",
"name": "With Scap",
"description": "",
"type": "windowsfiles",
"status": "0"
},
{
"id": "1000048",
"name": "test12122",
"description": "",
"type": "scapWindows",
"status": "0"
},
{
"id": "1000049",
"name": "Test",
"description": "",
"type": "scapWindows",
"status": "0"
},
}
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

```json
{
    "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 "",
}

**type is "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> OPTINAL

"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": ""

"owner": {
  "id": "1",
  "username": "head",
  "firstname": ",
  "lastname": ""

"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"

"error_code": 0,
"error_msg": "",
"warnings": [],
"timestamp": 1435249000

"auditFile/{id}" Methods

"auditFile/{id}" Methods

164
GET

Gets the AuditFile associated with {id}.

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
**name
**description
**type
**statusgroups
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**

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": ""
},
"owner": {
  "id": "1",
  "username": "head",
  "firstname": "",
  "lastname": ""
},
"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"
}
"error_code": 0,
"error_msg": "",
"warnings": [],
"timestamp": 1435249000
PATCH
Edits the AuditFile associated with {id}, changing only the passed in fields.

**Request Parameters**
(All fields are optional)
See /auditFile::POST for parameters.

**Example Response**
See /auditFile/{id}::GET for example response.

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

**Request Parameters**
None

**Example Response**
Expand

{
    "type" : "regular",
    "response" : [
        {
            "id" : "1000001",
            "targetGID" : -1,
            "name" : "test"
        }
    ],
    "error_code" : 0,
    "error_msg" : "",
    "warnings" : []
}
Methods

POST

Refreshes the AuditFile associated with {id} 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 deprecation) 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",
    "timestamp" : 1401911117
  }
}
"modifiedTime" : "1435249000",
"lastRefreshedTime" : "1435249000",
"typeFields" : {
    "variables" : []
}
,"groups" : [],
"canUse" : "true",
"canManage" : "true",
"creator" : {
    "id" : "1",
    "username" : "head",
    "firstname" : "",
    "lastname" : ""
}
,"owner" : {
    "id" : "1",
    "username" : "head",
    "firstname" : "",
    "lastname" : ""
}
,"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"
}


```
{
  "error_code" : 0,
  "error_msg" : "",
  "warnings" : [],
  "timestamp" : 1435249000
}
```

/auditFile/{id}/share

Methods

POST

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

Request Parameters

Expand

{}

"groups" : [
  {
    "id" : &lt;number&gt;
  }...
]

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" : ""
},
"owner" : {
   "id" : "1",
   "username" : "head",
   "firstname" : "",
   "lastname" : ""
},
"ownerGroup" : {
   "id" : "0",
   "name" : "Full Access",
   "description" : "Full Access group"
},
"targetGroup" : {
   "id" : "-1",
   "name" : "",
   "description" : ""
Methods

GET

Exports the AuditFile associated with {id} 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.
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

** Request Parameters **

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 **

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 v1.4.0 L1"
},
{ "id" : "270",
"name" : "PCI v2.0/v3.0 Windows Best Practices"
},
{ "id" : "269",
"name" : "CIS SQL Server 2014 Database L1 OS v1.0.0"}
"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 v1.0.0"
},

{ "id": "235",
  "name": "AirWatch - TNS MDM Best Practices Audit v1.0.0"
},

{ "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 Usage"
},

{
  "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 (Generic)"
},

{
  "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 v1.4.0 L2"
},
{
  "id" : "221",
  "name" : "TNS File Analysis - Classified Documents"
},
{
  "id" : "220",
  "name" : "DISA STIG for Microsoft Dot Net Framework 4.0 v1r2 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 Information"
},
{"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 Address Info"
},
{"id": "209",
"name": "TNS File Analysis - Phone No. and Address Info"
},
{"id": "208",
"name": "TNS File Analysis - SWIFT Banking Wire Transfer Info"
},
{"id": "207",
"name": "TNS File Analysis - SWIFT Banking Wire Transfer Info"
}
AirWatch - CIS Google Android 4 v1.0.0 L2

TNS File Analysis - International Wire Transfer

CIS Oracle Linux 7 L1 v1.0.0

TNS File Analysis - Social Security Number (By State)

CIS VMware ESXi 5.5 v1.2.0 Level 1

TNS File Analysis - Non-Disclosure Agreements

TNS File Analysis - French Social Security Number

CIS Ubuntu 12.04 LTS Benchmark L1 v1.1.0
"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 Practices"
},
{
    "id" : "182",
    "name" : "TNS MongoDB 2.6 Best Practices Windows OS Audit v1.0"
},
{
    "id" : "181",
    "name" : "TNS MongoDB 2.6 Best Practices Linux OS Audit v1.0"
}
"id": "180",
"name": "TNS MongoDB 2.x Best Practices Database Audit v1.0"
},
{
"id": "179",
"name": "TNS MongoDB 2.4 Best Practices Windows OS Audit v1.0"
},
{
"id": "178",
"name": "TNS MongoDB 2.4 Best Practices Linux OS Audit v1.0"
},
{
"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 Settings audit"
},
{
  "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 v1r4"}
"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 V6R1"
},
{
  "id": "151",
  "name": "IBM iSeries Security Reference v5r4"
},
{
  "id": "150",
  "name": "TNS IBM Tivoli Enterprise Client Linux Best Practices"
},
{
  "id": "149",
  "name": "HIPAA Windows Audit"
},
{
  "id": "148",
  "name": "DISA STIG Cisco Network L2 Switch v8r8"
},
{
  "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 v1r3 Audit"
},
{
"id" : "137",
"name" : "DISA STIG OfficeSystem 2007 v4r9"
},
},
{
    "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 Switch v8r17"
},
{
    "id" : "124",
    "name" : "DISA STIG Cisco L2 Switch v8r17"
},
{
    "id" : "123",
    "name" : "DISA STIG Cisco Infrastructure Router and L3 Switch 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"
},
null
"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 v1.0.0"
}
{
  "id" : "70",
  "name" : "CIS SUSE Linux Enterprise Server 11 L1 v1.0.0"
}
{
  "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"
}
"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 Benchmark v1.2.0"
},
{
"id" : "33",
"name" : "CIS Windows 7 Specialized Security Desktop v1.2.0"
},
{
"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",
}
<table>
<thead>
<tr>
<th>id</th>
<th>name</th>
</tr>
</thead>
<tbody>
<tr>
<td>13</td>
<td><strong>MobileIron - CIS Apple iOS 8 v1.0.0 L2</strong></td>
</tr>
<tr>
<td>12</td>
<td><strong>CIS CentOS 7 L2 v1.0.0</strong></td>
</tr>
<tr>
<td>11</td>
<td><strong>CIS CentOS 7 L1 v1.0.0</strong></td>
</tr>
<tr>
<td>10</td>
<td><strong>CIS CentOS 6 L2 v1.0.0</strong></td>
</tr>
<tr>
<td>9</td>
<td><strong>CIS CentOS 6 L1 v1.0.0</strong></td>
</tr>
<tr>
<td>8</td>
<td><strong>CIS ISC BIND 9.0/9.5 v2.0.0</strong></td>
</tr>
<tr>
<td>7</td>
<td><strong>CIS Apple Safari v1.0.0</strong></td>
</tr>
<tr>
<td>6</td>
<td><strong>CIS Apache HTTP Server L2 v3.1</strong></td>
</tr>
<tr>
<td>5</td>
<td><strong>CIS Apache HTTP Server v3.1 L1</strong></td>
</tr>
</tbody>
</table>
"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*

**Request Parameters**

None

**Example Response**

Expand

```json
{
    "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" : "\"is the IP address assigned to your organization\",
    "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": "Blue Coat 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": "9",
"name": "Extreme ExtremeXOS",
"count": "1"
}
],
"error_code": 0,
"error_msg": "",
"warnings": [],
"timestamp": 1601418375
}
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
activeownerGroup

canManage
functional

**Legend**

*  
* = *always comes back*

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


**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": ""
        }
    }
}

[97x673]"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
ipListallIPs
repeatRule
start
end
duration
enabled
createdTime
modifiedTime
activeownerGroupcanManagefunctional

**Legend**

* = *always comes back*

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

**Request Parameters**

None

**Example Response**

Expand

```json
{
    "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",
```
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
}
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/:PATCH
- /asset::POST
- /dashboard//component::PATCH
- /dashboard//component::POST
- ****/query/:GET****
- /query::PATCH
- /query::POST

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.

Request Parameters

Expand

{
  "operations" : [
    {
      "api" : <string> "/asset" | "/asset/<id>" | "/query" | "/query/<id>" | "/dashboard/<id>/component" | "/dashboard/<id>/component/<id>,
      "method" : <string> "GET" | "PATCH" | "POST",
      "method" : "GET"
      "params" : <valid object parameters:see NOTE #1> DEFAULT {}}
}
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" : "ip",
                                "operator" : "eq",
                                "value" : "192.168.0.0\/24",
                                "pluginIDConstraint" : "-1",
                            }
                        ]
                    }
                }
            }
        }
    ]
}
"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
",
{
"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\/24",
"pluginIDConstraint" : "-1",
"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
}]
```

```
Configuration

/config

Methods

GET

Gets the system configuration types

Request Parameters

None

Example Response

Expand

```json
{
    "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"
},
/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/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" : 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"
}

Example Response
"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": "pdf",
"enabled": "true",
"attributeSets": []
}]}
"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" : "W3sidHlwZSI6ICJlbmRyeSIsIm5hbWUiOiAiRG9tYWluIENvbnRlbnQu",
},
{
  "id" : "2",
  "name" : "Apple Profile Manager",
  "description" : "",
  "value" : "profile_manager",
  "ipPref" : "Apple Profile Manager server : ",
  "pluginIDs" : [
    {
      "id" : "60032"
    }
  ],
  "editor" : "W3sidHlwZSI6ICJlbmRyeSIsIm5hbWUiOiAiJTIzX2F1ZXIiLCJyZXF1aXJlZCI6ICJ0cnVlIiwiZGVmYXVsdCI6ICJ5ZXMiLCJpZCI6ICJ2ZXJpZnlfc3NsIn1dfX19XQ=="
},
{
  "id" : "3",
  "name" : "Good MDM",
  "description" : "",
  "value" : "GoodMDM",
  "ipPref" : "GMC Server : ",
  "pluginIDs" : [
    {
      "id" : "66963"
    }
  ],
  "editor" : "W3sidHlwZSI6ICJlbmRyeSIsIm5hbWUiOiAiJTIzL0lCJyZXF1aXJlZCI6ICJ0cnVlIiwiZGVmYXVsdCI6ICJ5ZXMiLCJpZCI6IiJ9fV19fX1d"
},
{
    "id": "4",
    "name": "Mobile Iron",
    "description": "",
    "value": "MobileIron",
    "ipPref": "MobileIron VSP Admin Portal URL : ",
    "pluginIDs": [
        {
            "id": "72904"
        }
    ],
    "editor": "W3sidHlwZSI6ICJlbnRyeSIgIm5hbWUiOiJNb2JpbGVJcm9uIFZlciBJbnRlZ3JhdGlvbg=="
},
{
    "id": "5",
    "name": "AirWatch MDM",
    "description": "",
    "value": "AirWatch",
    "ipPref": "AirWatch Environment API URL : ",
    "pluginIDs": [
        {
            "id": "76460"
        }
    ],
    "editor": "W3sidHlwZSI6ICJlbnRyeSIgIm5hbWUiOiAiQWlyV2F0Y2ggRW5lcmF0ZSIsImlkZiI6MTg0Njg4MzIyNywiZXhwIjoxMTY1OTk1MjE0OTg2fQ=="
}
],
{
    "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"
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" : "",
   "timestamp" : 1410209808
}
"warnings" : [],
"timestamp" : 1410210283
}

/config/license/register

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,ScannerStatusTimeout",
"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"
   }
}
/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
}
```
**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 for Tenable products"
  },
  {
    "id" : 1,
    "name" : "Mail",
    "description" : "Configure SMTP settings for sending e-mail from Tenable"
  },
  null,
  {
    "id" : 3,
    "name" : "Security",
    "description" : "Configure login and display security settings"
  }
]}
```
"id" : 4,
"name" : "Miscellaneous",
"description" : "Settings for Web Proxy, Syslog, Notifications, and additional report types",
}
{
 "id" : 5,
 "name" : "Data Expiration",
 "description" : "Settings for how long data is retained"
}
{
 "id" : 6,
 "name" : "External Schedules",
 "description" : "Configure data retrieval settings for NNM and LCE"
}
{
 "id" : 7,
 "name" : "Plugins / Feed",
 "description" : "Manage Tenable plugins and feeds"
}
{
 "id" : 8,
 "name" : "SAML",
 "description" : "Settings for SAML 2.0 identity provider or Shibboleth"
}
{
 "id" : 9,
 "name" : "Lumin",
 "description" : "Configure settings for Lumin Synchronization"
}
",
"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."
    },
    "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.

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

**Example Response**

See /configSection/{id}::GET
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_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,
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_kv_url, hashicorp_namespace, hashicorp_username_source, hashicorp_userkey, hashicorp_passkey, hashicorp_secret, 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
  ** name
  ** description
  ** type
  creator
targetgroups
typeFields
tags
  createdTime
modifiedTime
canUse
canManage

Session user role not “1” (Administrator)

ownerGroup

Legend

* = always comes back

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

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"
            }
        ]
    }
}
POST

Adds a Credential.

Request Parameters
Expand

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

**type is “database”**

```
...

    "login" : <string>,
    "sid" : <string> DEFAULT "",
    "authType" : <string> "cyberark" | "Hashicorp" | "lieberman" | "password",
    "dbType" : <string> "Oracle" | "SQL Server" | "DB2" | "MySQL" | "PostgreSQL" | "Informix/DRDA" | "Sybase ASE" | "Apache Cassandra",
    "port" : <string> (valid port number),

**authType "password"**

-------------------

    "password" : <string>,

**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",
```

258
"vault_address" : <string> DEFAULT "",
"vault_account_name" : <string>,
"vault_cyberark_client_cert" : <string>,
"vault_cyberark_private_key" : <string>,
"vault_cyberark_private_key_passphrase" : <string>,
"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",

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",

259
"lieberman_verify_ssl" : <string> "false" | "true",
"lieberman_system_name" : <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" | "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"

authType "BeyondTrust"

"beyondtrust_host" : <string> (valid IP or IP host),
"beyondtrust_port" : <string> (valid port number),
"beyondtrust_api_key" : <string>,
"beyondtrust_duration" : <string>,

261
"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" | "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" |

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"

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" |

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" |

authType "publickey"

"privateKey" : <string>,
"passphrase" : <string> DEFAULT "",
"privilegeEscalation" : <string> "none" | "su" | "sudo" | "su+sudo" | "dzdo" |

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" | "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> DEFAULT "",
"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 "su" | "sudo" and authType "thycotic"
------------------------------------------------------
"escalationUsername" : <string> DEFAULT "",
"escalationPath" : <string> DEFAULT ""

}  

*type is “snmp”*

{  
  ...
  "communityString" : <string>
}

*type is “windows”*

{  
  ...
  "username" : <string>,
  "authType" : <string> "BeyondTrust" | "Centrify" | "cyberark" | "Hashicorp" | "  

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>,

268
"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 "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_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"

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>
}

**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" : ""
},
"owner" : {
    "id" : "1",
    "username" : "head",
    "firstname" : "Security Manager",
    "lastname" : ""
},
"ownerGroup" : {
    "id" : "0",
    "name" : "Full Access",
    "description" : "Full Access group"
},
"targetGroup" : {
    "id" : "-1",
    "name" : ""
}
/credential/{id}

Methods

GET

Gets the Credential associated with {id}.

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_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_real, 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_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_folder, vault_port, vault_username, vault_password, vault_cyberark_url, vault_safe, vault_app_id, 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_private_key, 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_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**
Allowed Fields

*id
**name
**description
**type
creatorGroups
target
typeFields
tags
createdTime
modifiedTime
canUse
canManage

Session user role not “1” (Administrator)

ownerOwnerGroup
targetGroup

Legend*

* = always comes back

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

Request Parameters

None

Example Response

Expand

```json
{
    "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" : ""
},
"owner" : {
    "id" : "1",
    "username" : "head",
    "firstname" : "Security Manager",
    "lastname" : ""
},
"ownerGroup" : {
    "id" : "0",
    "name" : "Full Access",
    "description" : "Full Access group"
},
"targetGroup" : {

PATCH

Edits the Credential associated with {id}, 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

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

**Request Parameters**

None

**Example Response**

Expand

```json
{
  "type" : "regular",
  "response" : "",
  "error_code" : 0,
  "error_msg" : "",
  "warnings" : [],
  "timestamp" : 1408723358
}
```

/credential/{id}/share

**Methods**

**POST**

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

Note: Admin users cannot share credentials. Application credentials cannot be shared.

**Request Parameters**

Expand

```json
{
  "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" : ""
    },
    "owner" : {
      "id" : "1",
      "username" : "head",
    }
  }
}
"firstname" : "Security Manager",
"lastname" : ""
},
"ownerGroup" : {
   "id" : "0",
   "name" : "Full Access",
   "description" : "Full Access group"
},
"targetGroup" : {
   "id" : -1,
   "name" : "",
   "description" : ""
}
},
"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}
Current Organization

/currentOrganization

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

Request Parameters

None

Example Response

Expand
{"type": "regular",
"response": {
   "name": "Org3",
   "zoneSelection": "auto_only",
   "ipInfoLinks": [
      {
         "name": "SANS",
         "link": "https:\/\/isc.sans.edu\/ipinfo.html?ip=%IP%"
      },
      {
         "name": "ARIN",
         "link": "http:\/\/whois.arin.net\/rest\//ip\/%IP%"
      }
   ],
   "zones": []
},
"error_code": 0,
"error_msg": "",
"warnings": [],
"timestamp": 1408974135
}
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
**username
**firstname
**lastname
**status
role
title
eemail
address
city
state
country
phone
fax
createdTime
modifiedTime
lastLogin
lastLoginIP
mustChangePassword
locked
failedLogins
authType
fingerprint
password
description
managedUsersGroups
managedObjectsGroupsuserPrefspreferences organization
ldapUsername
ldap**
**switchableUsers

Session user is not role “1” (Administrator)

**responsibleAsset**

group

Legend *
*

* = always comes back

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

**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",
"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"
  },
  "organization" : {
}
Organization User

Note: If the Current User is a linked user, the response includes a list of the users that can be switched to including the parent Administrator.

Expand

```json
{
    "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",
"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" : ""
},
"userPrefs" : [
  {
    "name" : "timezone",
    "value" : "America/Nome",
    "tag" : "system"
  }
],
"role" : {
  "id" : "2",
  "name" : "Security Manager",
  "description" : "The Security Manager role has full access to all actions at the organization level. A Security Manager can add, edit, view, and stop all scans. A Security Manager can also modify 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 Windows installed. This 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"
    },
    "organization" : {
      "id" : "0",
      "name" : "Tenable.sc Administration",
      "
    }
  }
]
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>,  
        }  
    ]}
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: /current-user/preferences?name=foo&tag=foo

```json
{
   "name" : <string> OPTIONAL,
   "tag" : <string> OPTIONAL
}
```

**Example Response**

Expand

```json
{
   "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
Example Response
See /currentUser::GET
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**

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_code": 0,
"error_msg": "",
"warnings": [],
"timestamp": 1419269719
}
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
lastUpdateTime
lastCompletedUpdateTime
cREATEDTIME
modifiedTime
SCHEDULE
definition
data

Legend

*
Request Parameters

None

Example Response

Expand

```json
{
    "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" : "cumulative",
                        "querySourceID" : null,
                        "querySourceView" : null,
                        "querySourceViewID" : 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",
}
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" : "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" | "lce" | "mobile" | "ticket" | "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 “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" | "never" | "rollover" | 
},
"strips" : <string> (comma separated list of numbers indicating columns)
],
"cells" : [
{
"conditionals" : [
{
"conditionalName" : <string>,
"conditionalOperator" : <string>,
"conditionalValue" : <string>,
"outputType" : <string>,
"outputColors" : <string>,
"outputText" : <string>
}
]
},
"dataSource" : {
"queryID" : <number> OPTIONAL
"querySourceType" : "alert" | "lce" | "mobile" | "ticket" | "user"
"querySourceID" : <number>,
"querySourceView" : <string>,
"sortColumn" : <string>,
"sortDirection" : <string>,
"iteratorID" : <number> DEFAULT "-1" (not set)
queryID is not provided
-----------------------
"query" : <query object>
},
"baseDataSource" : {
"queryID" : <number> OPTIONAL
"querySourceType" : "alert" | "lce" | "mobile" | "ticket" | "user"
"querySourceID" : <number>,
"querySourceView" : <string>,
"sortColumn" : <string>,
"sortDirection" : <string>,
"sortDirection" : <string>,  
"iteratorID" : <number> DEFAULT "-1" (not set)

queryID is not provided

-----------------------

"query" : <query object>

} OPTIONAL

...}

]

}

...

}

Schedule type is “ical”

NOTE: Applies to all types of Components. The schedule object for type matrix is located in the definition clusters. Otherwise, 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 format)

}

...

}

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" : "9223372036854775807",
    "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",
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
dataqueryStatus

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" : "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",
    "id": "161",
    "queryID": "81",
    "querySourceType": "cumulative",
    "querySourceID": null,
    "querySourceView": null,
    "sortColumn": "score",
    "sortDirection": "desc",
    "iteratorID": "-1",
  }
}
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 hosts that have been identified with plugin 74442. 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" : {

/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",
        "lastUpdateTime" : "1414440714",
        "lastCompletedUpdateTime" : "1414440714",
        "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
]
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

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

```json
{
    "type" : "regular",
    "response" : {
        "usable" : [
            {
                "id" : "1",
                "name" : "Vulnerability Overview",
                "description" : "Vulnerability Overview tab"
            },
            {
```
"id" : "2",
"name" : "Executive 7 Day",
"description" : "This dashboard provides an executive summary of a weekly status of the current vulnerability management program. It offers an overview analysis of a vulnerability management program that is easy to understand by managers, CISO's, and other executives. The first set of tables show a detailed ratio of vulnerabilities to the risk of exploitation, allowing for the identification of the vulnerabilities with the 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, tables, and graphs, this overview dashboard provides a summary for an executive. It includes useful trend information on vulnerabilities as well as 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 executive summary of a weekly status of the current vulnerability management program. It offers an overview analysis of a vulnerability management program that is easy to understand by managers, CISO's, and other executives. The first set of tables show a detailed ratio of vulnerabilities to the risk of exploitation, allowing for the identification of the vulnerabilities with the 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, tables, and graphs, this overview dashboard provides a summary for an executive. It includes useful trend information on vulnerabilities as well as how long they have existed within the network environment."
},
{
"id" : "8",
"name" : "Vulnerability Overview",
"description" : "Vulnerability Overview"}
Vulnerability Overview tab

This dashboard provides an executive summary of a weekly status of the current vulnerability management program that is easy to understand by managers, CISOs and other executives. The first set of tables show a detailed ratio of vulnerabilities to the risk of exploitation, and the vulnerabilities with top 10 most vulnerable assets. Using a bar chart and table, a high level summary is depicted.

Using a series of charts, tables, and graphs, this overview dashboard provides a summary for an executive understanding of vulnerabilities as well as useful trend information on vulnerabilities and how long they have existed within the network environment.

Vulnerability Overview tab

Using a series of charts, tables, and graphs, this overview dashboard provides a summary for an executive understanding of vulnerabilities as well as useful trend information on vulnerabilities and how long they have existed within the network environment.

Vulnerability Overview tab

Using a series of charts, tables, and graphs, this overview dashboard provides a summary for an executive understanding of vulnerabilities as well as useful trend information on vulnerabilities and how long they have existed within the network environment.
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**


{
    "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": ""
        },
        "ownerGroup": {
            "id": "0",
            "name": "Full Access",
            "description": "Full Access group"
        }
    }
}
"targetGroup" : {
    "id" : -1,
    "name" : "",
    "description" : ""
  },
"error_code" : 0,
"error_msg" : "",
"warnings" : [],
"timestamp" : 1414185335
}

/methods/{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
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**  
  

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",  
}
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 Components - 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 triggers on specific events such as:
- URLs on part of a known botnet,
- If DNS traffic is found on ports other than 53,
- If there have been more than 30 minutes of continuous DNS errors,
- Detected anomalies in DNS traffic or monitoring of BIND and Active Directory,
and any found known exploits of DNS."

"id" : "16",
"name" : "Threat Intelligence - Microsoft Windows Known Bad AutoRuns and Scheduled Tasks",
"description" : "This component provides a list of infected hosts that have been identified with plugin 74442. The ... a forensic analysis should be considered to determine the extent of the compromise. The table uses the IP Summary tool 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" : ""
},
"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",
      "filename" : "sample_dashboard.json",
      "order" : 1
   }
}
"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",
"creator" : {
  "id" : "1",
  "username" : "user",
  "firstname" : "user",
  "lastname" : "Security Manager"
},
"owner" : {
  "id" : "1",
  "username" : "user",
  "firstname" : "user",
  "lastname" : "Security Manager"
},
"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
Example Response

<?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>YTo1OntzOjc6InN0eWxlSUQiO3M6MjoiLTEiO3M6OToic3RhcnRUaW1lIjtzOjc6InVuZFRpbWUiO3M6MTA6IjE0MTY1MTg2ND ... I7czo5OiJmaXJzdFNlZW4iO3M6ODoib3BlcmF0b3IiO3M6MToiPSI7czo1OiJ2YWx1ZSI7czo0OiIwOjI1Ijt9fXM6NjoiZ3JvdXBzIjthOjA6e319fX19fQ==</definition>
        </component>
        <component>
            <name>Exploitable by Malware - Top 100 Vulnerabilities Exploitable by Malware</name>
            <description>This component shows a top 100 summary of the vulnerabilities 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. The component displays the vulnerability name, exploitability, and total hosts affected.</description>
            <componentType>table</componentType>
            <type>table</type>
            <column>1</column>
            <order>2</order>
        </component>
    </dashboardComponents>
</dashboardTab>
<schedule>FREQ=DAILY;INTERVAL=1</schedule>
<definition>
YTo1OntzOjc6InN0eWxlSUQiO3M6MjoiLTEiO3M6NzoiY29sdW1ucyI7YTo1OntpOjA7YToxOntzOjQ6Im5hbWUiO3M6ODoicGx1Z2luSUQiO31pOjE7YToxOntzOjQ6ImVuZFRpbWUiO3M6MTA6IjE0MTY1MTg2NDIiO3M6NzoiY29sdW1ucyI7YTo1OntpOjA7YToxOntzOjQ6IjE0MTY1MTg2NDIiO3M6NzoiY29sdW1ucyI7czo0OiJ2YWx1ZSI7czo3OiJ2YWx1ZSI7fX0=
</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>
YTo1OntzOjc6InN0eWxlSUQiO3M6MjoiLTEiO3M6NzoiY29sdW1ucyI7YTo1OntpOjA7YToxOntzOjQ6Im5hbWUiO3M6ODoicGx1Z2luSUQiO31pOjE7YToxOntzOjQ6ImVuZFRpbWUiO3M6MTA6IjE0MTY1MTg2NDIiO3M6NzoiY29sdW1ucyI7YTo1OntpOjA7YToxOntzOjQ6IjE0MTY1MTg2NDIiO3M6NzoiY29sdW1ucyI7czo0OiJ2YWx1ZSI7czo3OiJ2YWx1ZSI7fX0=
</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>
YTo1OntzOjc6InN0eWxlSUQiO3M6MjoiLTEiO3M6NzoiY29sdW1ucyI7YTo1OntpOjA7YToxOntzOjQ6Im5hbWUiO3M6ODoicGx1Z2luSUQiO31pOjE7YToxOntzOjQ6ImVuZFRpbWUiO3M6MTA6IjE0MTY1MTg2NDIiO3M6NzoiY29sdW1ucyI7YTo1OntpOjA7YToxOntzOjQ6IjE0MTY1MTg2NDIiO3M6NzoiY29sdW1ucyI7czo0OiJ2YWx1ZSI7czo3OiJ2YWx1ZSI7fX0=
</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>
YTo1OntzOjc6InN0eWxlSUQiO3M6MjoiLTEiO3M6NzoiY29sdW1ucyI7YTo1OntpOjA7YToxOntzOjQ6Im5hbWUiO3M6ODoicGx1Z2luSUQiO31pOjE7YToxOntzOjQ6ImVuZFRpbWUiO3M6MTA6IjE0MTY1MTg2NDIiO3M6NzoiY29sdW1ucyI7YTo1OntpOjA7YToxOntzOjQ6IjE0MTY1MTg2NDIiO3M6NzoiY29sdW1ucyI7czo0OiJ2YWx1ZSI7czo3OiJ2YWx1ZSI7fX0=
</definition>
</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" : ""
},
"ownerGroup" : {
  "id" : "0",
  "name" : "Full Access",
  "description" : "Full Access group"
},
"targetGroup" : {
  "id" : "-1",
  "name" : "",
  "description" : ""
},
"error_code" : 0,
"error_msg" : "",
"warnings" : [],
"timestamp" : 1414430665
Dashboard Template

/dashboardTemplate

Methods

GET

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

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" ...
  "searchString" : <string> (Search String Format. See NOTE#2) DEFAULT ""
}

Example Response
Expand

{
  "type" : "regular",
  "response" : [
    
  
}
"id" : "739",
"name" : "Executive 7 Day - Current Vulnerabilities",
"description" : "This dashboard provides an executive summary of a weekly status of the current vulnerability management program that provide an overview analysis of a vulnerability management program that is easy to understand by managers, CISO's and other executives.

The first set of tables show a detailed ratio of vulnerabilities to the risk of exploitation, ... 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 summary of the current Mobile Device Management (MDM) status. The dashboard contains columns to display different metrics such as the current vulnerability or threat 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 summary to the current Information Assurance Vulnerability Management (IAVM) program.

"id" : "383",
"name" : "Mitigated Patch Rates - Remediation Rates",
"description" : "On the bottom, I created a matrix chart that lists some very generic columns including:
- Now - 0-
- 24 to 50 is yellow
- Higher than 50 is green.

For 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 Over Time",
"description" : "This component is a 90 day summary chart tracking active vulnerabilities with low, medium, high, and critical severities.

"id" : "551",
"name" : "Executive Summary - Vulnerability Age",
"description" : "This component contains a matrix displaying vulnerability age. The columns identify new hosts (within 7 days), active (within 30 days), old (within 90 days), and greater than 90 days, respectively. The matrix displays the number of vulnerabilities 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 Operating 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 Summary by Severity",
"description" : "This component displays a severity summary of 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 - Vulnerability Mitigation",
"description" : "This component contains a matrix displaying mitigated vulnerability ages. The columns identify new hosts ... 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 Publication Age",
"description" : "This component provides a summary of vulnerabilities and patch release dates. The dates are summarized ... 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 Trend Windows Vulnerabilities",
"description" : "This component provides a 25-day trend of 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 User Management",
"description" : "This table provides a list of informational 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 - Vulnerability Publication Age",
"description" : "This component provides a summary of vulnerabilities and their release dates. The dates are summarized ... 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 Trend Linux Vulnerabilities",
"description" : "This component provides a 25-day trend of Linux 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 Trending by Type",
"description" : "This component trend analysis displays exploitable vulnerabilities discovered in the past 25 days, and how they have been categorized. 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 Asset 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 Vulnerability Breakdown",
"description" : "This component displays the newly discovered 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 Type Matrix",
"description" : "The component shows a summary of the remediated vulnerabilities that have been discovered over the past 24 hours. 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 Summary by Severity",
"description" : "This component displays a severity summary of 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 Vulnerability Trend",
"description" : "This component displays a trend analysis of previously remediated vulnerabilities discovered over the past 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 Vulnerability Trending by Type",
"description": "This component trend analysis displays previously mitigated vulnerabilities discovered in the past 25 days. 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 Asset Summary",
"description": "This component shows a mitigated 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": "861",
"name": "Executive 30 Day - Mitigated Asset Vulnerability Breakdown",
"description": "This component displays the newly discovered exploitable vulnerability count of the top 10 assets. The counts are displayed in descending order by the number of critical vulnerabilities."
}
,
{
"id": "846",
"name": "Executive 30 Day - Current Vulnerability Trending by Severity",
"description": "This component displays a trend analysis of vulnerabilities discovered over the past 25 days. Please note that these vulnerabilities were discovered between 25-24 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 Trending by Type",
"description": "This component trend analysis displays vulnerabilities discovered over the past 25 days, and by type. Please note that these vulnerabilities were discovered between 25-24 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 Asset Summary",
"description": "This component shows vulnerability analysis by 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 Vulnerability Breakdown",
"description": "This component displays the newly discovered vulnerability count of the top 10 assets. The data is sorted in descending order by the number of critical vulnerabilities."
}
"id": "548",
"name": "Executive Summary - CVSS Scoring",
"description": "This matrix component displays current 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 Patches by Operating System (Medium, Highs and Criticals)",
"description": "This component shows a table of the top 10 summary of the most vulnerable assets, sorted by the number of outstanding patches, and can 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 chart 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 of the top 10 most vulnerable networks. The bar chart contains the number of critical severities is used to sort the assets in the graph. The network sorting is based on the native class
'
"
",
{
"id": "553",
"name": "Executive Summary - CVSS Scoring (Previously Mitigated Items)",
"description": "This matrix displays mitigated vulnerabilities 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 Bulletins",
"description": "This component is a table showing a top 10 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 Matrix",
"description": "This component provides a summary of the vulnerabilities discovered within the past 7 days. The rows are filled with data based on the activity of the scanner, and columns can be removed if necessary.
"}
"id" : "692",
"name" : "Executive 7 Day - Current Vulnerability Summary by Severity",
"description" : "This component displays a severity summary of 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 Trending by Severity",
"description" : "This component displays a trend analysis of vulnerabilities discovered over the past 7 days. Please note that the chart is configured to show vulnerabilities discovered 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 Trending by Type",
"description" : "This component trend analysis displays vulnerabilities discovered over the past 7 days, and by type. Please note that the chart is configured to show vulnerabilities discovered 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 Asset Summary",
"description" : "This component shows vulnerability analysis by 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 Vulnerability Breakdown",
"description" : "This component displays the newly discovered vulnerability count of the top 10 assets. The counts are based on vulnerabilities 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 Type Matrix",
"description" : "The component shows a summary of the exploitable vulnerabilities that have been discovered over the past 7 days. If 0% - 50% of the vulnerabilities are exploitable by a framework, the cell is red on white 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 Summary by Severity",
"description" : "This component displays a severity summary of 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 Trending by Severity",
"description" : "This component displays a trend analysis of exploitable vulnerabilities discovered over the past 7 days. 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 Trending by Type",
"description" : "This component trend analysis displays exploitable vulnerabilities discovered in the past 7 days, and by type. 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 Asset 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 Vulnerability Breakdown",
"description" : "This component displays the newly discovered 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 Summary by Severity",
"description" : "This component displays a severity summary of 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 Vulnerability Trend",
"description" : "This component displays a trend analysis of previously remediated vulnerabilities discovered over the past 7 days. 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 Vulnerability Trending by Type",
"description" : "This component trend analysis displays previously mitigated vulnerabilities discovered in the past 7 days, and by type. 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 Asset Summary",
"description": "This component shows a mitigated 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": "708",
"name": "Executive 7 Day - Mitigated Asset Vulnerability Breakdown",
"description": "This component displays the newly discovered exploitable vulnerability count of the top 10 assets. 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 load for specific users."
},

{"id": "565",
"name": "This Weeks Tickets",
"description": "This table component is used to list recent Tenable.sc tickets."
},

{"id": "412",
"name": "Mobile Summary - Vulnerable Mobile Devices",
"description": "This component contains a matrix with columns for the device count, critical severity, high severity, and total severity. The rows represent the different device models. If the device model is case sensitive, the returned result will be 0. To ensure the correct values are displayed, use the Analysis > Mobile > Model Summary tool. If the device model is not case sensitive, 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 do not follow this pattern. Therefore the 'Android' row uses only the 'Model' field as the filter."
},

{"id": "409",
"name": "Mobile Summary - Device Type Summary Pie Chart",
"description": "This component provides a model summary of the 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 listing the 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, Critical and High Severity Summary",
"description" : "This component displays a bar chart that includes a device count, critical severity, and high severity. It enables users to view status of all managed device models, with a bar representing the count of devices with critical and high severities."
},

{  
"id" : "401",
"name" : "IAVM High Severity Summary Yr 2013",
"description" : "This component provides a pie chart of the top 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 trend analysis of IAVMs per year. Each year starting with 2013 through 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 a host 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 2013",
"description" : "This component displays a bar chart summary of 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 provides a 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 of the top 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 current statistics for each user with ticket entries"},
{
  "id" : "346",
  "name" : "Ticket Overview - Tickey Status Summary Last 30 Days",
  "description" : "Status summary of tickets created in the last 30 days."},
{
  "id" : "347",
  "name" : "Ticket Overview - Ticket Classification Summary - Last 30 Days",
  "description" : "Classification summary of tickets created in the last 30 days."},
{
  "id" : "349",
  "name" : "Ticket Overview - List of Tickets",
  "description" : "The 'List of Tickets' table displays tickets with more detail, including name, assignee, status, classification and modified date/time"},

"error_code" : 0,"error_msg" : ",
"warnings" : [],
"timestamp" : 1414182980

/dashboarThemeplate/{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*

**Expand Parameters**

components
**Request Parameters**

None

**Example Response**

Expand

```
{
    "type": "regular",
    "response": {
        "id": "1574",
        "name": "FTI Security Guidelines",

This dashboard focuses on IRS Publication 1075. Tenable's SC CV solution is well suited for meeting IRS Publication 1075 requirements as well.


"type": "collection",
        "suggestedNumColumns": "3",
        "suggestedColumnWidths": "33,34,33",
        "enabled": "true",
        "minUpgradeVersion": "4.8.1",
        "templatePubTime": "1414009276",
        "templateModTime": "1414009276",
        "templateDefModTime": "1414009276",
        "definitionModTime": "1414049413",
        "createdAt": "1414049413",
        "modifiedAt": "1414049413",
        "tags": [
            "anomalies",
            "compliance",
            "dlp",
            "fti",
            "mitigated",
            "network",
            "vulnerabilities"
        ],
        "requirements": [
```
<table>
<thead>
<tr>
<th>Component Name</th>
<th>Description</th>
<th>Order</th>
<th>Column</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerability Top Ten - Top 10 Remediations</td>
<td>This table displays the top 10 remediations for the network. Implementing the remediations will decrease the vulnerability of the network.</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Vulnerability Top Ten - Top 10 Exploitable Vulnerabilities</td>
<td>This table displays the top 10 exploitable vulnerabilities on the network. The list is sorted so that the severity and the number of hosts affected is shown. This will be helpful for those getting started with Tenable.sc.</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Vulnerability Top Ten - Top 10 Most Vulnerable Hosts</td>
<td>This table displays the 10 hosts on the network that have the greatest number of exploitable critical and high severity vulnerabilities. For each host, a bar graph of its critical and high severity vulnerabilities are shown.</td>
<td>1</td>
<td>3</td>
</tr>
</tbody>
</table>
{

"id" : "1100",
"name" : "Track Mitigation Progress - Vulnerability Summary by Seve
"description" : "Tenable.sc records when vulnerabilities are discov
"order" : "2",
"column" : "1"
},
{

"id" : "1102",
"name" : "Detect Changes - Changes in Last 72 Hours",
"description" : "This component assists in maintaining up-to-date i
"order" : "2",
"column" : "2"
},
{

"id" : "1572",
"description" : "This matrix provides a sense of how the network co
"order" : "2",
"column" : "3"
},
{

"id" : "1103",
"name" : "Monitor Security Solutions - Activity in Last 72 Hours",
"description" : "This component assists in monitoring security solu
"order" : "3",
"column" : "1"
},
{

"id" : "1570",
"name" : "Detect Suspicious Activity - Alerts in Last 72 Hours",
"description" : "This matrix presents warning indicators for potent
"order" : "3",
"column" : "2"
},

360


/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" : "Threat Detection & Vulnerability Assessments"
      },
      {
         "id" : "2",
         "name" : "Network Monitoring & Analysis",
         "description" : "Network Monitoring & Analysis"
      },
      {
         "id" : "3",
         "name" : "Compliance & Regulatory Reporting",
         "description" : "Compliance & Regulatory Reporting"
      }
   ]
}
"description" : "Aid with identifying vulnerabilities and potential threats.",
"collectionCount" : "74",
"collectionStatus" : "new",
"componentCount" : "388",
"componentStatus" : "new"
},
{
  "id" : "2",
  "name" : "Monitoring",
  "description" : "Provide intrusion monitoring, alerting and analysis.",
  "collectionCount" : "48",
  "collectionStatus" : "new",
  "componentCount" : "305",
  "componentStatus" : "new"
},
{
  "id" : "3",
  "name" : "Security Industry Trends",
  "description" : "Influenced by trends, reports, and analysis from industry leaders.",
  "collectionCount" : "15",
  "collectionStatus" : "new",
  "componentCount" : "90",
  "componentStatus" : "new"
},
{
  "id" : "4",
  "name" : "Executive",
  "description" : "Provide operational insight and metrics geared towards executives.",
  "collectionCount" : "11",
  "collectionStatus" : "new",
  "componentCount" : "70",
  "componentStatus" : "new"
},
{
  "id" : "5",
}
"name" : "Compliance & Configuration Assessment",
"description" : "Aid with configuration, change and compliance management",
"collectionCount" : "48",
"collectionStatus" : "new",
"componentCount" : "288",
"componentStatus" : "new"
},
{
"id" : "6",
"name" : "Discovery & Detection",
"description" : "Aid in trust identification, rogue detection, and new device discovery",
"collectionCount" : "21",
"collectionStatus" : "new",
"componentCount" : "113",
"componentStatus" : "new"
}
],
"error_code" : 0,
"error_msg" : "",
"warnings" : [],
"timestamp" : 1413925223
}
Device Information

/deviceInfo

Methods

GET

Gets the device information from the current user

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
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

**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 “uuid” exists**

{  
    "uuid" : <string> (valid uuid)
}

Parameter “ip” exists

{  
    "ip" : <string> (valid ip address),
    "dnsName" : <string> OPTIONAL
}

**Example Response**
{  
  "type" : "regular",
  "response" : {
    "repositories" : [
      {
        "id" : "2",
        "name" : "Rep2",
        "description" : ""
      }
    ],
    "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\?ip=192.168.0.1"
  },
  {
    "name" : "ARIN",
    "link" : "http:\/\/whois.arin.net\/rest\/ip\/192.168.0.1"
  }
],
"repository" : {
  "id" : "2",
  "name" : "Rep2",
  "description" : ""
},
"error_code" : 0,
"error_msg" : "",
"warnings" : [],
"timestamp" : 1409848524}
Director Insights

This API resource is only usable in Tenable.sc Director.

/mgmt/insights

Methods

GET

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":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": "2021-06-06", "licenseSize": 2048, "licensedIPCount": 1530],
"date": "2021-06-04", "licenseSize": 2048, "licensedIPCount": 0],
"date": "2021-06-02", "licenseSize": 2048, "licensedIPCount": 0],
"date": "2021-05-31", "licenseSize": 2048, "licensedIPCount": 0],
"date": "2021-05-29", "licenseSize": 2048, "licensedIPCount": 0],
"date": "2021-05-27", "licenseSize": 0, "licensedIPCount": 0],
"date": "2021-05-25", "licenseSize": 0, "licensedIPCount": 0],
"usage": ["sciName": "demo sci", "licenseSize": 2048, "licensedIPCount": 0],
"errors": {"error_code": 0, "error_msg": "", "warnings": []},
"timestamp": 1608216905}
Director Organization

This API resource is only available for administrators in Tenable.sc Director

/mgmt/organization

Methods

GET

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

```json
{
  "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/ipinfo.html?ip=%IP%"
    },
    {
      "name" : "ARIN",
      "link" : "http://whois.arin.net/rest/ip/%IP%"
    }
  ],
  "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 testing"
    },
    {
      "id" : "5",
      "name" : "LCE 192.168.1.1",
      "description" : "Copied from Box for testing"
    }
  ]}
<table>
<thead>
<tr>
<th>id</th>
<th>name</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>NEW LCE</td>
<td>Copied from Box for testing</td>
</tr>
<tr>
<td>5</td>
<td>qa-lce4x-lifeA</td>
<td>Copied from Box for testing</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>IPv6 Rep</td>
<td></td>
</tr>
<tr>
<td>26</td>
<td>agrepo</td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>mp asset tests IPv6</td>
<td>Copied from QA</td>
</tr>
</tbody>
</table>
{
    "id": "29",
    "name": "Test IPv6",
    "description": "",
    "type": "Local",
    "dataFormat": "IPv6",
    "groupAssign": "fullAccess"
}
],
"zones": [],
"ldaps": [],
"pubSites": [
    {
        "id": "2",
        "name": "Test1",
        "description": "",
        "type": "CMRS"
    }
]
},
{
    "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/ipinfo.html?ip=%IP%"
},
{  
  "name" : "ARIN",
  "link" : "http://whois.arin.net/rest/ip/%IP%"
}
]
,  
"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
iplInfoLinks
zoneSelection
restrictedIPs
vulnScoreLow
vulnScoreMedium
vulnScoreHigh
vulnScoreCritical
vulnScoringSystem
createdTime
modifiedTime
userCount
lces
repositories
zones
nessusManagerspubSitesldaps

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?ip=\%IP\%

        ],
        
        
            "name" : "ARIN",
            "link" : "http:\/\/whois.arin.net\/rest\/ip\/\%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":"CMRS"
  }
]
},
"error_code" : 0,
"error_msg" : ":",
"warnings" : [],
"timestamp" : 1418050303
}
**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

```plaintext
?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
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**

```
{
    "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"
},
"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", "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": "" }}
/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",
"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"
},
"organization": {
  "id": "2",
  "name": "Org on 192.2.0.2",
  "description": "Generated by automation!"
}
},
"error_code": 0,
"error_msg": "",
"warnings": [],
"timestamp": 1615490707
}

/mgm/scanResult/{id}/email

Methods

POST
Emails the Scan Result associated with Director {id}.
For documentation please consult the normal Scan Result email endpoint documentation.

/mgm/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

```json
{
  "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,
"total IPs": "256",
"scanned IPs": "8",
"agentScanUUID": "",
"agentScanContainerUUID": "",
"startTime": "1615491193",
"finishTime": "-1",
"created Time": "1615491185",
"scanDuration": "305",
"importDuration": "-1",
"ioSyncDuration": "-1",
"completed IPs": "26",
"completed Checks": "3228449",
"total Checks": "32645376",
"can Use": "true",
"can Manage": "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": {
/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

```json
{
   "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": ""
/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.
**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

```json
{
   "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": ""
         }
      }
   ],
}
```
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",
        "organizations": []
    }
}
"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

```json
{
    "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
}
**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

```text
?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
umScans
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":"1",
"authType":"password",
"eolDate":1672444800,
"SCI":{
   "id":"2",
   "name":"172.26.103.72",
   "description":"Update"
}
}]}
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",
  }
}
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
}
```
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"
            ]
        },
        {

```
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")
            }
        ]
    }
}
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'.",
                "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 09:20:01 -0400"
},
{
"rawLog": "Tue, 22 Jun 2021 09:20:01 -0400|qahead|policy|INFO|' [qahead] deleted organization policy 'Basic Policy' (id #1000002).
"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).
"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 09:20:01 -0400"
"date": "Tue, 22 Jun 2021 09:18:08 -0400"

]}
},
"error_code": 0,
"error_msg": "",
"warnings": [],
"timestamp": 1624372254
}
Feed

/feed

Methods

GET

Gets the status of feed uploads.

Request Parameters

None

Example Response

Expand

{
   "type" : "regular",
   "response" : {
      "sc" : {
         "updateTime" : "1418977807",
         "stale" : "true",
         "updateRunning" : "false"
      },
      "active" : {
         "updateTime" : "1419269875",
         "stale" : "false",
         "updateRunning" : "false"
      },
      "passive" : {
         "updateTime" : "1373297113",
         "stale" : "true",
         "updateRunning" : "false"
      },
      "lce" : {
         "updateTime" : "0",
         "status" : "success",
         "data" : {
            "type" : "regular",
            "activity" : {"active": true,"passive": true,"sc": true,"lce": true},
            "lastActivityTime": "1419269875"
         }
      }
   }
}
"stale": "true",
"updateRunning": "false"
}

"error_code": 0,
"error_msg": "",
"warnings": [],
"timestamp": 1419270370
}

/feed/{type}

Methods

GET

Gets the status of feed the upload associated with <type>

NOTE: {type} can be one of “active”, “passive”, “lce”, “sc”, or “all”

Request Parameters

None

Example Response

Expand

{
  "type": "regular",
  "response": {
    "updateTime": "0",
    "stale": "true",
    "updateRunning": "false"
  },
  "error_code": 0,
  "error_msg": "",
  "warnings": []
}
Methods
POST
Sends a job to update the Feed type associated with
NOTE: {type} can be one of "active", "passive", "lce", "sc", or "all"

Request Parameters
None

Example Response
Expand
{
  "type" : "regular",
  "response" : "",
  "error_code" : 0,
  "error_msg" : "",
  "warnings" : [],
  "timestamp" : 1419269719
}

/feeds/active/process
Methods
POST
Processes an uploaded feed update file and sends a job to update the Feed type associated with <type>
NOTE: {type} can be one of "active", "passive", "lce", or "sc"
**Request Parameters**

Expand

```json
{
    "filename" : <string>
}
```

**Example Response**

Expand

```json
{
    "type" : "regular",
    "response" : 
    ,
    "error_code" : 0,
    "error_msg" : 
    ,
    "warnings" : []
    ,
    "timestamp" : 1419269719
}
```
**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="Filedatal; filedata="<baseName>"
Content-Type: <contentType>

<dataFile>
<dataBoundary>
...

**returnContent is provided**

...
<dataBoundary>
Content-Disposition: form-data; name="returnContent"

<dataReturnContent>
...

...
context is 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 =
- destinationPort = OPTIONAL (do not provide the preceding colon if not specified)
- formHost =
- formPort = OPTIONAL (do not provide the preceding colon if not specified)
- contentLength =
- dataBoundary =
- maxFileSize = (maximum size allowed for an uploaded file; It is best to check this on the client first if possible)
- fileData =
- baseName =
- returnContent = “false” | “true” DEFAULT “false”
- context = “auditfile” | “tailoringfile”
Example Response

Expand

{
    "type": "regular",
    "response": {
        "filename": "4fk1r0",
        "originalFilename": "filename.zip",
        "content": "",
        "context": [
            {
                "dataStreamName": "scap_gov.nist_datastream_USGCB-ie8-1.2.3.1.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
Example Response

Expand

{
    "type": "regular",
    "response": {
        "filename": "\opt\sc4\orgs\26\tmp\1.1421854135.bEiuob"
    },
    "error_code": 0,
    "error_msg": "",
    "warnings": [],
    "timestamp": 1404311344
}
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

creatorassets

repository
owner
creator
ipListAllIPs
repeatRule
start
end
duration
enabled
createdTime
modifiedTime
activeownerGroup
canManage
functional

**Legend**

* = *always comes back*

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


**Request Parameters**

None

**Example Response**

Expand

```json
{
  "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" : "freezeTest",
    "firstname" : "",
    "lastname" : ""
},
"owner" : {
    "id" : "1",
    "username" : "freezeTest",
    "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",
  "createdAt" : "1418327716",
  "modifiedTime" : "1418327716",
  "assets" : [],
  "active" : "false",
  "creator" : {
    "id" : "1",
    "username" : "freezeTest",
    "firstname" : "",
    "lastname" : ""
  },
  "owner" : {
    "id" : "1",
    "username" : "freezeTest",
    "firstname" : "",
    "lastname" : ""
  },
  "repository" : {
    "id" : "-1",
    "name" : "",
    "description" : ""
  }
},
"error_code" : 0,
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

```json
{
    "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": ""
      },
      "owner": {
         "id": "1",
         "username": "freezeTest",
         "firstname": "",
         "lastname": ""
      },
      "repository": {
         "id": -1,
         "name": ""
      }
   }
}
/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
**Legend**
* = always comes back

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

**Request Parameters**
None

**Example Response**
Expand

```json
{
    "type" : "regular",
    "response" : {
        "id" : "21",
        "name" : "4",
        "description" : "",
        "repeatRule" : "FREQ=DAILY;INTERVAL=1",
        "start" : "TZID=America\/New_York:20141119T235800",
```
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
}
Group

group

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

Ices

repositories
definingAssets
userCount
userscreateDefaultObjects

Session User has ShareObjects Permission

assets
policies
queries
credentials
dashboardTabsarcsauditFiles

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" : "Full Access",
           "description" : "Full Access group"
       },
       {
           "id" : "2",
           "name" : "Group A",
           "description" : ""
       },
       {
           "id" : "3",
           "name" : "Group B",
           "description" : ""
       },
   ]
}
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"
  },  
  {  
    "id" : "39",
    "name" : "ipv6 rep",
    "description" : "Copied from QA 2",
    "lastVulnUpdate" : "1437805904",
    "type" : "Local",
    "dataFormat" : "IPv6"
  },  
  {  
    "id" : "44",
    "name" : "Test w/pluginPrefs",
    "description" : "",
    "lastVulnUpdate" : "0",
    "type" : "Local",
    "dataFormat" : "mobile"
  },  
  {  
    "id" : "57",
    "name" : "test mobile airwatch rep",
    "description" : ""
  }
]
null
/group/{id}

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

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
dashboardTabsarcscauditFiles

Legend*

* = always comes back

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

Request Parameters

None

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"
    }
  },
}
"type" : "Local",
"dataFormat" : "mobile"
}
,
{
 "id" : "57",
 "name" : "test mobile airwatch rep",
 "description" : "",
 "lastVulnUpdate" : "0",
 "type" : "Local",
 "dataFormat" : "mobile"
}
]
,"definingAssets" : [
{
 "id" : "0",
 "name" : "All Defined Assets",
 "description" : "All defining ranges of the Group in whose context

},
{
 "id" : "0",
 "name" : "All Defined Ranges",
 "description" : ""
}
]
,"userCount" : 0,
 "users" : [],
 "createDefaultObjects" : "false",
 "assets" : [],
 "policies" : [],
 "queries" : [],
 "credentials" : [],
 "dashboardTabs" : [],
 "auditFiles" : [],
 "arcs" : [
{
"id" : "18",
"name" : "Database Settings",
"description" : "The Database ARC presents a series of policy statements that measure percentage compliance against policies and controls established for systems based around these controls, and rapidly identify gaps in the database security programs or policies."}
}

"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
Job
/job

Methods
GET

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*
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" : ""
            }
        }
    ]
}
"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" : ""
}
}
"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***

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"
},
"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
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

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",
   }]}
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>
        }...
    ] 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>
        }...
    ] DEFAULT []
    ...
}

Example Response

Expand

{
    "type" : "regular",
    "response" : {

"organizations" : [
    {
      "id" : "8",
      "name" : "Org",
      "description" : "Testing for Policies with New Schema"
    },
    {
      "id" : "9",
      "name" : "Test Org",
      "description" : ""
    }
],
"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,
   "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" : ""
}
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

Request Parameters
None

Example Response
Expand
{
    "type": "regular",
    "response": {
        "organizations": [
            {
                "id": "8",
                "name": "Org",
                "description": "Testing for Policies with New Schema"
            }
        ],
        "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" : {
        "username"
    }
}
"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",
            "application",
            "connection",
        ]
    }
}
"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
}
LCE Client

/lce/{id}/client

Methods

GET

GETs the list of LCE Clients associated with LCE server, depending on access and permissions.

Request Parameters

None

Example Response

Expand

```json
{
  "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" : "2003",
  "serverIP" : "192.168.1.1",
  "serverPort" : "31300",
  "lastUpdated" : -1,
  "lifeState" : -1,
  "authState" : -1,
  "policyFile" : "default_windows_tenableclient.lcp"
"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
}
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",

```json
```
"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

Reveks 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
}
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_tenableclient.lcp",
            "clientType": "tenableclient",
            "osType": "windows",
            "name": "TNS-MSExchangeServer"
        },
        {
            "filename": "TNS-MSSQLServer_windows_tenableclient.lcp",
            "clientType": "tenableclient",
            "osType": "windows",
            "name": "TNS-MSSQLServer"
        },
        {
            "filename": "TNS-MalwareDetectionOnly_osx_lceclient.lcp",
            "clientType": "lceclient",
            "osType": "osx",
            "name": "TNS-MalwareDetectionOnly"
        }
    ]
}


```json
{
  "filename": "TNS-MalwareDetectionOnly_rhel_lceclient.lcp",
  "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_tenableclient.lcp",
  "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.lcp",
  "clientType": "lceclient",
  "osType": "osx",
  "name": "TNS-ProcessExecutionOnly"
},
{
  "filename": "TNS-ProcessExecutionOnly_rhel_lceclient.lcp",
  "clientType": "lceclient",
  "osType": "rhel",
  "name": "TNS-ProcessExecutionOnly"
}
```
"name": "TNS-ProcessExecutionOnly",
},
{
  "filename": "TNS-ProcessExecutionOnly_windows_tenableclient.lcp",
  "clientType": "tenableclient",
  "osType": "windows",
  "name": "TNS-ProcessExecutionOnly"
},
{
  "filename": "TNS-TenableProducts-LCE_rhel_lceclient.lcp",
  "clientType": "lceclient",
  "osType": "rhel",
  "name": "TNS-TenableProducts-LCE"
},
{
  "filename": "TNS-TenableProducts-Nessus_rhel_lceclient.lcp",
  "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.lcp",
  "clientType": "lceclient",
  "osType": "rhel",
  "name": "TNS-TenableProducts-PVS"
},
{
  "filename": "TNS-TenableProducts-SC_rhel_lceclient.lcp",
  "clientType": "lceclient",
  "name": "TNS-TenableProducts-PVS"
"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"
}
"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_hpx_lceclient.lcp",
  "clientType" : "lceclient",
  "osType" : "hpx",
  "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"
}
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" |
}

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"?>
<options xmlns : xi="http : //www.w3.org/2003/XInclude">
<example>
<one>File</one>
<body>Content</body>
</example>
</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
}
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

Session user role “1” (Administrator)

host
port
encryption
dn
dnsField
lowercase
timeLimit
password
username
attrEmail
attrName
attrPhone
attrUsername
ldapUserProvisioning
ldapUserSync
searchString
createdTime
modifiedTime
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" : "1",
         "name" : "Test Name",
         "description" : "Test Description"
      },
      {
         "id" : "2",
         "name" : "testName",
         "description" : "testDescription"
      }
   ],
   "error_code" : 0,
   "error_msg" : ""
}
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>
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" : "",
    "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

**Session user role “1” (Administrator)**

host
port
encryption
dn
dnsField
lowercase
timeLimit
password
username
attrEmail
attrName
attrPhone
attrUsername
ldapUserProvisioning
ldapUserSync
searchString
createdTime
modifiedTime
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" : "1",
    "name" : "Test Name",
    "description" : "Test Description"
  }
}
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
Delete 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": "",
    "timestamp": 1500911088
}
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

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" : ""
   },
   "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" : ""
   }
}
},
"error_code" : 0,
"error_msg" : "",
"warnings" : [],
"timestamp" : 1410210283}
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.

NOTE: Only IPv4 and Agent Repositories are supported

Request Parameters

Expand

{  
  "ioNetworksEnabled" : <string> "false" | "true",
  "repositories" : [
    
    
    ] DEFAULT []
}

Example Response

Expand

{  
  "type": "regular",
  "response": {
    "2" : {
      "enabled" : "true",
    }
{"ioNetworkUUID": "990a9c09-222d-4771-b25a-1fa7a8364322",
"firstSyncTime": "1573843474",
"lastSyncSuccess": "1573843474",
"lastSyncFailure": "-1",
"details": ""
},

"3": {
  "enabled": "true",
  "ioNetworkUUID": "b3a472c5-823f-477f-a082-70b32d279d36",
  "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
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
Methods

GET

GETs the schedule for daily synchronization of Assets to Lumin.

Request Parameters

None

Example Response

Expand

```json
{
    "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": "",
    "timestamp": 1572462204
}
```
/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
}
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
*descriptionvalueeditoripPref
pluginIDs

Legend*
*

* = always comes back

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

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"
    }
  ]
}
"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
ip
Pref
pluginIDs

Legend*

* = always comes back

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

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**

```
{
    "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
}

/notifications/{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
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
}
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
**name
**description
email
address
city
state
country
phone
delix
ipInfoLinks
zoneSelection
restrictedIPs
vulnScoreLow
vulnScoreMedium
vulnScoreHigh
vulnScoreCritical
vulnScoringSystem
createdTime
modifiedTime
userCount
lces
repositories
zones
nessusManagerspubSitesldaps

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",
            "name" : "Org",
            "description" : "New Org",
            "email" : "",
            "address" : "",
            "city" : "",
            "state" : "",
            "country" : "",
        }
    ]
}
"phone" : "",
"fax" : "",
"ipInfoLinks" : [
    {
        "name" : "SANS",
        "link" : "https:\/\/isc.sans.edu\/ipinfo.html?ip=%IP%"
    },
    {
        "name" : "ARIN",
        "link" : "http:\/\/whois.arin.net\/rest\/ip\/%IP%"
    }
],
"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 testing"
    },
    {
        "id" : "4",
        "name" : "NEW LCE",
        "description" : "Copied from Box for testing"
    },
    {
        "id" : "5",
        "name" : "",
        "description" : ""
    }
]
"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"
"groupAssign" : "fullAccess"

],
"zones" : [],
"ldaps" : [],
"pubSites" : [
{
  "id" : "2",
  "name" : "Test1",
  "description" : "",
  "type" : "CMRS"
}
],
{
  "id" : "9",
  "name" : "Test Org 1",
  "description" : "",
  "email" : "",
  "address" : "",
  "city" : "",
  "state" : "",
  "country" : "",
  "phone" : "",
  "fax" : "",
  "ipInfoLinks" : [
    {
      "name" : "SANS",
      "link" : "https:\/\/isc.sans.edu\/ipinfo.html?ip=%IP%"
    },
    {
      "name" : "ARIN",
      "link" : "http:\/\/whois.arin.net\/rest\/ip\/%IP%"
    }
  ],
  "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" : [],
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>,
  "zoneSelection" : <string> "auto_only" | "locked" | "selectable" | "selectable+auto_restricted",
  "restrictedIPs" : <string> (valid IP address or range of IP addresses) OPTIONAL
  "lces" : [
    {
      "id" : <number>
    }...
  ] DEFAULT [],
  "repositories" : [
    {
      "id" : <number>
    }...}
... ] DEFAULT [],
"pubSites" : [ }
    "id" : <number>
]...
] DEFAULT [],
"zones" : [ }
    "id" : <number>
]...
] 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>
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?ip=%IP%"
            },
            {
                "name": "ARIN",
                "link": "http:\\/\/whois.arin.net\/rest\\/ip\/%IP%"
            }
        ],
        "zoneSelection": "auto_only",
        "restrictedIPs": "",
        "vulnScoreLow": "1",
        "vulnScoreMedium": "3",
    }
}
"vulnScoreHigh" : "10",
"vulnScoreCritical" : "40",
"vulnScoringSystem" : "CVSSv2",
"createdTime" : "1418052290",
"modifiedTime" : "1418052290",
"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"
  }
],
"zones" : [],
"ldaps" : [],
"nessusManagers" : [],
"pubSites" : []
},
"error_code" : 0,
"error_msg" : "",
"warnings" : [],
"timestamp" : 1418052290
}
/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
**name
**description
email
address
city
state
country
phone
fax
ipInfoLinks
zoneSelection
restrictedIPv4s
vulnScoreLow
vulnScoreMedium
vulnScoreHigh
vulnScoreCritical
vulnScoringSystem
createdTime
modifiedTime
userCount
Lces
repositories
zones
nessusManagerspubSitesldaps

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",
    "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?ip=%IP%"
      }
    ]
  }
}
{  
  "name" : "ARIN",
  "link" : "http://www.whois.arin.net/rest/ip/%IP%"
}
],
"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 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": [
PATCH

Edits the Organization associated with {id}, 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:

```json
{
  ...
  "repositories" : [
    {
      "id" : <number>
      "allUsers" : <string> "false" | "true" OPTIONAL
    }
    ...
  ]
  ...
}
```

Example Response
See /organization/{id}::GET

**DELETE**

Deletes the Organization 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
}
```

/organization/{id}/acceptRiskRule

**Methods**

**GET**

Gets the list of Accept Risk Rules in the Organization associated with {id}, 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
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)

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" : ""
        },
        "organization" : {
            "id" : "8",
            "name" : "Org",
            "description" : "Testing for Policies with New Schema"
        },
        "user" : {
            "id" : "1",
            "username" : "head",
            "firstname" : "Security Manager",
            "lastname" : ""
        },
        "plugin" : {
            "id" : "0",
            "name" : "Open Port",
            "description" : ""
        }
    }
],
"error_code" : 0,
"error_msg" : "",
"warnings" : []
}
"timestamp" : 1410275054
}

/organization/{id}/recastRiskRule

Methods
GET

Gets the list of Recast Risk Rules in the Organization associated with {id}, 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*
*
 Filters

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)

 Example Response

{  "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" : ""
         },
         "organization" : {
            "id" : "8",
            "name" : "Org",
            "description" : "Testing for Policies with New Schema"}
      }
   ]
}


```json
{
    "user": {
        "id": "1",
        "username": "head",
        "firstname": "Security Manager",
        "lastname": ""
    },
    "plugin": {
        "id": "0",
        "name": "Open Port",
        "description": ""
    }
}
```
Organization Security Manager

This endpoint should only be used by administrators and will only impact Security Managers in the Full Access Group.

/organization/{orgID}/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
**firstname
**lastname
**status
role
username
title
e-mail
address
city
state
country
phone
fax
createdTime
modifiedTime
lastLogin
lastLoginIP
mustChangePassword
locked
failedLogins
authType
fingerprint
password
description
managedUsersGroups
managedObjectsGroupscanUsecanManagepreferences responsibleAsset
group
ldapUsername
dlapparent

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",
         "status": "0",
         "username": "head",
         "ldapUsername": "head",
         "firstname": "",
         "lastname": "",
         "description": "",
         "managedObjectsGroupscanUse": false,
         "canManagepreferences": false,
         "responsibleAsset": null,
         "group": null,
         "ldapUsername": "head",
         "dlapparent": false
      }
   ]
}
"title" : "",
"email" : "",
"address" : "",
"city" : "",
"state" : "",
"country" : "",
"phone" : "",
"fax" : "",
"createdTime" : "1433519288",
"modifiedTime" : "1453477493",
"lastLogin" : "1454347644",
"lastLoginIP" : "172.26.0.0",
"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 access to all actions at the organization level. A Security Manager can manage users and groups as well, even if they are part of the same group. Additionally, Security Managers are responsible for scanning. They can manage Access 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 Windows installed. This 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"
  },
  "organization" : {
    "id" : "0",
  },
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
  "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>,
"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"
authType “linked”

"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 parameter>,
"importDashboards" : <string> "false" | "true" DEFAULT <Target Group’s createDefaultObjects parameter>,
"importARCs" : <string> "false" | "true" DEFAULT <Target Group’s createDefaultObjects parameter>
"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",
    "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 access to all actions at the organization level. A Security Manager can personally or remotely view and stop running scans and reports. A Security Manager can set and change user 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 Windows installed."
},
"group" : {
/organization/{orgID}/securityManager/{id}

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
**firstname
**lastname
**status
**role
username
title
email
address
city
state
country
phone
fax
createdTime
modifiedTime
lastLogin
lastLoginIP
mustChangePassword
locked
failedLogins
authType
fingerprint
password
description
managedUsersGroups
managedObjectsGroups
scanUse
manage
preferences
responsibleAssetGroup
ldap
ldapUsername
parent

**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",
    "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",
    "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 access to all actions at the organization level. A Security Manager can perform all actions on the Security Manager and Security Group pages, including creating, editing, and deleting security groups. They can also manage the Access tab of User add/edit. This includes viewing and stopping running scans and reports."
},
"responsibleAsset" : {
    "id" : "19",
    "name" : "Windows Hosts",

PATCH

Edits the Security Manager associated with {id}.

If editing a linked user (a user whose authType = "linked"), you cannot modify roleID, groupId, authType,
parent, password, or mustChangePassword.

**Request Parameters**

(All fields are optional)

See /organization/{orgID}/securityManager::POST for parameters.

**Example Response**

See organization/{orgID}/securityManager/{id}::GET

**DELETE**

Deletes the Security Manager associated with {id}.

The objects owned by the user being deleted can be migrated to another user in the same organization by passing in the optional migrateUserID parameter.

**Request Parameters**

Expand

```
{
  "migrateUserID": <number> OPTIONAL
}
```

**Example Response**

Expand

```
{
  "type": "regular",
  "response": "",
  "error_code": 0,
  "error_msg": "",
  "warnings": [],
  "timestamp": 1402436001
}
```
**Organization User**

This endpoint may only be used by administrators.

/organization/{orgID}/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`
* `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
        },
        {
            "id": "36",
            "username": "GroupA",
            "firstname": "",
            "lastname": "",
            "canUse": true,
            "canManage": true
        },
        {
            "id": "37",
            "username": "GroupB",
            "firstname": "",
            "lastname": "",
            "canUse": true,
            "canManage": true
        }
    ],
    "error_code": 0,
    "error_msg": "",
    "warnings": [],
    "timestamp": 1454348491
}
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
**firstname
**lastname
**status
role
username
title
e-mail
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
ldapDapUsername
parent

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",
      "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 access to all actions at the organization level. A Security Manager can access the System Settings tab of User add/edit to manage user permissions. This role is required to configure email settings and rules. It can also view and stop running scans and reports."
},
"responsibleAsset" : {
    "id" : "19",
    "name" : "Windows Hosts",
    "description" : "The operating system detected has Windows installed. This 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",
"
"organization" : {
    "id" : "0",
    "name" : "Tenable.sc Administration",
    "description" : ""
}
}

"error_code" : 0,
"error_msg" : "",
"warnings" : [],
"timestamp" : 1454348768
}
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",
    }  
    ]
}
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"
}
],
"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"
    }
],
"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" : "OUTDATED",
            "update_status" : "UPDATE_REQUIRED",
            "update_start_time" : 1402435235,
            "update_progress" : 0,
            "update_end_time" : null
        }
    ]
}
"status" : "8200"
}
],
"error_code" : 0,
"error_msg" : "",
"warnings" : []
"timestamp" : 1402435137
}
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
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 portion of the “xrefs:” parameter is associated with a valid Xref field type. Valid Xref types at the time of this documentation are:


{
    "filterField" : <string> "copyright" | "description" | "exploitAvailable" | "family" | "id" | "name" | "patchPubDate" | ... | "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",
    "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":"15000",
      "name":"Debian DSA-163-1 : mhonarc - XSS",
      "description":"Jason Molenda and Hiromitsu Takagi found ways to exploit cross site scripting bugs in mhonarc, a mail to

 <MIMEExcs> text/html text/x-html <MIMEExcs>

The type 'text/x-html' is probably not used any more, but is good to
include it, just-in-case.

If you are concerned that this could block other similar updates, use
2.4.4-1.1 for the old
stable distribution (potato) and in version 2.5.11-1 for the unstable
distribution (sid)."
    },
    {
      "id":"15004",
      "name":"Debian DSA-167-1 : kdelibs - XSS",
      "description":"A cross site scripting problem has been discovered in Konqueror, a
famous browser for KDE and other programs using KHTML. The KDE team
report that Konqueror's cross site scripting protection fails to
initialize the domains on sub-(i)frames correctly. As a result,
JavaScript programs that use
the KHTML rendering engine may become victim of a cookie stealing and
other cross site scripting attacks."
    }
  ],
  "error_code":0,
  "error_msg":"",
  "warnings":[]
}

/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
cPort
dstPort
protocol
riskFactor
solution
seeAlso
synopsis
checkType
exploitEase
exploitAvailable
exploitFrameworks
cvssVector
cvssVectorBF
cvssV3Vector
cvssV3VectorBF
cvssV3BaseScore
cvssV3TemporalScore
cvssV3Score
vprScore
**vprContext**
stigSeverity
pluginPubDate
pluginModDate
patchPubDate
patchModDate
vulnPubDate
modifiedTime
md5xrefs

**Legend**
*

* = *always comes back*

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

**Request Parameters**
None

**Example Response**
Expand

```json
{
  "type" : "regular",
  "response" : {
    "id" : "0",
    "name" : "Open Port",
    "description" : "",
    "type" : "active",
    "copyright" : "",
    "version" : "",
    "sourceFile" : "",
    "dependencies" : "",
    "requiredPorts" : ""
  }
}
```
"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" : "",
"xrefs" : "",
"source" : "",
"family" : {
"id" : "42",
"name" : "Port scanners",
"type" : "active"}

}
"error_code" : 0,
"error_msg" : "",
"warnings" : [],
"timestamp" : 1408727888
}
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 portion of the “xrefs:” 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" | "IATV" | "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" | "..." | "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",
  "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

```json
{
    "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",

594
"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" : "" }
"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**

**Request Parameters**

None

**Example Response**

Expand

```json
{
    "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**

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 portion of the “xrefs:” parameter is associated with a valid Xref field type. Valid Xref types at the time of this documentation are:

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" : [

Potential security vulnerabilities have been identified in the HP System Management Homepage (SMH) for HP-UX. These vulnerabilities could be exploited remotely to allow cross site scripting (XSS).
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
**descriptionType
uri
authType
cert
username
password
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:\/\slash192.168.1.1\slashtest",
      "authType" : "password",
      "cert" : "",
      "username" : "test",
      "password" : "SET",
      "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>,
   "authType" : <string> "certificate" | "password",
   "organizations" : [
       {
           "id" : <number>
       }
   ]
}
```

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",
"authType" : "password",
"cert" : "",
"username" : "test",
"password" : "SET",
"maxChunkSize" : "0",
"createdTime" : "1404245619",
"modifiedTime" : "1404245619",
"organizations" : [ ]
},

"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
** descriptionType
uri
authType
cert
username
password
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

```json
{
    "type" : "regular",
    "response" : {
        "id" : "2",
    }
}
```
"name" : "test",
"description" : "desc",
"type" : "HTTP POST",
"uri" : "http:\/\/192.168.1.1\test",
"authType" : "password",
"cert" : "",
"username" : "test",
"password" : "SET",
"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
}
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"
}

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 query"
            }
        ]
    }
}


},
{
  "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 query"
},
{
"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: 'Test Asset 1"
},
{
"id" : "1435",
"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 en
"endOffset" : <number> OPTIONAL (integer),
"tool" : <string> "listalerts",
"filters" : [
    {
        "filterName" : <string> "alertName" | "createdEndTime" | "createdStartTime" |
                        "createdTimeFrame" | "description" | ... | "lastTriggeredStartTime" |
                        "lastTriggeredTimeFrame" | "modifiedEndTime" | "modifiedStartTime" |
                        "modifiedTimeFrame",
        "operator" : <string> ",",
        "value" : <string> | <number>
    }...
] DEFAULT []
...

Type: "Ice" (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”.

...
"operator" : <string> "=" | "!=" | "<=" | ">=",
"value" : (Format depends on filter's "filterName" parameter)

] DEFAULT []
...

sourceType "archive"

**Note:** sourceType will never be "archive." This is included for informational purposes only. Current functionality doesn't accept 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 "sortDir" : <string> "ASC" | "DESC" OPTIONAL (default "ASC" if not specified an "startOffset" : <number> OPTIONAL (integer; lower bound to returned record set. "endOffset" : <number> OPTIONAL (integer; upper bound to returned record set. "tool" : <string> "listvuln" | "sumdeviceid" | "summdmuser" | "summodel" | "sumoscpe" | "sumpluginid" | "vulndetails",
"filters" : [}
"filterName" : <string> "baseCVSSScore" | "cvssV3BaseScore" | "deviceID" | "deviceModel" | "deviceUser" | "deviceVersion" | ... | "pluginPublished" | "port" | "protocol" | "repository" | "repositoryIDs" | "serialNumber" | "severity" | "vulnPublished",

filterName "osCPE" | "baseCVSSScore" | "cvssV3BaseScore" | "pluginOutput" | "repository" | "repositoryIDs" | "deviceID" | "deviceModel" | "deviceUser" | "pluginID"

------------------------------------------------------------

"operator" : "=" | "!=",
"value" : (Format depends on filter's "filterName" parameter)

filterName "mdmType" | "pluginName" | "lastMitigated" | "lastSeen" | "vulnPublished" | "pluginModified" |... | "mitigatedStatus" | "pluginText" | "port" | "protocol" | "recastRisk" | "responsibleUser" | "severity" | "xref"

---------------------------------------------------------------------------------------------------------------------------------

"operator" : <string> "=" | "<=" | ">=" | "!=" | "between" | "outside" | "contains" | "excludes" | "in" | "!in",
"value" : (Format depends on filter's "filterName" parameter)

}...
] 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" | "assignedStartTime" | "assignedTimeFrame" | "assignee" | "assigneeID" | ... | "modifiedTimeFrame" | "owner" | "ownerID" | "resolvedEndTime" | "resolvedStartTime" | "resolvedTimeFrame" | "status",
    "value" : (Format depends on filter's "filterName" parameter)
}...
] 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" | "country" | "email" | "firstname" | "group" | "groupID" | ...
    "operator" : <string>,
    "value" : (Format depends on filter's "filterName" parameter)
  }
]
...

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),
"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).
"tool" : <string> "iplist" | "listmailclients" | "listos" | "listservices" | "listsshservers" | ...
"filters" : [
  {
    "filterName" : <string> "address" | "authType" | "country" | "email" | "firstname" | "group" | "groupID" | ...
    "operator" : <string>,
    "value" : (Format depends on filter's "filterName" parameter)
  }
]...
"filterName" : <string> "acceptRiskStatus" | "asset" | "assetID" | "auditFile" | "auditFileID" | "baseCVSSScore" | ...

"filterName" "acceptRiskStatus"

"operator" : <string> ";",
"value" : <string> "all" | "accepted" | "notAccepted"

NOTE: During evaluation on the Analysis page, or for various objects, presenting no "acceptRiskStatus" filter defaults to the "notAccepted" behavior.

"filterName" "asset"

"operator": <string> ";" | "~" (combination expression),

"filterName" "asset", operator ";"

"value" : [<comboRecord> {
   "id" : <number> (integer)
}...]

"filterName" "asset", operator "~"

"value" : <comboRecord> {
   "operator": <string> "complement" | "intersection" | "difference" | "union",
   "operand1": <comboRecord> | <number> (integer) | {
      "id" : <number> (integer)
   }
}

operator not "complement"

"operand2": <comboRecord> | <number> (integer) | {
   "id" : <number> (integer)
}
filterName "auditFile" | "policy" | "repository" | "responsibleUser"

"operator": <string> "=",
"value" : {
    "id" : <number> (integer)
}

filterName "baseCVSScore"

"operator" : <string> "=",
"value" : <string> (inclusive, nonnegative, decimal range, using a dash ["-"] delimiter)

filterName "benchmarkName"

"operator" : <string> "=" (fuzzy-left, right-anchored match),
"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 entire entries string) | "pcre" (i.e., Perl-compatible, regular expression, across entire entries string),

filterName "cpe", operator "=" | "~="

"value" : <string> (comma-separated or newline-separated list)

filterName "cpe", operator "pcre"
"value" : <string> (Perl-compatible, regular expression)

filterName "cveID" | "msbulletinID"

"operator" : <string> "==" (fuzzy match),
"value" : <string> (comma-separated or newline-separated list)

filterName "cvssVector"

"operator" : <string> "==",
"value" : <string> (comma-separated list of Simple or Complex CVSS vectors)

Simple CVSS Vector = <string> "AV:L" | "AV:A" | "AV:N" | "AC:H" | "AC:M" | "AC:L" | "Au:N" | "Au:S" | "Au:M" | "C:N" | ...

Complex CVSS Vector = <string> (slash-separated list of Simple CVSS Vectors where all entries must match)

filterName "cvssV3BaseScore"

"operator" : <string> "==",
"value" : <string> (inclusive, nonnegative, decimal range, using a dash "-" delimiter)

filterName "cvssV3Vector"

"operator" : <string> "==",
"value" : <string> (comma-separated list of Simple or Complex CVSS vectors)

Simple CVSS Vector = <string> "AV:P" | "AV:L" | "AV:A" | "AV:N" | "PR:H" | "PR:L" | "PR:N" | "PR:U" | ...

Complex CVSS Vector = <string> (slash-separated list of Simple CVSS Vectors where all entries must match)

filterName "daysMitigated" | "firstSeen" | "lastMitigated" | "lastSeen"

"operator": <string> "==" (relative with custom format),
"value" : <string> "<minDaysBack>:<maxDaysBack>" (Both minDaysBack and

filterName "dnsName"
"operator": <string> ",",
"value": <string> (comma-separated or newline-separated list of valid DNS names)

filterName "exploitAvailable"

"operator": <string> ",",
"value": <string> "true" | "false"

filterName "exploitFrameworks"

"operator": <string> "," (i.e., explicit for entire entries string) | 
"~=" (i.e., fuzzy match across entire entries string)
"value": <string>

filterName "family"

"operator": <string> "," | 
"!=",
"value": [ 
  { 
    "id": <number> (integer) 
  }...
]

filterName "ip"

"operator": <string> "," | 
"!=",
"value": <string> (comma-separated or newline-separated list of 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>:all" (Both 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> "=" | "!=" | "<=" | ">=",
"value": <number> (comma-separated or newline-separated list of 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" (i.e., Perl-compatible, regular expression),
"value": <string>

filterName "pluginText"

"operator": <string> "=" (i.e., fuzzy match, stripped text [forced]) | "pcre" (i.e., Perl-compatible, regular expression),
"value": <string>
filterName "pluginType"
----------------------
"operator": <string> ":=",
"value" : <string> "passive" | "lce" | "active" | "compliance" (comma-separated)

filterName "port" | "tcppport" | "udpport"
-----------------------------------------------
"operator" : <string> ":=" | ":!=" | ":<=" | ":>=",

filterName "port" | "tcppport" | "udpport", operator ":=" | ":!="
-----------------------------------------------
"value" : <number> (comma-separated or newline-separated list of integers or inclusive integer ranges, using a dash ["-"] delimiter, with each value between 0 and 65535)

filterName "port" | "tcppport" | "udpport", operator ":<=" | ":>="
-----------------------------------------------
"value" : <number> (integer, between 0 and 65535)

filterName "protocol"
----------------------
"operator": <string> ":=" | ":!=",
"value" : <string> (comma-separated or newline-separated list of integers)

filterName "recastRiskStatus"
-------------------------------
"operator" : <string> ":=",
"value" : <string> "recast" | "notRecast"

filterName "severity"
----------------------
"operator": <string> ":=" | ":!=",
"value" : <string> (comma-separated or newline-separated list of integers)
{
   "id" : <number> (integer)
}...
sourceType null

Note: sourceType will always be null. Current functionality doesn’t accept sourceType parameter,
and will always set it to default QUERY_NOT_TREND (null)

...  
"tool" : <string> "cceipdetail" | "cveipdetail" | "iavmipdetail" | "ipcount" | 
...  
sourceType “cumulative”

Note: sourceType will never be “cumulative.” This is included for informational purposes only. Current functionality doesn’t accept sourceType parameter, and will always set it to default QUERY_NOT_TREND (null)

...  
"tool" : <string> "cceipdetail" | "cveipdetail" | "iavmipdetail" | "ipcount" | 
"scanID" : <number> 
...

Example Response

Expand

{
  "type" : "regular",
  "response" : {
    "id" : "12",
    "creatorID" : "1",
    "ownerID" : "1",
    "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"
},
"owner" : {
  "id" : "1",
  "username" : "JohnD",
  "firstname" : "John",
  "lastname" : "Doe"
},
"ownerGroup" : {
  "id" : "0",
  "name" : "Full Access",
  "description" : "Full Access group"
},
"targetGroup" : {
  "id" : "-1",
  "name" : "",
  "description" : ""
}
/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",
    "creatorID" : "1",
    "ownerID" : "1",
    "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"
},
"owner" : {
  "id" : "1",
  "username" : "JohnD",
  "firstname" : "John",
  "lastname" : "Doe"
},
"ownerGroup" : {
  "id" : "0",
  "name" : "Full Access",
  "description" : "Full Access group"
},
"targetGroup" : {
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",
    "creatorID" : "1",
    "ownerID" : "1",
    "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" : ""

}, 
"owner" : { 
  "id" : "1", 
  "username" : "head", 
  "firstname" : "Security Manager", 
  "lastname" : ""

}, 
"ownerGroup" : { 
  "id" : "0", 
  "name" : "Full Access", 
  "description" : "Full Access group"

}, 
"targetGroup" : { 
  "id" : "-1",
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
}
**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
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:

**Example Response**

Expand

```json
{
    "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" : ""
            }
        }
    ]
}
```
POST

Adds a Recast Risk Rule to one repository.

**Request Parameters**

Expand

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

Example Response
{  
  "type": "regular",
  "response": [
    {
      "id": "1",
      "repID": "18",
      "orgID": "8",
      "userID": "1",
      "pluginID": "0",
      "newSeverity": "0",
      "hostType": "all",
      "hostValue": "",
      "port": "any",
      "protocol": "any",
      "comments": "",
      "order": "1",
      "status": "0",
      "createdTime": "1410281580",
      "modifiedTime": "1410281580",
      "repository": {
        "id": "18",
        "name": "New Rep 1",
        "description": ""
      },
      "organization": {
        "id": "8",
        "name": "Org",
        "description": "Testing for Policies with New Schema"
      },
      "user": {
        "id": "1",
        "username": "head",
        "firstname": "Security Manager",
        "lastname": "Security Manager"
      }
    }
  ]
}
"lastname" : ""
},
"plugin" : {
  "id" : "0",
  "name" : "Open Port",
  "description" : ""
}
],
"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
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",
    "createdTime" : "1410281580",
  }
}
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
}

/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
}
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.

{  
    "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 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",
"creatorID" : "1",
"ownerID" : "1",
"reportDefinitionID" : "-1",
"jobID" : "1614",
"name" : "Test Scan",
"description" : "This report identifies installed software across a series of hosts, utilizing Nessus plugin 22869, and captures the host Scan Date, and is followed by the host Operating System and a list of installed software, and version (if available).
\n"type" : "pdf",
"status" : "Completed",
"running" : "false",
"errorDetails" : "Error removing components.
Error removing component #6.
Error deleting Data Source #10.
Error retrieving owner of Query.
User #1 not found.
",
"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"
},
"owner" : {
"id" : "1",
"username" : "head",
"firstname" : "test",
"lastname" : "User"
},
"ownerGroup" : {
  "id" : "0",
  "name" : "Full Access",
  "description" : "Full Access group"
}
], ...

"manageable" : [
{
  "id" : "1",
  "creatorID" : "1",
  "ownerID" : "1",
  "reportDefinitionID" : "-1",
  "jobID" : "1614",
  "name" : "Test Scan",
  "description" : "This report identifies installed software across a series of hosts, utilizing Nessus plugin 22869, 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.
  Error removing component #6.
  Error deleting Data Source #10.
  Error retrieving owner of Query. 
  User #1 not found.

  "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"
},
"owner": {
  "id": "1",
  "username": "head",
  "firstname": "test",
  "lastname": "User"
},
"ownerGroup": {
  "id": "0",
  "name": "Full Access",
  "description": "Full Access group"
}
], ...
]
"error_code": 0,
"error_msg": "",
"warnings": [],
"timestamp": 1404919744
}
/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

```json
{
    "type": "regular",
    "response": {
        "id": "1",
        "creatorID": "1",
        "ownerID": "1",
        "reportDefinitionID": "-1",
        "jobID": "1614",
        "name": "Test Scan",
        "description": "This report identifies installed software across a series of hosts, utilizing Nessus plugin 22869, and documents each host's Scanning 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.
Error removing component #6.
Error deleting Data Source #10.
Error retrieving owner of Query.
User #1 not found."
    },
    "totalSteps": "8",
    "completedSteps": "4",
    "startTime": "1403298387",
    "finishTime": "1403299387",
    "ownerGID": "0",
    "pubSites": [
        {
            "id": "2",
            "name": "test",
            "description": "desc"
        }
    ]
}
```
DELETE

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

Request Parameters

None

Example Response

Expand
/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" : "",
    "timestamp" : 1403100582
}
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
}

POST

Downloads the report associated with {id}. 

---

ентр

"warnings" : [],
"timestamp" : 1406924039
}
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
}
```
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
emailTargetType
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

** 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" : "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:2:{s:4:"name";}};
  "encryptionPassword" : "",
  "status" : "0",
  "shareUsers" : [],
  "emailUsers" : [],
  "emailTargets" : "",
  "emailTargetType" : "1",
  "createdTime" : "1410369405",
  "modifiedTime" : "1410369421",
  "pubSites" : [],
  "sources" : [}
null
"owner" : {
    "id" : "1",
    "username" : "head",
    "firstname" : "Security Manager",
    "lastname" : ""
},
"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" : "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";"encryptionPassword";}};s:8:"status";"0";s:9:"shareUsers";a:0;"emailUsers";a:0;"emailTargets";"";s:10:"emailTargetType";"1";"createdTime";"1410369657";"modifiedTime";"1410369657";"pubSites";a:0;"sources" : [
  {
    "id" : "4",
    "queryID" : "12",
    "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" : "8",
  "type" : "template",
  "start" : "",
  "repeatRule" : "",
  "nextRun" : 0
},
"creator" : {
  "id" : "1",
  "username" : "head",
  "firstname" : "Security Manager",
  "lastname" : ""
},
"owner" : {
  "id" : "1",
  "username" : "head",
  "firstname" : "Security Manager",
  "lastname" : ""
},
"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",
"stylesheet": "-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";}}
"encryptionPassword": "",
"status": "0",
"shareUsers": []
}
"emailUsers" : [],
"emailTargets" : "",
"emailTargetType" : "1",
"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" : ""
},
"owner" : {  
  "id" : "1",
  "username" : "head",
  "firstname" : "Security Manager",
  "lastname" : ""
},
"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" : "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";""}};e:0:"";s:8:"type";"";s:7:"name";"";s:9:"data";"";s:10:"guid";"";s:5:"rows";"";s:22:"isAjaxSortable";"false";s:4:"text";"";s:4:"sort";"false";s:4:"dir";"false";s:4:"checkbox";"false";}">
"encryptionPassword" : "",
"status" : "0",
"shareUsers" : [],
"emailUsers" : [],
"emailTargets" : "",
"emailTargetType" : "1",
"createdTime" : "1410369657",
"modifiedTime" : "1410369657",
"pubSites" : [],
"sources" : [
    {
        "id" : "4",
        "queryID" : "12",
        "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" : "8",
"type" : "template",
"start" : "",
"repeatRule" : "",
"nextRun" : 0
},
"creator" : {
"id" : "1",
"username" : "head",
"firstname" : "Security Manager",
"lastname" : ""
},
"owner" : {
"id" : "1",
"username" : "head",
"firstname" : "Security Manager",
"lastname" : ""
},
"ownerGroup" : {
"id" : "0",
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),  
    "emailTargetType" : <number> 1 (Email target "To") | 2 (Email target "Bcc") DEFAULT...
}

schedule["type"] is "ical"
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" | "patched",
    "sortColumn" : <string>,
    "sortDirection" : <string>,
    "iteratorID" : <number> DEFAULT "-1" (not set)

    queryID is not provided
    -----------------------
    "query" : <query object>,
  }
}

..."styleFamily" : <number>,
"definition" : {
  "chapters" : [
    {
      "...

****NOTE: ARC Objects may not be passed. ARCs must be created separately before added to a Report.

..."styleFamily" : <number>,
"definition" : {
  "chapters" : [
    {"schedule" : {
      "start" : <string> (This value takes the iCal format),
      "repeatRule" : <string> (This value takes the repeat rule format)
    },
    ...
"tag" : <string> "section" | "group" | "iterator" | "component",
"name" : <string>,
"styleID" : <number> DEFAULT "-1" (not set),
"elements" : [
  {
    "tag" : <string> "arc" | "section" | "group" | "iterator" | "component",
    "id" : <number> DEFAULT -1,
  }
]

"elements parameter is provided

"styleID" : <number> DEFAULT "-1" (not set),
"displayDataPoints" : <number>,
"columns" : [
  {
    "name" : <string>
  }
] OPTIONAL?,

"definition" : {
  "dataSource" : {
    "queryID" : <number> OPTIONAL,
    "querySourceType" : <string> "archive" | "cumulative" | "individual" | "lce" | "mobile" | "patched",
    "querySourceID" : <number>,
    "querySourceView" : <string> "" | "new" | "all"
  }
}
"sortColumn" : <string>,
"sortDirection" : <string>,
"iteratorID" : <number> DEFAULT "-1" (not set)

queryID is not provided
-------------------------------
"query" : <query object>,
}
}
"dataPoints" : <string> "all" (php int max 9223372036854775807)

  tag "component"
  ----------------
  **see/dashboard/component::POST for additional variables**
...
]...
]...
],...
...

  type "asr"
...

  "definition" : {
    "asrInfo" : {
      "includeARF" : <string> "false" | "true" (required)
      "content" : <string> "benchmark" | ???? (required)

      content "benchmark"
      ---------------------
      "benchmarks" : []
    },
    "dataSource" : {
      "queryID" : <number> OPTIONAL (if provided, must be associated with a vuln query),
      "querySourceType" : <string> "archive" | "cumulative" | "individual" |
"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 associated with a vulnerability 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";}}}
"encryptionPassword" : ""
"status" : "0",
"shareUsers" : [],
"emailUsers" : [],
"emailTargets" : "",
"emailTargetType" : "1",
"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" : ""
},

"owner" : {
  "id" : "1",
  "username" : "head",
  "firstname" : "Security Manager",
  "lastname" : ""
},

"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
eemailTargets
eemailTargetType
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

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:7:"encryptionPassword": "",
"status": "0",
"shareUsers": [],
"emailUsers": [],
"emailTargets": "",
"emailTargetType": "1",
"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": ""
},
"owner": {
    "id": "1",
    "username": "head",
    "firstname": "Security Manager",
    "lastname": ""
},
"ownerGroup": {
    "id": "0",
    "name": "Full Access",
    "description": "Full Access group"
},
"attributeSet": {
    "id": "5",
    "name": "test",
    "description": ""
}
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
{ 
    "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:14:"encryptionPassword";"
        "status" : "0",
        "shareUsers" : [],
        "emailUsers" : [],
        "emailTargets" : "";
    }
}
"emailTargetType" : "1",
"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" : ""
},
"owner" : {
"id" : "1",
"username" : "head",
"firstname" : "Security Manager",
"lastname" : ""
},
"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
}
Report Image

/report/image

Methods

GET

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

```json
{
   "type": "regular",
   "response": [
      {
         "id": "1",
         "name": "Fake",
         "description": "faked from SQLite Manager"
      }
   ],
   "error_code": 0,
   "error_msg": "",
   "warnings": [],
   "timestamp": 1418679112
}
```

**POST**

Adds a Report Image.

**Request Parameters**

Expand

NOTE: The 'image' field is for GET only. It cannot be added or modified directly

```json
{
   "name": <string>,
   "description": <string> DEFAULT "",
   "type": <string> "Logo" | "Watermark",
   "filename": <string>,
   "originalFilename": <string> DEFAULT (filename)
}
```

**Example Response**
/report/image/{id}

Methods

GET

Gets the Report Image associated with {id}.

Fields Parameter
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" : "iVBORw0KGgoAAAANSUhEUgAAABwAAAOCAQAAACxYlW0AAAAC0lEQVQ4nO
XsAIAADnRA4bJFQAAAABJRU5ErkJggg==",
"creator" : {
  "id" : "1",
  "username" : "head",
  "firstname" : "Security Manager",
  "lastname" : ""
}
},
"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
}
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 ",",
  "searchString" : <string> (Search String Format. See NOTE#2) DEFAULT ",",
  "startOffset" : <number> (Positive Integer) DEFAULT ",",
  "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 testing of SC-19907"
    },
    {
      "id" : "2",
```
"name" : "FakedDataTemplate2",
"description" : "This is a faked data template for the testing of 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 of SC-19907",
    "summary": null,
    "definition": null,
    "styleFamily": "1",
    "screenshotCount": "2",
    "enabled": "true",
    "minUpgradeVersion": null,
    "templatePubTime": null,
    "templateModTime": null,
  }
}
/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

```json
{
   "type" : "regular",
   "response" : [
      {
         "id" : "1",
         "name" : "Threat Detection & Vulnerability Assessments",
         "description" : "Aid with identifying vulnerabilities and potential threats",
         "count" : "71"
      },
      {
         "id" : "2",
         "name" : "Monitoring",
```
"description" : "Provide intrusion monitoring, alerting and analysis.",
"count" : "36"
},
{
"id" : "3",
"name" : "Security Industry Trends",
"description" : "Influenced by trends, reports, and analysis from industry leaders.",
"count" : "5"
},
{
"id" : "4",
"name" : "Executive",
"description" : "Provide operational insight and metrics geared towards executives.",
"count" : "19"
},
{
"id" : "5",
"name" : "Compliance & Configuration Assessment",
"description" : "Aid with configuration, change and compliance management.",
"count" : "57"
},
{
"id" : "6",
"name" : "Discovery & Detection",
"description" : "Aid in trust identification, rogue detection, and new device discovery.",
"count" : "23"
}
],
"error_code" : 0,
"error_msg" : "",
"warnings" : [],
"timestamp" : 1412091153
}
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
Allowed Fields
*id
**name
**description
type
dataFormat
vulnCount
remoteID
remoteIP
running
downloadFormat
lastSyncTime
lastVulnUpdate
createdTime
modifiedTime
luminFields
ipOverlapstransfertypeFields 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

```json
{
    "type": "regular",
    "response": [
        {
            "id": "37",
            "name": "ag repo1",
            "description": "Copied from QA"
        },
        {
            "id": "38",
            "name": "jm ipv4",
            "description": "copied from QA"
        },
        {
            "id": "39",
            "name": "ipv6 rep",
            "description": "Copied from QA (name changed)"
        },
        {
            "id": "43",
            "name": "Test Local mobile Repository",
            "description": "DevForm test of mobile repository post"
        },
        {
            "id": "44",
            "name": "Test w/\pluginPrefs",
            "description": ""
        }
    ]
}
```
POST

Adds a Repository.

NOTE: See Lumin for Lumin synchronization settings.

NOTE: The fields related to data expiration (activeVulnsLifetime, passiveVulnsLifetime, IceVulnsLifetime, 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",
  "type" : <string> "Local" | "Remote" | "Offline",
  "downloadFormat" : <string> "v2" DEFAULT "v2" (see Note),
  "organizations" : [
    {
      "id" : <number>,
      "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"

type "ical"
----------
"start" : <string> (This value takes the iCal format),
"repeatRule" : <string> (This value takes the repeat rule format)
}
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"
}

type "ical"

"start" : <string> (This value takes the iCal format),
"repeatRule" : <string> (This value takes the repeat rule format)
}

type "Local"

"correlation" : [
  {
    "id" : <number>
  }...
] DEFAULT [],

...}

NOTE #1: For Front-end, the valid preference names and types may be retrieved by looking at the editor
block from /mdm::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 format)
},
"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"
...
```plaintext
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 repol",
        "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 New Schema"
            }
        ],
        "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"
},
"error_code" : 0,
"error_msg" : "",
"warnings" : [],
"generateNessus" : false,
"timestamp" : 1423767366

/repository/{id}

Methods

GET

 Gets the Repository associated with {id}. 
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, IceVulnsLifetime, 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, IceVulnsLifetime, complianceVulnsLifetime, mitigatedVulnsLifetime, percentCapacityCumulative, percentCapacityPatched**

**dataFormat “IPv6”**: nessusSchedule, correlation, ipRange, ipCount, runningNessus, lastGenerateNessusTime, lastTrendUpdate, trendingDays, trendWithRaw, activeVulnsLifetime, passiveVulnsLifetime, complianceVulnsLifetime, mitigatedVulnsLifetime, percentCapacityCumulative, percentCapacityPatched

**Allowed Fields**

*id
**name
**description
type
dataFormat
vulnCount
remoteID
remoteIP
running
downloadFormat
lastSyncTime
lastVulnUpdate
createdTime
modifiedTime
transfertypeFields 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

```json
{
    "type" : "regular",
    "response" : {
        "id" : "37",
        "name" : "ag repol",
        "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 New Schema"
      }
    ],
    "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",
      "emptiness": true
    }
}
"trendingDays": "0",
"trendWithRaw": "true",
"percentCapacityCumulative": "71",
"percentCapacityPatched": "62"
},
"luminFields": {
  "firstSyncTime": "1573594357",
  "lastSyncSuccess": "1573594357",
  "lastSyncFailure": "-1",
  "details": "details for LuminFields",
  "enabled": "true",
  "repository": {
    "id": "37",
    "name": "ag repo1",
    "description": "Copied"
  }
},
"error_code": 0,
"error_msg": "",
"warnings": [],
"timestamp": 1423767366
}

**PATCH**

Edits the Repository associated with {id}, 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}, depending on access and permissions.

**Request Parameters**

None

**Example Response**

Expand

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

/repository/{id}/acceptRiskRule

**Methods**

**GET**

Gets the list of Accept Risk Rules in the Repository associated with {id}, 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)

**Session User is not role “1” (administrator)**

organizationIDs=<number>,... | <string> "all" DEFAULT :sessionOrgID:
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": ""
            },
            "organization": {
                "id": "8",
                "name": "Org",
                "description": "Testing for Policies with New Schema"
            },
            "user": {
                "id": "1",
                "username": "head",
                "firstname": "Security Manager",
                "lastname": ""
            },
            "plugin": {
                "id": "0",
                "name": "Open Port",
                "description": ""
            }
        }
    ]
}
/repository/{id}/recastRiskRule

**Methods**

**GET**

*Gets the list of Recast Risk Rules in the Repository associated with {id}, 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)

Session User is not role "1" (administrator)
organizationIDs=<number>,... | <string> "all" DEFAULT :sessionOrgID:

Example Response

Expand

{
  "type" : "regular",
  "response" : [
    {
      "id" : "1",
      "newSeverity" : "0",
      "hostType" : "all",
      "hostValue" : "",
      "port" : "any",
      "protocol" : "any",
      "order" : "1",
    },
  ],
}
/repository/{id}/assetIntersections

GET

Gets the ip or uuid 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

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 “uuid” exists

{  
    "uuid" : <string> (valid uuid)
}

Parameter “uuid” does not exist

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

The /repository/import resource.

**POST**

Starts an on-demand, import for the Repository associated with {id}. The data is specified by a previously uploaded, **gzip**ped tarball of Repository data obtained using /repository/{id}/export.

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

Expand

```json
{
    "file" : <string>
}
```

**Example Response**

Expand

```json
{
    "type" : "regular",
    "response" : {
        "objectID" : "100",
        "objectType" : "importRepository",
        "type" : "now",
        "ownerID" : "1"
    },
    "error_code" : 0,
    "error_msg" : "",
    "warnings" : [],
    "timestamp" : 1402950576
}
```

**/repository/{id}/export**

The `/repository/export` resource.

**GET**

Exports the Repository associated with `{id}` as a gzipped 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

The /repository/sync resource.

**POST**

Starts an on-demand synchronization of local data for the remote Repository associated with {id}.

**Request Parameters**

None

**Example Response**

Expand

```
{
    "type" : "regular",
    "response" : {
        "objectID" : "107",
        "objectType" : "repositorySynchronizationClient",
        "type" : "now",
        "definition" : {
            "action" : "download",
            "token" : "1039771703"
        }
    },
```
/repository/{id}/updateMobileData

The /repository/updateMobileData resource.

**POST**

Starts an on-demand process to update the mobile data for the Repository associated with {id}. This is considered a mobile scan process by Tenable.sc.

**Request Parameters**

None

**Example Response**

Expand

```json
{
    "type": "regular",
    "response": {
        "id": "156"
    },
    "error_code": 0,
    "error_msg": "",
    "warnings": [],
    "timestamp": 1402942558
}
```
/repository/{id}/deviceInfo

GET

Gets the device information for the Repository 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

*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 “uuid” exists

{
   "uuid" : <string> (valid uuid)
}

Parameter “ip” exists

{
   "ip" : <string> (valid ip address),
   "dnsName" : <string> OPTIONAL
}

Example Response

Expand

{
   "type" : "regular",
   "response" : {
       "ip" : "192.168.0.1",
   
   "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.html?ip=192.168.0.1"
  },
  {
    "name" : "ARIN",
    "link" : "http : \//whois.arin.net\rest\ip\/192.168.0.1"
  }
],

"repository" : {
    "id" : "2",
    "name" : "Rep2",
    "description" : ""
  },
  "error_code" : 0,
  "error_msg" : "",
  "warnings" : [],
  "timestamp" : 1409855674
}

/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" : "",
```
The /repository/fetchRemote 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**

Parameters must be passed in as query string (as opposed to JSON) in the format of: /repository/fetchRemote/?host=172.26.X.X

Example Response

```
{
    "type" : "regular",
    "response" : [
        {
            "id" : "1",
            "name" : "qarep_ipv4",
            "description" : "",
            "type" : "Local",
            "host" : "<string>
        }
    ]
}
```
"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" : [],
"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" : [149
   {
      "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",
    "lastGenerateNessusTime" : "1402891203"}
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.
Role

/role

Methods

GET

 Gets the list of Roles

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

creator
createdTime
modifiedTime
permManageApp
permManageGroups
permManageRoles
permManageImages
permManageGroupRelationships
permManageBlackoutWindows
permManageAttributeSets
permCreateTickets
permCreateAlerts
permCreateAuditFiles
permCreateLDAPAssets
permCreatePolicies
permPurgeTickets
permPurgeScanResults
permPurgeReportResults
permScan
permAgentsScan
permShareObjects
permUpdateFeeds
permUploadNessusResults
permViewOrgLogs
permManageAcceptRiskRules
permManageRecastRiskRules
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

```json
{
    "type" : "regular",
    "response" : [
        {
```
"id" : "0",
"name" : "No Role",
"description" : "This role is available as a catch-all role if a role gets deleted. It has virtually no permissions.",
"createdTime" : "0",
"modifiedTime" : "0",
"permManageApp" : "false",
"permManageGroups" : "false",
"permManageRoles" : "false",
"permManageImages" : "false",
"permManageGroupRelationships" : "false",
"permManageBlackoutWindows" : "false",
"permManageAttributeSets" : "false",
"permCreateTickets" : "false",
"permCreateAlerts" : "false",
"permCreateAuditFiles" : "false",
"permCreateLDAPAssets" : "false",
"permCreatePolicies" : "false",
"permPurgeTickets" : "false",
"permPurgeScanResults" : "false",
"permPurgeReportResults" : "false",
"permScan" : "none",
"permAgentsScan" : "false",
"permShareObjects" : "false",
"permUpdateFeeds" : "false",
"permUploadNessusResults" : "false",
"permViewOrgLogs" : "false",
"permManageAcceptRiskRules" : "false",
"permManageRecastRiskRules" : "false",
"organizationCounts" : [
   {
      "id" : "12",
      "userCount" : "0"
   }
],
"creator" : {
"id" : "1",
"username" : "head",
"firstname" : "",
"lastname" : ""
}

{
"id" : "2",
"name" : "Security Manager",
"description" : "The Security Manager role has full access to all actions at the organization level. A Security Manager can view and stop running scans and reports, as well as manage and control access 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",
"permShareObjects" : "true",
"permUpdateFeeds" : "true",
"permUploadNessusResults" : "true",
"permViewOrgLogs" : "true",
"permManageAcceptRiskRules" : "true",
"permManageRecastRiskRules" : "true"}
"organizationCounts" : [
  {
    "id" : "12",
    "userCount" : "1"
  }
],
"creator" : {
  "id" : "1",
  "username" : "head",
  "firstname" : ",",
  "lastname" : ""
}
],
{
  "id" : "3",
  "name" : "Security Analyst",
  "description" : "The Security Analyst role has the permission to perform all actions at the organizational level except those that are reserved for advanced users.
  "createdTime" : "0",
  "modifiedTime" : "0",
  "permManageApp" : "false",
  "permManageGroups" : "false",
  "permManageRoles" : "false",
  "permManageImages" : "true",
  "permManageGroupRelationships" : "false",
  "permManageBlackoutWindows" : "true",
  "permManageAttributeSets" : "true",
  "permCreateTickets" : "true",
  "permCreateAlerts" : "true",
  "permCreateAuditFiles" : "true",
  "permCreateLDAPAssets" : "true",
  "permCreatePolicies" : "true",
  "permPurgeTickets" : "true",
  "permPurgeScanResults" : "true",
  "permPurgeReportResults" : "true",
  "permScan" : "full",
}
"permAgentsScan" : "true",
"permShareObjects" : "true",
"permUpdateFeeds" : "true",
"permUploadNessusResults" : "true",
"permViewOrgLogs" : "true",
"permManageAcceptRiskRules" : "true",
"permManageRecastRiskRules" : "true",
"organizationCounts" : [
    {
        "id" : "12",
        "userCount" : "0"
    }
],
"creator" : {
    "id" : "1",
    "username" : "head",
    "firstname" : "",
    "lastname" : ""
},
"id" : "4",
"name" : "Vulnerability Analyst",
"description" : "The Vulnerability Analyst role can perform basic tasks within the application. A Vulnerability Analyst is allowed to look at security data, perform scans, share objects, view logs and work with tickets.",
"createdTime" : "0",
"modifiedTime" : "0",
"permManageApp" : "false",
"permManageGroups" : "false",
"permManageRoles" : "false",
"permManageImages" : "false",
"permManageGroupRelationships" : "false",
"permManageBlackoutWindows" : "false",
"permManageAttributeSets" : "false",
"permCreateTickets" : "true",
"permCreateAlerts" : "true"
"permCreateAuditFiles" : "true",
"permCreateLDAPAssets" : "true",
"permCreatePolicies" : "true",
"permPurgeTickets" : "false",
"permPurgeScanResults" : "false",
"permPurgeReportResults" : "false",
"permScan" : "full",
"permAgentsScan" : "true",
"permShareObjects" : "true",
"permUpdateFeeds" : "true",
"permUploadNessusResults" : "true",
"permViewOrgLogs" : "true",
"permManageAcceptRiskRules" : "false",
"permManageRecastRiskRules" : "false",
"organizationCounts" : [
  {
    "id" : "12",
    "userCount" : "0"
  }
],
"creator" : {
  "id" : "1",
  "username" : "head",
  "firstname" : "",
  "lastname" : ""
},
{
  "id" : "5",
  "name" : "Executive",
  "description" : "The Executive role is intended for users who are interested in a high level overview of their security posture and can perform scans or managing users. Executives would also be able to assign tasks to other users using the Ticketing interface.",
  "createdTime" : "0",
  "modifiedTime" : "0",
  "permManageApp" : "false",
  "permManageGroups" : "false"}
"permManageRoles" : "false",
"permManageImages" : "false",
"permManageGroupRelationships" : "false",
"permManageBlackoutWindows" : "false",
"permManageAttributeSets" : "false",
"permCreateTickets" : "true",
"permCreateAlerts" : "false",
"permCreateAuditFiles" : "false",
"permCreateLDAPAssets" : "false",
"permCreatePolicies" : "false",
"permPurgeTickets" : "false",
"permPurgeScanResults" : "false",
"permPurgeReportResults" : "false",
"permScan" : "none",
"permAgentsScan" : "false",
"permShareObjects" : "false",
"permUpdateFeeds" : "false",
"permUploadNessusResults" : "false",
"permViewOrgLogs" : "false",
"permManageAcceptRiskRules" : "false",
"permManageRecastRiskRules" : "false",
"organizationCounts" : [
{
   "id" : "12",
   "userCount" : "0"
}
],
"creator" : {
   "id" : "1",
   "username" : "head",
   "firstname" : "",
   "lastname" : ""
}
}
"id": "6",
"name": "Credential Manager",
"description": "The Credential Manager role can be used specifically for handling credentials. A Credential Manager can use a scan to create a report of the credential. This can be used by someone outside the security team to keep scanning credentials up to date.",
"createdTime": "0",
"modifiedTime": "0",
"permManageApp": "false",
"permManageGroups": "false",
"permManageRoles": "false",
"permManageImages": "false",
"permManageGroupRelationships": "false",
"permManageBlackoutWindows": "false",
"permManageAttributeSets": "false",
"permCreateTickets": "false",
"permCreateAlerts": "false",
"permCreateAuditFiles": "false",
"permCreateLDAPAssets": "false",
"permCreatePolicies": "false",
"permPurgeTickets": "false",
"permPurgeScanResults": "false",
"permPurgeReportResults": "false",
"permScan": "none",
"permAgentsScan": "false",
"permShareObjects": "true",
"permUpdateFeeds": "false",
"permUploadNessusResults": "false",
"permViewOrgLogs": "false",
"permManageAcceptRiskRules": "false",
"permManageRecastRiskRules": "false",
"organizationCounts": [
{
   "id": "12",
   "userCount": "0"
}
],
"creator": {
"id" : "1",
"username" : "head",
"firstname" : "",
"lastname" : ""
}
},
{
"id" : "7",
"name" : "Auditor",
"description" : "The Auditor role can access summary information to perform 3rd party audits. An Auditor can view... access to vulnerability and event data can be achieved by placing the user in an appropriately configured group.",
"createdTime" : "0",
"modifiedTime" : "0",
"permManageApp" : "false",
"permManageGroups" : "false",
"permManageRoles" : "false",
"permManageImages" : "false",
"permManageGroupRelationships" : "false",
"permManageBlackoutWindows" : "false",
"permManageAttributeSets" : "false",
"permCreateTickets" : "false",
"permCreateAlerts" : "false",
"permCreateAuditFiles" : "false",
"permCreateLDAPAssets" : "false",
"permCreatePolicies" : "false",
"permPurgeTickets" : "false",
"permPurgeScanResults" : "false",
"permPurgeReportResults" : "false",
"permScan" : "none",
"permAgentsScan" : "false",
"permShareObjects" : "false",
"permUpdateFeeds" : "false",
"permUploadNessusResults" : "false",
"permViewOrgLogs" : "true",
"permManageAcceptRiskRules" : "false",
"permManageRecastRiskRules" : "false"}
"organizationCounts" : [
    {
        "id" : "12",
        "userCount" : "0"
    }
],
"creator" : {
    "id" : "1",
    "username" : "head",
    "firstname" : "",
    "lastname" : ""
}
],
"error_code" : 0,
"error_msg" : ",
"warnings" : [
"timestamp" : 1445013119
}
}

POST

Adds an 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",
"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"

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",
"permShareObjects" : "false",
"permUpdateFeeds" : "true",
"permUploadNessusResults" : "false",
"permViewOrgLogs" : "true",
"permManageAcceptRiskRules" : "true",
"permManageRecastRiskRules" : "true",
"organizationCounts" : [
  {
    "id" : "0",
    "userCount" : "1"
  }
],
"creator" : {
  "id" : "1",
  "username" : "admin",
  "firstname" : "Admin",
  "lastname" : "User"
}
"error_code" : 0,
"error_msg" : "",
"warnings" : [],
"timestamp" : 1445013361
}

/role/{id}

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
permScanpermAgentsScan
permShareObjects
permUpdateFeeds
permUploadNessusResults
permViewOrgLogs
permManageAcceptRiskRules
permManageRecastRiskRules
organizationCounts

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" : "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",
"permShareObjects" : "false",
"permUpdateFeeds" : "true",
"permUploadNessusResults" : "false",
"permViewOrgLogs" : "true",
"permManageAcceptRiskRules" : "true",
"permManageRecastRiskRules" : "true",
"organizationCounts" : [
  {
    "id" : "0",
    "userCount" : "1"
  },
  {
    "id" : "12",
    "userCount" : "0"
  }
],
"creator" : {
}
"id" : "1",
"username" : "admin",
"firstname" : "Admin",
"lastname" : "User"
}

"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
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

```json
{
    "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}. 

759
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

```json
{
    "type" : "regular",
    "response" : {
```
### 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

```json
{
    "name" : <string>,
    "description" : <string>,
    "type" : <string> "saml2" | "shibboleth",
    "entityID" : <string>,
    "idp" : <string>,
    "usernameAttribute" : <string>,
    "singleSignOnService" : <string>,
    "singleLogoutService" : <string>,
    "certData" : <certData>
    "createdTime" : 1543852867,
    "modifiedTime" : 1546641092,
    "samlEnabled" : "true"
}
```

"error_code": 0,
"error_msg": "",
"warnings": [],
"timestamp": 1546642280
"singleLogoutService" : <string>,
"certData" : <string>,
"samlEnabled" : <string> "false" | "true"
}

Example Response
See /saml/[id]::GET

/saml/getMetadata

Methods
GET

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
}
Scan

/scan

Methods

GET

Gets the list of 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
**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

Legend*
*

* = always comes back

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

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

Request Parameters

Expand

```json
{
    "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" : {
```

```json
timestamp" : 1406828340
}
```

`
"type": "dependent" | "ical" | "never" | "rollover" | "template" <string>,
"reports": [
  {
    "id": <number>,
    "reportSource": <string> "cumulative" | "patched" | "individual" | "lce" | "archive" | "mobile"
  },...
] DEFAULT [],
"assets": [
  {
    "id": <number>
  },...
] DEFAULT [],
"credentials": [
  {
    "id": <number>
  },...
] DEFAULT [],
"emailOnLaunch": "false" | "true" DEFAULT "false",
"emailOnFinish": "false" | "true" DEFAULT "false",
"timeoutAction": "discard" | "import" | "rollover" DEFAULT "import",
"scanningVirtualHosts": "false" | "true" DEFAULT "false",
"rolloverType": "nextDay" | "template" DEFAULT "template",
"ipList": <string> DEFAULT "" (valid IP),
"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 schedule types, “enabled” is set to “true”.

...
"enabled": "false" | "true" DEFAULT "true"

Example Response

Expand

```json
{
  "type": "regular",
  "response": {
    "id": "4",
    "creatorID": "1",
    "ownerID": "1",
    "name": "POSTtest",
    "description": "This is a test for POST",
    "ipList": "",
    "type": "policy",
    "policyID": "1000002",
    "pluginID": "-1",
    "repositoryID": "2",
    "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 test"
},
"pluginPrefs" : [],
"creator" : {
   "id" : "1",
   "username" : "head3",
   "firstname" : "",
   "lastname" : ""
},
"owner" : { 
   "id" : "1",
   "username" : "head3",
   "firstname" : "",
   "lastname" : ""


```
{
  "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
}
```

**/scan/{id}**

**Methods**

**GET**

Gets the Scan associated with {id}.

**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
**name
**description
**status
ipList
type	policy
plugin
repository
zone
dhcpTracking
classifyMitigatedAge
eemailOnLaunch
eemailOnFinish
timeoutAction
scanningVirtualHosts
rolloverType
createdTime
modifiedTime
ownerGroup
creator
owner
reports
assets
credentials
numDependents
schedule
policy
policyPrefs
maxScanTime

Legend*
*

* = always comes back
Request Parameters

None

Expand Parameters

credentials

Example Response

Expand

{
  "type": "regular",
  "response": {
    "id": "4",
    "name": "POSTtest",
    "description": "This is a test for POST",
    "iplist": "",
    "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": "1",
      "type": "cron",
      "fields": {
        "cron": "* * * * *"
      }
    }
  }
}
"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 test"
},
"policyPrefs" : [],
"repository" : {
  "id" : "2",
  "name" : "test",
  "description" : "test"
},
"ownerGroup" : {
  "id" : "0",
  "name" : "Full Access",
  "description" : "Full Access group"
},
"creator" : {
  "id" : "1",
  "username" : "head3",
  "firstname" : ""
PATCH
Edits the Scan associated with {id}, 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}, depending on access and permissions.

**Request Parameters**
None
Example Response

```
{
  "type" : "regular",
  "response" : {
    "scans" : [
    {
      "id" : "1"
    }
  ],
  "error_code" : 0,
  "error_msg" : "",
  "warnings" : [],
  "timestamp" : 1406732180
}
```

/scan/{id}/copy

Methods

POST

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

Request Parameters

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

Expand

```json
{
    "type": "regular",
    "response": {
        "scan": {
            "id": "4",
            "name": "POSTtest",
            "description": "This is a test for POST",
            "ipList": "",
            "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 test"
},
"policyPrefs" : [],
"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" : ""
}
/scan/{id}/launch

Methods

POST

Launches the Scan associated with {id}.

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
}
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
**status
ip
port
useProxy
enabled
verifyHost
managePlugins
authType
cert
username
password
agentCapable
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

**Request Query Parameters**

None
Example Response
Expand
{
    "type" : "regular",
    "response" : [ 
        {
            "id" : "12",
            "name" : "Scanner 1",
            "description" : "Copied from QA",
            "status" : "1"
        },
        {
            "id" : "14",
            "name" : "Scanner using Safe Scan Range",
            "description" : "",
            "status" : "16"
        },
        {
            "id" : "15",
            "name" : "mp zone 1 scanner",
            "description" : "Copied from QA",
            "status" : "1"
        },
        {
            "id" : "16",
            "name" : "NessusTest",
            "description" : "Copied From QA",
            "status" : "32"
        },
        {
            "id" : "17",
            "name" : "sc",
            "description" : "",
            "status" : "2"
        }
    ]
}
POST
Adds a Scanner.

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",
  "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" : "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",
  }
}
"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",
"pluginSet" : null,
"loadedPluginSet" : null,
"serverUUID" : null,
"createdTime" : "1402435586",
"modifiedTime" : "1402435586",
"zones" : [
  {
    "id" : "1",
    "name" : "Big Zone",
    "description" : ""
  }
],
"nessusManagerOrgs" : [
  {
    "id" : "1",
    "name" : "Big Org",
    "description" : ""
  }
],
"error_code" : 0,
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
cert
username
password
agentCapable
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*

**Request Query Parameters**
None

**Example Response**

Expand

```json
{
    "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",
        "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",
        "pluginSet": null,
        "loadedPluginSet": null,
        "serverUUID": null,
```
"createdTime" : "1402435586",
"modifiedTime" : "1402435586",
"accessKey" : "",
"secretKey" : "",
"zones" : [
   {
      "id" : "1",
      "name" : "Big Zone",
      "description" : ""
   }
],
"nessusManagerOrgs" : [
   {
      "id" : "1",
      "name" : "Big Org",
      "description" : ""
   }
],
"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

```json
{
    "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

```json
{
    "scansGlob" : <string>
    "resultsSync" : {
        "id" : <number>
    } OPTIONAL
}
```
**Example Response**

Expand

```json
{
    "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 multiple file contents compliance audit",
            "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
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.)
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
* name
* description
* status
* policyTemplate
* policyProfileName

creator

tags

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 Template)

families

**Legend**

* = always comes back

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

**Request Parameters**

None

**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

```json
{
    "type" : "regular",
    "response" : {
        "usable" : [
            {
"id" : "1",
"name" : "test",
"description" : "desc",
"status" : "0"
            },

```
{
  "id": "2",
  "name": "test2",
  "description": "desc",
  "status": "0"
},
{
  "id": "3",
  "name": "test3",
  "description": "desc",
  "status": "0"
},
{
  "id": "4",
  "name": "test4",
  "description": "test desc",
  "status": "0"
},
{
  "id": "1000001",
  "name": "nesus upload - ibm credentials",
  "description": "",
  "status": "0"
},
{
  "id": "1000002",
  "name": "nesus upload - ibm credentials - uploaded one",
  "description": "Nessus Policy exported from Tenable.sc",
  "status": "0"
},
{
  "id": "1000003",
  "name": "IBM iSeries Credentials Name",
  "description": "Imported Nessus Policy",
  "status": "0"
}


},
{
  "id": "1000004",
  "name": "Nessus Upload 2",
  "description": "Imported Nessus Policy",
  "status": "0"
},
{
  "id": "1000005",
  "name": "Nessus Upload 3",
  "description": "Imported Nessus Policy",
  "status": "0"
},
{
  "id": "1000016",
  "name": "Tom Test",
  "description": "Imported Nessus Policy",
  "status": "0"
},
{
  "id": "1000017",
  "name": "Nessus Upload 4",
  "description": "Imported Nessus Policy",
  "status": "0"
},
{
  "id": "1000018",
  "name": "Tom Test 2",
  "description": "Imported Nessus Policy",
  "status": "0"
},
{
  "id": "1000019",
  "name": "DOCtest",
  "description": "desc"
"status": "0"
],
{
"id": "1000020",
"name": "test5",
"description": "test desc",
"status": "0"
}
],
"manageable": [
{
"id": "1000001",
"name": "nesus upload - ibm credentials",
"description": "",
"status": "0"
},
{
"id": "1000002",
"name": "nesus upload - ibm credentials - uploaded one",
"description": "Nessus Policy exported from Tenable.sc",
"status": "0"
},
{
"id": "1000003",
"name": "IBM iSeries Credentials Name",
"description": "Imported Nessus Policy",
"status": "0"
},
{
"id": "1000004",
"name": "Nessus Upload 2",
"description": "Imported Nessus Policy",
"status": "0"
}
]
"id" : "1000005",
"name" : "Nessus Upload 3",
"description" : "Imported Nessus Policy",
"status" : "0"
},
{
"id" : "1000016",
"name" : "Tom Test",
"description" : "Imported Nessus Policy",
"status" : "0"
},
{
"id" : "1000017",
"name" : "Nessus Upload 4",
"description" : "Imported Nessus Policy",
"status" : "0"
},
{
"id" : "1000018",
"name" : "Tom Test 2",
"description" : "Imported Nessus Policy",
"status" : "0"
},
{
"id" : "1000019",
"name" : "DOCtest",
"description" : "desc",
"status" : "0"
},
{
"id" : "1000020",
"name" : "test5",
"description" : "test desc",
"status" : "0"
}
POST

Adds a Policy (or AppPolicy).

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"
policyTemplate ID “1” (Advanced Template)

... "families" : [
  {
    "id" : <number>,
    "plugins" : [
      {
        "id" : <number>
      }...
    ] OPTIONAL (must be specified to effect a "mixed" Plugin Family type)
  }...
] DEFAULT []
...

Session User is not an administrator

{}

"ownerID" : <number> DEFAULT {creatorID}, (}

Example Response

Expand
{}

"type" : "regular",
"response" : [
  {
    "id" : "1000019",
    "name" : "DOCTest",
    "description" : "desc",
    "policyTemplate" : {
      "context" : "" (empty)
    }
  }
}
"id" : "1",
"name" : "Advanced Scan",
"description" : "Configure a scan without using any recommendations.

"policyProfileName" : "",
"generateXCCDFResults" : "false",
"creatorID" : "1",
"ownerID" : "1",
"context" : "",
"tags" : "",
"createdTime" : "1406224504",
"modifiedTime" : "1406224504",
"ownerGID" : "0",
"targetGID" : "-1",
"auditFiles" : [],
"preferences" : [],
"families" : [
  {
    "id" : "9",
    "name" : "AIX Local Security Checks",
    "count" : "11164"
  },
  {
    "id" : "54",
    "name" : "Amazon Linux Local Security Checks",
    "count" : "502"
  },
  {
    "id" : "35",
    "name" : "Backdoors",
    "count" : "102"
  },
  {
    "id" : "18",
    "name" : "CentOS Local Security Checks",
    "count" : "804"
  }
]
"count" : "1890"
},
{
    "id" : "6",
    "name" : "CGI abuses",
    "count" : "3235"
},
{
    "id" : "26",
    "name" : "CGI abuses : XSS",
    "count" : "600"
},
{
    "id" : "33",
    "name" : "CISCO",
    "count" : "576"
},
{
    "id" : "31",
    "name" : "Databases",
    "count" : "372"
},
{
    "id" : "3",
    "name" : "Debian Local Security Checks",
    "count" : "3179"
},
{
    "id" : "25",
    "name" : "Default Unix Accounts",
    "count" : "101"
},
{
    "id" : "22",
    "name" : "Denial of Service",
    "count" : "805"}
"count" : "107"
},
{
  "id" : "37",
  "name" : "DNS",
  "count" : "110"
},
{
  "id" : "57",
  "name" : "F5 Networks Local Security Checks",
  "count" : "154"
},
{
  "id" : "5",
  "name" : "Fedora Local Security Checks",
  "count" : "8067"
},
{
  "id" : "34",
  "name" : "Firewalls",
  "count" : "139"
},
{
  "id" : "13",
  "name" : "FreeBSD Local Security Checks",
  "count" : "2616"
},
{
  "id" : "19",
  "name" : "FTP",
  "count" : "244"
},
{
  "id" : "40",
  "name" : "Gain a shell remotely",
}
"count" : "274"
},
{
"id" : "30",
"name" : "General",
"count" : "198"
},
{
"id" : "7",
"name" : "Gentoo Local Security Checks",
"count" : "2071"
},
{
"id" : "2",
"name" : "HP-UX Local Security Checks",
"count" : "1974"
},
{
"id" : "56",
"name" : "Huawei Local Security Checks",
"count" : "14"
},
{
"id" : "50",
"name" : "Junos Local Security Checks",
"count" : "107"
},
{
"id" : "21",
"name" : "MacOS X Local Security Checks",
"count" : "717"
},
{
"id" : "47",
"name" : "Mandriva Local Security Checks",
"count" : "14"
}
"count" : "2970"
},
{
    "id" : "23",
    "name" : "Misc.",
    "count" : "972"
},
{
    "id" : "52",
    "name" : "Mobile Devices",
    "count" : "43"
},
{
    "id" : "43",
    "name" : "Netware",
    "count" : "14"
},
{
    "id" : "53",
    "name" : "Oracle Linux Local Security Checks",
    "count" : "1912"
},
{
    "id" : "55",
    "name" : "Palo Alto Local Security Checks",
    "count" : "20"
},
{
    "id" : "32",
    "name" : "Peer-To-Peer File Sharing",
    "count" : "72"
},
{
    "id" : "39",
    "name" : "Policy Compliance",
}
"count": "38"
},
{
  "id": "42",
  "name": "Port scanners",
  "count": "8"
},
{
  "id": "1",
  "name": "Red Hat Local Security Checks",
  "count": "3424"
},
{
  "id": "28",
  "name": "RPC",
  "count": "36"
},
{
  "id": "36",
  "name": "SCADA",
  "count": "198"
},
{
  "id": "51",
  "name": "Scientific Linux Local Security Checks",
  "count": "1760"
},
{
  "id": "24",
  "name": "Service detection",
  "count": "408"
},
{
  "id": "41",
  "name": "Settings",

"count": "66",
},
{
"id": "15",
"name": "Slackware Local Security Checks",
"count": "757"
},
{
"id": "12",
"name": "SMTP problems",
"count": "135"
},
{
"id": "45",
"name": "SNMP",
"count": "33"
},
{
"id": "4",
"name": "Solaris Local Security Checks",
"count": "3798"
},
{
"id": "8",
"name": "SuSE Local Security Checks",
"count": "7355"
},
{
"id": "14",
"name": "Ubuntu Local Security Checks",
"count": "2767"
},
{
"id": "48",
"name": "VMware ESX Local Security Checks",
"count": "810"
"count" : "94"
},
{
  "id" : "11",
  "name" : "Web Servers",
  "count" : "876"
},
{
  "id" : "20",
  "name" : "Windows",
  "count" : "3113"
},
{
  "id" : "10",
  "name" : "Windows : Microsoft Bulletins",
  "count" : "986"
},
{
  "id" : "29",
  "name" : "Windows : User management",
  "count" : "28"
}
],
"status" : "0",
"canUse" : "true",
"canManage" : "true",
"groups" : []
[
"error_code" : 0,
"error_msg" : "",
"warnings" : [],
"timestamp" : 1406224504
]
/policy/{id}

Methods

GET

Gets the Policy 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
policyTemplateType
policyTemplate
policyProfileName
creator
tags
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 Template)
families

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",
            "generateXCCDFResults" : "false",
            "context" : "",
            "policyTemplateID" : "1",
            "policyProfileName" : "",
            "name" : "test",
            "description" : "desc",
            "tags" : "",
            "createdTime" : "1406148027",
            "modifiedTime" : "1406148027",
            "status" : "0",
            "auditFiles" : []
        }
    ]
}
"preferences" : {
    "preference1" : "value1",
    "preference2" : "value2"
},
"families" : [
    {
        "id" : "9",
        "name" : "AIX Local Security Checks",
        "count" : "11164"
    },
    {
        "id" : "54",
        "name" : "Amazon Linux Local Security Checks",
        "count" : "502"
    },
    {
        "id" : "35",
        "name" : "Backdoors",
        "count" : "102"
    },
    {
        "id" : "18",
        "name" : "CentOS Local Security Checks",
        "count" : "1890"
    },
    {
        "id" : "6",
        "name" : "CGI abuses",
        "count" : "3235"
    },
    {
        "id" : "26",
        "name" : "CGI abuses : XSS",
        "count" : "600"
    }
]
{ "id": "33",  "name": "CISCO",  "count": "576" },
{ "id": "31",  "name": "Databases",  "count": "372" },
{ "id": "3",  "name": "Debian Local Security Checks",  "count": "3179" },
{ "id": "25",  "name": "Default Unix Accounts",  "count": "101" },
{ "id": "22",  "name": "Denial of Service",  "count": "107" },
{ "id": "37",  "name": "DNS",  "count": "110" },
{ "id": "57",  "name": "F5 Networks Local Security Checks",  "count": "154" },
{  "id" : "5",
  "name" : "Fedora Local Security Checks",
  "count" : "8067"
},
{  "id" : "34",
  "name" : "Firewalls",
  "count" : "139"
},
{  "id" : "13",
  "name" : "FreeBSD Local Security Checks",
  "count" : "2616"
},
{  "id" : "19",
  "name" : "FTP",
  "count" : "244"
},
{  "id" : "40",
  "name" : "Gain a shell remotely",
  "count" : "274"
},
{  "id" : "30",
  "name" : "General",
  "count" : "198"
},
{  "id" : "7",
  "name" : "Gentoo Local Security Checks",
  "count" : "2071"
},

[{"id": "2", "name": "HP-UX Local Security Checks", "count": "1974"}],
[{"id": "56", "name": "Huawei Local Security Checks", "count": "14"}],
[{"id": "50", "name": "Junos Local Security Checks", "count": "107"}],
[{"id": "21", "name": "MacOS X Local Security Checks", "count": "717"}],
[{"id": "47", "name": "Mandriva Local Security Checks", "count": "2970"}],
[{"id": "23", "name": "Misc.", "count": "972"}],
[{"id": "52", "name": "Mobile Devices", "count": "43"}]
}
{
  "id" : "28",
  "name" : "RPC",
  "count" : "36"
},
{
  "id" : "36",
  "name" : "SCADA",
  "count" : "198"
},
{
  "id" : "51",
  "name" : "Scientific Linux Local Security Checks",
  "count" : "1760"
},
{
  "id" : "24",
  "name" : "Service detection",
  "count" : "408"
},
{
  "id" : "41",
  "name" : "Settings",
  "count" : "66"
},
{
  "id" : "15",
  "name" : "Slackware Local Security Checks",
  "count" : "757"
},
{
  "id" : "12",
  "name" : "SMTP problems",
  "count" : "135"
}
{ "id": "45",  "name": "SNMP",  "count": "33" },  
{ "id": "4",  "name": "Solaris Local Security Checks",  "count": "3798" },  
{ "id": "8",  "name": "SuSE Local Security Checks",  "count": "7355" },  
{ "id": "14",  "name": "Ubuntu Local Security Checks",  "count": "2767" },  
{ "id": "48",  "name": "VMware ESX Local Security Checks",  "count": "94" },  
{ "id": "11",  "name": "Web Servers",  "count": "876" },  
{ "id": "20",  "name": "Windows",  "count": "3113" },
PATCH

Edits the Policy associated with {id}, 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}, 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

POST

Copies the Policy associated with {id}, depending on access and permissions.

NOTE: The policy that is associated with {id} 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",
      "description": "test",
   },
"policyTemplateID" : "1",
"policyProfileName" : "",
"generateXCCDFResults" : "false",
"creatorID" : "1",
"context" : null,
"tags" : "",
"status" : "0",
"createdTime" : "1410976021",
"modifiedTime" : "1410976021",
"auditFiles" : [],
"preferences" : [],
"families" : []
}

"error_code" : 0,
"error_msg" : "",
"warnings" : [],
"timestamp" : 1410976021

/policy/{id}/export

Methods

POST

Request Parameters

None

Example Response

None given. The response will be an xml file containing the Scan Policy.

/policy/{id}/share

Methods
POST

Shares the Policy associated with [id], depending on access and permissions

Request Parameters

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

Example Response

{  
  "type" : "regular",  
  "response" : {  
    "id" : "1000002",  
    "name" : "POST TEST",  
    "description" : "Test of post for use with scan post test",  
    "policyTemplateID" : "1",  
    "policyProfileName" : null,  
    "generateXCCDFResults" : "false",  
    "creatorID" : "1",  
    "ownerID" : "1",  
    "context" : "",  
    "tags" : "",  
    "createdTime" : "1406815230",  
    "modifiedTime" : "1406831623",  
    "ownerGID" : "0",  
    "targetGID" : "-1",  
  }  
}
"auditFiles" : [
    {
      "id" : "5",
      "creatorID" : "1",
      "name" : "Admin - Top 25 extended File Listener",
      "description" : "",
      "version" : "1",
      "type" : "windowsfiles",
      "status" : "0",
      "filename" : "scfile_RDzAqG",
      "originalFilename" : "Top25ext-FileLister.audit",
      "createdTime" : "1407436831",
      "modifiedTime" : "1408041922",
      "creator" : {
        "id" : "1",
        "username" : "head",
        "firstname" : "Security Manager",
        "lastname" : ""
      }
    },
    {
      "id" : "6",
      "creatorID" : "1",
      "name" : "Admin - Top 25 lite",
      "description" : "",
      "version" : "1",
      "type" : "windowsfiles",
      "status" : "0",
      "filename" : "scfile_GSghXU",
      "originalFilename" : "Top25lite.audit",
      "createdTime" : "1407436886",
      "modifiedTime" : "1408041931",
      "creator" : {
        "id" : "1",
        "username" : "head",
        "firstname" : "Security Manager",
        "lastname" : ""
      }
    }
]
"firstname": "Security Manager",
"lastname": ""
}
],
{
"id": "1000030",
"creatorID": "1",
"ownerID": "1",
"name": "Basic Audit File",
"description": "",
"version": "1",
"type": "windowsfiles",
"context": null,
"status": "0",
"filename": "scfile_KZxUpL",
"originalFilename": "Top25ext-FileLister.audit",
"createdTime": "1407860973",
"modifiedTime": "1407860973",
"creator": {
  "id": "1",
  "username": "head",
  "firstname": "Security Manager",
  "lastname": ""
},
"owner": {
  "id": "1",
  "username": "head",
  "firstname": "Security Manager",
  "lastname": ""
}
},
{
"id": "1000047",
"creatorID": "1",
"ownerID": "1",
"name": "Basic Audit File",
"description": "",
"version": "1",
"type": "windowsfiles",
"context": null,
"status": "0",
"filename": "scfile_KZxUpL",
"originalFilename": "Top25ext-FileLister.audit",
"createdTime": "1407860973",
"modifiedTime": "1407860973",
"creator": {
  "id": "1",
  "username": "head",
  "firstname": "Security Manager",
  "lastname": ""
},
"owner": {
  "id": "1",
  "username": "head",
  "firstname": "Security Manager",
  "lastname": ""
}
}
"name" : "With Scap",
"description" : "",
"version" : "1",
"type" : "windowsfiles",
"context" : null,
"status" : 0,
"filename" : "scfile_SQWESp",
"originalFilename" : "Top25ext-FileLister.audit",
"createdTime" : "1408112071",
"modifiedTime" : "1408112876",
"creator" : {
    "id" : "1",
    "username" : "head",
    "firstname" : "Security Manager",
    "lastname" : ""
},
"owner" : {
    "id" : "1",
    "username" : "head",
    "firstname" : "Security Manager",
    "lastname" : ""
}
},
{
    "id" : "1000048",
    "creatorID" : "1",
    "ownerID" : "1",
    "name" : "test12122",
    "description" : "",
    "version" : "1.2",
    "type" : "scapWindows",
    "context" : null,
    "status" : 0,
    "filename" : "scfile_jWKztr",
    "originalFilename" : "SCAP1.2_multiple_datastreams.zip",
}
"createdTime" : "1408112282",
"modifiedTime" : "1408740774",
"creator" : {
"id" : "1",
    "username" : "head",
    "firstname" : "Security Manager",
    "lastname" : ""
},
"owner" : {
    "id" : "1",
    "username" : "head",
    "firstname" : "Security Manager",
    "lastname" : ""
}
},
{
"id" : "1000049",
"creatorID" : "1",
"ownerID" : "1",
"name" : "Test",
"description" : "",
"version" : "1.2",
"type" : "scapWindows",
"context" : null,
"status" : "0",
"filename" : "scfile_VuyB0i",
"originalFilename" : "SCAP1.2_multiple_datastreams.zip",
"createdTime" : "1408740277",
"modifiedTime" : "1408740277",
"creator" : {
    "id" : "1",
    "username" : "head",
    "firstname" : "Security Manager",
    "lastname" : ""
}
}
"owner" : {
    "id" : "1",
    "username" : "head",
    "firstname" : "Security Manager",
    "lastname" : ""
}
},

"preferences" : [],
"families" : [],
"status" : "0",
"policyTemplate" : {
    "id" : "1",
    "name" : "Advanced",
    "description" : "Configure a policy without using any templates or recommendations."
},

"creator" : {
    "id" : "1",
    "username" : "head",
    "firstname" : "Security Manager",
    "lastname" : ""
},

"owner" : {
    "id" : "1",
    "username" : "head",
    "firstname" : "Security Manager",
    "lastname" : ""
},

"ownerGroup" : {
    "id" : "0",
    "name" : "Full Access",
    "description" : "Full Access group"
},

"targetGroup" : {
    "id" : -1,

/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" : 1409087451
}
/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
}

"timestamp" : 1407340545
}


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
**descriptioneditor, detailedEditor, createdTime, modifiedTime, templatePubTime, templateModTime, templateDefModTime

Legend*

* = always comes back

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

Request Parameters

None

Example Response

Expand

{
    "type" : "regular",
    "response" : [


```json
{
    "id": "2",
    "name": "Host Discovery",
    "description": "A simple scan to discover live hosts and open ports."
},
{
    "id": "3",
    "name": "Basic Network Scan",
    "description": "A full system scan suitable for any host."
},
{
    "id": "4",
    "name": "Credentialed Patch Audit",
    "description": "Authenticate to hosts and enumerate missing 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 known baseline."
},
{
    "id": "8",
    "name": "Internal PCI Network Scan",
    "description": "Perform an internal PCI DSS (11.2.1) vulnerability scan."
}
```
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
modifiedTimetemplatePubTimetemplateModTimetemplateDefModTime

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 open ports."
    "editor": "{\"sections\":[{\"name\":\"Setup\",\"id\":\"setup\",\"subsection":\"hostdiscovery\",\"editor":\"true\",\"editorId\":\"hostdiscovery\"}],\"sections":[]}
    "createdTime": "1423297810",
    "modifiedTime": "1424507404",
    "templateModTime": "1424474588",
    "templatePubTime": "1406151204",
    "templateDefModTime": "1424470185"
},
"error_code": 0,
"error_msg": "",
"warnings": [],
"timestamp": 1424979089
}
Scan Result

/scanResult

Methods

GET

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
importDurationdownloadAvailable
downloadFormat
dataFormat
resultType
resultSource
running
errorDetails
importErrorDetails
totalIPs
scannedIPs
startTime
finishTime
scanDurationcompletedIPscompletedChecks
totalChecks
agentScanUUID
agentScanContainerUUID

**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.

**Example Response**

Expand

```json
{
    "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

Request Parameters
None

Example Response
Expand
{
    "type" : "regular",
    "response" : {
        "id" : "11",
        "name" : "Weekly Scan",
        "description" : "",
        "details" : "Policy 'Basic 1'",
        "status" : "Completed",
        "importStatus" : "Error",
    }
}
"status" : "Completed",
"deadHostSize" : 171,
"deadHostIPs" : "192.168.0.0",
"scanners" : [
    {
        "id" : "12",
        "loadAvg" : "0.0",
        "chunkCompleted" : "120",
        "completedChecks" : "6360",
        "chunks" : [
            {
                "id" : "1",
                "name" : "fc136656-2ddd-58ab-bccc-78ad4c125567-130064/Chunk 1",
                "ips" : "192.168.0.0",
                "size" : "1",
                "completedHosts" : "0",
                "completedChecks" : "1",
                "scanningIPs" : "192.168.0.0",
                "scanningSize" : "1",
                "scannedIPs" : "",
                "scannedSize" : "0",
                "status" : "Running",
                "startTime" : "1455735612",
                "endTime" : "1455736826",
                "deadHostIPs" : "",
                "deadHostSize" : 0
            }
        ],
        "scannedSize" : 11,
        "scannedIPs" : "192.168.0.0",
        "scanningSize" : 0,
        "scanningIPs" : "",
        "awaitingDownloadSize" : 0,
        "awaitingDownloadIPs" : "",
        "deadHostSize" : 109,
    }
]
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": "",
    "repository": {
        "id": "38",
        "name": "jm ipv4",
        "description": "copied from 97"
    },
    "error_code": 0,
    "error_msg": "",
    "warnings": [],
    "timestamp": 1426878968
}
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": ""
},
"owner":{
  "id": "1",
  "username": "test user",
  "firstname": "",
  "lastname": ""
},
"scan": {
  "id": "18",
  "name": "test scan",
  "description": ""
},
"repository":{
  "id": "516",
  "name": "repo1",
  "description": ""
},
"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

"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": ""
},
"owner": {
   "id": "1",
   "username": "test user",
   "firstname": "",
   "lastname": ""
},
"scan": {
   "id": "18",
   "name": "test scan",
   "description": ""
},
"repository": {
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

{  
  "id" : "516",
  "name" : "repo1",
  "description" : "",

  "ownerGroup" : {
    "id" : "0",
    "name" : "Full Access",
    "description" : "Full Access group"
  }

  "error_code" : 0,
  "error_msg" : "",
  "warnings" : [],
  "timestamp" : 1406917515
}
"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' : ''
},
'owner' : {
'id' : '1',
'username' : 'test user',
'firstname' : '',
'lastname' : ''
},
'scan' : {
'id' : '18',
'name' : 'test scan',
'description' : ''
},
'repository' : {
'id' : '516',
'name' : 'repo1',
'description' : ''
},
'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.
Scan Zone

To avoid serious problems, do not modify existing Scan Zones while scans are in progress.

/zone

Methods

GET

GET

Gets the list of Zones

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
**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" : "5",
        "name" : "Test Zone #1",
        "description" : ",",
        "ipList" : "192.168.0.0/24",
        "createdAt" : "1426871916",
        "modifiedTime" : "1426881426",
        "scanners" : [
            {
                "id" : "2",
                "name" : "Nessus 192.168.1.1:1234",
                "description" : ",",
                "status" : "4"
            }
        ],
        "organizations" : [
            {
                "id" : "38",
                "name" : "Test Org",
                "description" : ","
            }
        ],
        "activeScanners" : 0,
        "totalScanners" : 1
    }
]
POST

Adds an Zone

Request Parameters

Expand

Note: A default for organizations is being set to an empty array; however, there is no logic for utilizing the organizations in any fashion so it was omitted.

{  
    "name" : <string>,  
    "description" : <string> DEFAULT "",  
    "ipList" : <string> (valid IP list),  
    "scanners" : [  
    {  
        "id" : <number>  
    }...
  
}
Example Response

Expand

{
   "type": "regular",
   "response": {
      "id": "3",
      "name": "TestDevformPost",
      "description": "Test of a post through DevForm",
      "ipList": "192.168.1.1",
      "createdTime": "1408733617",
      "modifiedTime": "1408733617",
      "scanners": [
         {
            "id": "11",
            "name": "Cent5x64-NessC1",
            "description": "",
            "status": "1025"
         }
      ],
      "organizations": [],
      "activeScanners": 1,
      "totalScanners": 1
   },
   "error_code": 0,
   "error_msg": "",
   "warnings": [],
   "timestamp": 1408733617
}

/zone/{id}
Methods

GET

Gets the Zone 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
**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" : "5",
        "name" : "Test Zone #1",
        "description" : "",
        "ipList" : "192.168.0.0/24",
        "createdTime" : "1426871916",
        "modifiedTime" : "1426881426",
        "scanners" : [
            {
                "id" : "2",
                "name" : "Nessus 172.168.0.1:8834",
                "description" : "",
                "status" : "4"
            }
        ],
        "organizations" : [
            {
                "id" : "38",
                "name" : "Test Org",
                "description" : ""
            }
        ],
        "activeScanners" : 0,
        "totalScanners" : 1
    },
    "error_code" : 0,
    "error_msg" : "",
    "warnings" : [],
    "timestamp" : 1426882592
}
PATCH
Edits the Role associated with {id}, changing only the passed in fields.

Request Parameters
(All fields are optional)
See /zone::POST for parameters.

Example Response
See /zone/{id}::GET

DELETE
Deletes the 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
}
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 Microsoft 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
/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", "macAddress": "", "dnsName": "", "osCPE": "cpe:/o:microsoft:windows_server_2016", "repository": { "id": "1", "name": "Repo", "description": "", "dataFormat": "IPv4" } } }, "error_code": 0, "error_msg": "", "warnings": [], "timestamp": 1546642280 }
**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

```json
[
  {
    "hash" : "1fab2df0da66974356208fc695de",
    "type" : "dsa",
    "comment" : "tns@scautotest",
    "key" : "AAA346sfqmF+ICrDHGyl1354RkqiEEYk\/Xb6Gsd8PTVn1dKIjEV645sPXBnqXhAoQ"
  },
  {
    "hash" : "694a87b1fa16asvwe062d66be1110",
    "type" : "dsa",
    "comment" : "tns@scbuild1",
    "key" : "AAAAB\/fogTEadsfURiLQj0mH11gp+x\:/E9R57wBYl7oDEjjz123523uEWgwaevawU"
  }
]
```
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.

```json
{
    "key" : <string:"type key comment">,
    "comment" : <string:"some comment">
}
```

**Example Response**

Expand

```json
{
    "type":"regular",
    "response": {
        "hash" : "63c84acew353verdfdcb39ed",
        "comment" : "tns@scautotest3",
        "key" : "AAAAaIwRkqiEEYk/Xb6Gsd8PTVn1dKIjEVD0LKqLtg5sPXBnqXhAoQBLmLgm\/d1XQ",
        "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 AAAABURLhAMUqUpGu4rI5e7sdfU4Yc7FCLO+GZSePYyouoQ5ntoay0VCzBL2Uvuy7SLUaCjgXGPjUZ1CTdBC0g/l7t4Lk\n\nts@johndoe

**/sshKey/installRemoteKey**

**Methods**

**POST**

Installs the Public SSH key for Tenable.sc on to the specified, remote host.

**Request Parameters**

Expand

```json
{
    "host" : <string>,
    "username" : <string>,
    "password" : <string>
}
```

**Example Response**

Expand

```json
{
    "type" : "regular",
    "response" : {
        "comment" : "tns@John-Dev",
        "key" : "AAAAB3NzaC154629gho/5K8Dawv4398dtmz2kiCAQdiZwtJnXv9KYKrzVqGCNQD4",
        "type" : "ssh-dss"
    },
    "error_code" : 0,
    "error_msg" : "",
    "warnings" : [],
    "timestamp" : 1403011994
}
```
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 GET with status. All fields are returned, by default, here.

Request Parameters
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"
},
"error_code" : 0,
"error_msg" : "",
"warnings" : [],
"timestamp" : 1405023348
}
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" : "Default report style",
        },
        ...
    ],
    "error_code" : 0,
    "error_msg" : "",
    "warnings" : [],
    "timestamp" : 1421273343
}

/style/{id}

Methods

GET

Gets the Style associated with {id}. 


Request Parameters

None

Example Response

Expand

```json
{
    "type": "regular",
    "response": {
        "id": "1",
        "name": "Letter",
        "description": "",
        "type": "paper",
        "attributes": []
    },
    "error_code": 0,
    "error_msg": "",
    "warnings": [],
    "timestamp": 1421273493
}
```
StyleFamily

/styleFamily

Methods

GET

GETs all the Style Families available to the current user

Request Parameters

None

Example Response

{  "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 Family 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
}
System

/system

Methods

GET

Gets the system initialization information.

NOTE #1: This should only be called prior to login

NOTE #2: SAML/Card/certificate users will automatically receive a token attribute included in the response element or an error response indicating an authentication failure, provided their card is inserted. The token attribute corresponds to the same element received in from /token::POST call.

NOTE #3: SAML users will automatically receive a token attribute included in the response element or an error response indicating an authentication failure. The token attribute corresponds to the same element received in from /token::POST call.

Request Parameters

None

Example Response

Expand

```json
{
    "type" : "regular",
    "response" : {
        "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"
]
}
],
"version": "5.12.0",
"buildID": "201905293482"
"banner" : "",
"releaseID" : "201905293482",
"uuid" : "12345678-9101-2345-6789-012345678901",
"logo" : "assets/mariana/images/sc4icon.png",
"serverAuth" : "any",
"serverClassification" : "None",
"sessionTimeout" : "3600",
"licenseStatus" : "Valid",
"ACAS" : "false",
"freshInstall" : "no",
"headerText" : "",
"loginNotifications" : "false",
"PasswordComplexity" : "false",
"telemetryEnabled" : "true",
"SAML" : "false",
"SerializationDisabled" : "true",
"timezones" : [
  {
    "name" : "Africa/Abidjan",
    "gmtOffset" : 0
  },
  {
    "name" : "Africa/Accra",
    "gmtOffset" : 0
  },
  {
    "name" : "Africa/Addis_Ababa",
    "gmtOffset" : 3
  },
  {
    "name" : "Africa/Algiers",
    "gmtOffset" : 1
  },
  {
    "name" : "Africa/Asmara",
    "gmtOffset" : 0
  }
]
"gmtOffset" : 3
],
{
    "name" : "Africa/Bamako",
    "gmtOffset" : 0
},
{
    "name" : "Africa/Bangui",
    "gmtOffset" : 1
},
{
    "name" : "Africa/Banjul",
    "gmtOffset" : 0
},
{
    "name" : "Africa/Bissau",
    "gmtOffset" : 0
},
{
    "name" : "Africa/Blantyre",
    "gmtOffset" : 2
},
{
    "name" : "Africa/Brazzaville",
    "gmtOffset" : 1
},
{
    "name" : "Africa/Bujumbura",
    "gmtOffset" : 2
},
{
    "name" : "Africa/Cairo",
    "gmtOffset" : 2
}
"name" : "Africa/Casablanca",
"gmtOffset" : 1
},
{
  "name" : "Africa/Ceuta",
  "gmtOffset" : 2
},
{
  "name" : "Africa/Conakry",
  "gmtOffset" : 0
},
{
  "name" : "Africa/Dakar",
  "gmtOffset" : 0
},
{
  "name" : "Africa/Dar_es_Salaam",
  "gmtOffset" : 3
},
{
  "name" : "Africa/Djibouti",
  "gmtOffset" : 3
},
{
  "name" : "Africa/Douala",
  "gmtOffset" : 1
},
{
  "name" : "Africa/El_Aaiun",
  "gmtOffset" : 1
},
{
  "name" : "Africa/Freetown",
  "gmtOffset" : 0
},
{
    "name" : "Africa/Gaborone",
    "gmtOffset" : 2
},
{
    "name" : "Africa/Harare",
    "gmtOffset" : 2
},
{
    "name" : "Africa/Johannesburg",
    "gmtOffset" : 2
},
{
    "name" : "Africa/Juba",
    "gmtOffset" : 3
},
{
    "name" : "Africa/Kampala",
    "gmtOffset" : 3
},
{
    "name" : "Africa/Khartoum",
    "gmtOffset" : 2
},
{
    "name" : "Africa/Kigali",
    "gmtOffset" : 2
},
{
    "name" : "Africa/Kinshasa",
    "gmtOffset" : 1
},
{
    "name" : "Africa/Lagos",
    "gmtOffset" : 1
}
{
  "name" : "Africa/Libreville",
  "gmtOffset" : 1
},
{
  "name" : "Africa/Lome",
  "gmtOffset" : 0
},
{
  "name" : "Africa/Luanda",
  "gmtOffset" : 1
},
{
  "name" : "Africa/Lubumbashi",
  "gmtOffset" : 2
},
{
  "name" : "Africa/Lusaka",
  "gmtOffset" : 2
},
{
  "name" : "Africa/Malabo",
  "gmtOffset" : 1
},
{
  "name" : "Africa/Maputo",
  "gmtOffset" : 2
},
{
  "name" : "Africa/Maseru",
  "gmtOffset" : 2
},
{
  "name" : "Africa/Mbabane",
}
"gmtOffset" : 2
},
{
    "name" : "Africa/Mogadishu",
    "gmtOffset" : 3
},
{
    "name" : "Africa/Monrovia",
    "gmtOffset" : 0
},
{
    "name" : "Africa/Nairobi",
    "gmtOffset" : 3
},
{
    "name" : "Africa/Ndjamena",
    "gmtOffset" : 1
},
{
    "name" : "Africa/Niamey",
    "gmtOffset" : 1
},
{
    "name" : "Africa/Nouakchott",
    "gmtOffset" : 0
},
{
    "name" : "Africa/Ouagadougou",
    "gmtOffset" : 0
},
{
    "name" : "Africa/Porto-Novo",
    "gmtOffset" : 1
},
"name" : "Africa/Sao_Tome",
"gmtOffset" : 1
},
{
"name" : "Africa/Tripoli",
"gmtOffset" : 2
},
{
"name" : "Africa/Tunis",
"gmtOffset" : 1
},
{
"name" : "Africa/Windhoek",
"gmtOffset" : 2
},
{
"name" : "America/Adak",
"gmtOffset" : -9
},
{
"name" : "America/Anchorage",
"gmtOffset" : -8
},
{
"name" : "America/Anguilla",
"gmtOffset" : -4
},
{
"name" : "America/Antigua",
"gmtOffset" : -4
},
{
"name" : "America/Araguaina",
"gmtOffset" : -3
},
{ "name" : "America/Argentina/Buenos_Aires", "gmtOffset" : -3 },

{ "name" : "America/Argentina/Catamarca", "gmtOffset" : -3 },

{ "name" : "America/Argentina/Cordoba", "gmtOffset" : -3 },

{ "name" : "America/Argentina/Jujuy", "gmtOffset" : -3 },

{ "name" : "America/Argentina/La_Rioja", "gmtOffset" : -3 },

{ "name" : "America/Argentina/Mendoza", "gmtOffset" : -3 },

{ "name" : "America/Argentina/Rio_Gallegos", "gmtOffset" : -3 },

{ "name" : "America/Argentina/Salta", "gmtOffset" : -3 },

{ "name" : "America/Argentina/San_Juan", "gmtOffset" : -3 }


},
{
    "name" : "America/Argentina/San_Luis",
    "gmtOffset" : -3
},
{
    "name" : "America/Argentina/Tucuman",
    "gmtOffset" : -3
},
{
    "name" : "America/Argentina/Ushuaia",
    "gmtOffset" : -3
},
{
    "name" : "America/Aruba",
    "gmtOffset" : -4
},
{
    "name" : "America/Asuncion",
    "gmtOffset" : -4
},
{
    "name" : "America/Atikokan",
    "gmtOffset" : -5
},
{
    "name" : "America/Bahia",
    "gmtOffset" : -3
},
{
    "name" : "America/Bahia_Banderas",
    "gmtOffset" : -5
},
{
    "name" : "America/Barbados",
}
"gmtOffset" : -4
},
{
  "name" : "America/Belem",
  "gmtOffset" : -3
},
{
  "name" : "America/Belize",
  "gmtOffset" : -6
},
{
  "name" : "America/Blanc-Sablon",
  "gmtOffset" : -4
},
{
  "name" : "America/Boa_Vista",
  "gmtOffset" : -4
},
{
  "name" : "America/Bogota",
  "gmtOffset" : -5
},
{
  "name" : "America/Boise",
  "gmtOffset" : -6
},
{
  "name" : "America/Cambridge_Bay",
  "gmtOffset" : -6
},
{
  "name" : "America/Campo_Grande",
  "gmtOffset" : -4
},


"name" : "America/Cancun",
"gmtOffset" : -5
},
{
  "name" : "America/Caracas",
  "gmtOffset" : -4
},
{
  "name" : "America/Cayenne",
  "gmtOffset" : -3
},
{
  "name" : "America/Cayman",
  "gmtOffset" : -5
},
{
  "name" : "America/Chicago",
  "gmtOffset" : -5
},
{
  "name" : "America/Chihuahua",
  "gmtOffset" : -6
},
{
  "name" : "America/Costa_Rica",
  "gmtOffset" : -6
},
{
  "name" : "America/Creston",
  "gmtOffset" : -7
},
{
  "name" : "America/Cuiaba",
  "gmtOffset" : -4
},


{
    "name": "America/Curacao",
    "gmtOffset": -4
},
{
    "name": "America/Danmarkshavn",
    "gmtOffset": 0
},
{
    "name": "America/Dawson",
    "gmtOffset": -7
},
{
    "name": "America/Dawson_Creek",
    "gmtOffset": -7
},
{
    "name": "America/Denver",
    "gmtOffset": -6
},
{
    "name": "America/Detroit",
    "gmtOffset": -4
},
{
    "name": "America/Dominica",
    "gmtOffset": -4
},
{
    "name": "America/Edmonton",
    "gmtOffset": -6
},
{
    "name": "America/Eirunepe",
    "gmtOffset": -5
}
},
{
    "name" : "America/El_Salvador",
    "gmtOffset" : -6
},
{
    "name" : "America/Fort_Nelson",
    "gmtOffset" : -7
},
{
    "name" : "America/Fortaleza",
    "gmtOffset" : -3
},
{
    "name" : "America/Glace_Bay",
    "gmtOffset" : -3
},
{
    "name" : "America/Godthab",
    "gmtOffset" : -2
},
{
    "name" : "America/Goose_Bay",
    "gmtOffset" : -3
},
{
    "name" : "America/Grand_Turk",
    "gmtOffset" : -4
},
{
    "name" : "America/Grenada",
    "gmtOffset" : -4
},
{
    "name" : "America/Guadeloupe",
}
"gmtOffset" : -4
},
{
    "name" : "America/Guatemala",
    "gmtOffset" : -6
},
{
    "name" : "America/Guayaquil",
    "gmtOffset" : -5
},
{
    "name" : "America/Guyana",
    "gmtOffset" : -4
},
{
    "name" : "America/Halifax",
    "gmtOffset" : -3
},
{
    "name" : "America/Havana",
    "gmtOffset" : -4
},
{
    "name" : "America/Hermosillo",
    "gmtOffset" : -7
},
{
    "name" : "America/Indiana/Indianapolis",
    "gmtOffset" : -4
},
{
    "name" : "America/Indiana/Knox",
    "gmtOffset" : -5
},
"name" : "America/Indiana/Marengo",
"gmtOffset" : -4
},
{
"name" : "America/Indiana/Petersburg",
"gmtOffset" : -4
},
{
"name" : "America/Indiana/Tell_City",
"gmtOffset" : -5
},
{
"name" : "America/Indiana/Vevay",
"gmtOffset" : -4
},
{
"name" : "America/Indiana/Vincennes",
"gmtOffset" : -4
},
{
"name" : "America/Indiana/Winamac",
"gmtOffset" : -4
},
{
"name" : "America/Inuvik",
"gmtOffset" : -6
},
{
"name" : "America/Iqaluit",
"gmtOffset" : -4
},
{
"name" : "America/Jamaica",
"gmtOffset" : -5
},


},
{
    "name" : "America/Managua",
    "gmtOffset" : -6
},
{
    "name" : "America/Manaus",
    "gmtOffset" : -4
},
{
    "name" : "America/Marigot",
    "gmtOffset" : -4
},
{
    "name" : "America/Martinique",
    "gmtOffset" : -4
},
{
    "name" : "America/Matamoros",
    "gmtOffset" : -5
},
{
    "name" : "America/Mazatlan",
    "gmtOffset" : -6
},
{
    "name" : "America/Menominee",
    "gmtOffset" : -5
},
{
    "name" : "America/Merida",
    "gmtOffset" : -5
},
{
    "name" : "America/Metlakatla",
}
"gmtOffset" : -8
},
{
    "name" : "America/Mexico_City",
    "gmtOffset" : -5
},
{
    "name" : "America/Miquelon",
    "gmtOffset" : -2
},
{
    "name" : "America/Moncton",
    "gmtOffset" : -3
},
{
    "name" : "America/Monterrey",
    "gmtOffset" : -5
},
{
    "name" : "America/Montevideo",
    "gmtOffset" : -3
},
{
    "name" : "America/Montserrat",
    "gmtOffset" : -4
},
{
    "name" : "America/Nassau",
    "gmtOffset" : -4
},
{
    "name" : "America/New_York",
    "gmtOffset" : -4
},

"name" : "America/Nipigon",
"gmtOffset" : -4
},
{
"name" : "America/Nome",
"gmtOffset" : -8
},
{
"name" : "America/Noronha",
"gmtOffset" : -2
},
{
"name" : "America/North_Dakota/Beulah",
"gmtOffset" : -5
},
{
"name" : "America/North_Dakota/Center",
"gmtOffset" : -5
},
{
"name" : "America/North_Dakota/New_Salem",
"gmtOffset" : -5
},
{
"name" : "America/Ojinaga",
"gmtOffset" : -6
},
{
"name" : "America/Panama",
"gmtOffset" : -5
},
{
"name" : "America/Pangnirtung",
"gmtOffset" : -4
},
{
  "name": "America/Paramaribo",
  "gmtOffset": -3
},
{
  "name": "America/Phoenix",
  "gmtOffset": -7
},
{
  "name": "America/Port-au-Prince",
  "gmtOffset": -4
},
{
  "name": "America/Port_of_Spain",
  "gmtOffset": -4
},
{
  "name": "America/Porto_Velho",
  "gmtOffset": -4
},
{
  "name": "America/Puerto_Rico",
  "gmtOffset": -4
},
{
  "name": "America/Punta_Arenas",
  "gmtOffset": -3
},
{
  "name": "America/Rainy_River",
  "gmtOffset": -5
},
{
  "name": "America/Rankin_Inlet",
  "gmtOffset": -5
}
},
{
    "name": "America/Recife",
    "gmtOffset": -3
},
{
    "name": "America/Regina",
    "gmtOffset": -6
},
{
    "name": "America/Resolute",
    "gmtOffset": -5
},
{
    "name": "America/Rio_Branco",
    "gmtOffset": -5
},
{
    "name": "America/Santarem",
    "gmtOffset": -3
},
{
    "name": "America/Santiago",
    "gmtOffset": -4
},
{
    "name": "America/Santo_Domingo",
    "gmtOffset": -4
},
{
    "name": "America/Sao_Paulo",
    "gmtOffset": -3
},
{
    "name": "America/Scoresbysund",
    "gmtOffset": -3
}
{"gmtOffset": 0},
{
    "name": "America/Sitka",
    "gmtOffset": -8
},
{
    "name": "America/St_Barthelemy",
    "gmtOffset": -4
},
{
    "name": "America/St_Johns",
    "gmtOffset": -2.5
},
{
    "name": "America/St_Kitts",
    "gmtOffset": -4
},
{
    "name": "America/St_Lucia",
    "gmtOffset": -4
},
{
    "name": "America/St_Thomas",
    "gmtOffset": -4
},
{
    "name": "America/St_Vincent",
    "gmtOffset": -4
},
{
    "name": "America/Swift_Current",
    "gmtOffset": -6
},
"name" : "America/Tegucigalpa",
"gmtOffset" : -6
},
{
"name" : "America/Thule",
"gmtOffset" : -3
},
{
"name" : "America/Thunder_Bay",
"gmtOffset" : -4
},
{
"name" : "America/Tijuana",
"gmtOffset" : -7
},
{
"name" : "America/Toronto",
"gmtOffset" : -4
},
{
"name" : "America/Tortola",
"gmtOffset" : -4
},
{
"name" : "America/Vancouver",
"gmtOffset" : -7
},
{
"name" : "America/Whitehorse",
"gmtOffset" : -7
},
{
"name" : "America/Winnipeg",
"gmtOffset" : -5
},
{
    "name" : "America/Yakutat",
    "gmtOffset" : -8
},
{
    "name" : "America/Yellowknife",
    "gmtOffset" : -6
},
{
    "name" : "Antarctica/Casey",
    "gmtOffset" : 8
},
{
    "name" : "Antarctica/Davis",
    "gmtOffset" : 7
},
{
    "name" : "Antarctica/DumontDUrville",
    "gmtOffset" : 10
},
{
    "name" : "Antarctica/Macquarie",
    "gmtOffset" : 11
},
{
    "name" : "Antarctica/Mawson",
    "gmtOffset" : 5
},
{
    "name" : "Antarctica/McMurdo",
    "gmtOffset" : 12
},
{
    "name" : "Antarctica/Palmer",
    "gmtOffset" : -3
}
"name" : "Antarctica/Rothera",
"gmtOffset" : -3
},
{
"name" : "Antarctica/Syowa",
"gmtOffset" : 3
},
{
"name" : "Antarctica/Troll",
"gmtOffset" : 2
},
{
"name" : "Antarctica/Vostok",
"gmtOffset" : 6
},
{
"name" : "Arctic/Longyearbyen",
"gmtOffset" : 2
},
{
"name" : "Asia/Aden",
"gmtOffset" : 3
},
{
"name" : "Asia/Almaty",
"gmtOffset" : 6
},
{
"name" : "Asia/Amman",
"gmtOffset" : 3
},
{
"name" : "Asia/Anadyr",
"gmtOffset" : 908
}
"gmtOffset" : 12
},
{
  "name" : "Asia/Aqtau",
  "gmtOffset" : 5
},
{
  "name" : "Asia/Aqtobe",
  "gmtOffset" : 5
},
{
  "name" : "Asia/Ashgabat",
  "gmtOffset" : 5
},
{
  "name" : "Asia/Atyrau",
  "gmtOffset" : 5
},
{
  "name" : "Asia/Baghdad",
  "gmtOffset" : 3
},
{
  "name" : "Asia/Bahrain",
  "gmtOffset" : 3
},
{
  "name" : "Asia/Baku",
  "gmtOffset" : 4
},
{
  "name" : "Asia/Bangkok",
  "gmtOffset" : 7
},
"name": "Asia/Barnaul",
"gmtOffset": 7
},
{
"name": "Asia/Beirut",
"gmtOffset": 3
},
{
"name": "Asia/Bishkek",
"gmtOffset": 6
},
{
"name": "Asia/Brunei",
"gmtOffset": 8
},
{
"name": "Asia/Chita",
"gmtOffset": 9
},
{
"name": "Asia/Choibalsan",
"gmtOffset": 8
},
{
"name": "Asia/Colombo",
"gmtOffset": 5.5
},
{
"name": "Asia/Damascus",
"gmtOffset": 3
},
{
"name": "Asia/Dhaka",
"gmtOffset": 6
},
{ "name" : "Asia/Dili", "gmtOffset" : 9 },
{ "name" : "Asia/Dubai", "gmtOffset" : 4 },
{ "name" : "Asia/Dushanbe", "gmtOffset" : 5 },
{ "name" : "Asia/Famagusta", "gmtOffset" : 3 },
{ "name" : "Asia/Gaza", "gmtOffset" : 3 },
{ "name" : "Asia/Hebron", "gmtOffset" : 3 },
{ "name" : "Asia/Ho_Chi_Minh", "gmtOffset" : 7 },
{ "name" : "Asia/Hong_Kong", "gmtOffset" : 8 },
{ "name" : "Asia/Hovd", "gmtOffset" : 7 }
},
{
  "name" : "Asia/Irkutsk",
  "gmtOffset" : 8
},
{
  "name" : "Asia/Jakarta",
  "gmtOffset" : 7
},
{
  "name" : "Asia/Jayapura",
  "gmtOffset" : 9
},
{
  "name" : "Asia/Jerusalem",
  "gmtOffset" : 3
},
{
  "name" : "Asia/Kabul",
  "gmtOffset" : 4.5
},
{
  "name" : "Asia/Kamchatka",
  "gmtOffset" : 12
},
{
  "name" : "Asia/Karachi",
  "gmtOffset" : 5
},
{
  "name" : "Asia/Kathmandu",
  "gmtOffset" : 5.75
},
{
  "name" : "Asia/Khandyga",

{
  "name" : "Asia/Kolkata",
  "gmtOffset" : 5.5
},
{
  "name" : "Asia/Krasnoyarsk",
  "gmtOffset" : 7
},
{
  "name" : "Asia/Kuala_Lumpur",
  "gmtOffset" : 8
},
{
  "name" : "Asia/Kuching",
  "gmtOffset" : 8
},
{
  "name" : "Asia/Kuwait",
  "gmtOffset" : 3
},
{
  "name" : "Asia/Macau",
  "gmtOffset" : 8
},
{
  "name" : "Asia/Magadan",
  "gmtOffset" : 11
},
{
  "name" : "Asia/Makassar",
  "gmtOffset" : 8
}
"name" : "Asia/Manila",
"gmtOffset" : 8
},
{
 "name" : "Asia/Muscat",
 "gmtOffset" : 4
},
{
 "name" : "Asia/Nicosia",
 "gmtOffset" : 3
},
{
 "name" : "Asia/Novokuznetsk",
 "gmtOffset" : 7
},
{
 "name" : "Asia/Novosibirsk",
 "gmtOffset" : 7
},
{
 "name" : "Asia/Omsk",
 "gmtOffset" : 6
},
{
 "name" : "Asia/Oral",
 "gmtOffset" : 5
},
{
 "name" : "Asia/Phnom_Penh",
 "gmtOffset" : 7
},
{
 "name" : "Asia/Pontianak",
 "gmtOffset" : 7
},


```json
[
  {
    "name": "Asia/Pyongyang",
    "gmtOffset": 9
  },
  {
    "name": "Asia/Qatar",
    "gmtOffset": 3
  },
  {
    "name": "Asia/Qyzylorda",
    "gmtOffset": 6
  },
  {
    "name": "Asia/Riyadh",
    "gmtOffset": 3
  },
  {
    "name": "Asia/Sakhalin",
    "gmtOffset": 11
  },
  {
    "name": "Asia/Samarkand",
    "gmtOffset": 5
  },
  {
    "name": "Asia/Seoul",
    "gmtOffset": 9
  },
  {
    "name": "Asia/Shanghai",
    "gmtOffset": 8
  },
  {
    "name": "Asia/Singapore",
    "gmtOffset": 8
  }
]
```
},
{
    "name": "Asia/Srednekolymsk",
    "gmtOffset": 11
},
{
    "name": "Asia/Taipei",
    "gmtOffset": 8
},
{
    "name": "Asia/Tashkent",
    "gmtOffset": 5
},
{
    "name": "Asia/Tbilisi",
    "gmtOffset": 4
},
{
    "name": "Asia/Tehran",
    "gmtOffset": 4.5
},
{
    "name": "Asia/Thimphu",
    "gmtOffset": 6
},
{
    "name": "Asia/Tokyo",
    "gmtOffset": 9
},
{
    "name": "Asia/Tomsk",
    "gmtOffset": 7
},
{
    "name": "Asia/Ulaanbaatar",
}
"gmtOffset" : 8
},
{
  "name" : "Asia/Urumqi",
  "gmtOffset" : 6
},
{
  "name" : "Asia/Ust-Nera",
  "gmtOffset" : 10
},
{
  "name" : "Asia/Vientiane",
  "gmtOffset" : 7
},
{
  "name" : "Asia/Vladivostok",
  "gmtOffset" : 10
},
{
  "name" : "Asia/Yakutsk",
  "gmtOffset" : 9
},
{
  "name" : "Asia/Yangon",
  "gmtOffset" : 6.5
},
{
  "name" : "Asia/Yekaterinburg",
  "gmtOffset" : 5
},
{
  "name" : "Asia/Yerevan",
  "gmtOffset" : 4
}
"name": "Atlantic/Azores",
"gmtOffset": 0
},
{
"name": "Atlantic/Bermuda",
"gmtOffset": -3
},
{
"name": "Atlantic/Canary",
"gmtOffset": 1
},
{
"name": "Atlantic/Cape_Verde",
"gmtOffset": -1
},
{
"name": "Atlantic/Faroe",
"gmtOffset": 1
},
{
"name": "Atlantic/Madeira",
"gmtOffset": 1
},
{
"name": "Atlantic/Reykjavik",
"gmtOffset": 0
},
{
"name": "Atlantic/South_Georgia",
"gmtOffset": -2
},
{
"name": "Atlantic/St_Helena",
"gmtOffset": 0
},

},

{  
  "name" : "Australia/Lord_Howe",
  "gmtOffset" : -10.5
},

{  
  "name" : "Australia/Melbourne",
  "gmtOffset" : 10
},

{  
  "name" : "Australia/Perth",
  "gmtOffset" : 8
},

{  
  "name" : "Australia/Sydney",
  "gmtOffset" : 10
},

{  
  "name" : "Europe/Amsterdam",
  "gmtOffset" : 2
},

{  
  "name" : "Europe/Andorra",
  "gmtOffset" : 2
},

{  
  "name" : "Europe/Astrakhan",
  "gmtOffset" : 4
},

{  
  "name" : "Europe/Athens",
  "gmtOffset" : 3
},

{  
  "name" : "Europe/Belgrade",

"gmtOffset" : 2 },
{
    "name" : "Europe/Berlin",
    "gmtOffset" : 2
},
{
    "name" : "Europe/Bratislava",
    "gmtOffset" : 2
},
{
    "name" : "Europe/Brussels",
    "gmtOffset" : 2
},
{
    "name" : "Europe/Bucharest",
    "gmtOffset" : 3
},
{
    "name" : "Europe/Budapest",
    "gmtOffset" : 2
},
{
    "name" : "Europe/Busingen",
    "gmtOffset" : 2
},
{
    "name" : "Europe/Chisinau",
    "gmtOffset" : 3
},
{
    "name" : "Europe/Copenhagen",
    "gmtOffset" : 2
},
"name" : "Europe/Dublin",
"gmtOffset" : 1
},
{
  "name" : "Europe/Gibraltar",
  "gmtOffset" : 2
},
{
  "name" : "Europe/Guernsey",
  "gmtOffset" : 1
},
{
  "name" : "Europe/Helsinki",
  "gmtOffset" : 3
},
{
  "name" : "Europe/Isle_of_Man",
  "gmtOffset" : 1
},
{
  "name" : "Europe/Istanbul",
  "gmtOffset" : 3
},
{
  "name" : "Europe/Jersey",
  "gmtOffset" : 1
},
{
  "name" : "Europe/Kaliningrad",
  "gmtOffset" : 2
},
{
  "name" : "Europe/Kiev",
  "gmtOffset" : 3
}


},
{
    "name": "Europe/Monaco",
    "gmtOffset": 2
},
{
    "name": "Europe/Moscow",
    "gmtOffset": 3
},
{
    "name": "Europe/Oslo",
    "gmtOffset": 2
},
{
    "name": "Europe/Paris",
    "gmtOffset": 2
},
{
    "name": "Europe/Podgorica",
    "gmtOffset": 2
},
{
    "name": "Europe/Prague",
    "gmtOffset": 2
},
{
    "name": "Europe/Riga",
    "gmtOffset": 3
},
{
    "name": "Europe/Rome",
    "gmtOffset": 2
},
{
    "name": "Europe/Samara",
    "gmtOffset": 2
},
}
"gmtOffset" : 4
],
{
  "name" : "Europe/San_Marino",
  "gmtOffset" : 2
},
{
  "name" : "Europe/Sarajevo",
  "gmtOffset" : 2
},
{
  "name" : "Europe/Saratov",
  "gmtOffset" : 4
},
{
  "name" : "Europe/Simferopol",
  "gmtOffset" : 3
},
{
  "name" : "Europe/Skopje",
  "gmtOffset" : 2
},
{
  "name" : "Europe/Sofia",
  "gmtOffset" : 3
},
{
  "name" : "Europe/Stockholm",
  "gmtOffset" : 2
},
{
  "name" : "Europe/Tallinn",
  "gmtOffset" : 3
},
"name" : "Europe/Tirane",
"gmtOffset" : 2
},
{
  "name" : "Europe/Ulyanovsk",
  "gmtOffset" : 4
},
{
  "name" : "Europe/Uzhgorod",
  "gmtOffset" : 3
},
{
  "name" : "Europe/Vaduz",
  "gmtOffset" : 2
},
{
  "name" : "Europe/Vatican",
  "gmtOffset" : 2
},
{
  "name" : "Europe/Vienna",
  "gmtOffset" : 2
},
{
  "name" : "Europe/Vilnius",
  "gmtOffset" : 3
},
{
  "name" : "Europe/Volgograd",
  "gmtOffset" : 3
},
{
  "name" : "Europe/Warsaw",
  "gmtOffset" : 2
},

null
{ "name": "Indian/Mahe", "gmtOffset": 4 },
{ "name": "Indian/Maldives", "gmtOffset": 5 },
{ "name": "Indian/Mauritius", "gmtOffset": 4 },
{ "name": "Indian/Mayotte", "gmtOffset": 3 },
{ "name": "Indian/Reunion", "gmtOffset": 4 },
{ "name": "Pacific/Apia", "gmtOffset": 13 },
{ "name": "Pacific/Auckland", "gmtOffset": 12 },
{ "name": "Pacific/Bougainville", "gmtOffset": 11 },
{ "name": "Pacific/Chatham",}
"gmtOffset" : 12.75
},
{
"name" : "Pacific/Chuuk",
"gmtOffset" : 10
},
{
"name" : "Pacific/Easter",
"gmtOffset" : -6
},
{
"name" : "Pacific/Efate",
"gmtOffset" : 11
},
{
"name" : "Pacific/Enderbury",
"gmtOffset" : 13
},
{
"name" : "Pacific/Fakaofo",
"gmtOffset" : 13
},
{
"name" : "Pacific/Fiji",
"gmtOffset" : 12
},
{
"name" : "Pacific/Funafuti",
"gmtOffset" : 12
},
{
"name" : "Pacific/Galapagos",
"gmtOffset" : -6
},
{
"name" : "Pacific/Gambier",
"gmtOffset" : -9
},
{
"name" : "Pacific/Guadalcanal",
"gmtOffset" : 11
},
{
"name" : "Pacific/Guam",
"gmtOffset" : 10
},
{
"name" : "Pacific/Honolulu",
"gmtOffset" : -10
},
{
"name" : "Pacific/Kiritimati",
"gmtOffset" : 14
},
{
"name" : "Pacific/Kosrae",
"gmtOffset" : 11
},
{
"name" : "Pacific/Kwajalein",
"gmtOffset" : 12
},
{
"name" : "Pacific/Majuro",
"gmtOffset" : 12
},
{
"name" : "Pacific/Marquesas",
"gmtOffset" : -9.5
},
{
    "name" : "Pacific/Midway",
    "gmtOffset" : -11
},
{
    "name" : "Pacific/Nauru",
    "gmtOffset" : 12
},
{
    "name" : "Pacific/Niue",
    "gmtOffset" : -11
},
{
    "name" : "Pacific/Norfolk",
    "gmtOffset" : 11
},
{
    "name" : "Pacific/Noumea",
    "gmtOffset" : 11
},
{
    "name" : "Pacific/Pago_Pago",
    "gmtOffset" : -11
},
{
    "name" : "Pacific/Palau",
    "gmtOffset" : 9
},
{
    "name" : "Pacific/Pitcairn",
    "gmtOffset" : -8
},
{
    "name" : "Pacific/Pohnpei",
    "gmtOffset" : 11
}

{
  "name" : "Pacific/Port_Moresby",
  "gmtOffset" : 10
},
{
  "name" : "Pacific/Rarotonga",
  "gmtOffset" : -10
},
{
  "name" : "Pacific/Saipan",
  "gmtOffset" : 10
},
{
  "name" : "Pacific/Tahiti",
  "gmtOffset" : -10
},
{
  "name" : "Pacific/Tarawa",
  "gmtOffset" : 12
},
{
  "name" : "Pacific/Tongatapu",
  "gmtOffset" : 13
},
{
  "name" : "Pacific/Wake",
  "gmtOffset" : 12
},
{
  "name" : "Pacific/Wallis",
  "gmtOffset" : 12
},
{
  "name" : "UTC",
}
/system/debug

Methods

GET

GETs the list of debug items.

Request Query Parameters

None

Example Response

Expand

{
   "type" : "regular",
   "response" : [
      {
         "id" : "0",
         "name" : "Accept Risk",
         "category" : "uncommon",
         "sizeWarning" : "false",
         "enabled" : "false"
      },
      {
      }
   ]
}


"id" : "1",
"name" : "Activity Log",
"category" : "uncommon",
"sizeWarning" : "false",
"enabled" : "true"
},
{
"id" : "2",
"name" : "Apply All Risk",
"category" : "uncommon",
"sizeWarning" : "false",
"enabled" : "false"
},
{
"id" : "3",
"name" : "Convert Compliance",
"category" : "rare",
"sizeWarning" : "false",
"enabled" : "false"
},
{
"id" : "4",
"name" : "Convert Name DB",
"category" : "rare",
"sizeWarning" : "false",
"enabled" : "false"
},
{
"id" : "5",
"name" : "Convert Repositories",
"category" : "rare",
"sizeWarning" : "false",
"enabled" : "false"
},
"id" : "6",
"name" : "Custom Plugin Upload",
"category" : "rare",
"sizeWarning" : "false",
"enabled" : "false"
},
{
"id" : "7",
"name" : "DB Locks",
"category" : "common",
"sizeWarning" : "false",
"enabled" : "false"
},
{
"id" : "8",
"name" : "Dev Migration",
"category" : "rare",
"sizeWarning" : "false",
"enabled" : "false"
},
{
"id" : "9",
"name" : "Evaluate ARC",
"category" : "rare",
"sizeWarning" : "false",
"enabled" : "false"
},
{
"id" : "10",
"name" : "Evaluate ARC Policy Statement Status",
"category" : "rare",
"sizeWarning" : "false",
"enabled" : "false"
}
"id" : "11",
"name" : "Evaluate AR Sync Status",
"category" : "rare",
"sizeWarning" : "false",
"enabled" : "false"
},
{
"id" : "12",
"name" : "Evaluate Blackout Window Status",
"category" : "rare",
"sizeWarning" : "false",
"enabled" : "false"
},
{
"id" : "13",
"name" : "Evaluate Dashboard Component Status",
"category" : "rare",
"sizeWarning" : "false",
"enabled" : "false"
},
{
"id" : "14",
"name" : "Evaluate Dashboard Element",
"category" : "rare",
"sizeWarning" : "false",
"enabled" : "false"
},
{
"id" : "15",
"name" : "Evaluate Matrix Cluster",
"category" : "rare",
"sizeWarning" : "false",
"enabled" : "false"
},
"id" : "16",
"name" : "Evaluate Query Status",
"category" : "rare",
"sizeWarning" : "false",
"enabled" : "false"
},
{
"id" : "17",
"name" : "Evaluate Report Status",
"category" : "rare",
"sizeWarning" : "false",
"enabled" : "false"
},
{
"id" : "18",
"name" : "Evaluate Scan Status",
"category" : "rare",
"sizeWarning" : "false",
"enabled" : "false"
},
{
"id" : "19",
"name" : "Expire Accepted Risk",
"category" : "rare",
"sizeWarning" : "false",
"enabled" : "false"
},
{
"id" : "20",
"name" : "Export",
"category" : "uncommon",
"sizeWarning" : "false",
"enabled" : "false"
}
"id" : "21",
"name" : "Feed Update",
"category" : "uncommon",
"sizeWarning" : "false",
"enabled" : "false"
},
{
"id" : "22",
"name" : "Flush Vulns",
"category" : "uncommon",
"sizeWarning" : "false",
"enabled" : "false"
},
{
"id" : "23",
"name" : "IDS Correlations",
"category" : "rare",
"sizeWarning" : "false",
"enabled" : "false"
},
{
"id" : "24",
"name" : "IDS Signatures",
"category" : "rare",
"sizeWarning" : "false",
"enabled" : "false"
},
{
"id" : "25",
"name" : "Import",
"category" : "common",
"sizeWarning" : "false",
"enabled" : "false"
}
"id" : "26",
"name" : "Import ARC",
"category" : "rare",
"sizeWarning" : "false",
"enabled" : "false"
},
{
"id" : "27",
"name" : "Import Dashboard",
"category" : "uncommon",
"sizeWarning" : "false",
"enabled" : "false"
},
{
"id" : "28",
"name" : "Import Mobile",
"category" : "rare",
"sizeWarning" : "false",
"enabled" : "false"
},
{
"id" : "29",
"name" : "Import Report",
"category" : "rare",
"sizeWarning" : "false",
"enabled" : "false"
},
{
"id" : "30",
"name" : "Industrial Plugin Update",
"category" : "uncommon",
"sizeWarning" : "false",
"enabled" : "false"}


```
"id" : "31",
"name" : "Industrial Plugin Update Testing",
"category" : "rare",
"sizeWarning" : "false",
"enabled" : "false"
},
{
  "id" : "32",
  "name" : "Industrial Results",
  "category" : "uncommon",
  "sizeWarning" : "false",
  "enabled" : "false"
},
{
  "id" : "33",
  "name" : "Job Activity",
  "category" : "uncommon",
  "sizeWarning" : "false",
  "enabled" : "false"
},
{
  "id" : "34",
  "name" : "Job Daemon",
  "category" : "uncommon",
  "sizeWarning" : "false",
  "enabled" : "false"
},
{
  "id" : "35",
  "name" : "LCE Plugin Update",
  "category" : "rare",
  "sizeWarning" : "false",
  "enabled" : "false"
},
`

"940"
"id": "36",
"name": "LCE Status",
"category": "rare",
"sizeWarning": "false",
"enabled": "false"
},
{
"id": "37",
"name": "Licensing",
"category": "rare",
"sizeWarning": "false",
"enabled": "false"
},
{
"id": "38",
"name": "Mark Assets Prepared",
"category": "rare",
"sizeWarning": "false",
"enabled": "false"
},
{
"id": "39",
"name": "Migrate User Files",
"category": "rare",
"sizeWarning": "false",
"enabled": "false"
},
{
"id": "40",
"name": "Migration",
"category": "uncommon",
"sizeWarning": "false",
"enabled": "false"
},
null
"id" : "46",
"name" : "Passive Plugin Update Testing",
"category" : "rare",
"sizeWarning" : "false",
"enabled" : "false"
},
{
"id" : "47",
"name" : "Password Convert",
"category" : "rare",
"sizeWarning" : "false",
"enabled" : "false"
},
{
"id" : "48",
"name" : "Patch",
"category" : "rare",
"sizeWarning" : "false",
"enabled" : "false"
},
{
"id" : "49",
"name" : "Performance Log",
"category" : "uncommon",
"sizeWarning" : "false",
"enabled" : "false"
},
{
"id" : "50",
"name" : "Plugin Update",
"category" : "uncommon",
"sizeWarning" : "false",
"enabled" : "false"
}
"id": "51",
"name": "Plugin Update Testing",
"category": "rare",
"sizeWarning": "false",
"enabled": "false"
},
{
"id": "52",
"name": "Prepare Assets",
"category": "common",
"sizeWarning": "false",
"enabled": "false"
},
{
"id": "53",
"name": "Publishing",
"category": "rare",
"sizeWarning": "false",
"enabled": "false"
},
{
"id": "54",
"name": "Recast Risk",
"category": "uncommon",
"sizeWarning": "false",
"enabled": "false"
},
{
"id": "55",
"name": "Remote Client Tools",
"category": "rare",
"sizeWarning": "false",
"enabled": "false"
},
"id": "56",
"name": "Remote Client Tools",
"category": "rare",
"sizeWarning": "false",
"enabled": "false"}
"id" : "56",
"name" : "Reporting",
"category" : "common",
"sizeWarning" : "true",
"enabled" : "false"
},
{
"id" : "57",
"name" : "Resolve Host Names",
"category" : "uncommon",
"sizeWarning" : "false",
"enabled" : "false"
},
{
"id" : "58",
"name" : "Run Alert",
"category" : "rare",
"sizeWarning" : "false",
"enabled" : "false"
},
{
"id" : "59",
"name" : "Save Policy",
"category" : "rare",
"sizeWarning" : "false",
"enabled" : "false"
},
{
"id" : "60",
"name" : "Scan",
"category" : "common",
"sizeWarning" : "true",
"enabled" : "false"
}
"id": "61",
"name": "Scanner Status",
"category": "uncommon",
"sizeWarning": "false",
"enabled": "false"
}
{
"id": "62",
"name": "Session",
"category": "rare",
"sizeWarning": "false",
"enabled": "false"
}
{
"id": "63",
"name": "Simple Activity",
"category": "uncommon",
"sizeWarning": "false",
"enabled": "false"
}
{
"id": "64",
"name": "Synchronize Agent Results",
"category": "common",
"sizeWarning": "false",
"enabled": "false"
}
{
"id": "65",
"name": "Synchronize Repository",
"category": "common",
"sizeWarning": "false",
"enabled": "false"
}
"id" : "66",
"name" : "Take Repository Snapshots",
"category" : "uncommon",
"sizeWarning" : "false",
"enabled" : "false"
},

{
"id" : "67",
"name" : "Update DNS Assets",
"category" : "common",
"sizeWarning" : "false",
"enabled" : "false"
},

{
"id" : "68",
"name" : "Update LCE Silos",
"category" : "rare",
"sizeWarning" : "false",
"enabled" : "false"
},

{
"id" : "69",
"name" : "Update LCE Types",
"category" : "rare",
"sizeWarning" : "false",
"enabled" : "false"
},

{
"id" : "70",
"name" : "Update LDAP Assets",
"category" : "common",
"sizeWarning" : "false",
"enabled" : "false"
}
"id" : "71",
"name" : "Disk I/O Errors",
"category" : "common",
"sizeWarning" : "false",
"enabled" : "false"
}
]
"error_code" : 0,
"error_msg" : "",
"warnings" : []
"timestamp" : 1551190238
}

PATCH
Edits one or more debug items. Only the debug items specified are modified.

Request Parameters
Expand
{
 "debugs" : [
 { "id" : <number>,
 "enabled" : <string> "false" | "true"
 }
 ... ]
}

Example Response
See /system/debug::GET

/system/diagnostics
The /system/diagnostics resource.
Methods

GET

Gets the system diagnostics information.

Fields Parameter

Expand

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

\[ ?fields=<field>,... \]

Allowed Fields

**statusJava**
**statusRPM**
**statusDisk**
**statusThresholdDisk**
**statusLastChecked**
**diagnosticsGenerated**
**diagnosticsGenerateState**
**touchDebuggingEnabled**
**migrationFailure**

Legend*

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

Request Parameters

None

Example Response

Expand
The `/system/diagnostics/generate` resource.

Methods

POST

Starts an on-demand, diagnostics analysis for the System that can be downloaded after its job completes.

Request Parameters

Expand

```json
{
    "type": "regular",
    "response": {
        "statusJava": "true",
        "statusRPM": "true",
        "statusDisk": "true",
        "statusThresholdDisk": "5\%",
        "statusLastChecked": "1425532201",
        "diagnosticsGenerated": 1425563166,
        "diagnosticsGenerateState": "-1",
        "touchDebuggingEnabled": false,
        "migrationFailure": false
    },
    "error_code": 0,
    "error_msg": "",
    "warnings": [],
    "timestamp": 1425571142
}
```

/system/diagnostics/generate
Example Response
Expand
{
   "type" : "regular",
   "response" : "",
   "error_code" : 0,
   "error_msg" : "",
   "warnings" : [],
   "timestamp" : 1425574362
}

/system/diagnostics/download
The /system/diagnostics/download resource.

Methods

POST
Downloads the system diagnostics, debug file that was last generated.

NOTE: The /system/diagnostics/generate command should be used to generate a diagnostics file of the System for download.
Request Parameters
None

Example Response
None given. The response will be a zip or gzip ped file containing the System’s diagnostics information.

/system/locale

Methods

GET

Retrieves the current Locale set in Tenable.sc.

Request Parameters
None

Example Response
Expand
{
    "type" : "regular",
    "response" : {
        "code" : "ja",
        "name" : "Japanese",
    },
    "error_code" : 0,
    "error_msg" : "",
    "warnings" : [],
    "timestamp" : 1494360454
}

PATCH

Change the Locale to the one selected by the admin
NOTE: Only available languages can be used. See available Locales by calling /system/locales::GET (see below). An empty string resets to the default locale (English).

**Request Parameters**

Expand

```json
{
    "PluginLocale" : <String>
}
```

**Example Response**

Expand

```json
{
    "type" : "regular",
    "response" : "ja",
    "error_code" : 0,
    "error_msg" : "",
    "warnings" : [],
    "timestamp" : 1494360819
}
```

/system/locales

**Methods**

**GET**

States the current locale set in Tenable.sc.

**Request Parameters**

None

**Example Response**

Expand
/system/logFiles

Methods

GET

GETs the list of log files available to the user

Request Parameters

None

Example Response for Admins

Expand
Example Response for Security Managers

Expand

{
   "type": "regular",
   "response": [
   {
      "organization": {
         "id": 0,
         "name": "Application",
         "description": ""
      },
      "basenames": ["202106"
      ]
   },
   {
      "organization": {
         "id": 1,
         "name": "Org",
         "description": ""
      },
      "basenames": ["202106"
      ]
   }
   ],
   "error_code": 0,
   "error_msg": "",
   "warnings": [],
   "timestamp": 1624370508
}
"response": [  
  {  
    "basenames": [  
      "202106"  
    ]  
  },  
  
  "error_code": 0,  
  "error_msg": "",  
  "warnings": [],  
  "timestamp": 1624371093  
}  

/system/logs

Methods

POST

Returns the available log messages based on user permissions and the query filters

Request Parameters

Expand

{
  "date" : scLog basename (eg. "201412") | "all",  
  "query": {  
    "startOffset" : <number>,  
    "endOffset" : <number>,  
    "filters" : [  
      {  
        "filterName" : "keywords",  
        "operator" : "=",  
        "value" : <string>  
      },  
      {  
      
      

956
"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": 124,
    "endOffset": 3,
    "results": [
    {
        "rawLog": "Tue, 22 Jun 2021 09:42:00 -0400|expireAcceptedRisk|message|INFO|0|Expire accepted risk job #813 has ended."
    }
    }
}
"organization": {  
  "id": 0,  
  "name": "Application",  
  "description": ""
},  
"severity": {  
  "id": "0",  
  "name": "INFO",  
  "description": "Information"  
},  
"module": "message",  
"source": "expireAcceptedRisk",  
"date": "Tue, 22 Jun 2021 09:42:00 -0400"
},  
{"rawLog": "Tue, 22 Jun 2021 09:42:00 -0400|expireAcceptedRisk|message|INFO|0|Expire accepted risk job #813 starting...",  
"message": "Expire accepted risk job #813 starting...",  
"organization": {  
  "id": 0,  
  "name": "Application",  
  "description": ""
},  
"severity": {  
  "id": "0",  
  "name": "INFO",  
  "description": "Information"  
},  
"module": "message",  
"source": "expireAcceptedRisk",  
"date": "Tue, 22 Jun 2021 09:42:00 -0400"
},  
{"rawLog": "Tue, 22 Jun 2021 09:40:48 -0400|admin|auth|INFO|0|Successful login for 'admin' from 192.168.36.43 (authentication type: tns).",  
"message": "Successful login for 'admin' from 192.168.36.43 (authentication type: tns).",  
"organization": {  
  "id": 0,  
  "name": "Application",  
  "description": ""
},  
"severity": {  
  "id": "0",  
  "name": "INFO",  
  "description": "Information"  
},  
"module": "message",  
"source": "admin|auth",  
"date": "Tue, 22 Jun 2021 09:40:48 -0400"
/system/logs/download

**Methods**

**POST**

Downloads log messages that are available to the user based on the query parameter.

NOTE: The system logs are downloaded as a CSV file.

**Request Parameters**

Expand

```
{  
    "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>
    }
  }
]
}

"Thu, 24 Jun 2021 11:42:00 -0400", "expireAcceptedRisk", "message", "INFO", "Application", "Expire accepted risk job #2181 has ended."

"Thu, 24 Jun 2021 11:42:00 -0400", "expireAcceptedRisk", "message", "INFO", "Application", "Expire accepted risk job #2181 starting..."
**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 description"
        },
        {
          "id": "4065",
          "name": "ScannerB",
          "description": "This is a description"
        }
      ]
    }
  ]
}
"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" : "3124ff6ca5a4f4ba20557da5b829b2a",
"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
**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*

**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

```json
{
   "type" : "regular",
   "response" : {
      "usable" : [
         {
            "id" : "1",
            "name" : "TestTicket",
            "description" : ""
         }
      ],
      "manageable" : [
```

```json
```
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" | ... 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
{  
    "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": ""  
        },  
        "owner": {  
            "id": "1",  
            "username": "head",  
            "firstname": "Security Manager",  
            "lastname": ""  
        },  
        "assignee": {  
            "id": "1",  
            "username": "head",  
            "firstname": "Security Manager",  
            "lastname": ""  
        }  
    }  
}
*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*

**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"
        },
        "owner": {
            "id": "1",
            "username": "head",
            "firstname": "hi",
            "lastname": "User"
        },
        "assignee": {
            "id": "1",
            "username": "head",
            "firstname": "hi",
            "lastname": "User"
        }
    }
}
PATCH

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

**Request Parameters**

(All fields are optional)

See /ticket::POST for parameters.

**Example Response**

See /ticket/{id}::GET
**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": "1"
        "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
User

/user

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.
- 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

Expand

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

?fields=<field>,...

Allowed Fields

*id
**username
**firstname
**lastname
**status
role
title
eemail
address
city
state
country
phone
fax
createdTime
modifiedTime
lastLogin
lastLoginIP
mustChangePassword
locked
failedLogins
authType
fingerprint
password
description
canUse
canManage
managedUsersGroups
managedObjectsGroups
preferences
ldap
Usernames
linkedUsers
parent

Session user is not role “1” (Administrator)

** responsibleAsset
** group

Legend*
*

* = always comes back

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

** 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
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",
         "locked": "false",
         "failedLogins": "0",
         "authType": "tns",
         "fingerprint": null
      }
   ]
}
"password" : "SET",
"preferences" : [
  {
    "name" : "timezone",
    "value" : "America/New_York",
    "tag" : ""
  }
],
"canUse" : true,
"canManage" : true,
"role" : {
  "id" : "1",
  "name" : "Administrator",
  "description" : "Role defining an administrator of the application"
},
"ldap" : {
  "id" : "-1",
  "name" : "",
  "description" : ""
},
"linkedUsers" : [
  {
    "user" {
      "id" : "2",
      "username" : "head",
      "firstname" : "John",
      "lastname" : "Doe"
    },
    "organization" : {
      "id" : "1",
      "name" : "Org1",
      "description" : ""
    }
  }
]
Organization User

Expand

{
    "type" : "regular",
    "response" : [

        {
            "id" : "1",
            "username" : "head",
            "firstname" : "",
            "lastname" : "",
            "canUse" : true,
            "canManage" : true
        },

        {
            "id" : "36",
            "username" : "GroupA",
            "firstname" : "",
            "lastname" : "",
            "canUse" : true,
            "canManage" : true
        },

        {
            "id" : "37",
            "username" : "GroupB",
            "firstname" : "",
            "lastname" : "",
            "canUse" : true,
            "canManage" : true
        }
    ]
}
"canUse" : true,
"canManage" : true
}

"error_code" : 0,
"error_msg" : "",
"warnings" : [],
"timestamp" : 1454348491
}

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

{
  "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
  "address" : <string> DEFAULT "",
  "city" : <string> DEFAULT "",
  "state" : <string> DEFAULT "",
  "country" : <string> DEFAULT "",
  "phone" : <string> DEFAULT "",
  "fax" : <string> DEFAULT "",

987
"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"

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 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" : "1454349916",
"lastLoginIP" : "172.20.0.0",
"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 access to all actions at the organization level. A Security Manager can manage groups 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 Windows installed."
},
"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"
   }
},
"organization" : {
   "id" : "0",
   "name" : "Tenable.sc Administration",
   "description" : ""
}
"error_code" : 0,
"error_msg" : "",
"warnings" : [],
"timestamp" : 1454350250
}

/user/{id}

Methods

GET

Gets the User associated with {id}. 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

Expand

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

?fields=<field>,...

Allowed Fields

*id
**username
**firstname
**lastname
**status
role
title
email
address
city
state
country
phone
fax
createdTime
modifiedTime
lastLogin
lastLoginIP
mustChangePassword
locked
failedLogins
authType
fingerprint
password
description
canUse
canManage
managedUsersGroups
managedObjectsGroups
canUse
canManage
preferences
ldap
linkedUsers
parent

Session user is not role “1” (Administrator)

**responsibleAsset**

**group**

**Legend**

* = always comes back

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

**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": "172.20.0.0",
        "mustChangePassword": "false",
        "locked": "false",
        "failedLogins": "0",
        "authType": "tns",
        "fingerprint": "null",
        "password": "SET",
        "managedUsersGroups": [],
        "managedObjectsGroups": [],
        "preferences": []
    }
}


{
    "name": "timezone",
    "value": "America/New_York",
    "tag": ""
}
]
"canUse": true,
"canManage": true,
"role": {
    "id": "1",
    "name": "Administrator",
    "description": "Role defining an administrator of the application"
},
"group": {
    "id": "-1",
    "name": "",
    "description": ""
},
"ldap": {
    "id": "-1",
    "name": "",
    "description": ""
},
linkedUsers: [
    {
        "user": {
            "id": "2",
            "username": "head",
            "firstname": "John",
            "lastname": "Doe"
        },
        "organization": {
            "id": "1",
            "name": "Org1",
            "description": ""
        }
    }
]
Organization User

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",
        "timestamp": 1454350376
    }
}
"lastLoginIP" : "172.20.0.0",
"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 access to all actions at the organization level. A Security Manager...
}
}
"responsibleAsset" : {
    "id" : "19",
    "name" : "Windows Hosts",
    "description" : "The operating system detected has Windows installed."
},
"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"
    },
    "organization" : {
        "id" : "0",
        "name" : "Tenable.sc Administration",
        "description" : ""
    }
},
"error_code" : 0,
"error_msg" : "",
"warnings" : []
"timestamp" : 1454350250
}
**PATCH**

Edits the User associated with {id}, 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`.

**Request Parameters**

(All fields are optional)

See `/user::POST` for parameters.

**Example Response**

See `/user/{id}::GET`

**DELETE**

Deletes the User associated with {id}, 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**

```json
{
    "orgID" : <number> OPTIONAL,
    "migrateUserID": <number> OPTIONAL
}
```

**Session user is not an Administrator**

```json
{
    "migrateUserID": <number> OPTIONAL
}
```

**Example Response**

Expand

```json
{
    "type" : "regular",
    "response" : "",
    "error_code" : 0,
    "error_msg" : "",
    "warnings" : []
}
```
"timestamp" : 1402436001
}