Tenable Identity Exposure Key Features Guide

Last Revised: July 15, 2025

Table of Contents

Welcome to the Tenable Identity Exposure Key Features Guide

Welcome to Tenable Identity Exposure, formerly known as Tenable AD. This document is designed to enhance your experience by offering a comprehensive overview of the product's features and functionality, whether it's deployed on-premises or through SAAS. This resource aims to assist you whether you're a newcomer seeking guidance or an experienced user looking to deepen your understanding.

Throughout this document, you'll find various sections exploring a range of topics, including optimizing product usage and managing Indicators of Attack and Indicators of Exposure. It's important to note that while this document provides valuable insights, it's not intended to be a rigid rulebook for Tenable Identity Exposure usage. Instead, it offers recommendations for achieving a seamless and effective utilization of the platform.

About this Guide

This guide is based on the **Tenable Identity Exposure SaaS User Guide** which you can consult for comprehensive details.

The examples shown in this guide to highlight Tenable Identity Exposure's capabilities do not represent an exhaustive list and may not directly translate to every unique environment. For optimal security measures, we recommend visiting our official documentation or professional services for further details and guidance.

Key Stakeholders

The individual stakeholders in Tenable Identity Exposure differ based on your organization's size, structure, security policies, and the intended use cases. Establishing precise roles and responsibilities for each stakeholder enables the efficient adoption and utilization of the product.

When working with Tenable Identity Exposure, it's essential to grasp the diverse stakeholders involved. These individuals and groups assume varying roles in identifying, mitigating, and reporting identity-based security risks. Here's a comprehensive breakdown:

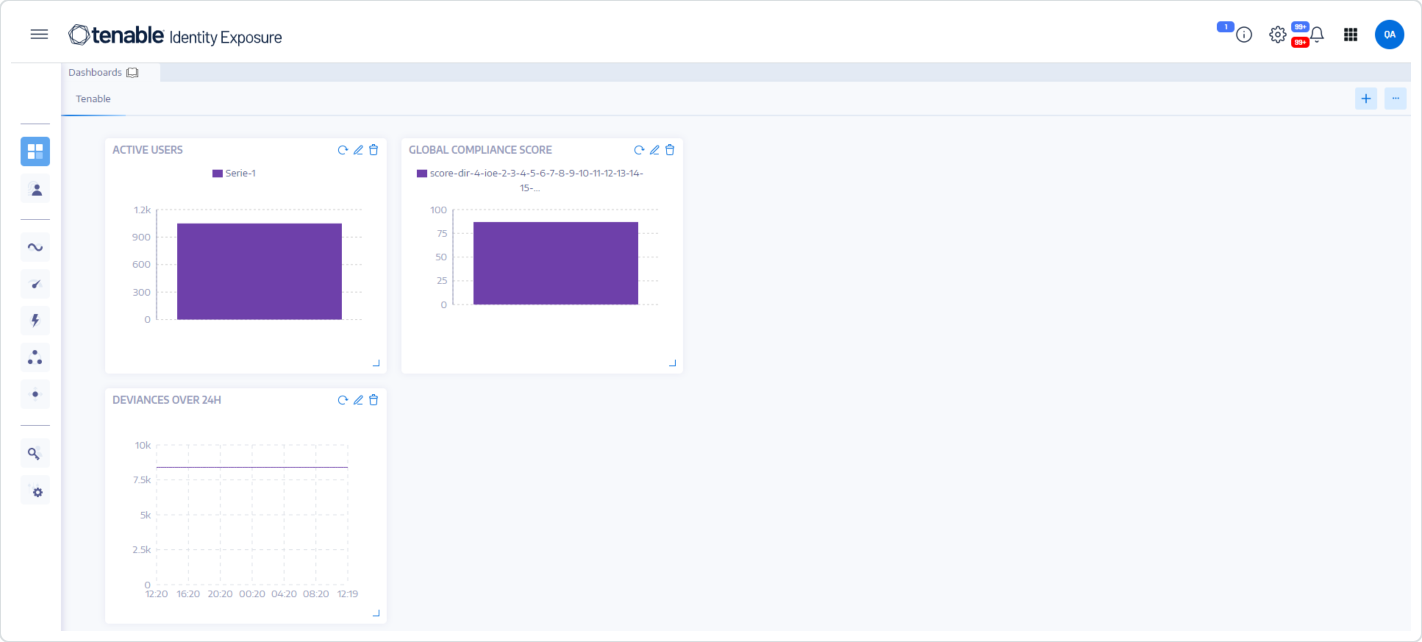
- **Security Team**: Oversees and administers the Tenable solution, leveraging data analysis to identify and respond to vulnerabilities and risks promptly.

- **IT Operations Team**: Facilitates the infrastructure and integration support for the Tenable solution, ensuring seamless connectivity with other security tools and user directories.
- **Application Development Teams**: Charged with securing applications and promptly addressing any exposed identities flagged by Tenable.
- **Identity and Access Management** (IAM) Team: Manages user accounts, permissions, and access controls, collaborating closely with IT security counterparts to address issues pinpointed by Tenable Identity Exposure.
- **Business Unit Leaders**: Hold ultimate responsibility for the security posture of their teams and applications. They review reports, prioritize risk mitigation strategies, and allocate resources to enhance Active Directory security measures.

Dashboards

Dashboards allow you to visualize data and trends affecting the security of your Active Directory. You can customize them with widgets to display charts and counters according to your requirements.

The Tenable Identity Exposure dashboard acts as a real-time command center for your organization's Active Directory (AD) security. It provides a comprehensive overview (e.g. a real-time, centralized view) of your identity landscape, highlighting critical vulnerabilities, pinpointing potential attack vectors, and enabling proactive risk mitigation.



Key Dashboard Features

- **At-a-glance overview**: Get a rapid pulse check on your security state, with key metrics like compliance score, top risks, and user activity trends displayed prominently.
- **Drilling down into details**: Dive deeper into specific areas with interactive widgets that break down risk factors by severity, user category, and other relevant criteria.
- **Customizable focus**: Build personalized dashboards tailored to your priorities, using pre-built templates or crafting your own layouts. For example, for creating a dashboard for popular misconfiguration against common recurring IoEs:

    - Ensure SDProp Consistency
    - Domain Controllers Managed by Illegitimate Users
    - Dangerous Kerberos Delegation
- **Real-time monitoring**: Stay informed of emerging threats and suspicious activity with continuous updates and alerts.
- **Actionable insights**: Gain practical recommendations for remediation, prioritized based on severity and potential impact.

See also

- Dashboards
- Video tutorial on dashboards

Trail Flow

Tenable Identity Exposure's Trail Flow shows the real-time monitoring and analysis of events affecting your AD infrastructure. It allows you to identify critical vulnerabilities and their recommended courses of remediation.

Using the **Trail Flow** page, you can go back in time and load previous events or search for specific events. You can also use its search box at the top of the page to search for threats and detect malicious patterns.

The Trail Flow tracks the following events:

- **User and group changes**: Includes the creation, deletion, and modification of accounts and groups.
- **Permission alterations**: Encompasses modifications to access controls on objects such as files, folders, and printers.
- **System configuration adjustments**: Involves changes to Group Policy Objects (GPOs) and other critical settings.
- **Suspicious activities**: Encompasses unauthorized attempts, privilege escalations, and other events that raise red flags.

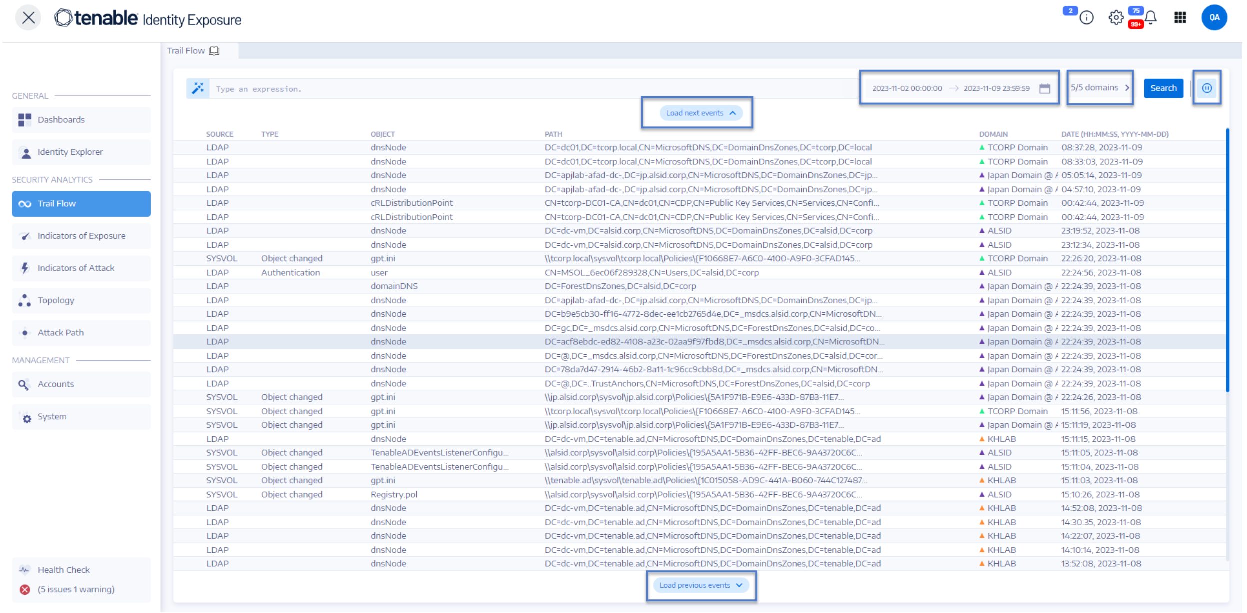
Tenable Identity Exposure offers these capabilities to leverage the Trail Flow data:

- **Searchable and filterable**: Easy navigation through the event stream by using keywords or specific criteria, enabling focused attention on pertinent activities while minimizing extraneous noise.
- **Detailed event information**: Each event entry furnishes exhaustive details, encompassing the affected object, the user responsible for the change, the protocol utilized, and associated Indicators of Exposure (IoEs).
- **Visualized relationships**: The ability to illustrate the relationships between events, illuminating how seemingly unrelated activities may contribute to a broader attack campaign.

To access the Trail Flow:

- In Tenable Identity Exposure, click **Trail Flow** in the navigation bar on the left.

  The Trail Flow page opens with a list of events. For more information, see Trail Flow Table.



SOURCE	TYPE	OBJECT	PATH	DOMAIN	DATE (HH:MM:SS, YYYY-MM-DD)
LDAP		dnsNode	DC=dc01,DC=tcorp.local,CN=MicrosoftDNS,DC=DomainDnsZones,DC=tcorp,DC=local	▲ TCORP Domain	08:37:28, 2023-11-09
LDAP		dnsNode	DC=dc01,DC=tcorp.local,CN=MicrosoftDNS,DC=DomainDnsZones,DC=tcorp,DC=local	▲ TCORP Domain	08:33:03, 2023-11-09
LDAP		dnsNode	DC=apjlab-afad-dc-,DC=jp.alsid.corp,CN=MicrosoftDNS,DC=DomainDnsZones,DC=jp...	▲ Japan Domain @ /	05:05:14, 2023-11-09
LDAP		dnsNode	DC=apjlab-afad-dc-,DC=jp.alsid.corp,CN=MicrosoftDNS,DC=DomainDnsZones,DC=jp...	▲ Japan Domain @ /	04:57:10, 2023-11-09
LDAP		cRLDistributionPoint	CN=tcorp-DC01-CA,CN=dc01,CN=CDP,CN=Public Key Services,CN=Services,CN=Confi...	▲ TCORP Domain	00:42:44, 2023-11-09
LDAP		cRLDistributionPoint	CN=tcorp-DC01-CA,CN=dc01,CN=CDP,CN=Public Key Services,CN=Services,CN=Confi...	▲ TCORP Domain	00:42:44, 2023-11-09
LDAP		dnsNode	DC=dc-vm,DC=alsid.corp,CN=MicrosoftDNS,DC=DomainDnsZones,DC=alsid,DC=corp	▲ ALSID	23:19:52, 2023-11-08
LDAP		dnsNode	DC=dc-vm,DC=alsid.corp,CN=MicrosoftDNS,DC=DomainDnsZones,DC=alsid,DC=corp	▲ ALSID	23:12:34, 2023-11-08
SYSVOL	Object changed	gpt.ini	\\tcorp.local\sysvol\tcorp.local\Policies\{F10668E7-A6C0-4100-A9F0-3CFAD145...	▲ TCORP Domain	22:26:20, 2023-11-08
LDAP	Authentication	user	CN=MSOL_6ec06f289328,CN=Users,DC=alsid,DC=corp	▲ ALSID	22:24:56, 2023-11-08
LDAP		domainDNS	DC=ForestDnsZones,DC=alsid,DC=corp	▲ Japan Domain @ /	22:24:39, 2023-11-08
LDAP		dnsNode	DC=apjlab-afad-dc-,DC=jp.alsid.corp,CN=MicrosoftDNS,DC=DomainDnsZones,DC=jp...	▲ Japan Domain @ /	22:24:39, 2023-11-08
LDAP		dnsNode	DC=b9e5cb30-ff16-4772-8dec-ee1cb2765d4e,DC=_msdcs.alsid.corp,CN=MicrosoftDN...	▲ Japan Domain @ /	22:24:39, 2023-11-08
LDAP		dnsNode	DC=gc,DC=_msdcs.alsid.corp,CN=MicrosoftDNS,DC=ForestDnsZones,DC=alsid,DC=co...	▲ Japan Domain @ /	22:24:39, 2023-11-08
LDAP		dnsNode	DC=acf8ebdc-ed82-4108-a23c-02aa9f97fbd8,DC=_msdcs.alsid.corp,CN=MicrosoftDN...	▲ Japan Domain @ /	22:24:39, 2023-11-08
LDAP		dnsNode	DC=@,DC=_msdcs.alsid.corp,CN=MicrosoftDNS,DC=ForestDnsZones,DC=alsid,DC=cor...	▲ Japan Domain @ /	22:24:39, 2023-11-08
LDAP		dnsNode	DC=78da7d47-2914-46b2-8a11-1c96cc9cbb8d,DC=_msdcs.alsid.corp,CN=MicrosoftDN...	▲ Japan Domain @ /	22:24:39, 2023-11-08
LDAP		dnsNode	DC=@,DC=..TrustAnchors,CN=MicrosoftDNS,DC=ForestDnsZones,DC=alsid,DC=corp	▲ Japan Domain @ /	22:24:39, 2023-11-08
SYSVOL	Object changed	gpt.ini	\\jp.alsid.corp\sysvol\jp.alsid.corp\Policies\{5A1F971B-E9E6-433D-87B3-11E7...	▲ Japan Domain @ /	22:24:26, 2023-11-08
SYSVOL	Object changed	gpt.ini	\\tcorp.local\sysvol\tcorp.local\Policies\{F10668E7-A6C0-4100-A9F0-3CFAD145...	▲ TCORP Domain	15:11:56, 2023-11-08
SYSVOL	Object changed	gpt.ini	\\jp.alsid.corp\sysvol\jp.alsid.corp\Policies\{5A1F971B-E9E6-433D-87B3-11E7...	▲ Japan Domain @ /	15:11:19, 2023-11-08
LDAP		dnsNode	DC=dc-vm,DC=tenable.ad,CN=MicrosoftDNS,DC=DomainDnsZones,DC=tenable,DC=ad	▲ KHLAB	15:11:15, 2023-11-08
SYSVOL	Object changed	TenableADEventsListenerConfigu...	\\alsid.corp\sysvol\alsid.corp\Policies\{195A5AA1-5B36-42FF-BEC6-9A43720C6C...	▲ ALSID	15:11:05, 2023-11-08
SYSVOL	Object changed	TenableADEventsListenerConfigu...	\\alsid.corp\sysvol\alsid.corp\Policies\{195A5AA1-5B36-42FF-BEC6-9A43720C6C...	▲ ALSID	15:11:04, 2023-11-08
SYSVOL	Object changed	gpt.ini	\\tenable.ad\sysvol\tenable.ad\Policies\{1C015058-AD9C-441A-B060-744C127487...	▲ KHLAB	15:11:03, 2023-11-08
SYSVOL	Object changed	Registry.pol	\\alsid.corp\sysvol\alsid.corp\Policies\{195A5AA1-5B36-42FF-BEC6-9A43720C6C...	▲ ALSID	15:10:26, 2023-11-08
LDAP		dnsNode	DC=dc-vm,DC=tenable.ad,CN=MicrosoftDNS,DC=DomainDnsZones,DC=tenable,DC=ad	▲ KHLAB	14:52:08, 2023-11-08
LDAP		dnsNode	DC=dc-vm,DC=tenable.ad,CN=MicrosoftDNS,DC=DomainDnsZones,DC=tenable,DC=ad	▲ KHLAB	14:30:35, 2023-11-08
LDAP		dnsNode	DC=dc-vm,DC=tenable.ad,CN=MicrosoftDNS,DC=DomainDnsZones,DC=tenable,DC=ad	▲ KHLAB	14:22:07, 2023-11-08
LDAP		dnsNode	DC=dc-vm,DC=tenable.ad,CN=MicrosoftDNS,DC=DomainDnsZones,DC=tenable,DC=ad	▲ KHLAB	14:10:14, 2023-11-08
LDAP		dnsNode	DC=dc-vm,DC=tenable.ad,CN=MicrosoftDNS,DC=DomainDnsZones,DC=tenable,DC=ad	▲ KHLAB	13:52:08, 2023-11-08

To select a timeframe:

To select a domain:

To view an event:

To pause and restart the Trail Flow:

To load the next or previous events:

How does the data appear in the Trail Flow?

1. When you perform an action within your Active Directory (AD) interface, such as:

   - Creating a new user account
   - Modifying a user's group membership

- Resetting a password
- Disabling an account
- Enabling an account
- Deleting an account
- Moving an object
- Modifying permissions

2. The Active Directory (AD) automatically generates an event log entry, capturing details of the operation, including:
    - Timestamp
    - Administrator performing the action
    - Object(s) affected
    - Specific changes made
3. Tenable Identity Exposure continuously collects and analyzes these event logs and correlates events, identifies patterns, an detects anomalies.
4. The Trail Flow page visualizes the operation's flow and impact:
    - Timeline: Displays a chronological sequence of events, highlighting the recent operation.
    - Object Details: Provides specific information about the affected objects, including their attributes and relationships.
    - Change History: Shows a history of modifications made to the object(s), including the current operation.
    - Risk Insights: Identifies potential risks associated with the operation, such as excessive permissions or membership in sensitive groups.
    - Compliance Information: Indicates any compliance violations related to the operation.

See also

- Trail Flow overview
- Trail Flow Use Cases
- Trail Flow video tutorial

Reporting Center

The **Reporting Center** in Tenable Identity Exposure provides a valuable feature that allows you to export important data as reports to key stakeholders within an organization. The reporting center offers a means to create reports from a predefined list, ensuring an efficient and streamlined process.

It offers the following functions:

- **Granular filtering**: Refine reports using granular filters based on date range, domain, Indicator of Attack (IoA), Indicator of Exposure (IoE), and more, ensuring laser-focused insights.
- **Automated delivery**: Schedule reports for automatic generation and delivery at desired intervals, streamlining security monitoring and reporting processes.
- **Flexible exporting**: Export reports in various formats like CSV for further analysis, sharing using reports access key, or integration with existing reporting workflows.

Administrators can create different types of report for different users with flexible reporting timeframes of up to one quarter. The ability to share critical identity data from Tenable Identity Exposure empowers the organization to mitigate proactively risk and identify potential identity-based attacks.

To download a report, users receive an email with a URL to a page in which they enter a report access key that they received from their administrator. Reports are available for download for 30 days, after which they age out and Tenable Identity Exposure deletes them. Users must download their reports before Tenable Identity Exposure generates a new one for the specified timeframe and overwrites the previous one.

To access the reporting center:

1. In Tenable Identity Exposure, select **Systems** > **Configuration**.
2. Under **Reporting**, click **Reporting Center**.

   A pane opens with a list of configured reports and their associated information, such as report name, type, domain, profile, period, recurrence, and recipient emails.

See also

- Reporting Center
- Set Permissions for a Role

Indicators of Exposure

Tenable Identity Exposure measures the security maturity of your AD infrastructures through Indicators of Exposure (IoEs) and assigns severity levels to the flow of events that it monitors and analyzes. Tenable Identity Exposure triggers alerts when it detects security regressions.

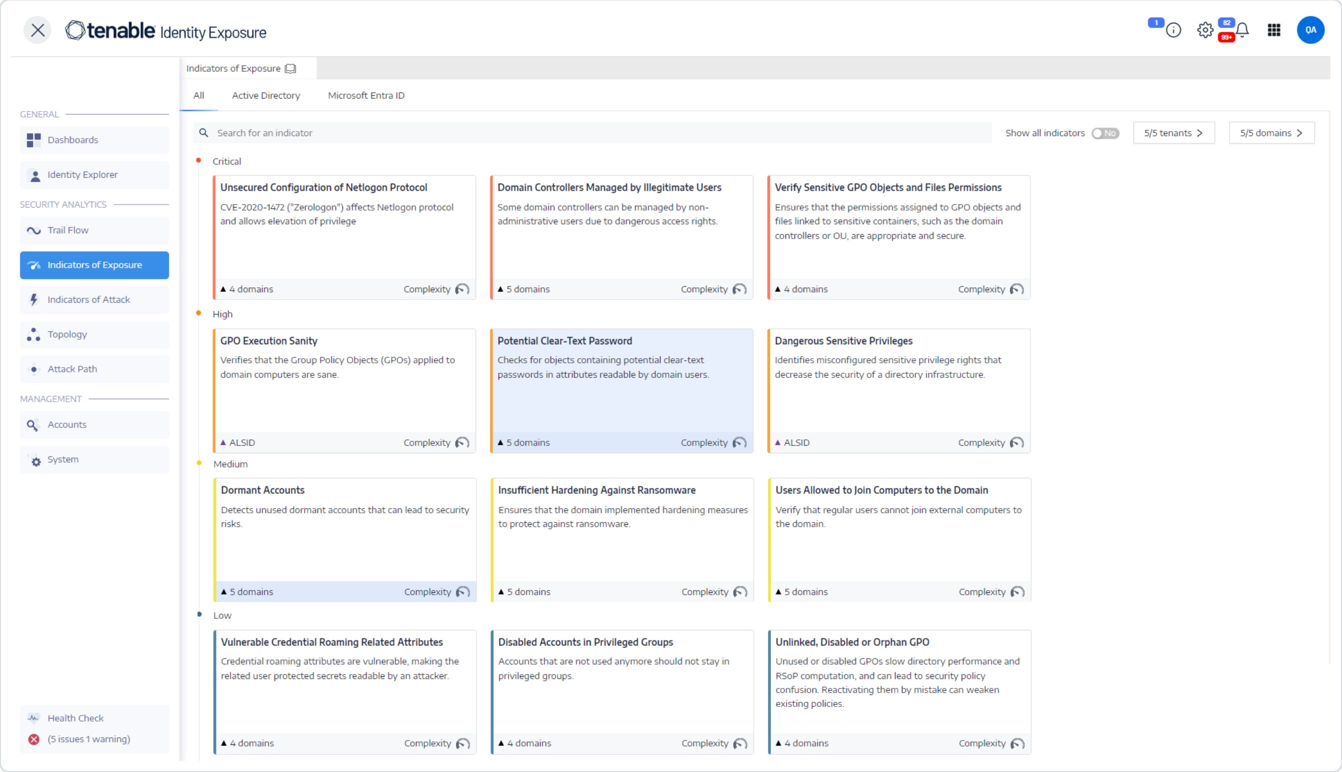
These IoEs are pre-configured, and any deviations from the established norms trigger corresponding alerts.

To display IoEs:

1. In Tenable Identity Exposure, click **Indicators of Exposure** in the navigation pane.

   The **Indicators of Exposure** pane opens. By default, Tenable Identity Exposure shows only the IoEs that contain deviances.

2. (Optional) To show all IoEs, click the **Show all indicators** toggle to **Yes**.



Critical

Unsecured Configuration of Netlogon Protocol
CVE-2020-1472 ("Zerologon") affects Netlogon protocol and allows elevation of privilege
▲ 4 domains — Complexity

Domain Controllers Managed by Illegitimate Users
Some domain controllers can be managed by non-administrative users due to dangerous access rights.
▲ 5 domains — Complexity

Verify Sensitive GPO Objects and Files Permissions
Ensures that the permissions assigned to GPO objects and files linked to sensitive containers, such as the domain controllers or OU, are appropriate and secure.
▲ 4 domains — Complexity

High

GPO Execution Sanity
Verifies that the Group Policy Objects (GPOs) applied to domain computers are sane.
▲ ALSID — Complexity

Potential Clear-Text Password
Checks for objects containing potential clear-text passwords in attributes readable by domain users.
▲ 5 domains — Complexity

Dangerous Sensitive Privileges
Identifies misconfigured sensitive privilege rights that decrease the security of a directory infrastructure.
▲ ALSID — Complexity

Medium

Dormant Accounts
Detects unused dormant accounts that can lead to security risks.
▲ 5 domains — Complexity

Insufficient Hardening Against Ransomware
Ensures that the domain implemented hardening measures to protect against ransomware.
▲ 5 domains — Complexity

Users Allowed to Join Computers to the Domain
Verify that regular users cannot join external computers to the domain.
▲ 5 domains — Complexity

Low

Vulnerable Credential Roaming Related Attributes
Credential roaming attributes are vulnerable, making the related user protected secrets readable by an attacker.
▲ 4 domains — Complexity

Disabled Accounts in Privileged Groups
Accounts that are not used anymore should not stay in privileged groups.
▲ 4 domains — Complexity

Unlinked, Disabled or Orphan GPO
Unused or disabled GPOs slow directory performance and RSoP computation, and can lead to security policy confusion. Reactivating them by mistake can weaken existing policies.
▲ 4 domains — Complexity

Tenable Identity Exposure IoEs come with a range of features designed to boost your investigative capabilities :

- **Searchable and filterable**: Effortlessly explore the IoE by applying filters based on forest and domain.
- **Export capability**: Deviance object will allow you to export the IoE's in CSV format.
- **Action on IoE incidents**: Remove an exposure from the whitelist/re-enable it.

The data from IoEs include:

- **Information section**: This section provides executive summary about each Indicator of Exposure (IoE), including known attack tools, affected domains, and relevant documentation.
- **Vulnerability details**:This section provides more in depth information above the misconfiguration in Active Directory.
- **Deviant objects**: This section highlights misconfigurations in Active Directory that may contribute to broader attack surfaces.
- **Recommendation**: This section guides you through effective configuration strategies to minimize your attack surface.

Level of Severity

Severity levels allow you to assess the severity of the detected vulnerabilities and to prioritize remediation actions.

The **Indicators of Exposure** pane shows IoEs as follows:

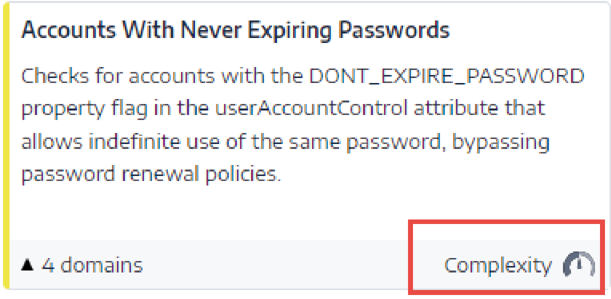
- By severity level using color codes.
- Vertically — from most severe to least severe(red for top priority and blue for least priority).
- Horizontally — from most complex to least complex. Tenable Identity Exposure computes the complexity indicator dynamically to indicate the level of difficulty to remediate the deviant IoE.

Severity	Description
Critical — Red	Shows how to prevent attacks and compromise of the Active Directory by certain unprivileged users.
High — Orange	Deals with either post-exploitation techniques leading to credential theft or

	security bypass or with exploitation techniques that require chaining to be dangerous.
Medium — Yellow	Indicates a limited risk for the Active Directory infrastructure.
Low — Blue	Shows good security practices. Certain business contexts may allow low-impact deviances that do not necessarily affect AD security. These deviances have an impact on the AD only if an administrator makes an error such as by activating an inactive account.

Prioritization of Remediation

You prioritize remediation efforts on high-severity IoEs identified by the system. Additionally, you can further prioritize within the critical category using the risk meter within the IoE.



Accounts With Never Expiring Passwords

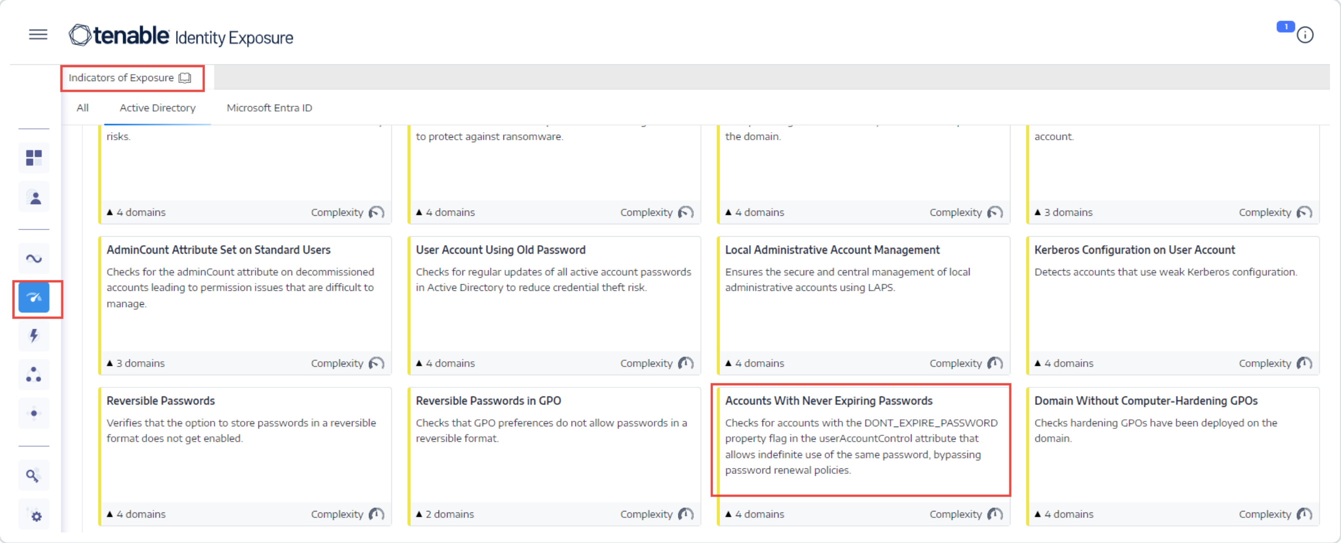
Checks for accounts with the DONT_EXPIRE_PASSWORD property flag in the userAccountControl attribute that allows indefinite use of the same password, bypassing password renewal policies.

If you believe that the IoE falls within your organization's purview or operational mandate, you can allowlist it.

Use Case

The following use case focuses on the IoE called "Accounts with Never Expiring Passwords".

1. When Tenable Identity Exposure flags an IoE, it appears in the Indicators of Exposure pane:



risks.

▲ 4 domains Complexity

to protect against ransomware.

▲ 4 domains Complexity

the domain.

▲ 4 domains Complexity

account.

▲ 3 domains Complexity

AdminCount Attribute Set on Standard Users

Checks for the adminCount attribute on decommissioned accounts leading to permission issues that are difficult to manage.

▲ 3 domains Complexity

User Account Using Old Password

Checks for regular updates of all active account passwords in Active Directory to reduce credential theft risk.

▲ 4 domains Complexity

Local Administrative Account Management

Ensures the secure and central management of local administrative accounts using LAPS.

▲ 4 domains Complexity

Kerberos Configuration on User Account

Detects accounts that use weak Kerberos configuration.

▲ 4 domains Complexity

Reversible Passwords

Verifies that the option to store passwords in a reversible format does not get enabled.

▲ 4 domains Complexity

Reversible Passwords in GPO

Checks that GPO preferences do not allow passwords in a reversible format.

▲ 2 domains Complexity

Accounts With Never Expiring Passwords

Checks for accounts with the DONT_EXPIRE_PASSWORD property flag in the userAccountControl attribute that allows indefinite use of the same password, bypassing password renewal policies.

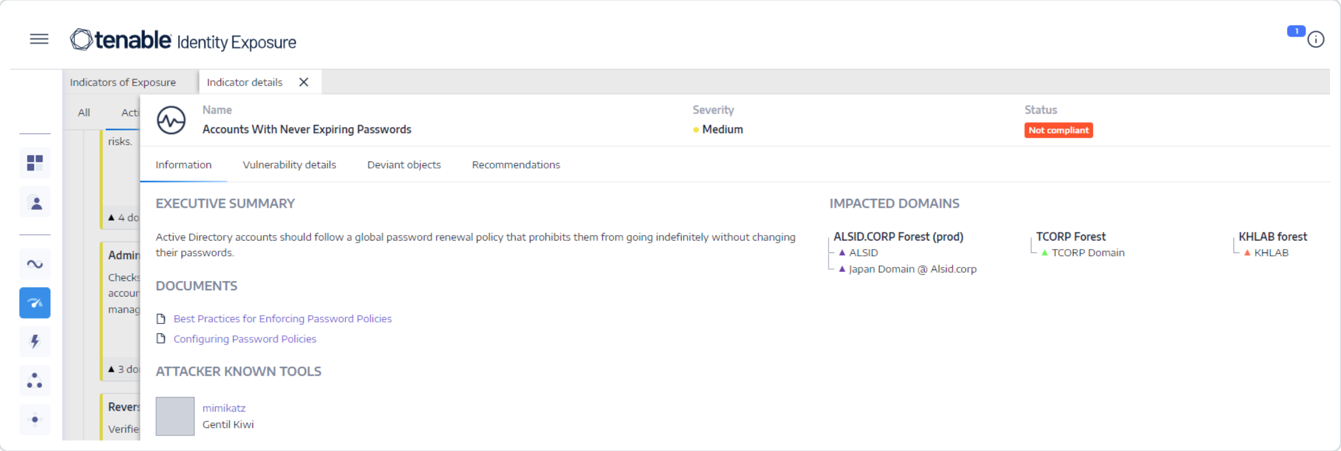
▲ 4 domains Complexity

Domain Without Computer-Hardening GPOs

Checks hardening GPOs have been deployed on the domain.

▲ 4 domains Complexity

2. To get more insights about the IoE, click on the IoE to access additional details. Within the information page, you'll discover an executive summary providing a concise overview, details regarding potential attack tools associated with the IoE, affected domains, and relevant documentation to help you understand and address the issue effectively.



Name: Accounts With Never Expiring Passwords

Severity: Medium

Status: Not compliant

EXECUTIVE SUMMARY

Active Directory accounts should follow a global password renewal policy that prohibits them from going indefinitely without changing their passwords.

DOCUMENTS

- Best Practices for Enforcing Password Policies
- Configuring Password Policies

ATTACKER KNOWN TOOLS

mimikatz
Gentil Kiwi

IMPACTED DOMAINS

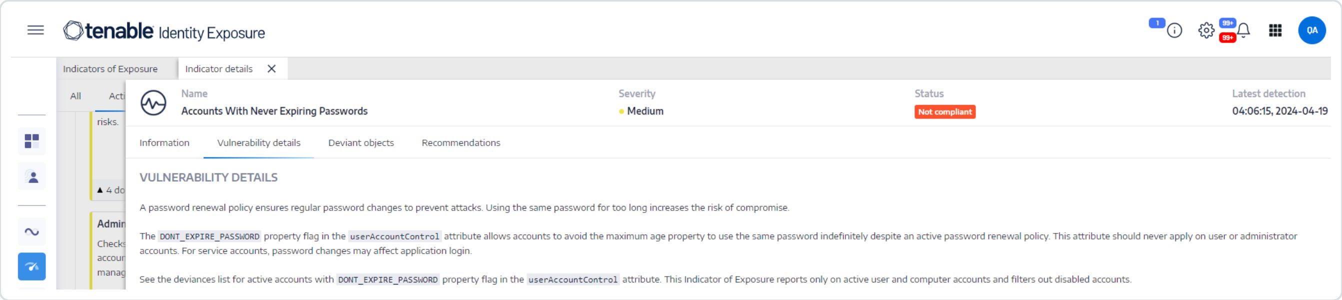
ALSID.CORP Forest (prod)
- ▲ ALSID
- ▲ Japan Domain @ Alsid.corp

TCORP Forest
- ▲ TCORP Domain

KHLAB forest
- ▲ KHLAB

3.

4. For more details about the IoE, click on the “Vulnerability details” tab.



tenable Identity Exposure

Indicators of Exposure | Indicator details

Name: Accounts With Never Expiring Passwords
Severity: Medium
Status: Not compliant
Latest detection: 04:06:15, 2024-04-19

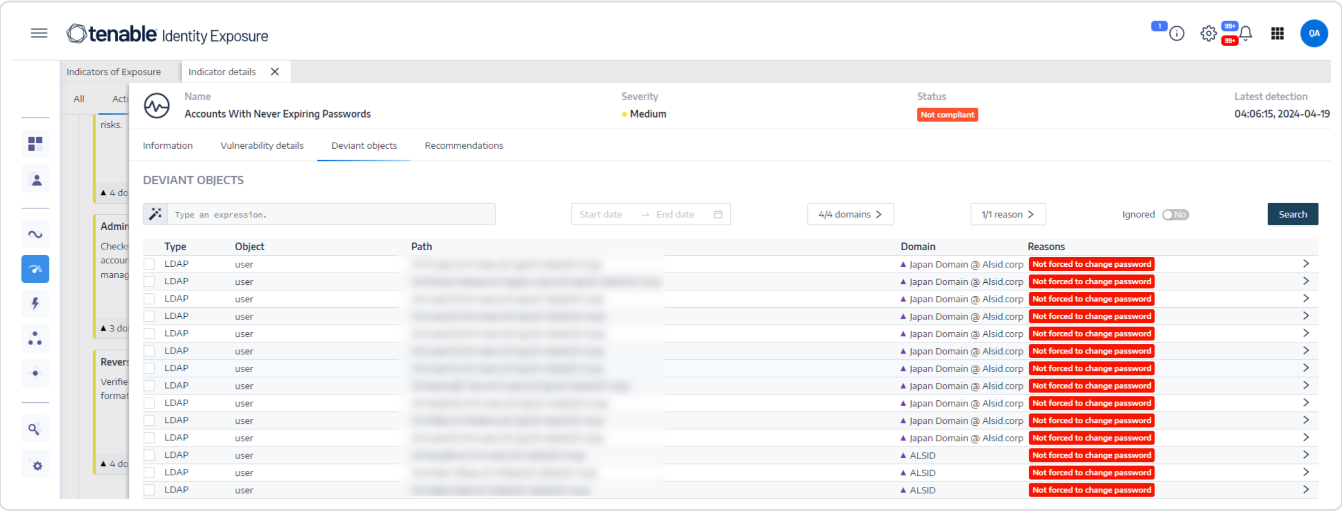
VULNERABILITY DETAILS

A password renewal policy ensures regular password changes to prevent attacks. Using the same password for too long increases the risk of compromise.

The `DONT_EXPIRE_PASSWORD` property flag in the `userAccountControl` attribute allows accounts to avoid the maximum age property to use the same password indefinitely despite an active password renewal policy. This attribute should never apply on user or administrator accounts. For service accounts, password changes may affect application login.

See the deviances list for active accounts with `DONT_EXPIRE_PASSWORD` property flag in the `userAccountControl` attribute. This Indicator of Exposure reports only on active user and computer accounts and filters out disabled accounts.

5. To verify which accounts have the "Account with never expiring password" setting enabled, click on the "Deviant objects." This action will allow you to access a list of accounts that possess this configuration within your system.



tenable Identity Exposure

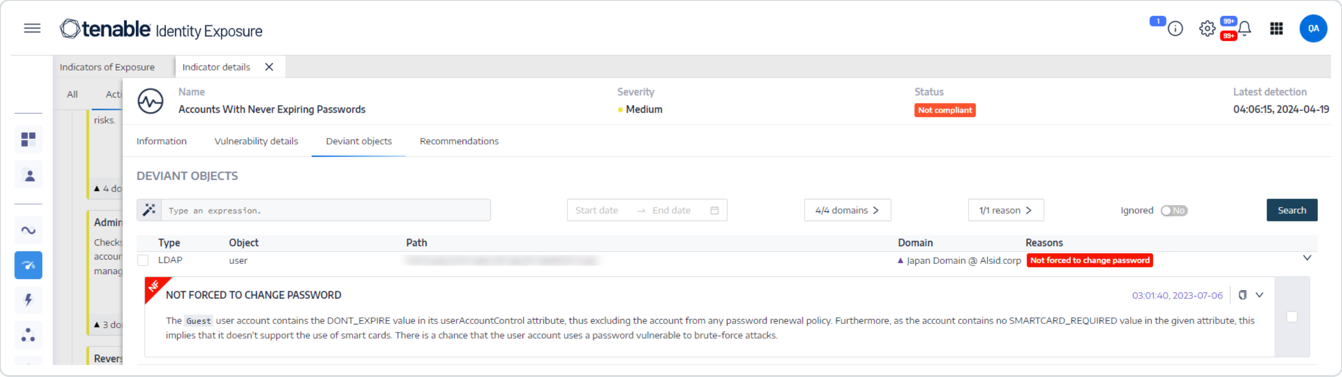
Indicators of Exposure | Indicator details

Name: Accounts With Never Expiring Passwords
Severity: Medium
Status: Not compliant
Latest detection: 04:06:15, 2024-04-19

DEVIANT OBJECTS

Type	Object	Path	Domain	Reasons
LDAP	user	[redacted]	Japan Domain @ Alsid.corp	Not forced to change password
LDAP	user	[redacted]	Japan Domain @ Alsid.corp	Not forced to change password
LDAP	user	[redacted]	Japan Domain @ Alsid.corp	Not forced to change password
LDAP	user	[redacted]	Japan Domain @ Alsid.corp	Not forced to change password
LDAP	user	[redacted]	Japan Domain @ Alsid.corp	Not forced to change password
LDAP	user	[redacted]	Japan Domain @ Alsid.corp	Not forced to change password
LDAP	user	[redacted]	Japan Domain @ Alsid.corp	Not forced to change password
LDAP	user	[redacted]	Japan Domain @ Alsid.corp	Not forced to change password
LDAP	user	[redacted]	Japan Domain @ Alsid.corp	Not forced to change password
LDAP	user	[redacted]	Japan Domain @ Alsid.corp	Not forced to change password
LDAP	user	[redacted]	Japan Domain @ Alsid.corp	Not forced to change password
LDAP	user	[redacted]	ALSID	Not forced to change password
LDAP	user	[redacted]	ALSID	Not forced to change password
LDAP	user	[redacted]	ALSID	Not forced to change password

6. Click on the deviant object to see the accounts that the IoE flagged.



tenable Identity Exposure

Indicators of Exposure | Indicator details

Name: Accounts With Never Expiring Passwords
Severity: Medium
Status: Not compliant
Latest detection: 04:06:15, 2024-04-19

DEVIANT OBJECTS

Type	Object	Path	Domain	Reasons
LDAP	user	[redacted]	Japan Domain @ Alsid.corp	Not forced to change password

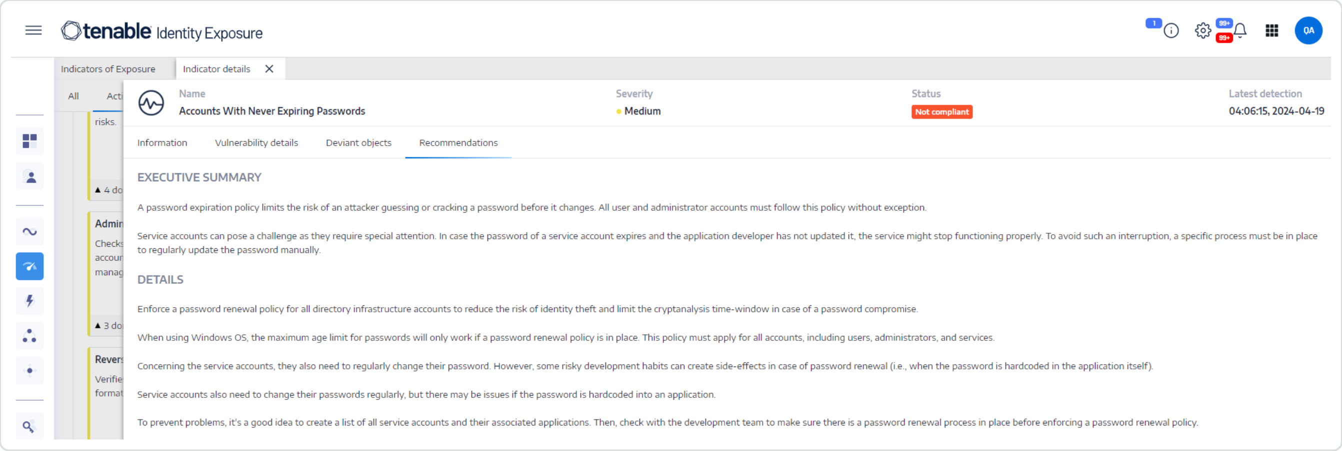
NOT FORCED TO CHANGE PASSWORD — 03:01:40, 2023-07-06

The `Guest` user account contains the DONT_EXPIRE value in its userAccountControl attribute, thus excluding the account from any password renewal policy. Furthermore, as the account contains no SMARTCARD_REQUIRED value in the given attribute, this implies that it doesn't support the use of smart cards. There is a chance that the user account uses a password vulnerable to brute-force attacks.

7. Consult your Active Directory administrator to understand why the affected account has the "Accounts With Never Expiring Passwords" option enabled.

8. Based on the response, you can either choose to whitelist the account or assist your Active Directory administrator in making recommendations to address the issue.

9. For recommendations, you can refer to the recommendation section of the IoE.



Name: Accounts With Never Expiring Passwords

Severity: ● Medium

Status: Not compliant

Latest detection: 04:06:15, 2024-04-19

EXECUTIVE SUMMARY

A password expiration policy limits the risk of an attacker guessing or cracking a password before it changes. All user and administrator accounts must follow this policy without exception.

Service accounts can pose a challenge as they require special attention. In case the password of a service account expires and the application developer has not updated it, the service might stop functioning properly. To avoid such an interruption, a specific process must be in place to regularly update the password manually.

DETAILS

Enforce a password renewal policy for all directory infrastructure accounts to reduce the risk of identity theft and limit the cryptanalysis time-window in case of a password compromise.

When using Windows OS, the maximum age limit for passwords will only work if a password renewal policy is in place. This policy must apply for all accounts, including users, administrators, and services.

Concerning the service accounts, they also need to regularly change their password. However, some risky development habits can create side-effects in case of password renewal (i.e., when the password is hardcoded in the application itself).

Service accounts also need to change their passwords regularly, but there may be issues if the password is hardcoded into an application.

To prevent problems, it's a good idea to create a list of all service accounts and their associated applications. Then, check with the development team to make sure there is a password renewal process in place before enforcing a password renewal policy.

10. If the account has an exception or is known to work as expected, you can ignore the IoE by navigating to **Deviance object** > Select the respective deviance > **Ignore** selected object (or) stop ignoring the selected object based on the requirement.

See also

- Indicators of Exposure
- Indicator of Exposure video tutorial
- Customize an Indicator

Indicators of Attack

Tenable Identity Exposure Indicators of Attack (IoA) help your organization detect and take immediate action when the most advanced exploit techniques try to compromise your Active Directory (AD) infrastructures, including:

- **Top 3 incidents**: A unified presentation of IoAs displays a real-time timeline along with the top three incidents that have affected your AD, as well as the distribution of attacks, all within a single interface.
- **Details on IoA**: Within the Tenable Identity Exposure, the IoA panel provides information on attacks that have taken place within your AD.
- **Incidents Involving IoA**: The list of IoA incidents offers comprehensive details regarding specific attacks targeting your AD. This information empowers you to respond appropriately based on the severity level of the IoA.

The Indicators of Attack feature comes with a range of features designed to boost your investigative capabilities:

- **Searchable and filterable**: Effortlessly explore the IoA by utilizing the timeline, or apply filters based on forest, domain, and criticality level for efficient and targeted results.
- **Export Capability**: Permits the export of IoA data in PDF, CSV, or PPTX formats.
- **Modify Chart Type:** Provides the option to change the chart type, allowing you to display either the distribution of attack severity or the top three attacks along with their respective occurrence counts.
- **Action on IoA incidents**: Allow you to select an incident to close or reopen.

Level of Severity

Tenable Identity Exposure detects and assigns severity levels to attacks:

Level	Description
Critical — Red	Detected a proven post-exploitation attack that requires domain dominance as a prerequisite.

High — Orange	Detected a major attack that allows an attacker to reach domain dominance.
Medium — Yellow	The IoA is related to an attack that could lead to a dangerous escalation of privileges or allow access to sensitive resources.
Low — Blue	Alerts to suspicious behaviors related to reconnaissance actions or low-impact incidents.

Prioritization of Remediation

Recognize critical and high-impact IoAs that align with your specific security risks and concerns.

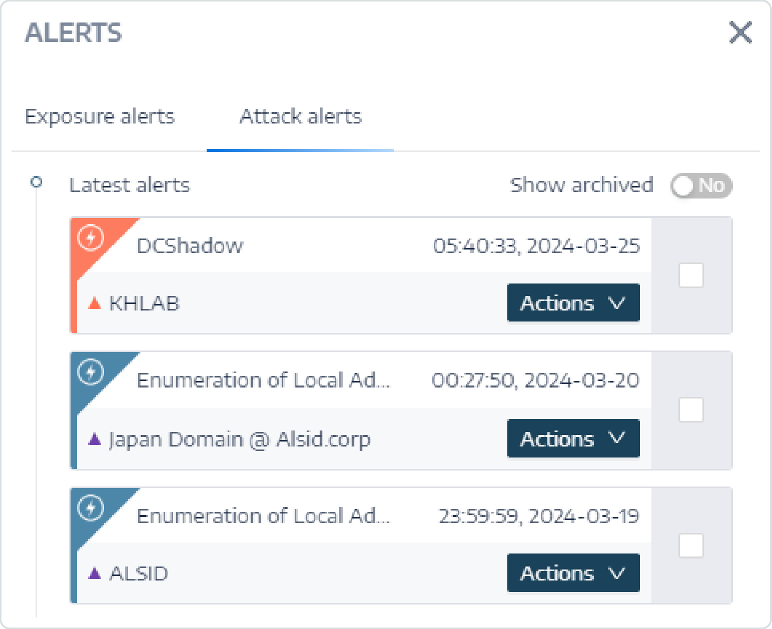
To mitigate the risk of false positives or the oversight of legitimate attacks, it is crucial to calibrate IoAs according to your environment. This entails :

- Adjusting thresholds: Calibrate IoA sensitivity to reduce false positives, ensuring alerts are meaningful and actionable.
- Whitelisting accounts and Activities: Exclude legitimate activities from triggering IoAs, enhancing alert accuracy and streamlining investigations.
- Correlating IoAs: Analyze relationships between different IoAs to identify broader attack patterns.

Tip: Refer to the Tenable Identity Exposure Indicators of Attack Reference Guide (available at https://www.tenable.com/downloads/identity-exposure) for more details on options and recommended values. Apply these options and values to each IoA in the security profile.

Use Case

1. Upon the activation of an IoA, select "Indicators of Attack" from the navigation pane or click on the bell icon located at the top right of the home page.

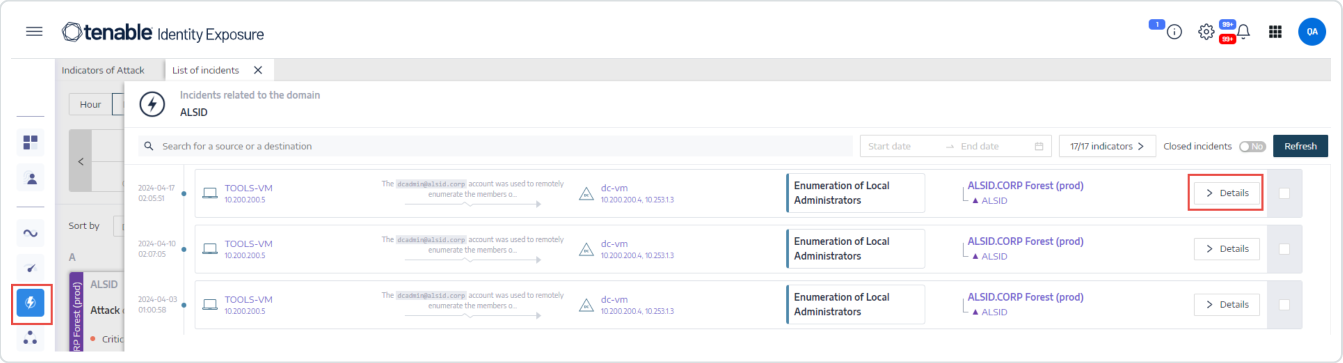


DCShadow 05:40:33, 2024-03-25
KHLAB

Enumeration of Local Ad... 00:27:50, 2024-03-20
Japan Domain @ Alsid.corp

Enumeration of Local Ad... 23:59:59, 2024-03-19
ALSID

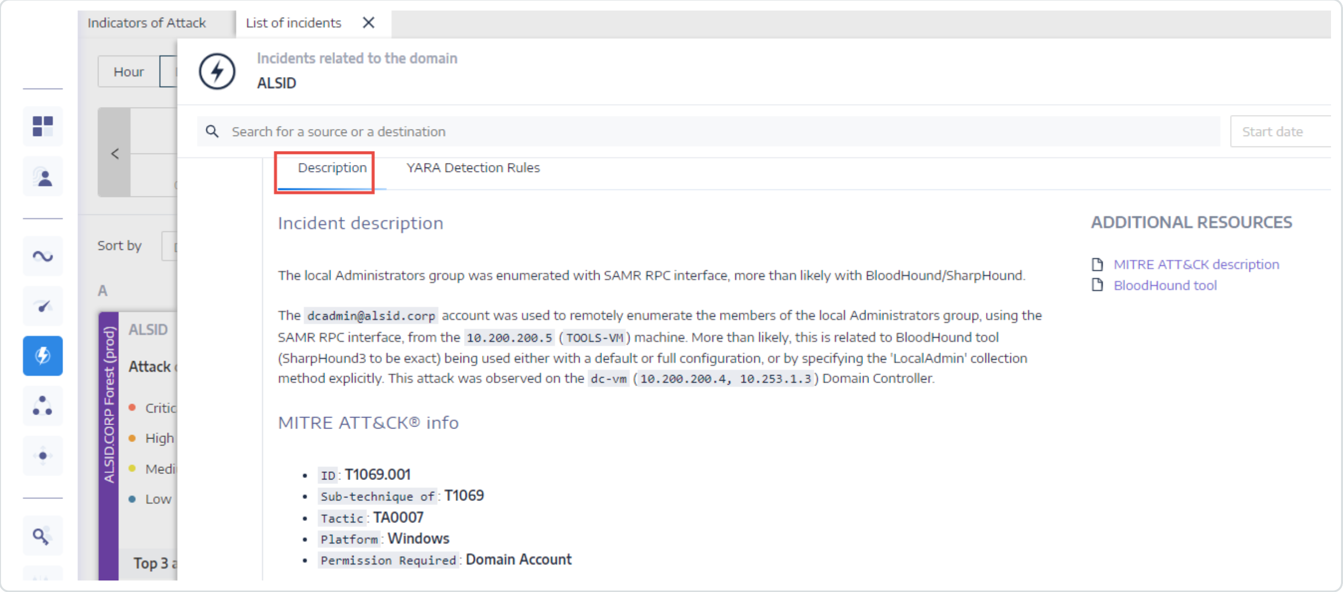
2. Each indicator will give you detailed information about the incident and allow you to take appropriate action after review:
   - When the attack happened
   - Description of the attack
   - Source of the attack
   - Target of the attack
   - MITRE ATT&CK® information
   - YARA detection rules
   - Additional resources
3. Select "Details" to access the Description, as illustrated in this example, focusing on the Enumeration of Local Administrators.



Incidents related to the domain
ALSID

2024-04-17 02:05:51	TOOLS-VM 10.200.200.5	The dcadmin@alsid.corp account was used to remotely enumerate the members o...	dc-vm 10.200.200.4, 10.253.1.3	Enumeration of Local Administrators	ALSID.CORP Forest (prod) ALSID	Details
2024-04-10 02:07:05	TOOLS-VM 10.200.200.5	The dcadmin@alsid.corp account was used to remotely enumerate the members o...	dc-vm 10.200.200.4, 10.253.1.3	Enumeration of Local Administrators	ALSID.CORP Forest (prod) ALSID	Details
2024-04-03 01:00:58	TOOLS-VM 10.200.200.5	The dcadmin@alsid.corp account was used to remotely enumerate the members o...	dc-vm 10.200.200.4, 10.253.1.3	Enumeration of Local Administrators	ALSID.CORP Forest (prod) ALSID	Details

4. The Description tab provides information about specific attacks on your Active Directory (AD).



Incidents related to the domain
ALSID

Incident description

The local Administrators group was enumerated with SAMR RPC interface, more than likely with BloodHound/SharpHound.

The `dcadmin@alsid.corp` account was used to remotely enumerate the members of the local Administrators group, using the SAMR RPC interface, from the `10.200.200.5` (`TOOLS-VM`) machine. More than likely, this is related to BloodHound tool (SharpHound3 to be exact) being used either with a default or full configuration, or by specifying the 'LocalAdmin' collection method explicitly. This attack was observed on the `dc-vm` (`10.200.200.4, 10.253.1.3`) Domain Controller.

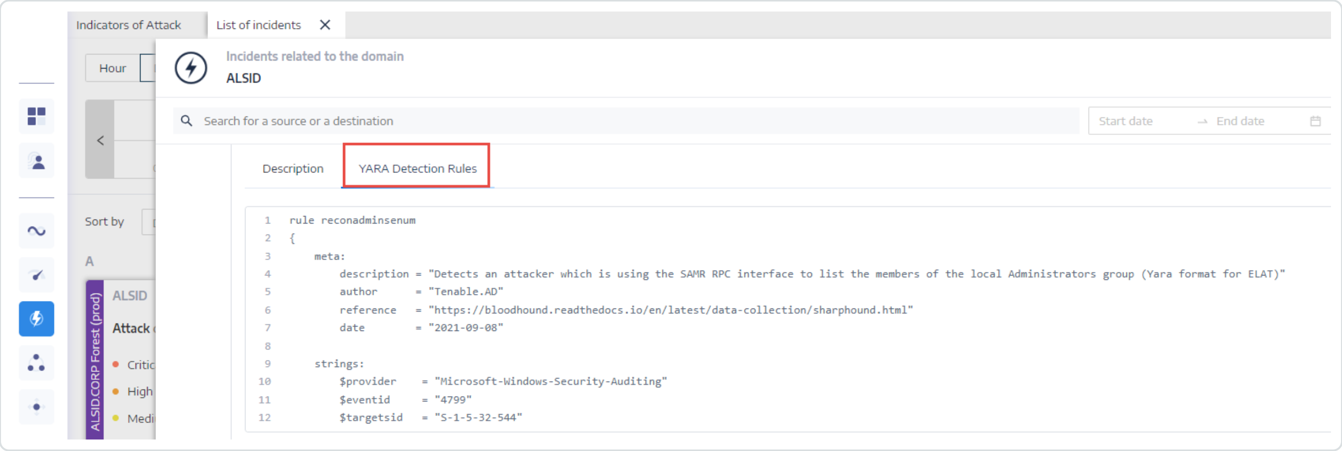
MITRE ATT&CK® info

- `ID`: T1069.001
- `Sub-technique of`: T1069
- `Tactic`: TA0007
- `Platform`: Windows
- `Permission Required`: Domain Account

ADDITIONAL RESOURCES

MITRE ATT&CK description
BloodHound tool

5. The YARA Detection Rules tab provides information on the YARA rules employed by Tenable Identity Exposure for detecting Active Directory attacks at the network level, enhancing the overall detection capabilities of Tenable Identity Exposure.



```
rule reconadminsenum
{
    meta:
        description = "Detects an attacker which is using the SAMR RPC interface to list the members of the local Administrators group (Yara format for ELAT)"
        author      = "Tenable.AD"
        reference   = "https://bloodhound.readthedocs.io/en/latest/data-collection/sharphound.html"
        date        = "2021-09-08"

    strings:
        $provider    = "Microsoft-Windows-Security-Auditing"
        $eventid     = "4799"
        $targetsid   = "S-1-5-32-544"
```

6. Collaborate with the Active Directory Administrator or the relevant stakeholder to examine and resolve the incident, deciding whether to close or reopen it, and implementing measures to prevent its recurrence.

7. If this is a recognized or authorized attack, you have the option to customize the IoA accordingly, to prevent the IoA from flagging it in future instances.

See also

- Indicators of Attack
- Customize an Indicator
- Indicators of Attack video tutorial

Configuring Microsoft Entra ID as an Identity Provider

In addition to Active Directory, Tenable Identity Exposure supports Microsoft Entra ID (formerly Azure AD or AAD) to expand the scope of identities in an organization. This capability leverages new Indicators of Exposure that focus on risks specific to Microsoft Entra ID.

To integrate Microsoft Entra ID with Tenable Identity Exposure, follow closely this on-boarding process:

1. Have the Prerequisites
2. Check the Permissions
3. Check Network Flows
4. Configure Microsoft Entra ID settings
5. Activate Microsoft Entra ID support
6. Enable tenant scans

Prerequisites

You need a Tenable Cloud account to log in to “cloud.tenable.com” and use the Microsoft Entra ID support feature. This Tenable Cloud account is the same email address used for your Welcome Email. If you do not know your email address for “cloud.tenable.com,” please contact Support. All customers with a valid license (On-Premises or SaaS) can access the Tenable Cloud at “cloud.tenable.com”. This account allows you to configure Tenable scans for your Microsoft Entra ID and collect the scan results.

> **Note**: You do not need a valid **Tenable Vulnerability Management** license to access Tenable Cloud. A currently valid standaloneTenable Identity Exposure license (On-Premises or SaaS) is sufficient.

> **Note**: Tenable Identity Exposure **does not support Microsoft Entra ID in the National Clouds**, including the China and US Government dedicated areas. Microsoft Entra ID offers National Clouds, which are physically isolated instances of Azure designed for specific regulatory and compliance needs. Tenable Identity Exposure only supports the global Microsoft Entra ID environment, excluding the China National Cloud and the US Government National Cloud. For more information about Microsoft Entra ID National Clouds, see Microsoft Entra Authentication & National Clouds - Microsoft Identity Platform.

Permissions

The support of Microsoft Entra ID requires the collecting of data from Microsoft Entra ID such as users, groups, applications, service principals, roles, permissions, policies, logs, etc. It collects this data using Microsoft Graph API and service principal credentials following Microsoft recommendations.

- You must sign in to Microsoft Entra ID as **a user with permissions to grant tenant-wide administrator consent** on Microsoft Graph, which must have the Global Administrator or Privileged Role Administrator role (or any custom role with appropriate permissions), according to Microsoft.
- To access the configuration and data visualization for Microsoft Entra ID, your **Tenable Identity Exposure user role** must have the appropriate permissions. For more information, see Set Permissions for a Role.

Network Flows

Allow the following addresses on port 443 outbound from the Security Engine Node server to activate Entra ID support:

- sensor.cloud.tenable.com
- cloud.tenable.com

License Count

Tenable does not count duplicate identities against the license **only when the Tenable Cloud sync feature is enabled**. Without this feature, it cannot match accounts from Microsoft Entra ID and Active Directory, causing it to count each account separately.

- **Without Tenable Cloud sync**: A single user with both an AD account and an Entra ID account count as two separate users against the license.
- **With Tenable Cloud sync enabled**: The system consolidates multiple accounts into a single identity, ensuring that a user with multiple accounts is counted only once.

Configure Microsoft Entra ID settings

Use the following procedures (adapted from the Microsoft Quickstart: Register an application with the Microsoft identity platform documentation) to configure all required settings in Microsoft Entra ID.

1. **Create an application:**

   a. In the Azure Admin portal, open the **App registrations** page.

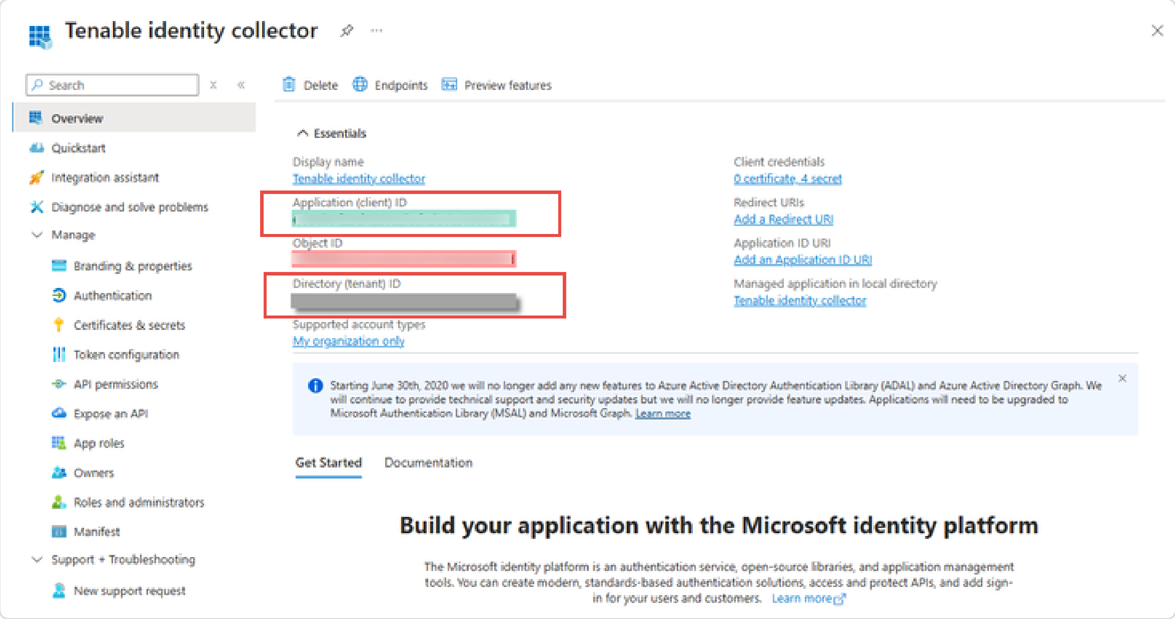
   b. Click **+ New registration**.

   c. Give the application a name (Example: "Tenable Identity Collector"). For the other options, you can leave the default values as they are.

   d. Click **Register**.

   e. On the Overview page for this newly created app, make a note of the "Application (client) ID" and the "Directory (tenant) ID", which you will later need in the step To add a new Microsoft Entra ID tenant:

   > **Caution**: Be sure you select the **Application ID** and **not** the **Object ID** for the configuration to work.



Tenable identity collector

Display name: Tenable identity collector

Application (client) ID: [redacted]

Object ID: [redacted]

Directory (tenant) ID: [redacted]

Supported account types: My organization only

Client credentials: 0 certificate, 4 secret

Redirect URIs: Add a Redirect URI

Application ID URI: Add an Application ID URI

Managed application in local directory: Tenable identity collector

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

Build your application with the Microsoft identity platform

The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create modern, standards-based authentication solutions, access and protect APIs, and add sign-in for your users and customers. Learn more

2. **Add credentials to the application:**

   a. In the Azure Admin portal, open the **App registrations** page.

   b. Click on the application you created.

   c. In the left-hand menu, click **Certificates & secrets**.

d. Click **+ New client secret**.

e. In the **Description** box, give a practical name to this secret and an **Expiry** value compliant with your policies. Remember to renew this secret near its expiry date.

f. Save the secret value in a secure location because Azure only shows this once, and you must recreate it if you lose it.

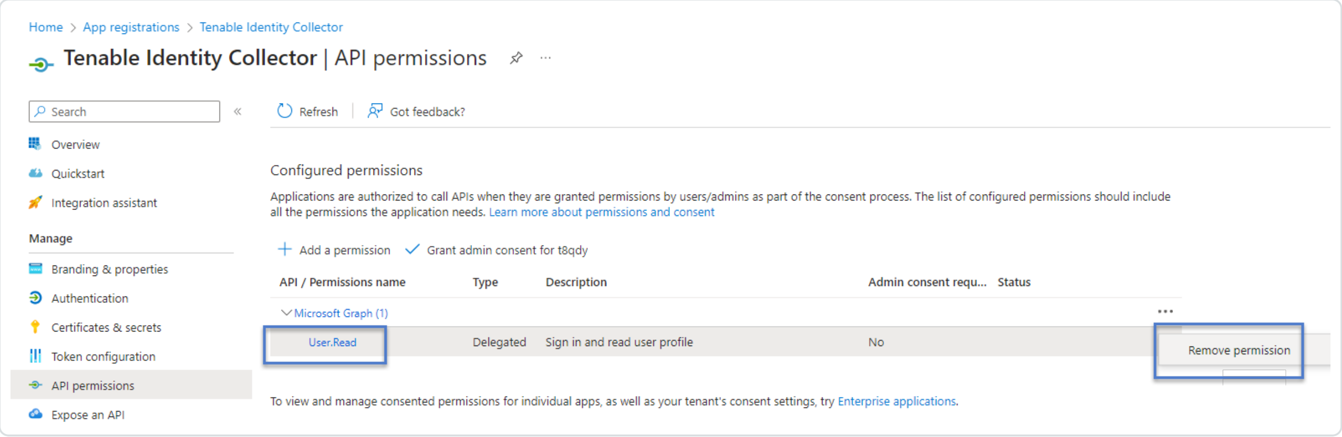
3. **Assign permissions to the application:**

a. In the Azure Admin portal, open the [**App registrations**]() page.

b. Click on the application you created.

c. In the left-hand menu, click **API permissions**.

d. Remove the existing `User.Read` permission:



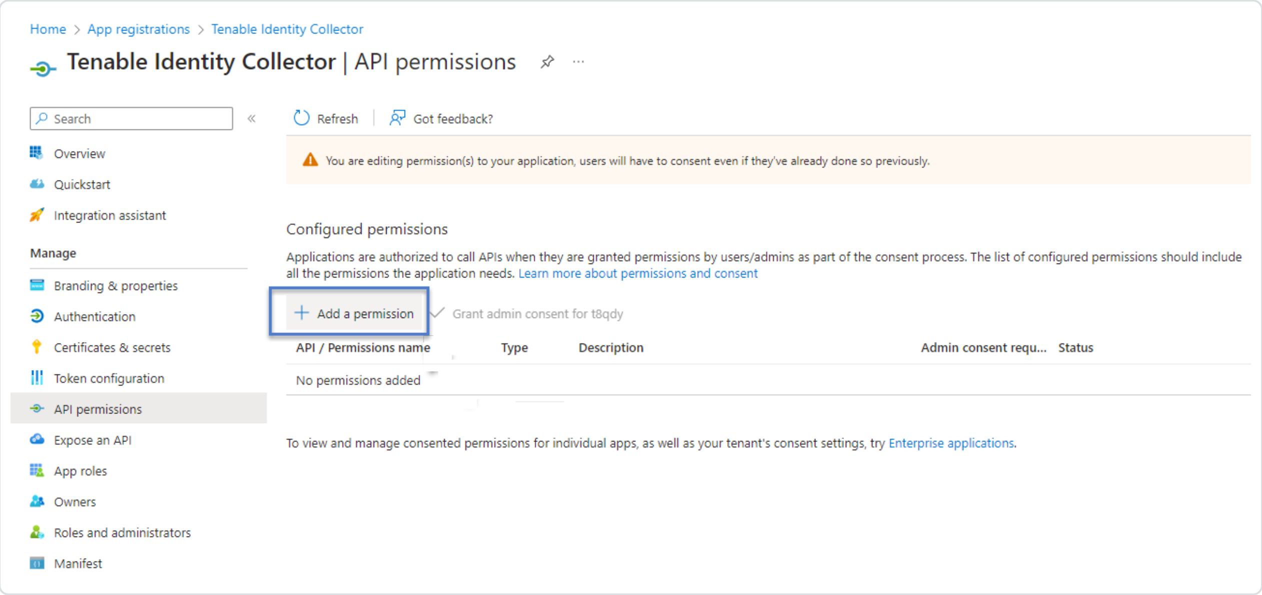
Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

API / Permissions name	Type	Description	Admin consent requ...	Status
∨ Microsoft Graph (1)				
User.Read	Delegated	Sign in and read user profile	No	

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try Enterprise applications.

e. Click **+ Add a permission**:



Tenable Identity Collector | API permissions

⚠ You are editing permission(s) to your application, users will have to consent even if they've already done so previously.

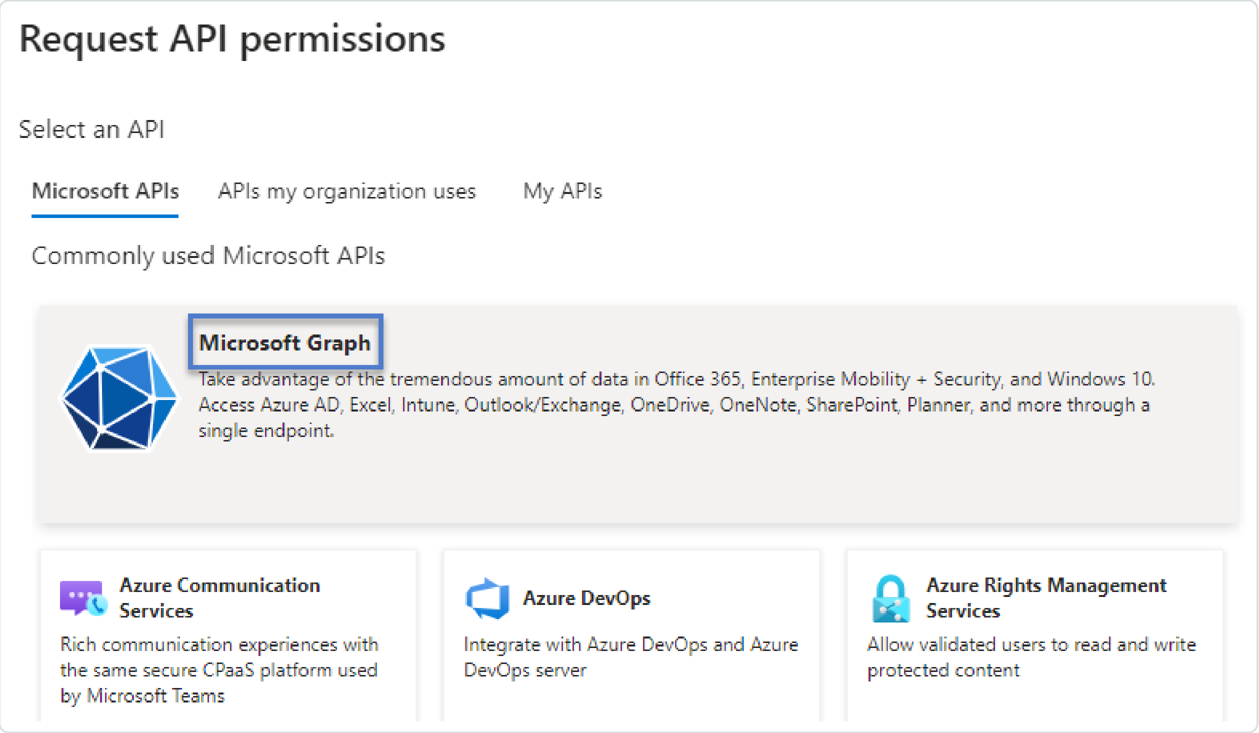
Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

API / Permissions name	Type	Description	Admin consent requ...	Status
No permissions added				

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try Enterprise applications.

f. Select **Microsoft Graph**:



Request API permissions

Select an API

Commonly used Microsoft APIs

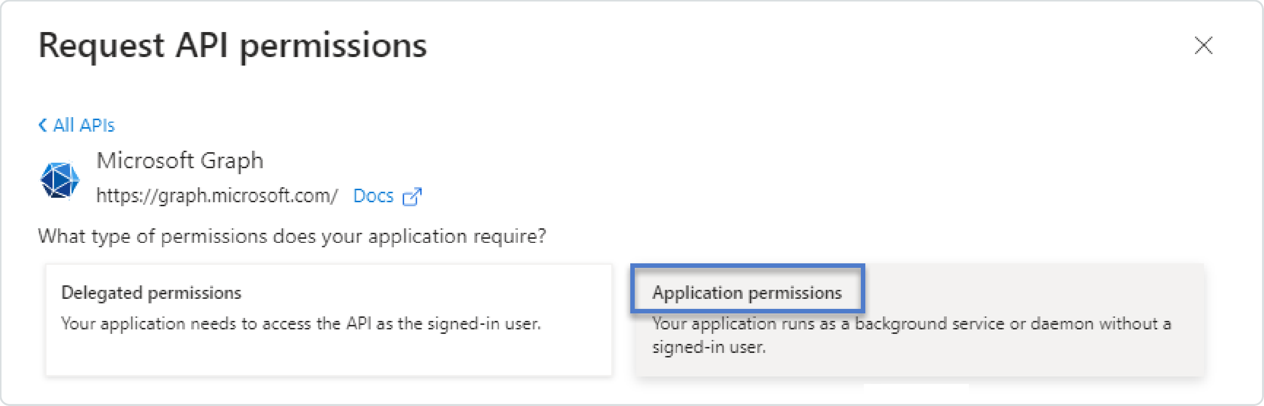
Microsoft Graph
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

Azure Communication Services
Rich communication experiences with the same secure CPaaS platform used by Microsoft Teams

Azure DevOps
Integrate with Azure DevOps and Azure DevOps server

Azure Rights Management Services
Allow validated users to read and write protected content

g. Select **Application permissions** (not "Delegated permissions").



Request API permissions

< All APIs

Microsoft Graph

https://graph.microsoft.com/ Docs

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

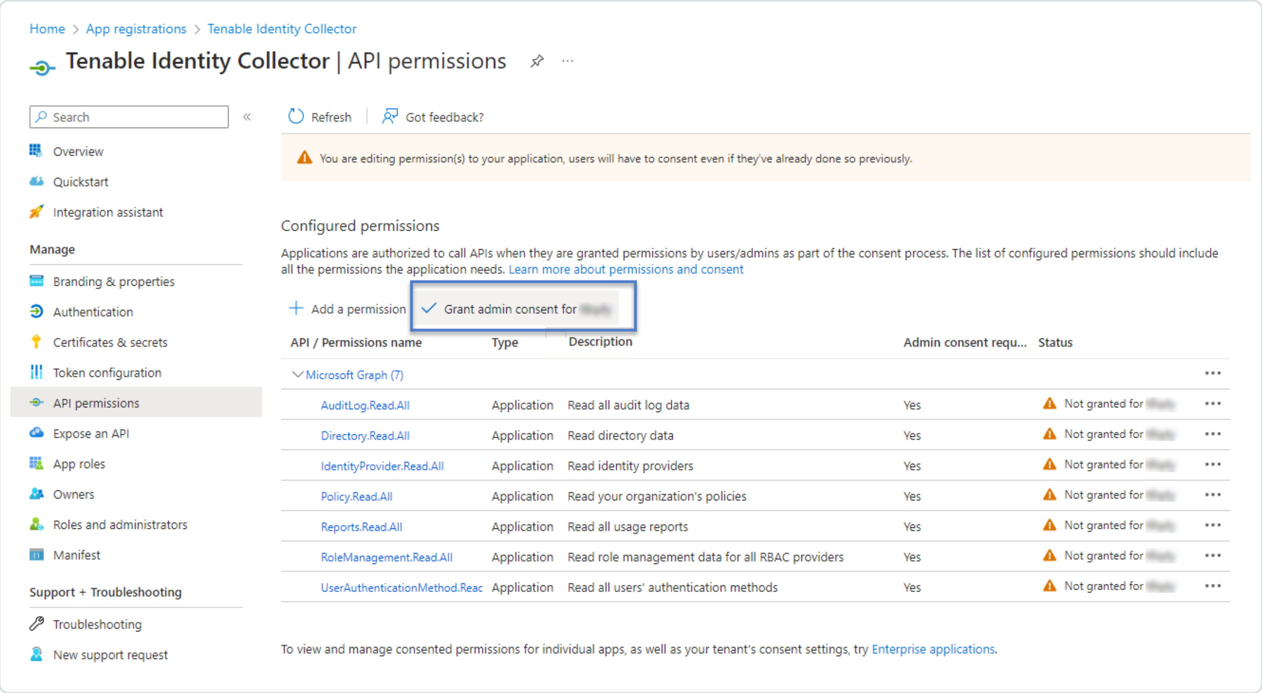
Your application runs as a background service or daemon without a signed-in user.

h. Use the list or the search bar to find and select all the following permissions:

- `AuditLog.Read.All`
- `Directory.Read.All`
- `IdentityProvider.Read.All`
- `Policy.Read.All`
- `Reports.Read.All`
- `RoleManagement.Read.All`
- `UserAuthenticationMethod.Read.All`

i. Click **Add permissions**.

j. Click **Grant admin consent for <tenant name>** and click **Yes** to confirm:



Tenable Identity Collector | API permissions

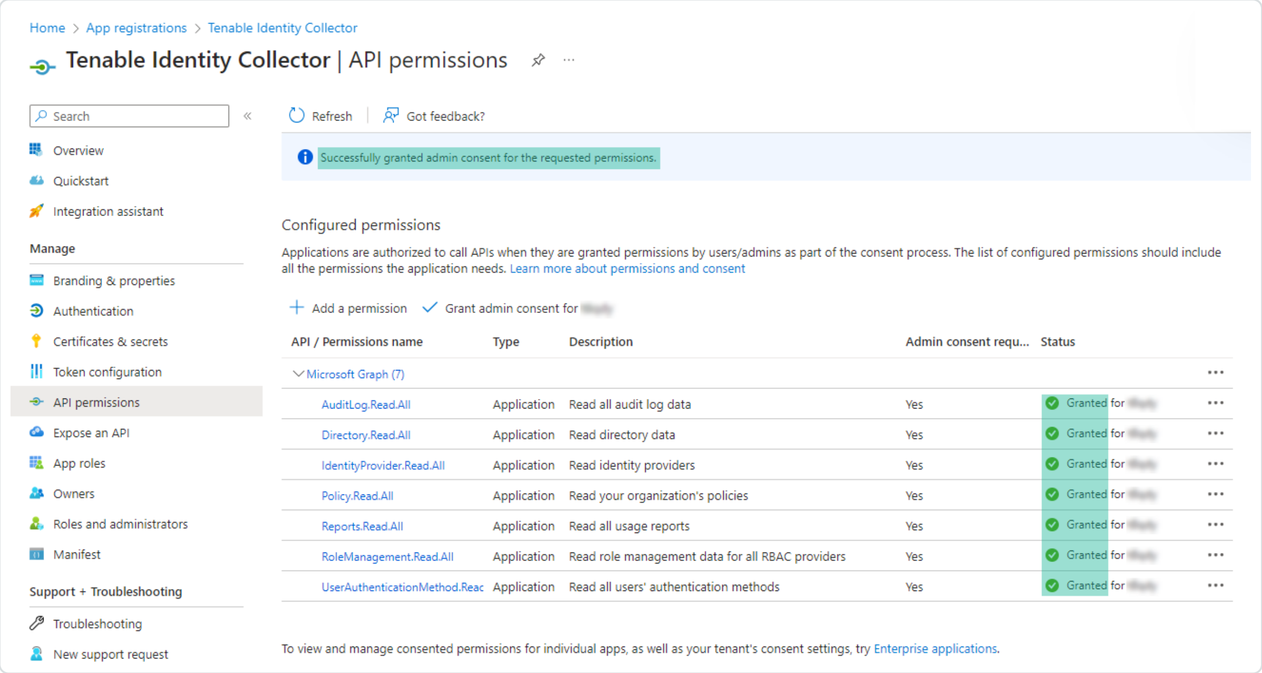
You are editing permission(s) to your application, users will have to consent even if they've already done so previously.

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (7)				
AuditLog.Read.All	Application	Read all audit log data	Yes	Not granted for [redacted]
Directory.Read.All	Application	Read directory data	Yes	Not granted for [redacted]
IdentityProvider.Read.All	Application	Read identity providers	Yes	Not granted for [redacted]
Policy.Read.All	Application	Read your organization's policies	Yes	Not granted for [redacted]
Reports.Read.All	Application	Read all usage reports	Yes	Not granted for [redacted]
RoleManagement.Read.All	Application	Read role management data for all RBAC providers	Yes	Not granted for [redacted]
UserAuthenticationMethod.Reac	Application	Read all users' authentication methods	Yes	Not granted for [redacted]

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try Enterprise applications.



Tenable Identity Collector | API permissions

Successfully granted admin consent for the requested permissions.

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (7)				
AuditLog.Read.All	Application	Read all audit log data	Yes	Granted for [redacted]
Directory.Read.All	Application	Read directory data	Yes	Granted for [redacted]
IdentityProvider.Read.All	Application	Read identity providers	Yes	Granted for [redacted]
Policy.Read.All	Application	Read your organization's policies	Yes	Granted for [redacted]
Reports.Read.All	Application	Read all usage reports	Yes	Granted for [redacted]
RoleManagement.Read.All	Application	Read role management data for all RBAC providers	Yes	Granted for [redacted]
UserAuthenticationMethod.Reac	Application	Read all users' authentication methods	Yes	Granted for [redacted]

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try Enterprise applications.

4. After you configure all the required settings in Microsoft Entra ID:

   a. In Tenable Vulnerability Management, create a new credential of type "Microsoft Azure".

   b. Select the "Key" authentication method and enter the values that you retrieved in the previous procedure: Tenant ID, Application ID, and Client Secret.

Activate Microsoft Entra ID support

- To use **Microsoft Entra ID**, you must activate the feature in Tenable Identity Exposure settings.
- See Identity 360, Exposure Center, and Microsoft Entra ID Support Activation for instructions.

Enable tenant scans

To add a new Microsoft Entra ID tenant:

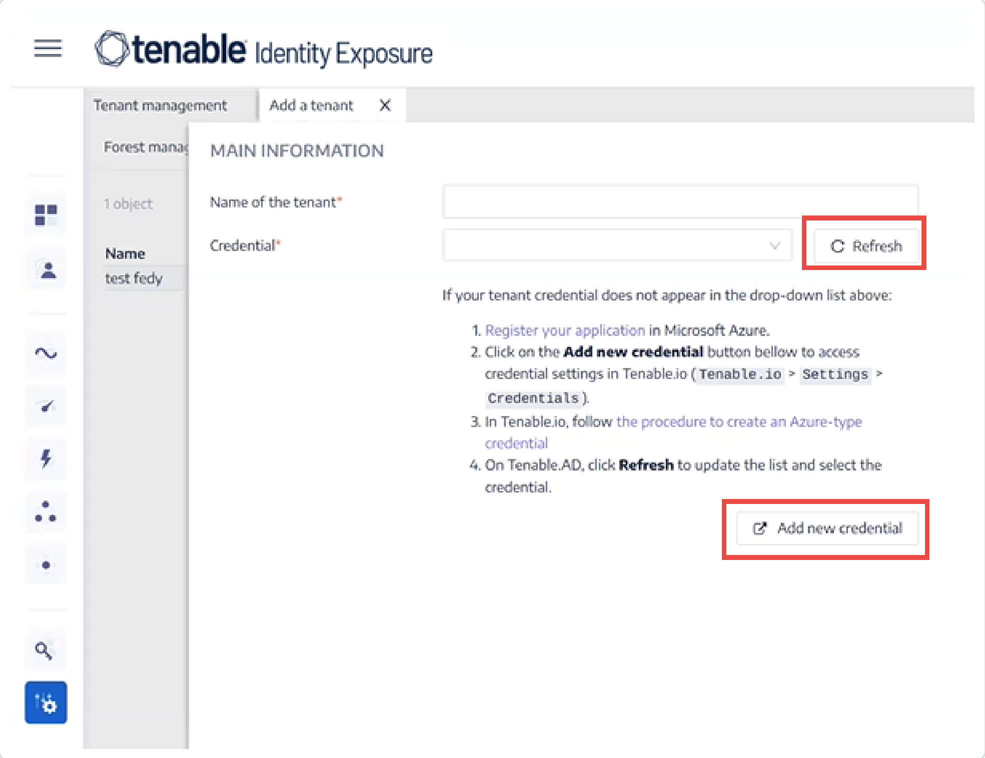
Adding a tenant links Tenable Identity Exposure with the Microsoft Entra ID tenant to perform scans on that tenant.

1. In the Configuration page, click on the **Identity Providers** tab.

   The **Tenant Management** page opens.

2. Click on **Add a tenant**.

   The **Add a tenant** page opens.

   MAIN INFORMATION

   Name of the tenant*

   Credential*

   If your tenant credential does not appear in the drop-down list above:

   1. Register your application in Microsoft Azure.
   2. Click on the **Add new credential** button bellow to access credential settings in Tenable.io (`Tenable.io` > `Settings` > `Credentials`).
   3. In Tenable.io, follow the procedure to create an Azure-type credential
   4. On Tenable.AD, click **Refresh** to update the list and select the credential.

3. In the **Name of the tenant** box, type a name.

4. In the **Credentials** box, click the drop-down list to select a credential.

5. If your credential does not appear in the list, you can either:

   - Create one in Tenable Vulnerability Management (Tenable Vulnerability Management > **Settings** > **Credentials**). For more information, see the procedure to create an Azure-type credential in Tenable Vulnerability Management.

   - Check that you have the "Can use" or "Can edit" permission for the credential in Tenable Vulnerability Management. Unless you have these permissions, Tenable Identity Exposure does not show the credential in the drop-down list.

6. Click **Refresh** to update the drop-down list of credentials.

7. Select the credential you created.

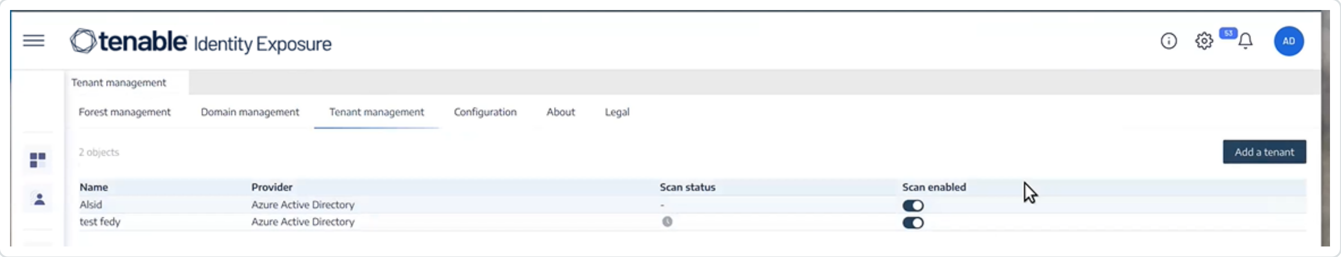
8. Click **Add**.

   A message confirms that Tenable Identity Exposure added the tenant, which now appears in the list on the Tenant Management page.

To enable scans for the tenant:

> **Note**: Tenant scans do not occur in real time and require at least 45 minutes before Microsoft Entra ID data is visible in the Identity Explorer, depending on the tenant size.

- Select a tenant on the list and click the toggle to **Scan enabled**.



2 objects

Name	Provider	Scan status	Scan enabled
Alsid	Azure Active Directory	-	●
test fedy	Azure Active Directory	●	●

Tenable Identity Exposure requests a scan on the tenant and the results appear in the Indicator of Exposure page.

> **Note**: The mandatory minimum time delay between two scans is **30 minutes** and occurs at least once per day. Depending on the tenant size, most customers' data refresh multiple times per day.

Attack Path

Tenable Identity Exposure offers several ways to visualize the potential vulnerability of a business asset through graphical representations.

- **Attack Path**: Shows the possible paths that an attacker can take to compromise an asset from an entry point.
- **Blast Radius**: Shows the possible lateral movements into the Active Directory from any asset.
- **Asset Exposure**: Shows all paths that can potentially take control of an asset.

Understanding the attack path enables you to identify necessary mitigation steps to block attackers from exploiting vulnerabilities. This might involve patching systems, hardening configurations, implementing stronger access controls, or raising awareness among users.

Benefits of using Attack Path in Tenable Identity Exposure:

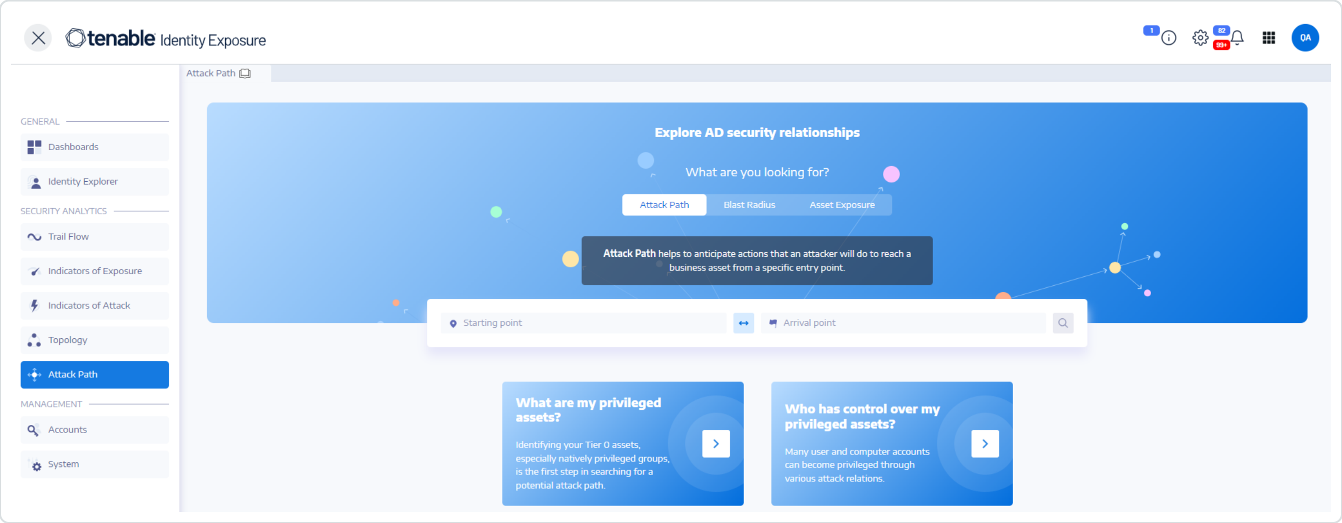
- **Proactive security**: It helps anticipate and address potential attack vectors before they are exploited.
- **Prioritization**: It guides towards focusing security efforts on the most critical vulnerabilities and attack paths.
- **Visualization**: It provides a clear and easy-to-understand representation of complex security relationships within your AD.
- **Communication**: It facilitates communication of security risks to stakeholders by offering visual evidence of potential attack scenarios.

To display the Attack Path:

You specify the starting point, which could be any asset in your AD (e.g., a user account, computer, group). You define the arrival point, representing the asset the attacker ultimately aims to compromise (e.g., a domain controller, sensitive data server).

1. In Tenable Identity Exposure, click **Attack Path** on the sidebar menu.

   The **Attack Path** pane appears.



Explore AD security relationships

What are you looking for?

Attack Path helps to anticipate actions that an attacker will do to reach a business asset from a specific entry point.

What are my privileged assets?

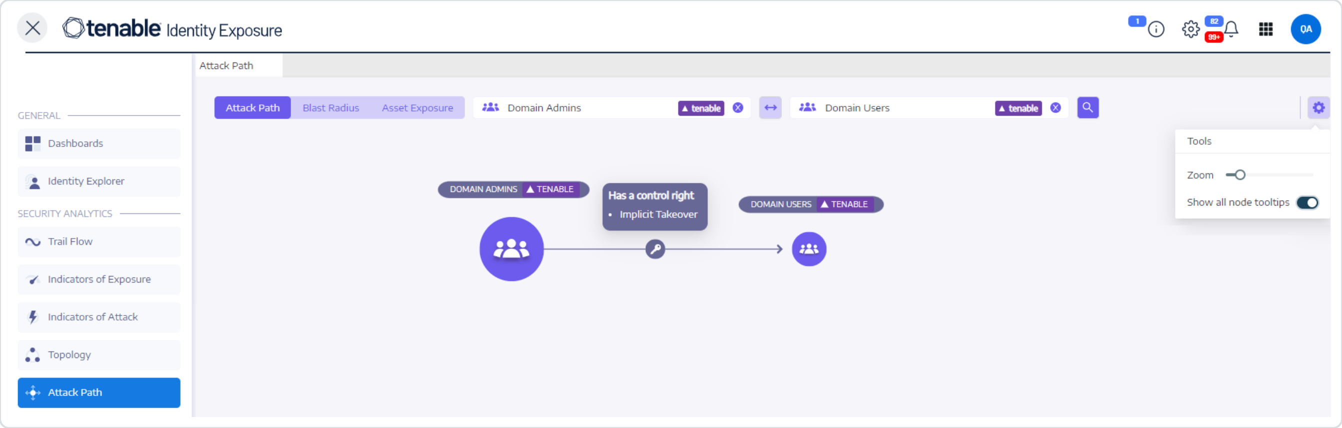
Identifying your Tier 0 assets, especially natively privileged groups, is the first step in searching for a potential attack path.

Who has control over my privileged assets?

Many user and computer accounts can become privileged through various attack relations.

2. In the banner, click **Attack Path**.
3. In the **Starting point** box, type the asset at the entry point.
4. In the **Arrival point** box, type the asset at the end of the path.
5. Click the 🔍 icon.

   Tenable Identity Exposure displays the attack path between the two assets.



Domain Admins tenable ↔ Domain Users tenable

Has a control right
- Implicit Takeover

Zoom

Show all node tooltips

6. Optionally, you can click on the ⚙ icon to do the following:
   - Click the **Zoom** slider to adjust the magnification of the graphics.
   - Click the **Show all node tooltips** toggle to display information about the assets.

To display the Blast Radius:

Tenable Identity Exposure displays a graphical representation of the potential attack path, highlighting the connections between assets. Each connection represents a potential vulnerability or misconfiguration that the attacker could exploit to move laterally within your AD. You can zoom in and out to gain a better understanding of the path's details.

1. In Tenable Identity Exposure, click **Attack Path** on the sidebar menu.

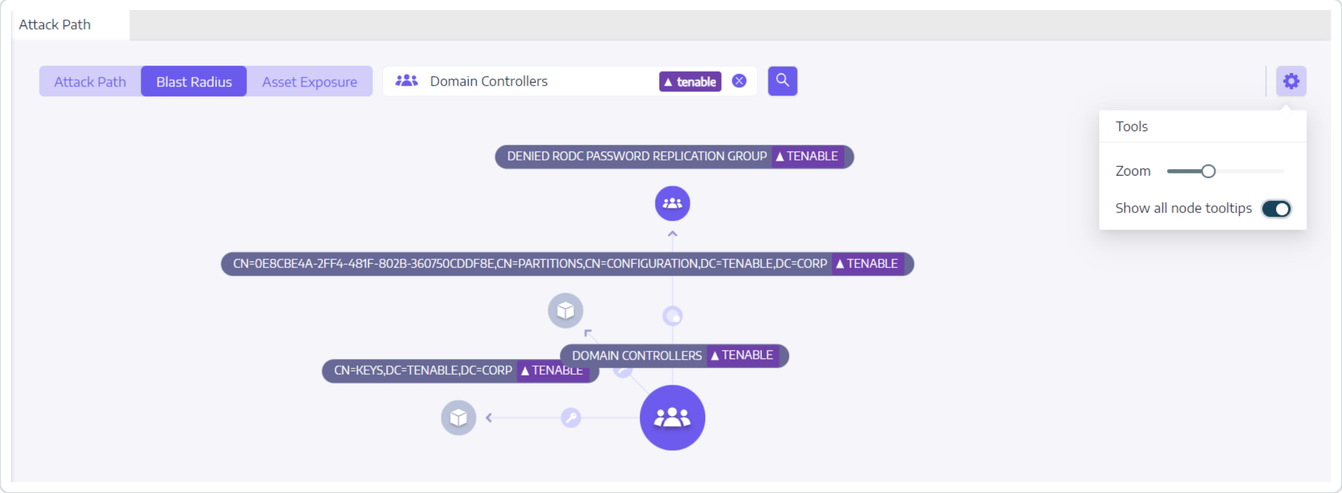
   The **Attack Path** pane appears.

2. In the banner, click **Blast Radius**.

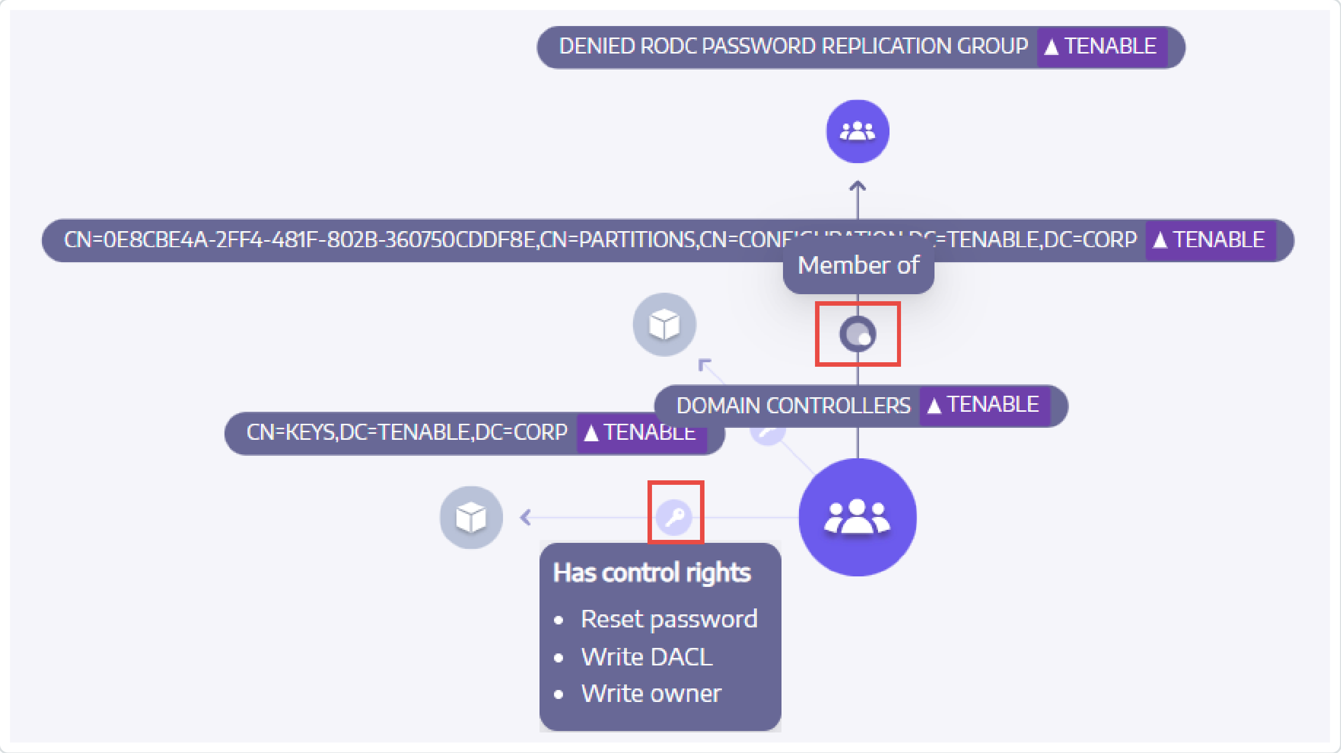
3. In the **Search for an object** box, type the name of an asset.

4. Click the 🔍 icon.

   Tenable Identity Exposure displays the lateral connections radiating from that asset:



5. Click on the icons on the arrows between the assets to display the relations between them.


DENIED RODC PASSWORD REPLICATION GROUP ▲TENABLE
CN=0E8CBE4A-2FF4-481F-802B-360750CDDF8E,CN=PARTITIONS,CN=CONF Member of C=TENABLE,DC=CORP ▲TENABLE
DOMAIN CONTROLLERS ▲TENABLE
CN=KEYS,DC=TENABLE,DC=CORP ▲TENABLE
Has control rights
• Reset password
• Write DACL
• Write owner

To display the Asset Exposure:

Each step in the attack path is associated with a risk score, indicating the severity of the vulnerability. This helps you prioritize which paths pose the most significant threat and require immediate attention. You can also click on individual connection points for more details about the specific vulnerability or misconfiguration involved.

1. In Tenable Identity Exposure, click **Attack Path** on the sidebar menu.

   The **Attack Path** pane appears.

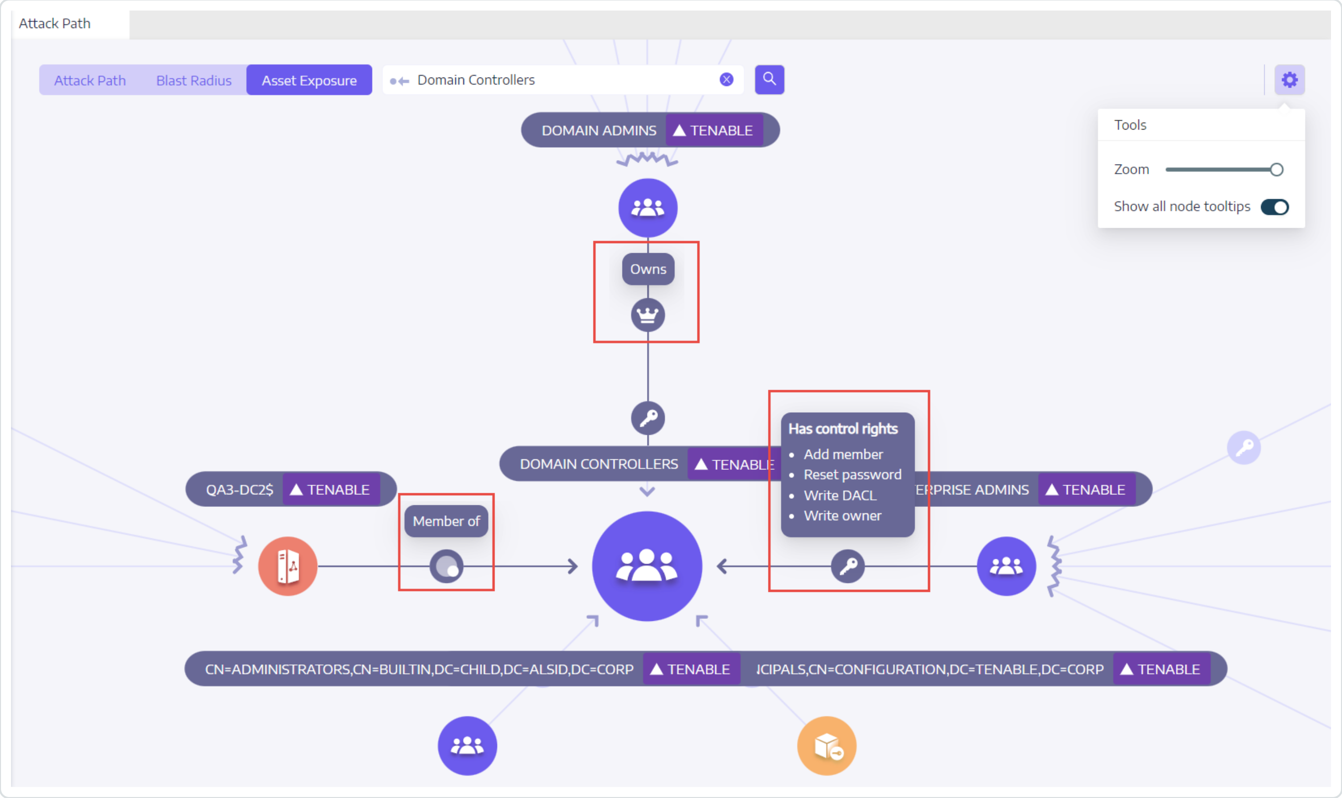
2. In the banner, click **Asset Exposure**.

3. In the **Search for an object** box, type the name of an asset.

4. Click the 🔍 icon.

   Tenable Identity Exposure displays the paths leading to the asset and the relations between the assets.

5. Click on the icons on the arrows between the assets to display the relations between them.



Has control rights

- Add member
- Reset password
- Write DACL
- Write owner

To pin an attack path:

See also

- Attack Relations
- Identifying Tier 0 Assets
- Accounts with Attack Paths
- Attack Path Node Types

User Management

Key aspects

- **Roles**: Default roles include Administrator, Security Analyst, User, and Guest, each with varying permissions. Custom roles allow granular control for specific needs.
- **Permissions**: Permissions define what users can access and do within Tenable Identity Exposure. These range from viewing reports and dashboards to managing users, configuring indicators, and performing actions like disabling accounts.
- **Scoping**Tenable Identity Exposure allows scoping permissions to specific domains, groups, or even individual objects within Active Directory. This ensures users only access relevant data based on their role and responsibilities.

Benefits

- **Enhanced Active Directory security**: Granular access control minimizes the risk of unauthorized access to sensitive identity data.
- **Improved efficiency and workflows**: Users have access to the tools and data they need, streamlining investigations and incident response.
- **Compliance adherence**: Role-based access control helps meet compliance requirements for identity and access management within Active Directory.

See also

- User Roles

Tenable Identity Exposure Integration

Integrate Tenable Identity Exposure with your SIEM, SOC, or SOAR solution to achieve real-time monitoring, automated response, and improved alert management.

Real-Time Monitoring with Syslog Integration

Gain instantaneous alerts for critical Indicators of Exposure (IoEs) through seamless Syslog integration.

Key Benefits

- **Centralized logging**: Aggregate Tenable Identity Exposure events with other security solutions for comprehensive analysis.
- **Real-time notifications**: Receive immediate notifications about potential identity exposures and attacks.
- **Improved security management**: Correlate events from different sources to identify complex threats faster.
- **Enhanced SIEM visibility**: Integrate Tenable Identity Exposure data seamlessly into your SIEM, boosting situational awareness and correlation analysis.
- **Streamlined workflow**: Automate alert triage and response based on Syslog data, optimizing security operations.

Example of IoEs for Real-time Monitoring

- **ADCS Dangerous Misconfigurations**: Detect/identify changes to AD Certificate Servers potentially indicating "Certified Pre-owned" attacks.
- **GPO Execution Sanity**: Detects/identifies attempts to install backdoors through script execution within Group Policies.
- **Users Allowed to Join Computers to the Domain**: Recognize unauthorized domain computer additions, a signature pre-attack of "RBCD" backdoor attacks.

Automating Response with SOAR Platforms

Leverage existing Security Orchestration, Automation, and Response (SOAR) platforms to execute automated remediation actions based on TIE data. The key benefits are the following:

- **Rapid mitigation**: Minimize downtime and impact by automating responses to critical IoEs.
- **Improved efficiency**: Free up security teams from repetitive tasks, allowing them to focus on strategic security initiatives.
- **Enhanced security measures**: Proactively address detected misconfigurations and strengthen your overall security status.

Important: Troubleshooting or assistance in automation script is out of scope for Tenable Support. Please contact our Professional Service team for assistance.