Tenable Identity Exposure 3.x User and Administrator Guide

Last Revised: March 25, 2024

Table of Contents

Welcome to Tenable Identity Exposure

Last updated: 3/25/2024

Tenable Identity Exposure (formerly known as Tenable.ad) allows you to secure your infrastructure by anticipating threats, detecting breaches, and responding to incidents and attacks. Using an intuitive dashboard to monitor your active directory in real-time, you can identify at a glance the most critical vulnerabilities and their recommended courses of remediation. Tenable Identity Exposure's indicators of attack and indicators of exposure allow you to discover underlying issues affecting your active directory, identify dangerous trust relationships, and analyze in-depth details of attacks.

> The Indicators of Attack and Indicators of Exposure features are available depending on the license that you purchased.

To get started, see Get Started With Tenable Identity Exposure.

> **Note:** Tenable Identity Exposure can be purchased alone or as part of the Tenable One package. For more information, see Tenable One.

> **Tip:** The *Tenable Identity Exposure User Guide* is available in English, Japanese, German, Korean, Simplified Chinese, and Traditional Chinese. The *Tenable Identity Exposure* user interface is available in English, Japanese, German, French, Korean, Simplified Chinese, and Traditional Chinese. To change the user interface language, see User Preferences.

For additional information on Tenable Identity Exposure, review the following customer education materials:

- Tenable Identity Exposure Self Help Guide
- Tenable Identity Exposure Introduction (Tenable University)

Tenable One Exposure Management Platform

Tenable One is an Exposure Management Platform to help organizations gain visibility across the modern attack surface, focus efforts to prevent likely attacks and accurately communicate cyber risk to support optimal business performance.

The platform combines the broadest vulnerability coverage spanning IT assets, cloud resources, containers, web apps and identity systems, builds on the speed and breadth of vulnerability coverage from Tenable Research and adds comprehensive analytics to prioritize actions and communicate cyber risk. Tenable One allows organizations to:

- Gain comprehensive visibility across the modern attack surface
- Anticipate threats and prioritize efforts to prevent attacks
- Communicate cyber risk to make better decisions

Tenable Identity Exposure exists as a standalone product, or can be purchased as part of the Tenable One Exposure Management platform.

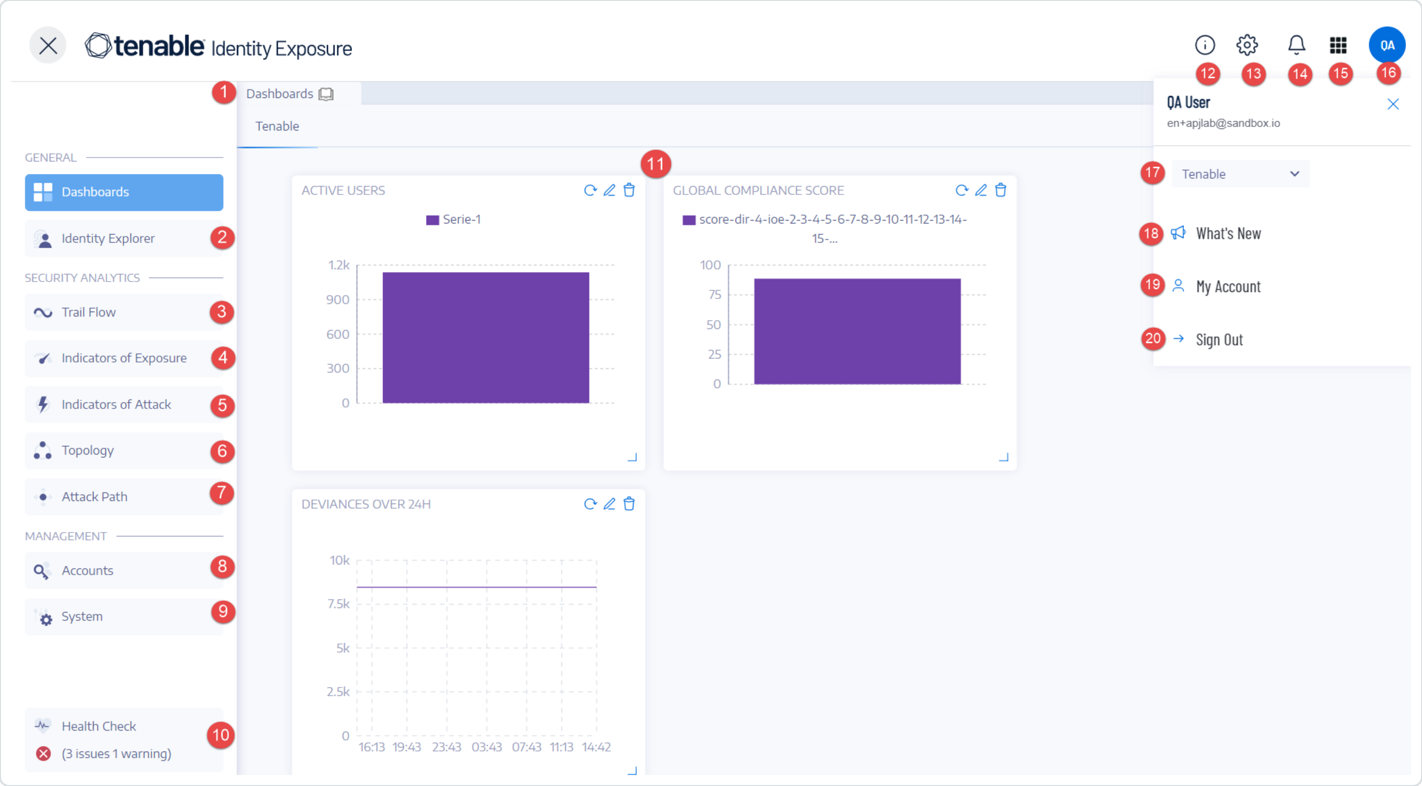
Tip: For additional information on getting started with Tenable One products, check out the Tenable One Deployment Guide.

Navigate Tenable Identity Exposure

After you log in to Tenable Identity Exposure, the home page opens, as shown in this example.

To expand or collapse the side navigation bar:

- To expand: click the ≡ menu at the top left of the window.
- To collapse: click the **X** at the top left of the window.



#	What it is	What it does
1	Dashboards	Dashboards allow you to manage and monitor efficiently and in a visual way security in an Active Directory infrastructure.
2	Identity Explorer	Tenable Identity Exposure's Identity Explorer view unifies identities across both Active Directory and Microsoft Entra ID. This view shows

		the Identity Risk Score (beta) for each listed asset and the potential reach of compromised identities.
3	Trail Flow	The Trail Flow shows the real-time monitoring and analysis of events affecting your Active Directory.
4	Indicators of Exposure	Tenable Identity Exposure uses Indicators of Exposure (IoEs) to measure the security maturity of your Active Directory and assign severity levels (Critical, High, Medium, or Low) to the flow of events that it monitors and analyzes.
5	Indicators of Attack	Through Indicators of Attack, Tenable Identity Exposure can detect attacks in real time.
6	Topology	The Topology page gives an interactive graph visualization of your Active Directory. It shows the forests, domains, and trust relationships that exist between them.
7	Attack Path	The Attack Path pages give graphical representations of Active Directory relationships: • Blast Radius: Evaluates lateral movements in the AD from a potentially compromised asset. • Attack Path: Anticipates privilege escalation techniques to reach an asset from a

		specific entry point. - Asset Exposure: Measures an asset's vulnerability using asset exposure visualization and tackles all escalation paths.
8, 9	Management **Required User Role**: Organizational User with appropriate permissions.	This section allows you to configure the following: - Accounts: User accounts, roles, and security profiles. - System: Forests and domains, application services, alerts, and authentication. For more information, see the Tenable Identity Exposure Administrator Guide.
10	Health Checks	Health checks provide you with real-time visibility into the configuration of your domains and service accounts in one consolidated view from which you can drill down for more detailed information.
11	Widgets	Widgets are customizable datasets on a dashboard. They can contain bar charts, line charts, and counters.
12	Product Updates	Information about the latest product features.
13	Settings	Access to system configuration, forest and domain management, license, user and role management, profiles, and activity logs.

14	Notifications (Bell)	A bell icon and badge counts notify you of attack alerts and/or exposure alerts waiting for your acknowledgment.
15	Application Switcher	Click this icon to switch between applications from the Tenable workspace.
16, 19	User profile icon (User Preferences)	Click this icon to access a submenu to security profiles, release notes, activity logs, preferences, or sign out.
17	Security Profiles	Security Profiles allow different types of users to review security analysis from different reporting angles.
18	What's New	Click to open the release notes for the most recent version of Tenable Identity Exposure.
20	Sign out	Click to sign out of Tenable Identity Exposure.

Log in to Tenable Identity Exposure

You access Tenable Identity Exposure's web application through a client URL.

To log in to Tenable Identity Exposure, select one of the following options:

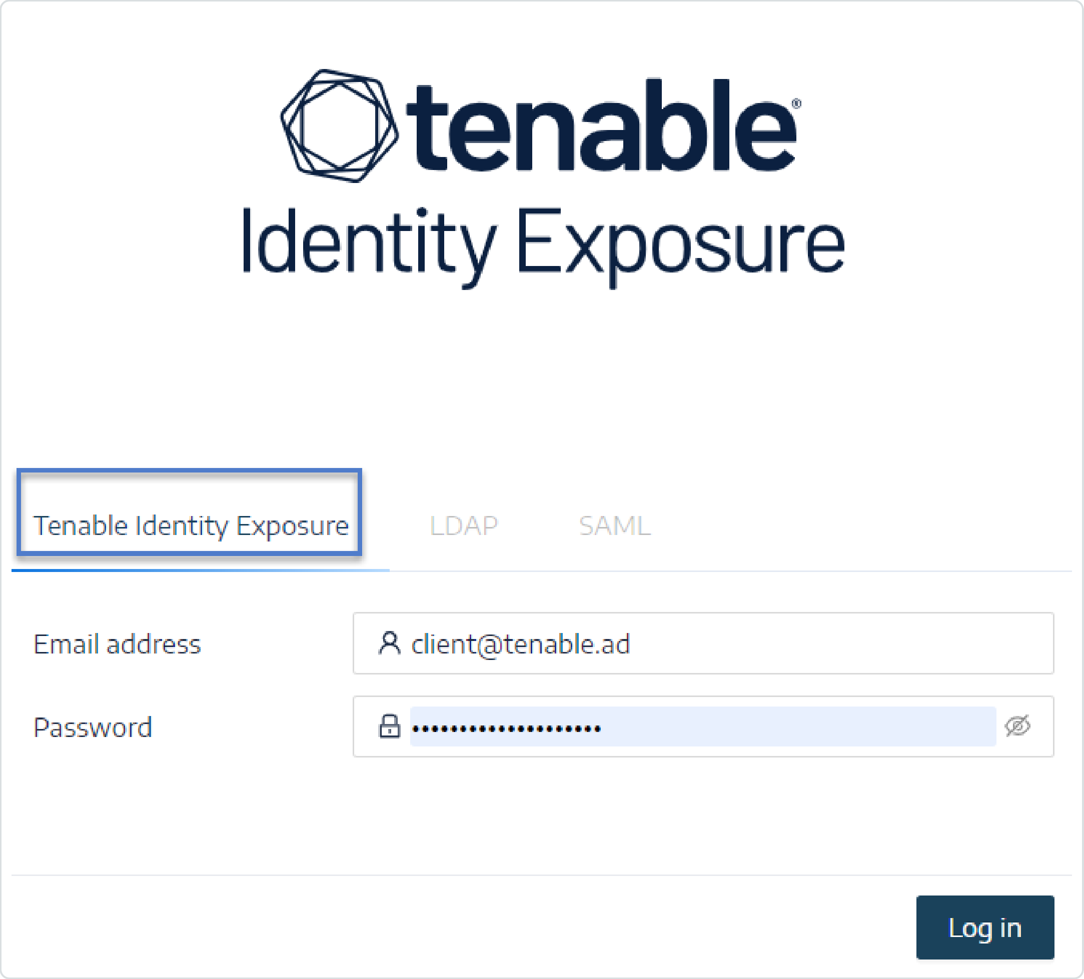
-
  - Using a Tenable Identity Exposure account
  - Using an LDAP account
  - Using SAML

Using a Tenable Identity Exposure account

To sign in with your Tenable Identity Exposure account:

1. In any browser, type your client URL (for example: client.tenable.ad) in the address bar.

   The **Log in** window appears.



Email address: client@tenable.ad

Password: ••••••••••••••••••••

2. Click the **Tenable Identity Exposure** tab.

3. Type your email address.

4. Type your password.

5. Click **Log in**.

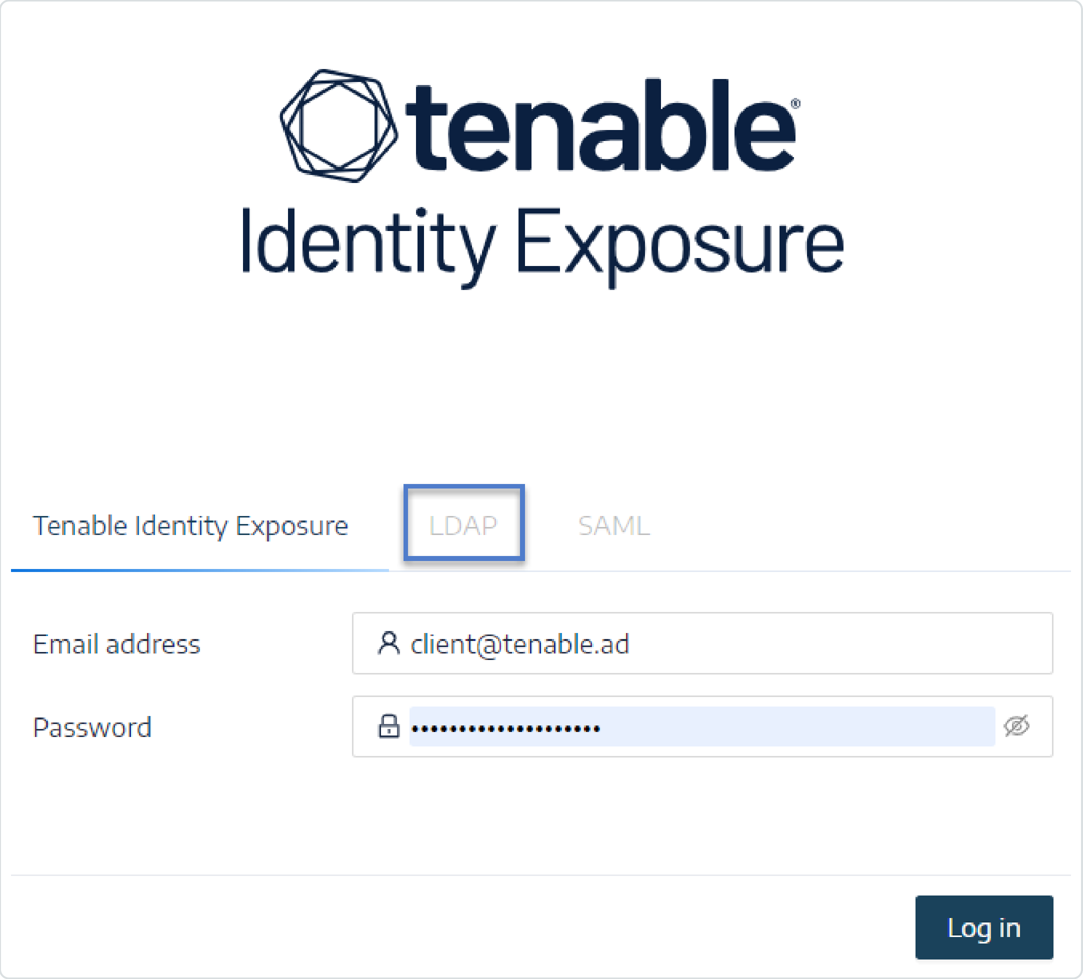
   The Tenable Identity Exposure page opens.

Using an LDAP account

To sign in with LDAP:

1. In any browser, type your client URL (for example: client.tenable.ad) in the address bar.

   The **Log in** window appears.



Email address: client@tenable.ad

Password: ••••••••••••••••••••

2. Click the **LDAP** tab.

3. Type your LDAP account name.

4. Type your LDAP password.

5. Click **Log in**.

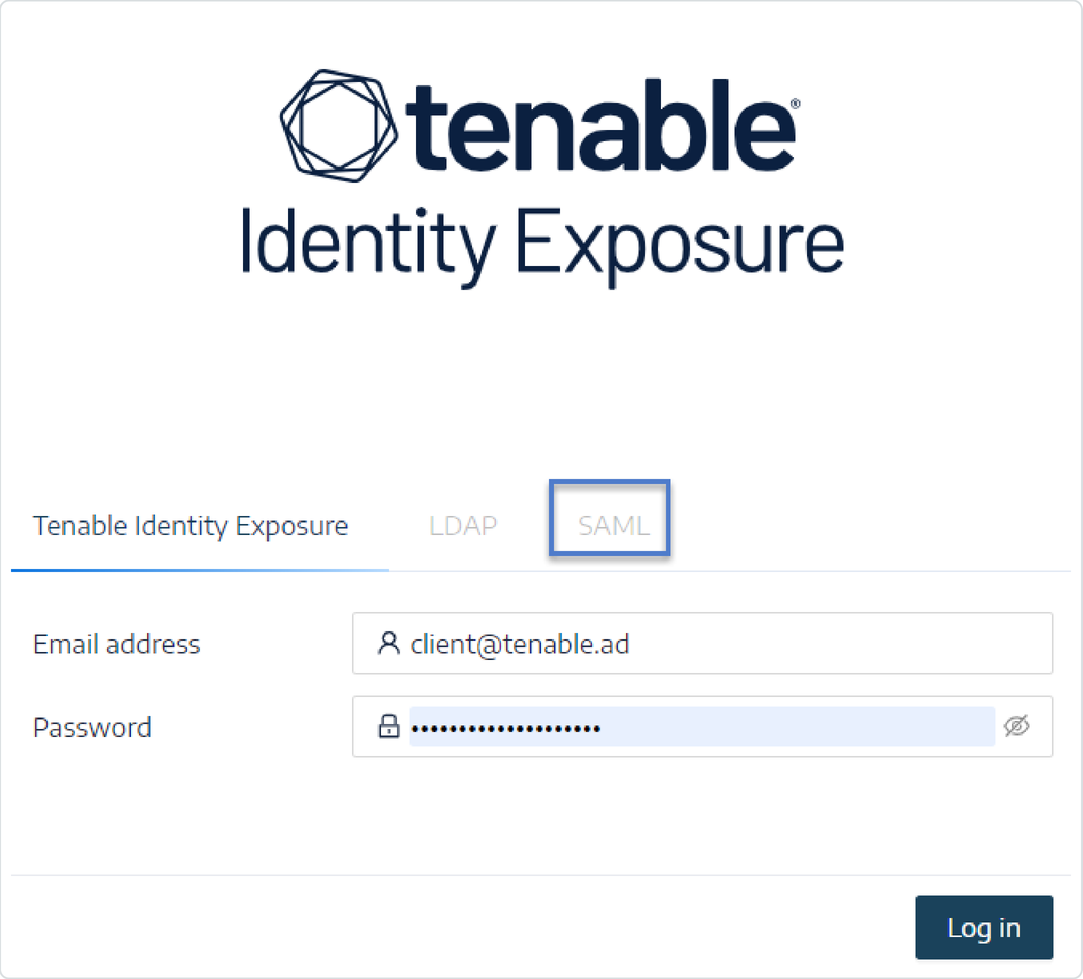
   The Tenable Identity Exposure page opens.

Using SAML

To sign in with SAML:

1. In any browser, type your client URL (for example: client.tenable.ad) in the address bar.

   The **Log in** window appears.



2. Click the **SAML** tab.

3. Click on the link to your Identity Provider (IDP).

   Tenable Identity Exposure redirects you to your SAML server for authentication.

4. Enter your company credentials on your IDP.

   You get redirected to Tenable Identity Exposure as a logged in user.

Caution: If your login fails repeatedly, Tenable Identity Exposure locks your account. Contact your administrator.

To sign out of Tenable Identity Exposure:

1. In Tenable Identity Exposure. click on your user icon.

   A submenu appears.

2. Click **Sign out**.

   Tenable Identity Exposure returns to the Log in page.

Access the Workspace

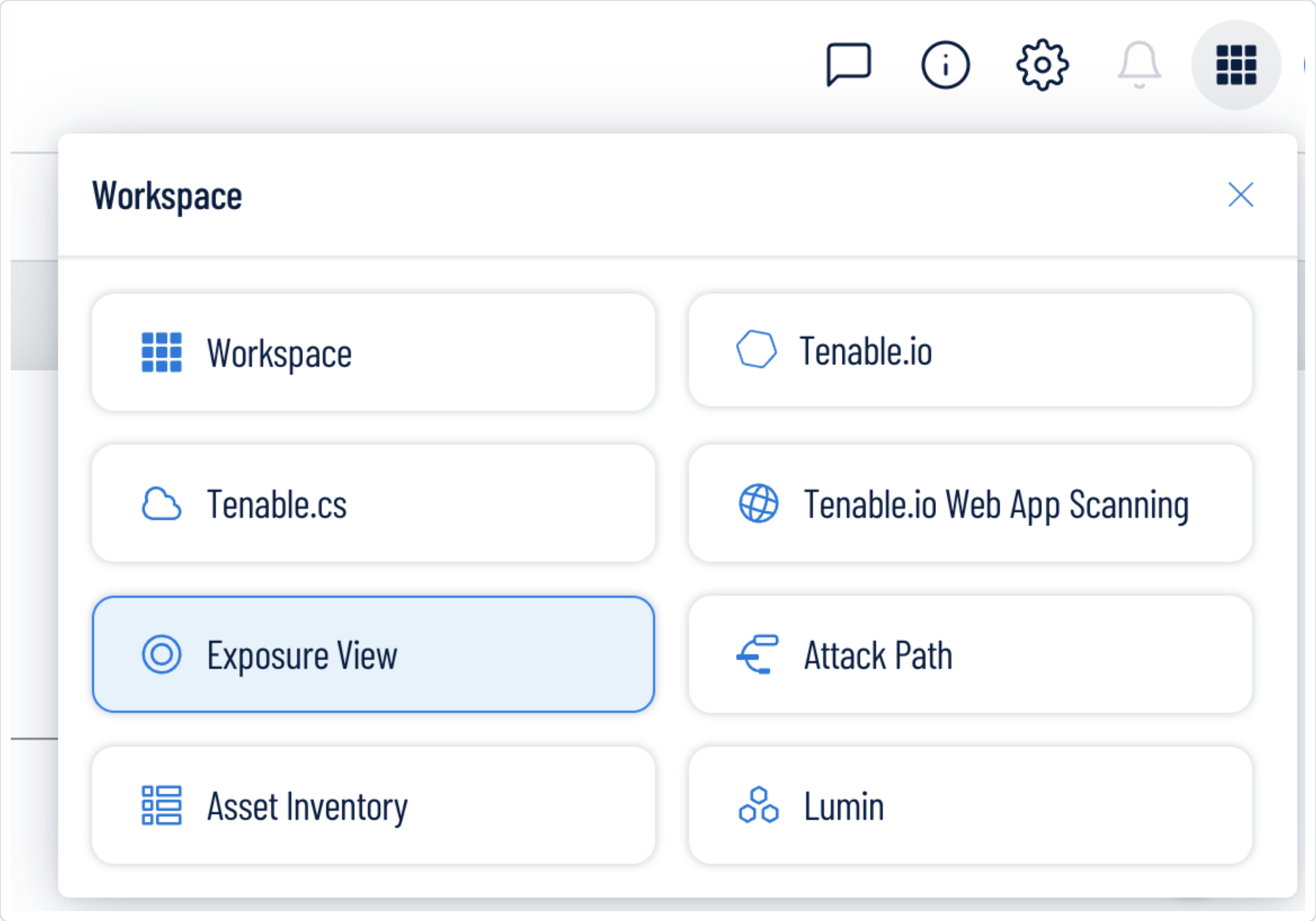
When you log in to Tenable, the **Workspace** page appears by default. On the **Workspace** page, you can switch between your Tenable applications or set a default application to skip the **Workspace** page in the future. You can also switch between your applications from the **Workspace** menu, which appears in the top navigation bar.

Open the Workspace Menu

To open the **Workspace** menu:

1. From any Tenable application, in the upper-right corner, click the ▦ button.

   The **Workspace** menu appears.



2. Click an application tile to open it.

View the Workspace Page

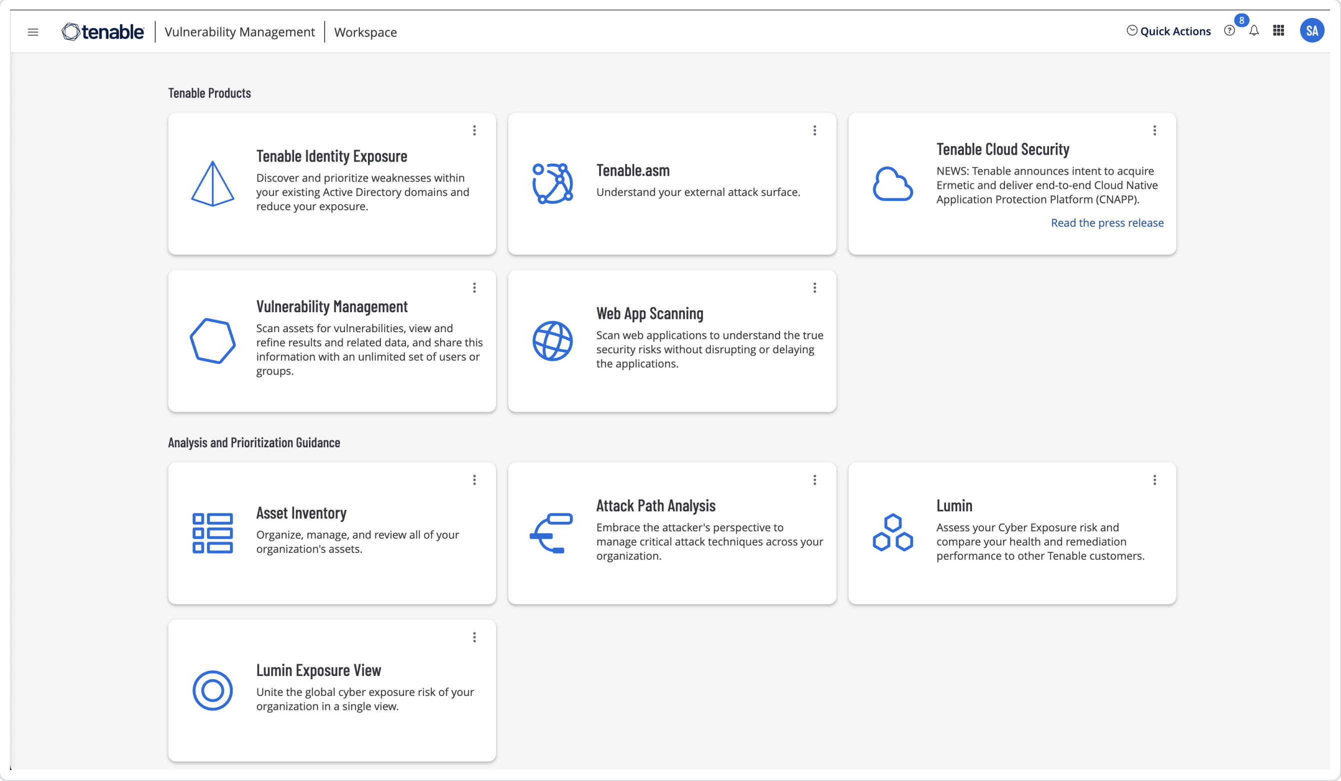
To view the Workspace page:

1. From any Tenable application, in the upper-right corner, click the ▦ button.

   The **Workspace** menu appears.

2. In the **Workspace** menu, click **Workspace**.

   The **Workspace** page appears.



Tenable Products

Tenable Identity Exposure
Discover and prioritize weaknesses within your existing Active Directory domains and reduce your exposure.

Tenable.asm
Understand your external attack surface.

Tenable Cloud Security
NEWS: Tenable announces intent to acquire Ermetic and deliver end-to-end Cloud Native Application Protection Platform (CNAPP).
Read the press release

Vulnerability Management
Scan assets for vulnerabilities, view and refine results and related data, and share this information with an unlimited set of users or groups.

Web App Scanning
Scan web applications to understand the true security risks without disrupting or delaying the applications.

Analysis and Prioritization Guidance

Asset Inventory
Organize, manage, and review all of your organization's assets.

Attack Path Analysis
Embrace the attacker's perspective to manage critical attack techniques across your organization.

Lumin
Assess your Cyber Exposure risk and compare your health and remediation performance to other Tenable customers.

Lumin Exposure View
Unite the global cyber exposure risk of your organization in a single view.

Set a Default Application

When you log in to Tenable, the **Workspace** page appears by default. However, you can set a default application to skip the **Workspace** page in the future.

> By default, users with the **Administrator**, **Scan Manager**, **Scan Operator**, **Standard**, and **Basic** roles can set a default application. If you have another role, contact your administrator and request the **Manage** permission under **My Account**. For more information, see Custom Roles.

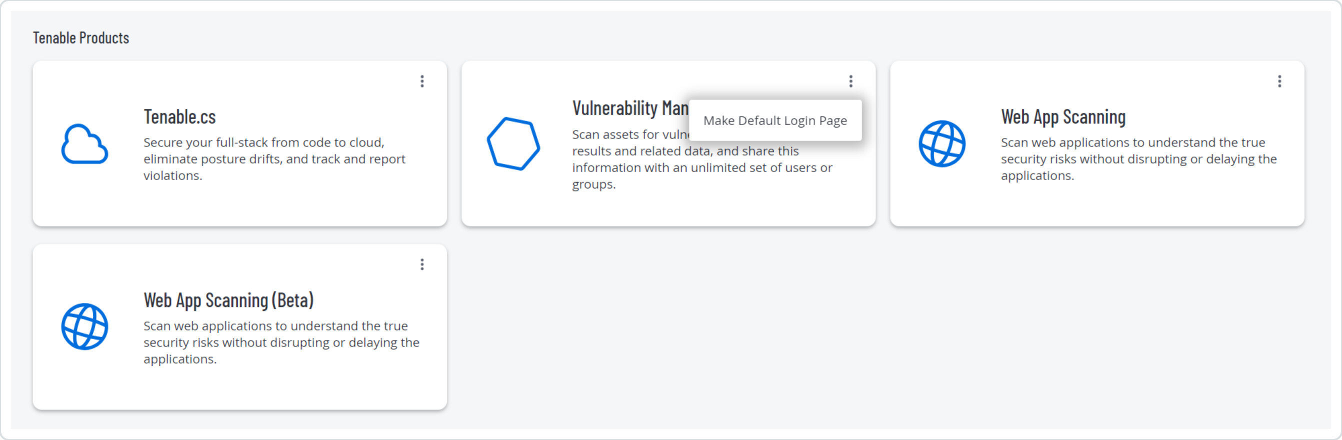
To set a default login application:

1. Log in to Tenable.

   The **Workspace** page appears.

2. In the top-right corner of the application to choose, click the ⋮ button.

   A menu appears.



Tenable Products

Tenable.cs

Secure your full-stack from code to cloud, eliminate posture drifts, and track and report violations.

Vulnerability Man

Scan assets for vuln

results and related data, and share this information with an unlimited set of users or groups.

Web App Scanning

Scan web applications to understand the true security risks without disrupting or delaying the applications.

Web App Scanning (Beta)

Scan web applications to understand the true security risks without disrupting or delaying the applications.

3. In the menu, click **Make Default Login Page**.

   This application now appears when you log in.

Remove a Default Application

To remove a default login application:

1. Log in to Tenable.

   The **Workspace** page appears.

2. In the top-right corner of the application to remove, click the ⋮ button.

   A menu appears.

3. Click **Remove Default Login Page**.

   The **Workspace** page now appears when you log in.

User Preferences

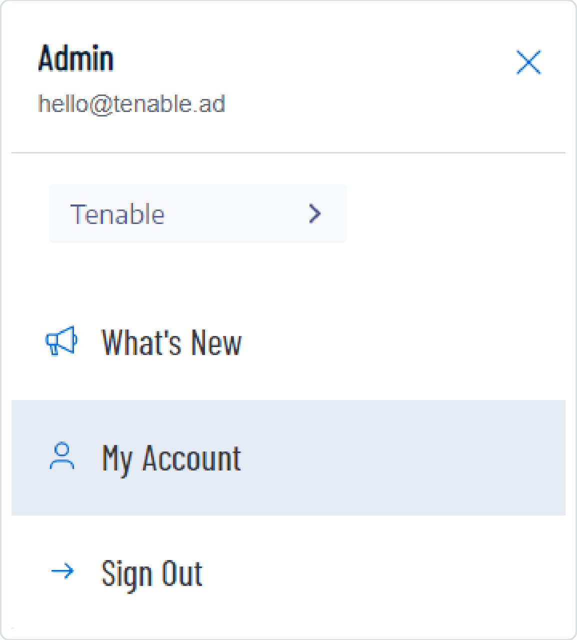
You can set your user preferences in Tenable Identity Exposure.

- To select your language:
- To select your profile:
- To change your password:
- To select your profile:

To set your preferences:

1. In Tenable Identity Exposure, click on your user profile icon at the top-right corner.

   A submenu appears.

2. Select **My Account**.

   The **Preferences** page appears.

To select your language:

a. In **Languages**, click the arrow of the drop-down list to select your preferred language.

b. Click **Save**.

A message confirms that Tenable Identity Exposure updated your preferences. The user interface shows the language you selected.

To select your profile:

Switching from one security profile to another changes the way Tenable Identity Exposure displays the configuration of indicators and the data representation on the dashboards, widgets, and trail flow.

a. Under **Preferences**, click **Profiles**.

b. In **Preferred profile**, click the drop-down arrow to select your default profile after you connect to Tenable Identity Exposure.

c. Click **Save**.

A message confirms that Tenable Identity Exposure updated your preferences.

For more information, see Security Profiles.

To change your password:

> **Note**: The password information is not available if you have a Tenable One license, in which case Tenable Vulnerability Management manages all your authentication settings. For more information, see Access Control in the Tenable Vulnerability Management User Guide.

a. Under **Preferences**, click **Credentials**.

b. Provide the following:

   - Your old password.
   - Your new password.

c. In the **New password confirmation** box, retype the new password.

d. Click **Save**.

A message confirms that Tenable Identity Exposure changed your password.

> **Note**: You cannot change a password for accounts connected through external providers such as LDAP or SAML in Tenable Identity Exposure.

To manage your API key:

a. Under **Preferences**, click **API key**.

   Your access token appears in the **Current API key** box.

b. You can do the following:

c. Click the ⧉ icon to copy the API key to the clipboard to use as needed.

d. Click **Refresh API key** to generate a new access token.

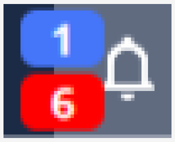
   A message asks you for confirmation.

   > **Note**: Refreshing the API key causes Tenable Identity Exposure to deactivate the current token.

For more details, see Use Public API.

Notifications

At the top right of the Tenable Identity Exposure home page, a bell icon and its badge counts notify you of attack alerts and/or exposure alerts waiting for your acknowledgment. When it receives new alerts, Tenable Identity Exposure increments the notification badge counts.

	**Blue**	Exposure alerts
	Red	Attack alerts

To display alerts:

1. In Tenable Identity Exposure, click the bell icon.

   The **Alerts** pane opens.

2. Do one of the following:

   - Click on the **Exposure alerts** tab to display exposure alerts.
   - Click on the **Attack alerts** tab to display attack alerts.

     A list of associated alerts appears.

To view the event associated with the alert:

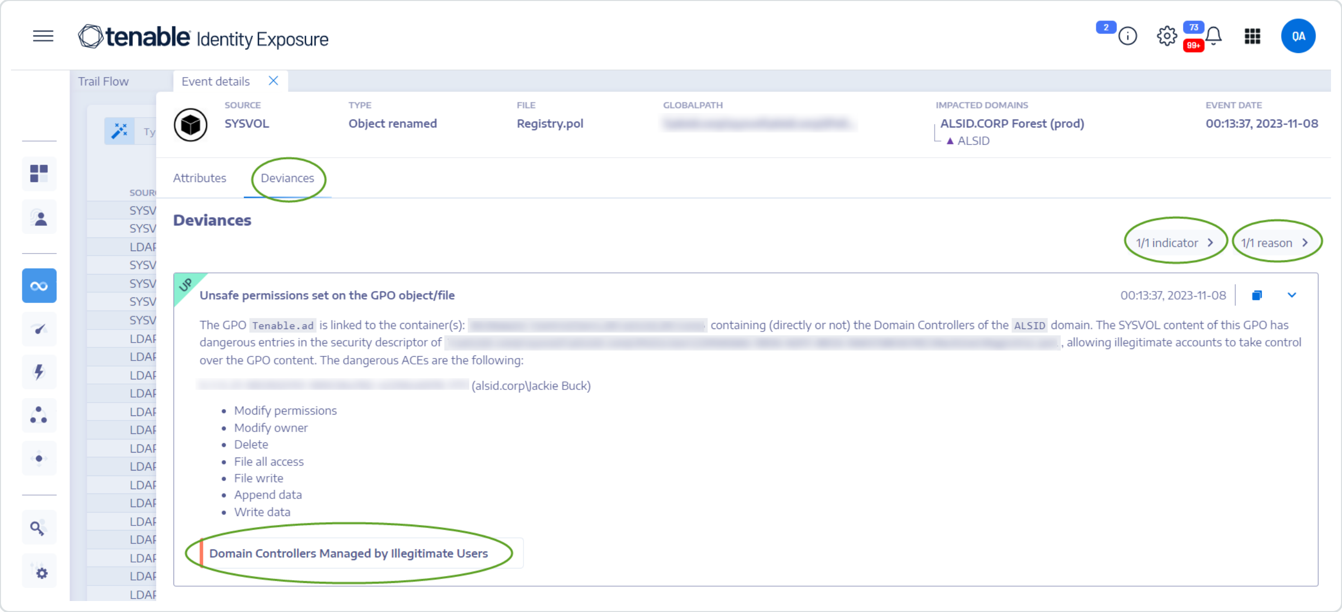
1. Select an alert from the list and click **Actions**> **See the deviance**.

   The Event details pane opens with the following information:

   - Source (Event collector)
   - Object type
   - File
   - Path
   - Impacted domains
   - Date
   - A list of attributes with values at the time of event and the current value

2. Click the **Deviances** tab.

   The **Deviances** pane opens with a list of deviances associated with the event.



SOURCE	TYPE	FILE	GLOBALPATH	IMPACTED DOMAINS	EVENT DATE
SYSVOL	Object renamed	Registry.pol	[redacted]	ALSID.CORP Forest (prod) ▲ ALSID	00:13:37, 2023-11-08

Deviances

Unsafe permissions set on the GPO object/file 00:13:37, 2023-11-08

The GPO `Tenable.ad` is linked to the container(s): [redacted] containing (directly or not) the Domain Controllers of the `ALSID` domain. The SYSVOL content of this GPO has dangerous entries in the security descriptor of [redacted], allowing illegitimate accounts to take control over the GPO content. The dangerous ACEs are the following:

[redacted] (alsid.corp\Jackie Buck)

- Modify permissions
- Modify owner
- Delete
- File all access
- File write
- Append data
- Write data

Domain Controllers Managed by Illegitimate Users

3. Click on **n/n Indicators** to display the pane for the Indicator of Exposure that triggered the alert.

4. Click on **n/n Reasons** to display the reasons for the alert.

5. Click on the arrow to expand or collapse the information for the alert.

6. Click on the Indicator name to display the Indicator details page.

To archive the alert:

After you view the alert, you can archive it.

1. In the list of alerts in the **Alerts** pane, select the checkbox for the alert that you want to archive.

   ○ Optionally, you can click the checkbox for **n/n objects selected** at the bottom of the pane to select all alerts in bulk.

2. At the bottom of the pane, click **Select an action** > **Archive**.

3. Click **OK**.

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.

Tenable Identity Exposure provides dashboard templates that you can use to focus on priority issues that concern your organization, including the following templates:

- **AD Compliance and Top Risks** — Compliance score, evolution, and risk criticality compliance
- **AD Risk 360** — Deviance evolution and issues by the severity level of the Indicator of Exposure
- **Password Management Risk** — Password-related issues
- **User Monitoring** — AD user evolution, user categories count
- **Native Admin Monitoring** — Administrative accounts metrics

To create a new dashboard using a template:

1. In Tenable Identity Exposure, click ⊞ or **Dashboards**. (This page also opens by default in Tenable Identity Exposure.)
2. You can do either of the following:
   - If the pane is empty: click **Add dashboards**.
   - If the pane already contains at least one dashboard: Click + > **Add new dashboard** at the top-right corner.

     The **Configure Dashboard Templates** pane opens.
3. Select the dashboards to add.
4. Click **Add dashboards**.
5. A message confirms that Tenable Identity Exposure created the dashboard and the widgets. The new dashboards appear under a tab in the **Dashboards** pane.

To add a custom dashboard:

1. In Tenable Identity Exposure, click ⊞ or **Dashboards**. (This page also opens by default in Tenable Identity Exposure.)

2. Click + > **Add new dashboard** at the top-right corner.

   The **Configure Dashboard Templates** pane opens.

3. Select the **Custom Dashboard** template at the bottom.

4. Type a name for the dashboard.

5. Click **Add dashboards**.

   A message confirms that Tenable Identity Exposure created the dashboard. The new dashboards appear under a tab in the **Dashboards** pane.

6. See Widgets for information on how to add widgets to your dashboard.

To rename a dashboard:

1. In the **Dashboards** pane, select the tab for the dashboard that you want to rename.

2. Click ... > **Edit Name** at the top-right corner.

   The **Configure the dashboard** pane opens.

3. In the **Name** box, type another name for the dashboard.

4. Click **Edit**.

   A message confirms that Tenable Identity Exposure updated the dashboard.

To delete a dashboard:

1. In the **Dashboards** pane, select the tab for the dashboard that you want to delete.

2. Click ... > **Delete dashboard** at the top-right corner.

   The **Delete the dashboard** pane opens to ask you to confirm the deletion.

3. Click **Delete**.

   A message confirms that Tenable Identity Exposure deleted the dashboard.

Widgets

Widgets in dashboards allow you to visualize your Active Directory data in the form of bar charts, line charts, and counters. You can customize widgets to display specific information and drag them around to reposition them on the dashboard.

You can add widgets to a newly created dashboard or an existing dashboard.

To add a widget to a dashboard:

1. In Tenable Identity Exposure, click ⊞ or **Dashboards**. (This page also opens by default in Tenable Identity Exposure.)
2. On the Dashboards pane, select the dashboard tab.
3. You can do one of the following:
   - If the dashboard is empty: click **Add widgets**.
   - If the dashboard already contains widgets: + > **Add widget to current dashboard** at the top-right corner.

     The **Add a widget** pane opens.
4. Click on a tile to select one of the following:
   - Bar chart
   - Line chart
   - Counter
5. In the **Name of the widget** box, type a name for the widget
6. Under **Widget Configuration**, in the **Type of data** box, click the arrow on the drop-down list to select one of the following:
   - Users count: The number of active users for the domain.
   - Deviances count: The number of deviances or security breaches detected.

  - Compliance score: A score of 0-100 that Tenable Identity Exposure computes by calculating the number of deviances detected and their severity levels.
  - Duration (for line chart): Click the arrow on the drop-down list to select the duration to display.

7. Under **Datasets Configuration**:

Datasets Configuration	
Status (User count)	Select Active, Inactive, or All.
Indicators	a. Click **Indicators** to select one or more indicators. The **Indicators of Exposure** pane opens. b. Select an indicator or indicators from the list. Optionally, you can also: ▪ Type an indicator name in the Search box. ▪ Select all indicators. ▪ Select all indicators of a specific severity level (critical, high, medium, or low). c. Click **Filter on selection**.
Domains	a. Click **Domains** to select one or more domains. The **Forests and Domains** pane opens. b. Select a domain from the list. Optionally, you can also: ▪ Type a domain name in the Search box. ▪ Select all domains. c. Click **Filter on selection**.

8. In **Name of the dataset**, type a name for the dataset.

9. Select the domain for the widget.

   Optionally, you can type a domain name in the Search box.

10. Click **Filter on selection**.

11. Optionally, you can click on **Add a new dataset** to add another dataset with different options for the widget.

12. Click **Add**.

    A message confirms that Tenable Identity Exposure added the widget.

To modify a widget:

1. In Tenable Identity Exposure, click **Dashboards**.

2. Select the dashboard that contains the widget you want to modify.

3. Select the widget.

4. Click the ✎ icon at the widget's top-right corner.

   The **Modify a widget** pane opens.

5. Modify as necessary.

6. Click **Edit**.

   A message confirms that Tenable Identity Exposure updated the widget.

To refresh a widget:

1. Select the widget.

2. Click the ↻ icon at the widget's top-right corner.

   The widget refreshes.

To delete a widget:

1. In Tenable Identity Exposure, click **Dashboards**.

2. Select the dashboard that contains the widget you want to delete.

3. Select the widget.

4. Click the 🗑 icon.

The Remove a widget pane opens. A message asks you to confirm the deletion.

5. Click **OK**.

   A message confirms that Tenable Identity Exposure deleted the widget from the dashboard.

See also

- Dashboards

Identity Explorer

Permissions: To access the configuration and data visualization for Microsoft Entra ID, your user role must have the appropriate permissions. For more information, see Set Permissions for a Role.

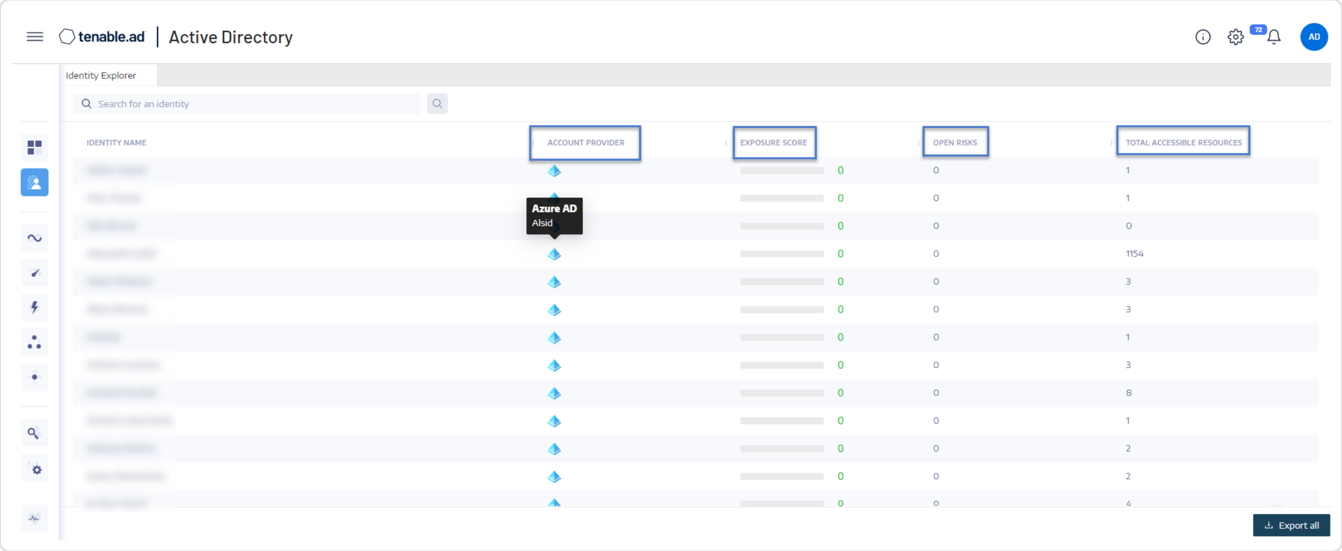
Tenable Identity Exposure's Identity Explorer view unifies identities across both Active Directory and Microsoft Entra ID . This view shows the Identity Risk Score (beta) for each listed asset and the potential reach of compromised identities.

To access the Identity Explorer:

Note: The Identity Explorer is only visible if you use the Microsoft Entra ID feature. For more information, see Microsoft Entra ID Support.

- In Tenable Identity Exposure, click on the Identity Explorer icon in the left navigation bar.

  The **Identity Explorer** pane opens.



IDENTITY NAME	ACCOUNT PROVIDER	EXPOSURE SCORE	OPEN RISKS	TOTAL ACCESSIBLE RESOURCES
[redacted]	◆	0	0	1
[redacted]	◆	0	0	1
[redacted]	◆	0	0	0
[redacted]	◆	0	0	1154
[redacted]	◆	0	0	3
[redacted]	◆	0	0	3
[redacted]	◆	0	0	1
[redacted]	◆	0	0	3
[redacted]	◆	0	0	8
[redacted]	◆	0	0	1
[redacted]	◆	0	0	2
[redacted]	◆	0	0	2
[redacted]	◆	0	0	4

The **Identity Explorer** pane shows the following information for total accessible resources:

- **Identity Name** — Name of the user account under the identity provider.
- **Account Provider** — The Identity Provider.

- **Exposure Score** — Tenable Identity Exposure calculates this metric by assessing the criticality of an asset or identity and its vulnerabilities for each identity provider, and aggregates it to provide an overall exposure score for a given identity.

  > **Note**: Tenable Identity Exposure only shows the Exposure Score if you have the Tenable One license.

- **Open Risks** — The number of findings that an Microsoft Entra ID Indicator of Exposure detects when it scans the asset. For more information, see Indicators of Exposure Related to Microsoft Entra ID.

- **Total Accessible Resources** — The number of resources of any type to which this asset has access (read, write, etc.)

To search for an identity:

1. In the **Identity Explorer** pane's **Search** box, type the name of the user or account.

2. Click the 🔍 icon.

   Tenable Identity Exposure shows the matching results.

To export identities:

1. At the bottom of the **Identity Explorer** pane, click **Export all**.

   The **Export Identities** pane opens.

2. Click **Export all**.

   Tenable Identity Exposure downloads the file to the local machine.

Trail Flow

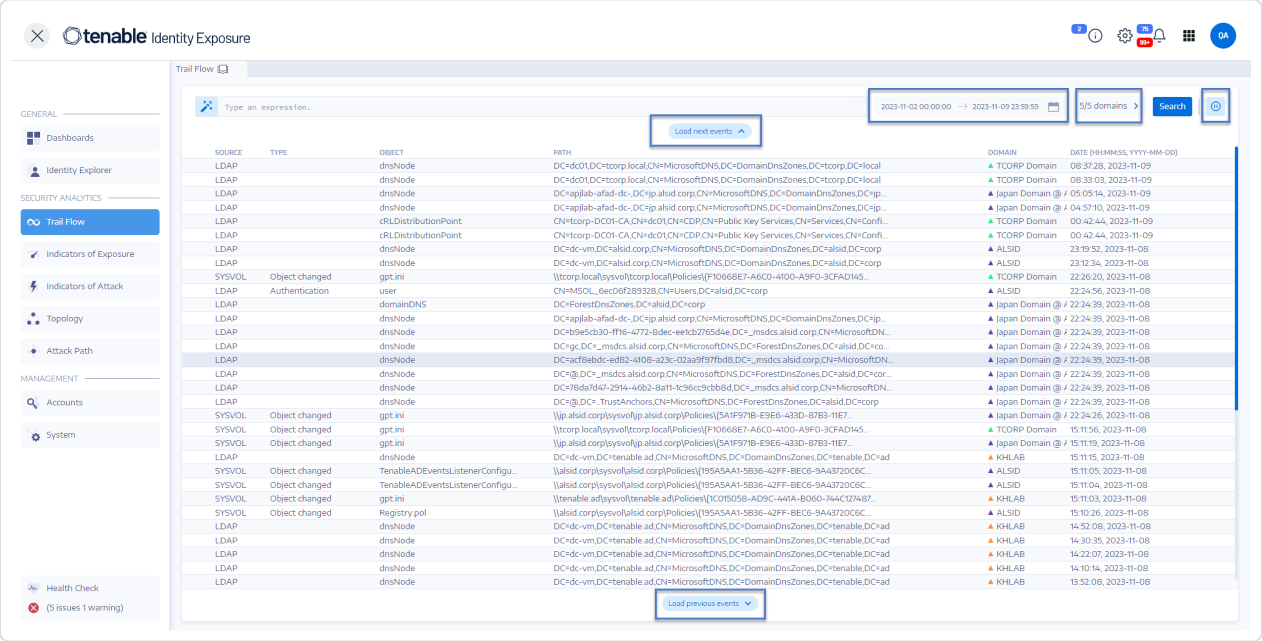
Tenable Identity Exposure's Trail Flow shows the real-time monitoring and analysis of events affecting your AD infrastructure. It allows you to identify critical vulnerabilities and their recommended courses of remediation.

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.

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:

1. At the top of the **Trail Flow** page, click on the calendar box.
2. Select a start date and an end date.
3. Click **Search**.

   Tenable Identity Exposure updates the Trail Flow table with the selected timeframe.

To select a domain:

1. At the top of the **Trail Flow** page, click **n/n domain >**.

   The **Forest and Domains** pane opens.

2. Select the forests and domains.

3. Click **Filter on selection**.

   Tenable Identity Exposure updates the Trail Flow table with information for the selected forest and domain.

To view an event:

- In the Trail Flow table, click on a line that contains the event you want to explore.

  The Event Details pane appears. For more information, see Event Details.

To pause and restart the Trail Flow:

- Do one of the following:

  - Click on the ⏸ icon to pause the Trail Flow.

    Pausing the Trail Flow stops the automatic vertical scrolling of the most recent events while the analysis continues to run in the background and allows you to run a search on events.

  - Click on the ▶ icon to restart the Trail Flow.

To load the next or previous events:

- In the Trail Flow page, do one of the following:

  - Click Load next events

  - Click Load previous events

Trail Flow Table

Tenable Identity Exposure lists the events in your Active Directory in the Trail Flow table continuously as they occur. It includes the following information:

Information	Description
Source	Indicates the origin of any security-related change in your AD infrastructures. There are two possible sources: • Lightweight Directory Access Protocol (LDAP) used to communicate with your AD infrastructure. • Server Message Block (SMB) protocol used to share files, printers, etc. **Tenable Identity Exposure** analyzes thoroughly LDAP and SMB traffic over your network to detect anomalies and potential threats. **Note**: Active Directory (AD) allows administrators to create group policies that control settings deployed on user and machine accounts. The Group Policy Object (GPO) stores these control settings. The Sysvol folder stores GPO files on the domain controller. It is important to monitor the contents of GPOs for the security of your AD because each domain member can apply or execute them with a high level of privileges.
Type	Shows the characteristic elements of an event such as: • ACL changed • SPN changed • Member removed • New member • New trust • Unknown file type added • New object • Object removed

	• Password changed • UAC changed • New GPO linked • GPO link removed • Owner change • File renamed • SPN created • Failed authentication reset • Failed authentication
Object	Indicates the class or file extension associated with an AD object. You can search for a directory object (user, computer, etc.) or a file with a specific file name extension (ini, XML, csv).
Path	Indicates the full path to an AD object to identify the unique location of this object in the AD.
Directory	Indicates the directory from which the change in your AD infrastructure came.
Date	Indicates the time of the event.

Search the Trail Flow Using the Wizard

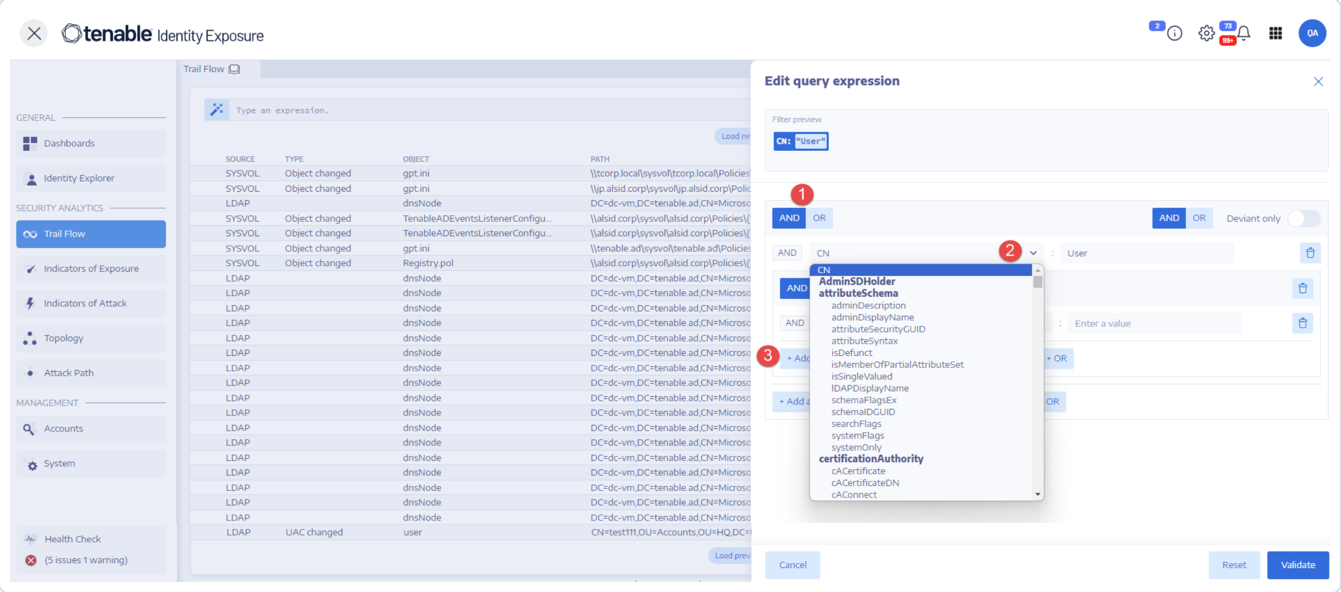
The search wizard allows you to create and combine query expressions.

- When you use frequent expressions in the search box, you can add them to a list of bookmarks for later use.
- When you enter an expression in the search box, Tenable Identity Exposure saves this expression in its History pane for you to reuse.

To search using the wizard:

1. In Tenable Identity Exposure, click **Trail Flow** to open the Trail Flow page.
2. Click on the icon.

   The **Edit Query Expression** pane opens. For more information, see [Customize Trail Flow Queries](#).



SOURCE	TYPE	OBJECT	PATH
SYSVOL	Object changed	gpt.ini	\\tcorp.local\sysvol\tcorp.local\Policies
SYSVOL	Object changed	gpt.ini	\\jp.alsid.corp\sysvol\jp.alsid.corp\Polic
LDAP		dnsNode	DC=dc-vm,DC=tenable.ad,CN=Microso
SYSVOL	Object changed	TenableADEventsListenerConfigu...	\\alsid.corp\sysvol\alsid.corp\Policies\{
SYSVOL	Object changed	TenableADEventsListenerConfigu...	\\alsid.corp\sysvol\alsid.corp\Policies\{
SYSVOL	Object changed	gpt.ini	\\tenable.ad\sysvol\tenable.ad\Policies
SYSVOL	Object changed	Registry.pol	\\alsid.corp\sysvol\alsid.corp\Policies\{
LDAP		dnsNode	DC=dc-vm,DC=tenable.ad,CN=Microso
LDAP		dnsNode	DC=dc-vm,DC=tenable.ad,CN=Microso
LDAP		dnsNode	DC=dc-vm,DC=tenable.ad,CN=Microso
LDAP		dnsNode	DC=dc-vm,DC=tenable.ad,CN=Microso
LDAP		dnsNode	DC=dc-vm,DC=tenable.ad,CN=Microso
LDAP		dnsNode	DC=dc-vm,DC=tenable.ad,CN=Microso
LDAP		dnsNode	DC=dc-vm,DC=tenable.ad,CN=Microso
LDAP		dnsNode	DC=dc-vm,DC=tenable.ad,CN=Microso
LDAP		dnsNode	DC=dc-vm,DC=tenable.ad,CN=Microso
LDAP		dnsNode	DC=dc-vm,DC=tenable.ad,CN=Microso
LDAP		dnsNode	DC=dc-vm,DC=tenable.ad,CN=Microso
LDAP		dnsNode	DC=dc-vm,DC=tenable.ad,CN=Microso
LDAP		dnsNode	DC=dc-vm,DC=tenable.ad,CN=Microso
LDAP		dnsNode	DC=dc-vm,DC=tenable.ad,CN=Microso
LDAP		dnsNode	DC=dc-vm,DC=tenable.ad,CN=Microso
LDAP		dnsNode	DC=dc-vm,DC=tenable.ad,CN=Microso
LDAP		dnsNode	DC=dc-vm,DC=tenable.ad,CN=Microso
LDAP	UAC changed	user	CN=test111,OU=Accounts,OU=HQ,DC=t

Filter preview

CN: "User"

AND CN : User

AND : Enter a value

CN
AdminSDHolder
attributeSchema
adminDescription
adminDisplayName
attributeSecurityGUID
attributeSyntax
isDefunct
isMemberOfPartialAttributeSet
isSingleValued
lDAPDisplayName
schemaFlagsEx
schemaIDGUID
searchFlags
systemFlags
systemOnly
certificationAuthority
cACertificate
cACertificateDN
cAConnect

3. To define the query expression in the panel, click on the **AND** or the **OR** operator button (1) to apply to the first condition.
4. Select an attribute from the drop-down menu and enter its value (2).
5. Do any of the following:

    - To add an attribute, click **+ Add a new rule** (3).

    - To add another condition, click **Add a new condition+AND** or **+OR** operator. Select an attribute from the drop-down menu and enter its value.

    - To restrict the search to deviant objects, click the **Deviant only** toggle to allow. Select the **+AND** or **+OR** operator to add the condition to the query.

    - To delete a condition or rule, click the 🗑 icon.

6. Click **Validate** to run the search or **Reset** to modify your query expressions.

See also

- Search the Trail Flow Manually
- Search the Trail Flow Using the Wizard
- Customize Trail Flow Queries
- Bookmark Queries
- Query History

Search the Trail Flow Manually

To filter events that match specific character strings or patterns, you can type an expression in the search box to refine results using the Boolean operators *****, **AND**, and **OR**. You can encapsulate **OR** statements with parentheses to modify search priority. The search looks for any specific value in an Active Directory attribute.

To search the Trail Flow manually:

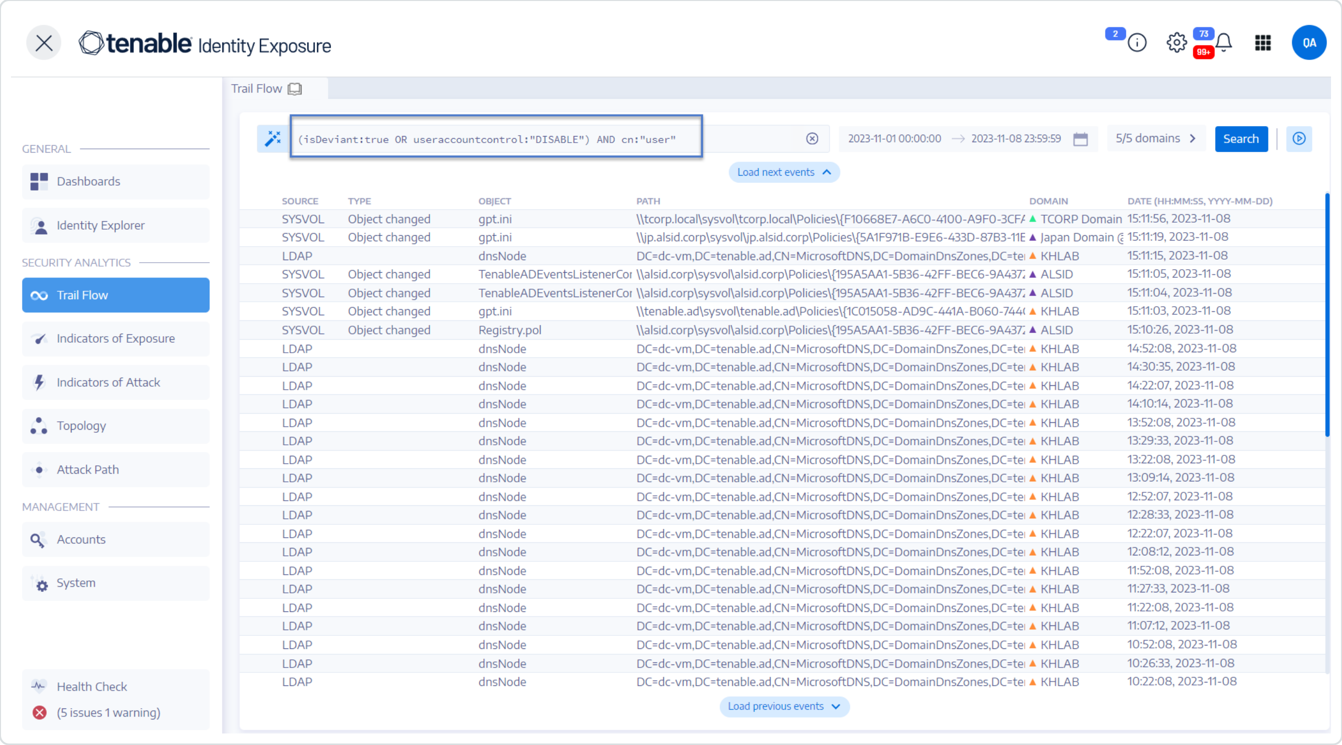
1. In Tenable Identity Exposure, click **Trail Flow** to open the Trail Flow page.
2. In the Search box, type a query expression.
3. You can filter the search results as follows:
   - Click on the **Calendar** box to select a start date and an end date.
   - Click on **n/n Domains** to select forests and domains.
4. Click **Search**.

   Tenable Identity Exposure updates the list with the results matching your search criteria.

Example:

The following example searches for:

- Deactivated user accounts that can endanger monitored AD infrastructures.
- Suspicious activities and anomalous account use.



`(isDeviant:true OR useraccountcontrol:"DISABLE") AND cn:"user"`

2023-11-01 00:00:00 → 2023-11-08 23:59:59

SOURCE	TYPE	OBJECT	PATH	DOMAIN	DATE (HH:MM:SS, YYYY-MM-DD)
SYSVOL	Object changed	gpt.ini	\\tcorp.local\sysvol\tcorp.local\Policies\{F10668E7-A6C0-4100-A9F0-3CF/	▲ TCORP Domain	15:11:56, 2023-11-08
SYSVOL	Object changed	gpt.ini	\\jp.alsid.corp\sysvol\jp.alsid.corp\Policies\{5A1F971B-E9E6-433D-87B3-11E	▲ Japan Domain @	15:11:19, 2023-11-08
LDAP		dnsNode	DC=dc-vm,DC=tenable.ad,CN=MicrosoftDNS,DC=DomainDnsZones,DC=te	▲ KHLAB	15:11:15, 2023-11-08
SYSVOL	Object changed	TenableADEventsListenerCor	\\alsid.corp\sysvol\alsid.corp\Policies\{195A5AA1-5B36-42FF-BEC6-9A437	▲ ALSID	15:11:05, 2023-11-08
SYSVOL	Object changed	TenableADEventsListenerCor	\\alsid.corp\sysvol\alsid.corp\Policies\{195A5AA1-5B36-42FF-BEC6-9A437	▲ ALSID	15:11:04, 2023-11-08
SYSVOL	Object changed	gpt.ini	\\tenable.ad\sysvol\tenable.ad\Policies\{1C015058-AD9C-441A-B060-744(	▲ KHLAB	15:11:03, 2023-11-08
SYSVOL	Object changed	Registry.pol	\\alsid.corp\sysvol\alsid.corp\Policies\{195A5AA1-5B36-42FF-BEC6-9A437	▲ ALSID	15:10:26, 2023-11-08
LDAP		dnsNode	DC=dc-vm,DC=tenable.ad,CN=MicrosoftDNS,DC=DomainDnsZones,DC=te	▲ KHLAB	14:52:08, 2023-11-08
LDAP		dnsNode	DC=dc-vm,DC=tenable.ad,CN=MicrosoftDNS,DC=DomainDnsZones,DC=te	▲ KHLAB	14:30:35, 2023-11-08
LDAP		dnsNode	DC=dc-vm,DC=tenable.ad,CN=MicrosoftDNS,DC=DomainDnsZones,DC=te	▲ KHLAB	14:22:07, 2023-11-08
LDAP		dnsNode	DC=dc-vm,DC=tenable.ad,CN=MicrosoftDNS,DC=DomainDnsZones,DC=te	▲ KHLAB	14:10:14, 2023-11-08
LDAP		dnsNode	DC=dc-vm,DC=tenable.ad,CN=MicrosoftDNS,DC=DomainDnsZones,DC=te	▲ KHLAB	13:52:08, 2023-11-08
LDAP		dnsNode	DC=dc-vm,DC=tenable.ad,CN=MicrosoftDNS,DC=DomainDnsZones,DC=te	▲ KHLAB	13:29:33, 2023-11-08
LDAP		dnsNode	DC=dc-vm,DC=tenable.ad,CN=MicrosoftDNS,DC=DomainDnsZones,DC=te	▲ KHLAB	13:22:08, 2023-11-08
LDAP		dnsNode	DC=dc-vm,DC=tenable.ad,CN=MicrosoftDNS,DC=DomainDnsZones,DC=te	▲ KHLAB	13:09:14, 2023-11-08
LDAP		dnsNode	DC=dc-vm,DC=tenable.ad,CN=MicrosoftDNS,DC=DomainDnsZones,DC=te	▲ KHLAB	12:52:07, 2023-11-08
LDAP		dnsNode	DC=dc-vm,DC=tenable.ad,CN=MicrosoftDNS,DC=DomainDnsZones,DC=te	▲ KHLAB	12:28:33, 2023-11-08
LDAP		dnsNode	DC=dc-vm,DC=tenable.ad,CN=MicrosoftDNS,DC=DomainDnsZones,DC=te	▲ KHLAB	12:22:07, 2023-11-08
LDAP		dnsNode	DC=dc-vm,DC=tenable.ad,CN=MicrosoftDNS,DC=DomainDnsZones,DC=te	▲ KHLAB	12:08:12, 2023-11-08
LDAP		dnsNode	DC=dc-vm,DC=tenable.ad,CN=MicrosoftDNS,DC=DomainDnsZones,DC=te	▲ KHLAB	11:52:08, 2023-11-08
LDAP		dnsNode	DC=dc-vm,DC=tenable.ad,CN=MicrosoftDNS,DC=DomainDnsZones,DC=te	▲ KHLAB	11:27:33, 2023-11-08
LDAP		dnsNode	DC=dc-vm,DC=tenable.ad,CN=MicrosoftDNS,DC=DomainDnsZones,DC=te	▲ KHLAB	11:22:08, 2023-11-08
LDAP		dnsNode	DC=dc-vm,DC=tenable.ad,CN=MicrosoftDNS,DC=DomainDnsZones,DC=te	▲ KHLAB	11:07:12, 2023-11-08
LDAP		dnsNode	DC=dc-vm,DC=tenable.ad,CN=MicrosoftDNS,DC=DomainDnsZones,DC=te	▲ KHLAB	10:52:08, 2023-11-08
LDAP		dnsNode	DC=dc-vm,DC=tenable.ad,CN=MicrosoftDNS,DC=DomainDnsZones,DC=te	▲ KHLAB	10:26:33, 2023-11-08
LDAP		dnsNode	DC=dc-vm,DC=tenable.ad,CN=MicrosoftDNS,DC=DomainDnsZones,DC=te	▲ KHLAB	10:22:08, 2023-11-08

Grammar and Syntax

A manual query expression uses the following grammar and syntax:

- Grammar: `EXPRESSION [OPERATOR EXPRESSION]*`
- Syntax: `__KEY__ __SELECTOR__ __VALUE__`

  where:

  - `__KEY__` refers to the AD object attribute to search (such as `CN`, `userAccountControl`, `members`, etc.)
  - `__SELECTOR__` refers to the operator: `:`, `>`, `<`, `>=`, `<=`.
  - `__VALUE__` refers to value to search for.

    You can use more keys to look for specific content:

  - `isDeviant` looks for events that created a deviance.

You can combine multiple Trail Flow query expressions using the **AND** and **OR** operators.

Examples:

- Look for all objects containing the string `alice` into the common name attribute: `cn:"alice"`
- Look for all objects containing the string `alice` in the common name attribute and which created a specific deviance: `isDeviant:"true" and cn:"alice"`
- Look for a GPO named Default Domain Policy: `objectClass:"groupPolicyContainer" and displayname:"Default Domain Policy"`
- Look for all deactivated accounts with a SID containing S-1-5-21: `userAccountControl:"DISABLE" and objectSid:"S-1-5-21"`
- Look for all `script.ini` files in Sysvol: `globalpath:"sysvol" and types:"SCRIPTSini"`

  > **Note**: Here, `types` refers to the object attribute and not the column header.

Customize Trail Flow Queries

The Trail Flow allows you to extend Tenable Identity Exposure capabilities beyond the default monitoring of Indicators of Exposure and Indicators of Attack. You can create custom queries to retrieve data quickly and also use the query as a custom alert that Tenable Identity Exposure can send to your Security Information and Event Management (SIEM).

The following examples show practical custom queries in Tenable Identity Exposure.

<table>
<tr><th>Use Case</th><th>Description</th></tr>
<tr><td>

GPO Startup and Shutdown binaries and Global SYSVOL path monitoring

</td><td>

Monitors for scripts in the boot startup path and/or the Global SYSVOL replication path. Attackers often use these scripts to abuse native AD services to proliferate ransomware quickly across an environment.

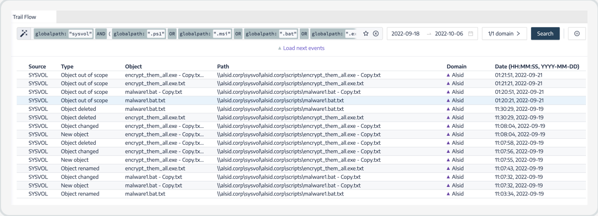
- **Scripts in startup path query:**

```
globalpath: "sysvol" AND types:
"Scriptsini"
```

> **Note**: Here, `types` refer to the object attribute and not the column header.

- **SYSVOL monitoring query**:

```
globalpath:"sysvol" AND
(globalpath:".ps1" OR globalpath:".msi"
OR globalpath:".bat" OR
globalpath:".exe")
```



Trail Flow

`globalpath: "sysvol"` `AND` (`globalpath: ".ps1"` `OR` `globalpath: ".msi"` `OR` `globalpath: ".bat"` `OR` `globalpath: ".ex`

2022-09-18 → 2022-10-06

1/1 domain >

Search

▲ Load next events

<table>
<tr><th>Source</th><th>Type</th><th>Object</th><th>Path</th><th>Domain</th><th>Date (HH:MM:SS, YYYY-MM-DD)</th></tr>
<tr><td>SYSVOL</td><td>Object out of scope</td><td>encrypt_them_all.exe - Copy.tx...</td><td>\\alsid.corp\sysvol\alsid.corp\scripts\encrypt_them_all.exe - Copy.txt</td><td>Alsid</td><td>01:21:51, 2022-09-21</td></tr>
<tr><td>SYSVOL</td><td>Object out of scope</td><td>encrypt_them_all.exe.txt</td><td>\\alsid.corp\sysvol\alsid.corp\scripts\encrypt_them_all.exe.txt</td><td>Alsid</td><td>01:21:21, 2022-09-21</td></tr>
<tr><td>SYSVOL</td><td>Object out of scope</td><td>malware1.bat - Copy.txt</td><td>\\alsid.corp\sysvol\alsid.corp\scripts\malware1.bat - Copy.txt</td><td>Alsid</td><td>01:20:51, 2022-09-21</td></tr>
<tr><td>SYSVOL</td><td>Object out of scope</td><td>malware1.bat.txt</td><td>\\alsid.corp\sysvol\alsid.corp\scripts\malware1.bat.txt</td><td>Alsid</td><td>01:20:21, 2022-09-21</td></tr>
<tr><td>SYSVOL</td><td>Object deleted</td><td>malware1.bat.txt</td><td>\\alsid.corp\sysvol\alsid.corp\scripts\malware1.bat.txt</td><td>Alsid</td><td>11:30:29, 2022-09-19</td></tr>
<tr><td>SYSVOL</td><td>Object deleted</td><td>encrypt_them_all.exe.txt</td><td>\\alsid.corp\sysvol\alsid.corp\scripts\encrypt_them_all.exe.txt</td><td>Alsid</td><td>11:30:29, 2022-09-19</td></tr>
<tr><td>SYSVOL</td><td>Object changed</td><td>encrypt_them_all.exe - Copy.tx...</td><td>\\alsid.corp\sysvol\alsid.corp\scripts\encrypt_them_all.exe - Copy.txt</td><td>Alsid</td><td>11:08:04, 2022-09-19</td></tr>
<tr><td>SYSVOL</td><td>New object</td><td>encrypt_them_all.exe - Copy.tx...</td><td>\\alsid.corp\sysvol\alsid.corp\scripts\encrypt_them_all.exe - Copy.txt</td><td>Alsid</td><td>11:08:04, 2022-09-19</td></tr>
<tr><td>SYSVOL</td><td>Object deleted</td><td>encrypt_them_all.exe - Copy.tx...</td><td>\\alsid.corp\sysvol\alsid.corp\scripts\encrypt_them_all.exe - Copy.txt</td><td>Alsid</td><td>11:07:58, 2022-09-19</td></tr>
<tr><td>SYSVOL</td><td>Object changed</td><td>encrypt_them_all.exe - Copy.tx...</td><td>\\alsid.corp\sysvol\alsid.corp\scripts\encrypt_them_all.exe - Copy.txt</td><td>Alsid</td><td>11:07:56, 2022-09-19</td></tr>
<tr><td>SYSVOL</td><td>New object</td><td>encrypt_them_all.exe - Copy.tx...</td><td>\\alsid.corp\sysvol\alsid.corp\scripts\encrypt_them_all.exe - Copy.txt</td><td>Alsid</td><td>11:07:55, 2022-09-19</td></tr>
<tr><td>SYSVOL</td><td>Object renamed</td><td>encrypt_them_all.exe.txt</td><td>\\alsid.corp\sysvol\alsid.corp\scripts\encrypt_them_all.exe.txt</td><td>Alsid</td><td>11:07:43, 2022-09-19</td></tr>
<tr><td>SYSVOL</td><td>Object changed</td><td>malware1.bat - Copy.txt</td><td>\\alsid.corp\sysvol\alsid.corp\scripts\malware1.bat - Copy.txt</td><td>Alsid</td><td>11:07:32, 2022-09-19</td></tr>
<tr><td>SYSVOL</td><td>New object</td><td>malware1.bat - Copy.txt</td><td>\\alsid.corp\sysvol\alsid.corp\scripts\malware1.bat - Copy.txt</td><td>Alsid</td><td>11:07:32, 2022-09-19</td></tr>
<tr><td>SYSVOL</td><td>Object renamed</td><td>malware1.bat.txt</td><td>\\alsid.corp\sysvol\alsid.corp\scripts\malware1.bat.txt</td><td>Alsid</td><td>11:03:34, 2022-09-19</td></tr>
</table>

</td></tr>
<tr><td>

Modifications of GPO Configuration

</td><td>

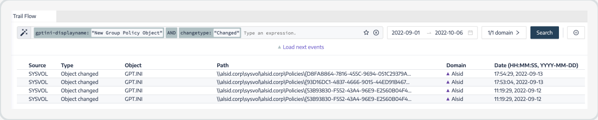
Monitors for modifications to GPO configurations. Attackers often use this method to downgrade security

</td></tr>
</table>

<table>
<tr>
<td></td>
<td>
settings to aid in persistence and/or account takeover.

- **GPO monitoring query:**

  `gptini-displayname:"New Group Policy Object" AND changetype:"Changed"`



gptini-displayname: "New Group Policy Object" AND changetype: "Changed" Type an expression.

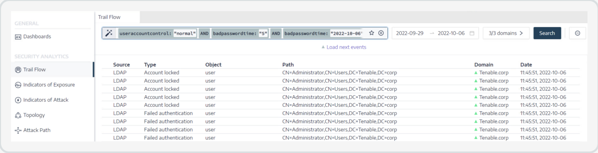
2022-09-01 → 2022-10-06 1/1 domain

<table>
<tr><th>Source</th><th>Type</th><th>Object</th><th>Path</th><th>Domain</th><th>Date (HH:MM:SS, YYYY-MM-DD)</th></tr>
<tr><td>SYSVOL</td><td>Object changed</td><td>GPT.INI</td><td>\\alsid.corp\sysvol\alsid.corp\Policies\{D8FA8864-7816-455C-9694-051C29379A...</td><td>Alsid</td><td>17:54:29, 2022-09-13</td></tr>
<tr><td>SYSVOL</td><td>Object changed</td><td>GPT.INI</td><td>\\alsid.corp\sysvol\alsid.corp\Policies\{93D16DC1-4837-4666-9015-44ED91B467...</td><td>Alsid</td><td>17:53:04, 2022-09-13</td></tr>
<tr><td>SYSVOL</td><td>Object changed</td><td>GPT.INI</td><td>\\alsid.corp\sysvol\alsid.corp\Policies\{53B93830-F552-43A4-96E9-E2560B04F4...</td><td>Alsid</td><td>11:19:29, 2022-09-12</td></tr>
<tr><td>SYSVOL</td><td>Object changed</td><td>GPT.INI</td><td>\\alsid.corp\sysvol\alsid.corp\Policies\{53B93830-F552-43A4-96E9-E2560B04F4...</td><td>Alsid</td><td>11:19:29, 2022-09-12</td></tr>
</table>
</td>
</tr>
<tr>
<td><b>Failed Authentication and Password Reset</b></td>
<td>
Monitors for multiple failed attempts to authenticate resulting in a lockout, which can act as an early warning flag for brute-force attempts.

> **Note**: You must set the lockout policy and date/time variables. For more information, see Authentication Using a Tenable Identity Exposure Account.

- **Failed authentication query:**

  `useraccountcontrol:"Normal" AND badpwdcount:"<ACCOUNT_LOCKOUT_THRESHOLD>" AND badpasswordtime:"<DATE_TIME_STAMP>"`



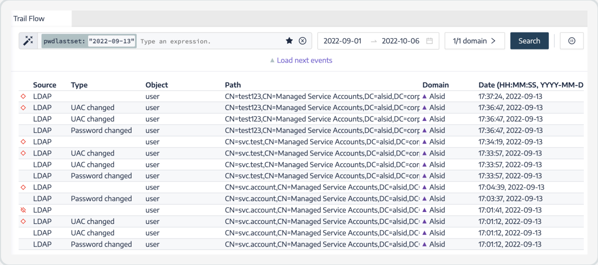
useraccountcontrol: "normal" AND badpasswordtime: "5" AND badpasswordtime: "2022-10-06"

2022-09-29 → 2022-10-06 3/3 domains

<table>
<tr><th>Source</th><th>Type</th><th>Object</th><th>Path</th><th>Domain</th><th>Date</th></tr>
<tr><td>LDAP</td><td>Account locked</td><td>user</td><td>CN=Administrator,CN=Users,DC=Tenable,DC=corp</td><td>Tenable.corp</td><td>11:45:51, 2022-10-06</td></tr>
<tr><td>LDAP</td><td>Account locked</td><td>user</td><td>CN=Administrator,CN=Users,DC=Tenable,DC=corp</td><td>Tenable.corp</td><td>11:45:51, 2022-10-06</td></tr>
<tr><td>LDAP</td><td>Account locked</td><td>user</td><td>CN=Administrator,CN=Users,DC=Tenable,DC=corp</td><td>Tenable.corp</td><td>11:45:51, 2022-10-06</td></tr>
<tr><td>LDAP</td><td>Account locked</td><td>user</td><td>CN=Administrator,CN=Users,DC=Tenable,DC=corp</td><td>Tenable.corp</td><td>11:45:51, 2022-10-06</td></tr>
<tr><td>LDAP</td><td>Account locked</td><td>user</td><td>CN=Administrator,CN=Users,DC=Tenable,DC=corp</td><td>Tenable.corp</td><td>11:45:51, 2022-10-06</td></tr>
<tr><td>LDAP</td><td>Failed authentication</td><td>user</td><td>CN=Administrator,CN=Users,DC=Tenable,DC=corp</td><td>Tenable.corp</td><td>11:45:51, 2022-10-06</td></tr>
<tr><td>LDAP</td><td>Failed authentication</td><td>user</td><td>CN=Administrator,CN=Users,DC=Tenable,DC=corp</td><td>Tenable.corp</td><td>11:45:51, 2022-10-06</td></tr>
<tr><td>LDAP</td><td>Failed authentication</td><td>user</td><td>CN=Administrator,CN=Users,DC=Tenable,DC=corp</td><td>Tenable.corp</td><td>11:45:51, 2022-10-06</td></tr>
<tr><td>LDAP</td><td>Failed authentication</td><td>user</td><td>CN=Administrator,CN=Users,DC=Tenable,DC=corp</td><td>Tenable.corp</td><td>11:45:51, 2022-10-06</td></tr>
</table>

- **Password reset query:**

  `pwdlastset:"<DATE_TIME_STAMP"`
</td>
</tr>
</table>

<table>
<tr>
<td></td>
<td>


Trail Flow

pwdlastset: "2022-09-13" Type an expression. | 2022-09-01 → 2022-10-06 | 1/1 domain > | Search

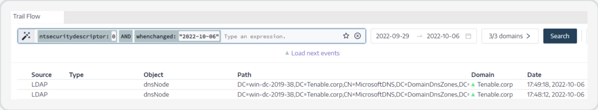
▲ Load next events

<table>
<tr><th></th><th>Source</th><th>Type</th><th>Object</th><th>Path</th><th>Domain</th><th>Date (HH:MM:SS, YYYY-MM-D</th></tr>
<tr><td>◇</td><td>LDAP</td><td></td><td>user</td><td>CN=test123,CN=Managed Service Accounts,DC=alsid,DC=corp</td><td>▲ Alsid</td><td>17:37:24, 2022-09-13</td></tr>
<tr><td>◇</td><td>LDAP</td><td>UAC changed</td><td>user</td><td>CN=test123,CN=Managed Service Accounts,DC=alsid,DC=corp</td><td>▲ Alsid</td><td>17:36:47, 2022-09-13</td></tr>
<tr><td></td><td>LDAP</td><td>UAC changed</td><td>user</td><td>CN=test123,CN=Managed Service Accounts,DC=alsid,DC=corp</td><td>▲ Alsid</td><td>17:36:47, 2022-09-13</td></tr>
<tr><td></td><td>LDAP</td><td>Password changed</td><td>user</td><td>CN=test123,CN=Managed Service Accounts,DC=alsid,DC=corp</td><td>▲ Alsid</td><td>17:36:47, 2022-09-13</td></tr>
<tr><td>◇</td><td>LDAP</td><td></td><td>user</td><td>CN=svc.test,CN=Managed Service Accounts,DC=alsid,DC=cor</td><td>▲ Alsid</td><td>17:34:19, 2022-09-13</td></tr>
<tr><td>◇</td><td>LDAP</td><td>UAC changed</td><td>user</td><td>CN=svc.test,CN=Managed Service Accounts,DC=alsid,DC=cor</td><td>▲ Alsid</td><td>17:33:57, 2022-09-13</td></tr>
<tr><td></td><td>LDAP</td><td>UAC changed</td><td>user</td><td>CN=svc.test,CN=Managed Service Accounts,DC=alsid,DC=cor</td><td>▲ Alsid</td><td>17:33:57, 2022-09-13</td></tr>
<tr><td></td><td>LDAP</td><td>Password changed</td><td>user</td><td>CN=svc.test,CN=Managed Service Accounts,DC=alsid,DC=cor</td><td>▲ Alsid</td><td>17:33:57, 2022-09-13</td></tr>
<tr><td>◇</td><td>LDAP</td><td></td><td>user</td><td>CN=svc.account,CN=Managed Service Accounts,DC=alsid,DC=</td><td>▲ Alsid</td><td>17:04:39, 2022-09-13</td></tr>
<tr><td></td><td>LDAP</td><td>Password changed</td><td>user</td><td>CN=svc.account,CN=Managed Service Accounts,DC=alsid,DC=</td><td>▲ Alsid</td><td>17:03:37, 2022-09-13</td></tr>
<tr><td>◇</td><td>LDAP</td><td></td><td>user</td><td>CN=svc.account,CN=Managed Service Accounts,DC=alsid,DC=</td><td>▲ Alsid</td><td>17:01:41, 2022-09-13</td></tr>
<tr><td>◇</td><td>LDAP</td><td>UAC changed</td><td>user</td><td>CN=svc.account,CN=Managed Service Accounts,DC=alsid,DC=</td><td>▲ Alsid</td><td>17:01:12, 2022-09-13</td></tr>
<tr><td></td><td>LDAP</td><td>UAC changed</td><td>user</td><td>CN=svc.account,CN=Managed Service Accounts,DC=alsid,DC=</td><td>▲ Alsid</td><td>17:01:12, 2022-09-13</td></tr>
<tr><td></td><td>LDAP</td><td>Password changed</td><td>user</td><td>CN=svc.account,CN=Managed Service Accounts,DC=alsid,DC=</td><td>▲ Alsid</td><td>17:01:12, 2022-09-13</td></tr>
</table>
</td>
</tr>
<tr>
<td><b>Object Permissions Added, Removed, or Changed</b></td>
<td>
Monitors for unauthorized modifications to ACL rights and related object permission sets. Attackers abuse this method to elevate permissions.

> **Note**: You must supply the date/time variable.

- **Object permissions query:**

```
ntsecuritydescriptor:0 AND
whenchanged:"DATE_TIME_STAMP"
```



Trail Flow

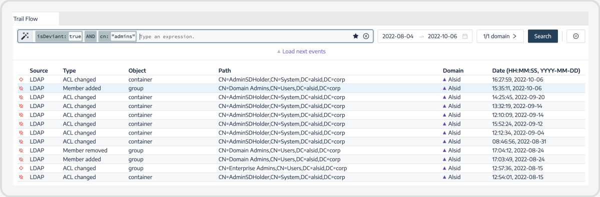
ntsecuritydescriptor: 0 AND whenchanged: "2022-10-06" Type an expression. | 2022-09-29 → 2022-10-06 | 3/3 domains > | Search

▲ Load next events

<table>
<tr><th>Source</th><th>Type</th><th>Object</th><th>Path</th><th>Domain</th><th>Date</th></tr>
<tr><td>LDAP</td><td></td><td>dnsNode</td><td>DC=win-dc-2019-38,DC=Tenable.corp,CN=MicrosoftDNS,DC=DomainDnsZones,DC=</td><td>▲ Tenable.corp</td><td>17:49:18, 2022-10-06</td></tr>
<tr><td>LDAP</td><td></td><td>dnsNode</td><td>DC=win-dc-2019-38,DC=Tenable.corp,CN=MicrosoftDNS,DC=DomainDnsZones,DC=</td><td>▲ Tenable.corp</td><td>17:48:12, 2022-10-06</td></tr>
</table>
</td>
</tr>
<tr>
<td><b>Changes to Admins Resulting in a Deviance</b></td>
<td>
Built-in Administrative groups and custom groups are sensitive groups that require close monitoring for deviances or configuration changes that can introduce risk. This query lets you quickly review recent changes that could have adversely affected security settings within the admins group.

- **Changes to Admins query:**

```
isDeviant:true AND cn:"admins"
```
</td>
</tr>
</table>



Trail Flow

`isDeviant: true` AND `cn: "admins"` Type an expression.

2022-08-04 → 2022-10-06

1/1 domain >

▲ Load next events

	Source	Type	Object	Path	Domain	Date (HH:MM:SS, YYYY-MM-DD)
◇	LDAP	ACL changed	container	CN=AdminSDHolder,CN=System,DC=alsid,DC=corp	▲ Alsid	16:27:59, 2022-10-06
⊘	LDAP	Member added	group	CN=Domain Admins,CN=Users,DC=alsid,DC=corp	▲ Alsid	15:35:11, 2022-10-06
⊘	LDAP	ACL changed	container	CN=AdminSDHolder,CN=System,DC=alsid,DC=corp	▲ Alsid	14:25:45, 2022-09-20
⊘	LDAP	ACL changed	container	CN=AdminSDHolder,CN=System,DC=alsid,DC=corp	▲ Alsid	13:32:19, 2022-09-14
⊘	LDAP	ACL changed	container	CN=AdminSDHolder,CN=System,DC=alsid,DC=corp	▲ Alsid	12:10:09, 2022-09-14
⊘	LDAP	ACL changed	container	CN=AdminSDHolder,CN=System,DC=alsid,DC=corp	▲ Alsid	15:52:24, 2022-09-12
⊘	LDAP	ACL changed	container	CN=AdminSDHolder,CN=System,DC=alsid,DC=corp	▲ Alsid	12:12:34, 2022-09-04
⊘	LDAP	ACL changed	container	CN=AdminSDHolder,CN=System,DC=alsid,DC=corp	▲ Alsid	08:46:56, 2022-08-31
⊘	LDAP	Member removed	group	CN=Domain Admins,CN=Users,DC=alsid,DC=corp	▲ Alsid	17:04:12, 2022-08-24
⊘	LDAP	Member added	group	CN=Domain Admins,CN=Users,DC=alsid,DC=corp	▲ Alsid	17:03:49, 2022-08-24
◇	LDAP	ACL changed	group	CN=Enterprise Admins,CN=Users,DC=alsid,DC=corp	▲ Alsid	12:57:36, 2022-08-15
⊘	LDAP	ACL changed	container	CN=AdminSDHolder,CN=System,DC=alsid,DC=corp	▲ Alsid	12:54:01, 2022-08-15

See also

- Search the Trail Flow Manually
- Search the Trail Flow Using the Wizard
- Bookmark Queries
- Query History
- Trail Flow Use Cases

Bookmark Queries

When you use frequent query expressions, you can add them to a list of customized bookmarks to use again.

To bookmark a query expression:

1. In Tenable Identity Exposure, click **Trail Flow** to open the Trail Flow page.
2. Click the 🪄 icon next to the Search box.

   The **Edit Query Expression** pane opens.
3. Type a query expression in the Search box.
4. Click the ☆ icon at the right of the Search box.

   The **Add to Your Bookmarks** box appears.
5. In the **Choose a folder** box, click the drop-down arrow to select a folder from the list.
6. (Optional) Click the **Create a new folder** toggle to **Yes**. In the **Name of the folder** box, type a name for the bookmarks folder.
7. In the **Name of the bookmark** box, type a name for the bookmark.
8. Click **Add**.

   A message confirms that Tenable Identity Exposure added the bookmark to the list.

To use a bookmarked query expression:

1. In Tenable Identity Exposure, click **Trail Flow** to open the Trail Flow page.
2. Click inside the Search box.

   The **History** and **Bookmarks** tab appear under the Search box.
3. Click the **Bookmarks** tab.

   The list of bookmarks appears.
4. Click the bookmark to select it.

   Tenable Identity Exposure loads the query expression and runs the search.

To manage your bookmarks:

1. In Tenable Identity Exposure, click **Trail Flow** to open the Trail Flow page.
2. Click inside the Search box.

   The **History** and **Bookmarks** tab appear under the Search box.
3. Click the **Bookmarks** tab.

   The list of bookmarks appears.
4. Click **Manage your bookmarks**.

   The **Bookmarks** pane opens.
5. Do any of the following:

   - Search for a bookmark:

     a. Type the bookmark name in the Search box.

     b. Select a folder from the drop-down list.

   - Edit the name of a bookmark or a bookmark folder:

     a. Click the ✎ icon for the bookmark or bookmark folder.

     b. In the **Name of the bookmark** or **Name of the folder** box, type a new name for the bookmark or the bookmark folder.

     c. Click **Edit**.

        A message confirms that Tenable Identity Exposure updated the bookmark or bookmark folder name.

   - Delete a bookmark of bookmark folder:

     - Click the 🗑 icon for the bookmark or bookmark folder.

See also

- Search the Trail Flow Manually
- Search the Trail Flow Using the Wizard

- Customize Trail Flow Queries
- Query History
- Trail Flow Use Cases

Query History

When you enter an expression in the search box,Tenable Identity Exposure saves this expression in its History pane for you to reuse.

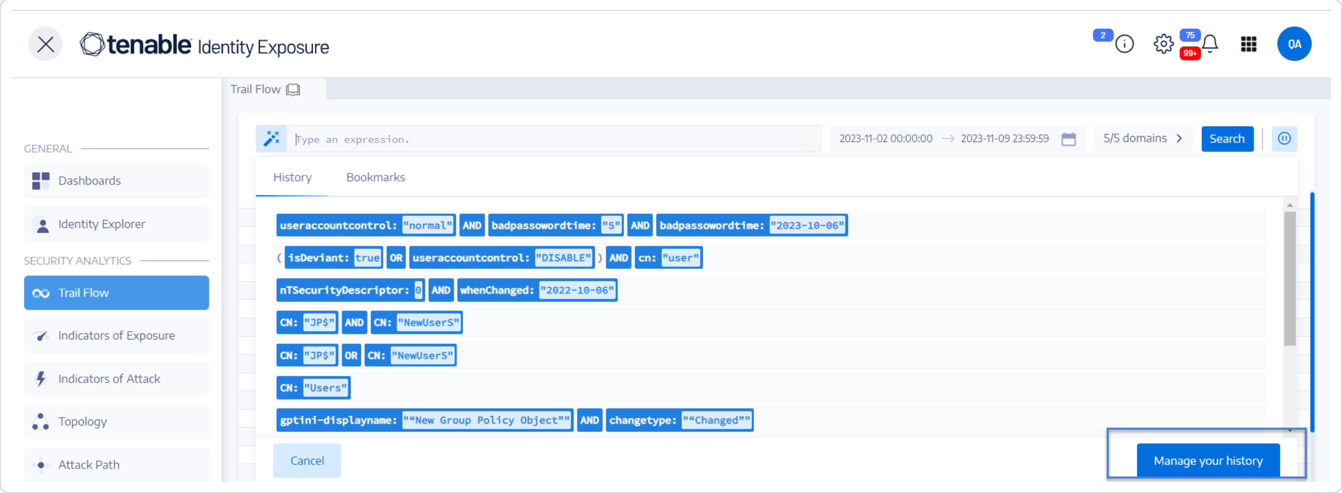
To use a query expression in the history:

1. In Tenable Identity Exposure, click **Trail Flow** to open the Trail Flow page.
2. Click inside the Search box.

   The **History** and **Bookmarks** tab appear under the Search box.
3. Click the **History** tab.

   The list of query expressions appears.
4. Click to select a query expression to use.

   Tenable Identity Exposure loads the query expression and runs the search.



```
useraccountcontrol: "normal" AND badpassowordtime: "5" AND badpassowordtime: "2023-10-06"
( isDeviant: true OR useraccountcontrol: "DISABLE" ) AND cn: "user"
nTSecurityDescriptor: 0 AND whenChanged: "2022-10-06"
CN: "JP$" AND CN: "NewUserS"
CN: "JP$" OR CN: "NewUserS"
CN: "Users"
gptini-displayname: "“New Group Policy Object”" AND changetype: "“Changed”"
```

To manage your query expression history:

1. In Tenable Identity Exposure, click **Trail Flow** to open the Trail Flow page.
2. Click inside the Search box.

   The **History** and **Bookmarks** tab appear under the Search box.
3. Click the **History** tab.

The list of query expressions appears.

4. Click **Manage your history**.

   The **History** pane opens.

5. Do any of the following:

- Search for a query expression:

  a. Type a query expression in the Search box.

  b. Click the calendar box to select a start date and an end date.

  c. Click **Search**.

- To delete a query expression from the history:

  - Click the 🗑 icon.

- To clear all query expressions from the history:

  a. Click **Clear selection**.

     A message asks you to confirm the deletions.

  b. Click **Confirm**.

See also

- Search the Trail Flow Manually
- Search the Trail Flow Using the Wizard
- Customize Trail Flow Queries
- Bookmark Queries
- Trail Flow Use Cases

Display Deviant Events

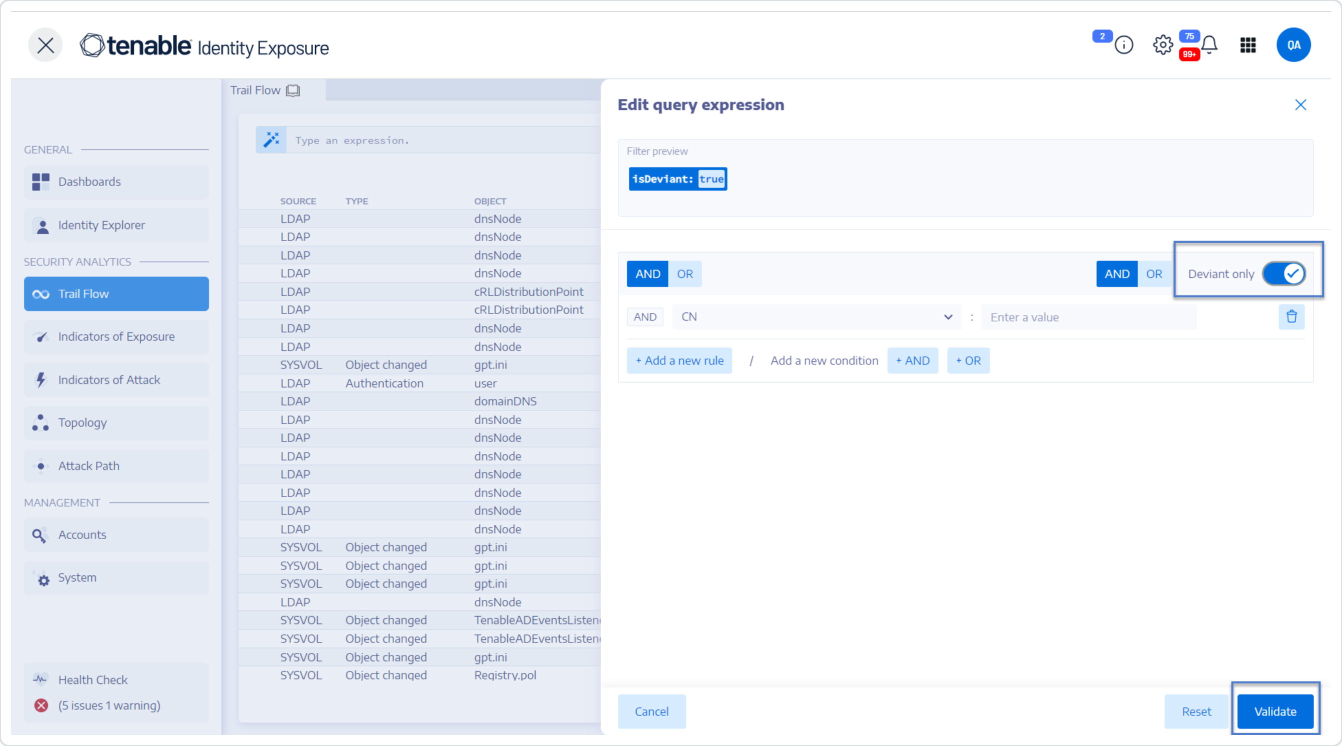
You can zero in directly on deviant events in the Trail Flow table.

To display only deviant events:

1. In Tenable Identity Exposure, click **Trail Flow** to open the Trail Flow page.

2. Click the icon next to the Search box.

   The **Edit Query Expression** pane opens.



Filter preview

`isDeviant: true`

Deviant only: on

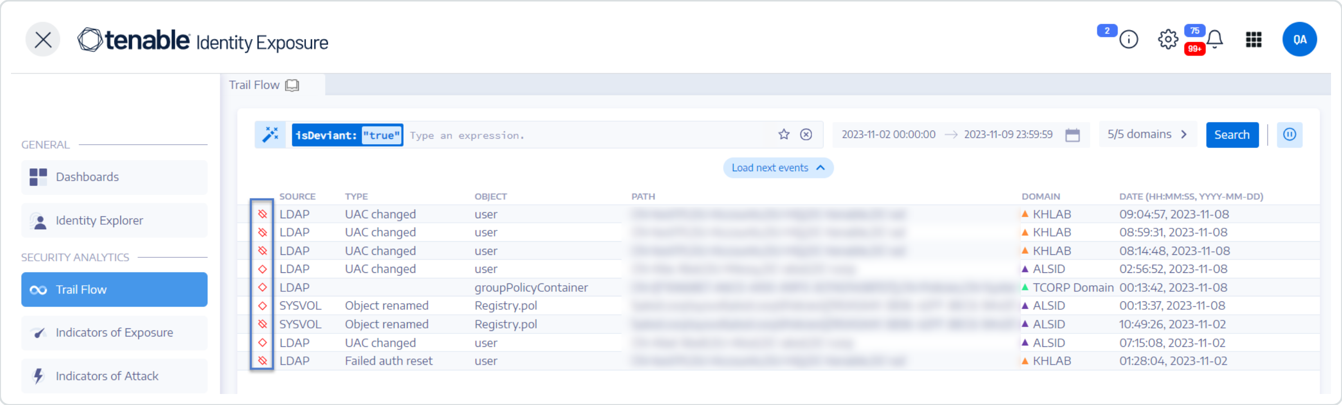
AND CN : Enter a value

SOURCE	TYPE	OBJECT
LDAP		dnsNode
LDAP		dnsNode
LDAP		dnsNode
LDAP		dnsNode
LDAP		cRLDistributionPoint
LDAP		cRLDistributionPoint
LDAP		dnsNode
LDAP		dnsNode
SYSVOL	Object changed	gpt.ini
LDAP	Authentication	user
LDAP		domainDNS
LDAP		dnsNode
LDAP		dnsNode
LDAP		dnsNode
LDAP		dnsNode
LDAP		dnsNode
LDAP		dnsNode
LDAP		dnsNode
SYSVOL	Object changed	gpt.ini
SYSVOL	Object changed	gpt.ini
SYSVOL	Object changed	gpt.ini
LDAP		dnsNode
SYSVOL	Object changed	TenableADEventsListen
SYSVOL	Object changed	TenableADEventsListen
SYSVOL	Object changed	gpt.ini
SYSVOL	Object changed	Registry.pol

3. Click the **Deviant only** toggle to Allow.

4. Click **Validate**.

   Tenable Identity Exposure updates the Trail Flow table with a list of events with a red diamond next to the source.



isDeviant: "true" Type an expression.

2023-11-02 00:00:00 → 2023-11-09 23:59:59

	SOURCE	TYPE	OBJECT	PATH	DOMAIN	DATE (HH:MM:SS, YYYY-MM-DD)
⊘	LDAP	UAC changed	user	[redacted]	▲ KHLAB	09:04:57, 2023-11-08
⊘	LDAP	UAC changed	user	[redacted]	▲ KHLAB	08:59:31, 2023-11-08
⊘	LDAP	UAC changed	user	[redacted]	▲ KHLAB	08:14:48, 2023-11-08
◇	LDAP	UAC changed	user	[redacted]	▲ ALSID	02:56:52, 2023-11-08
◇	LDAP		groupPolicyContainer	[redacted]	▲ TCORP Domain	00:13:42, 2023-11-08
◇	SYSVOL	Object renamed	Registry.pol	[redacted]	▲ ALSID	00:13:37, 2023-11-08
⊘	SYSVOL	Object renamed	Registry.pol	[redacted]	▲ ALSID	10:49:26, 2023-11-02
◇	LDAP	UAC changed	user	[redacted]	▲ ALSID	07:15:08, 2023-11-02
⊘	LDAP	Failed auth reset	user	[redacted]	▲ KHLAB	01:28:04, 2023-11-02

where:

- ◇ The Trail Flow detected a deviance in the Tenable Identity Exposure security profile.
- ◆ The Trail Flow detected a deviance in other security profiles.
- ⊘ Shows that changes resolved the deviance.

Event Details

The Trail Flow in Tenable Identity Exposure provides detailed information on each event affecting your Active Directory (AD). Details on a specific event allow you to review technical information and take remedial actions that the Indicator of Exposure (IoE)'s severity level requires.

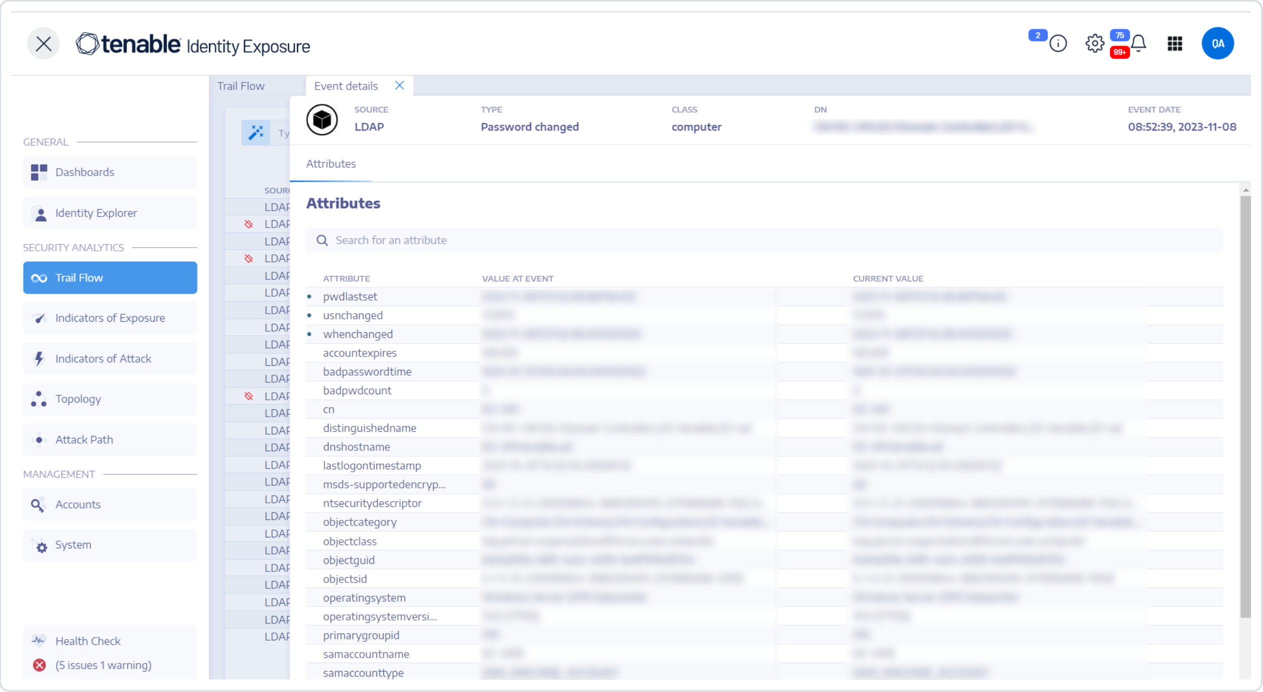
To view event details:

1. In Tenable Identity Exposure, click **Trail Flow** to open the Trail Flow page.
2. Click to select an entry in the Trail Flow table.

   The **Event details** pane opens.

IoE, Event, and Deviant Object

- An **Indicator of Exposure** (IoE) describes a threat that affects the AD. Tenable Identity Exposure's IoEs assesses security levels after receiving an event in real time. IoEs can include several technical vulnerabilities. IoEs provide information on detected vulnerabilities, associated deviant objects, and recommendations for remedial actions.
- An **event** indicates a change related to security that can appear in an AD. It can be a password change, a user creation, a new or modified GPO, or a new delegated right, etc. An event can change the compliance status of an IoE from compliant to non-compliant.
- A **deviant object** is a technical element — either on its own or associated with another deviant object — that allows the IoE's attack vector to work.



SOURCE	TYPE	CLASS	DN	EVENT DATE
LDAP	Password changed	computer	[redacted]	08:52:39, 2023-11-08

Attributes

ATTRIBUTE	VALUE AT EVENT	CURRENT VALUE
• pwdlastset	[redacted]	[redacted]
• usnchanged	[redacted]	[redacted]
• whenchanged	[redacted]	[redacted]
accountexpires	[redacted]	[redacted]
badpasswordtime	[redacted]	[redacted]
badpwdcount	[redacted]	[redacted]
cn	[redacted]	[redacted]
distinguishedname	[redacted]	[redacted]
dnshostname	[redacted]	[redacted]
lastlogontimestamp	[redacted]	[redacted]
msds-supportedencryp...	[redacted]	[redacted]
ntsecuritydescriptor	[redacted]	[redacted]
objectcategory	[redacted]	[redacted]
objectclass	[redacted]	[redacted]
objectguid	[redacted]	[redacted]
objectsid	[redacted]	[redacted]
operatingsystem	[redacted]	[redacted]
operatingsystemversi...	[redacted]	[redacted]
primarygroupid	[redacted]	[redacted]
samaccountname	[redacted]	[redacted]
samaccounttype	[redacted]	[redacted]

Attributes Table

The Attributes table includes the following columns:

Column	Description
Attributes	Indicates the attributes of the AD object associated with the event that you selected in the Trail Flow table. Attributes describe the object characteristics. Multiple attributes can describe a single AD object.
Value at event	Indicates the attribute value at the time that the event occurred.
Current value	Indicates the value of the attribute in the AD at the moment when you are viewing it.

Tip: To display the value of the attribute before the event occurred, hover the blue dot on the left (if any).

To search for an attribute:

- In the **Event details** pane, type a string in the Search box.

  Tenable Identity Exposure narrows the list to attributes matching the search string.

For more information, see Attribute Changes.

Deviances

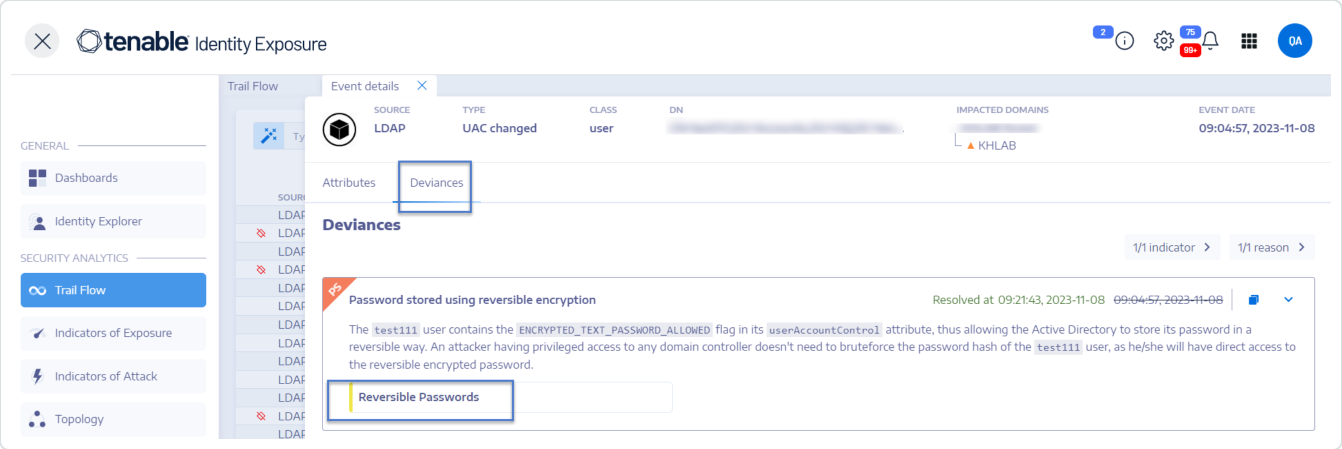
If an event in the Trail Flow contains deviances, the Event Details pane also displays them to allow you to drill down to the source of the problem.

To display deviances:

1. In Tenable Identity Exposure, click **Trail Flow** to open the Trail Flow page.
2. Click to select an entry in the Trail Flow table.

   The **Event details** pane opens.
3. Select the **Deviances** tab.

   Tenable Identity Exposure displays the list of deviances and the IoEs that triggered them.



SOURCE: LDAP
TYPE: UAC changed
CLASS: user
DN: [redacted]
IMPACTED DOMAINS: [redacted] KHLAB
EVENT DATE: 09:04:57, 2023-11-08

Deviances

Password stored using reversible encryption — Resolved at 09:21:43, 2023-11-08 ~~09:04:57, 2023-11-08~~

The `test111` user contains the `ENCRYPTED_TEXT_PASSWORD_ALLOWED` flag in its `userAccountControl` attribute, thus allowing the Active Directory to store its password in a reversible way. An attacker having privileged access to any domain controller doesn't need to bruteforce the password hash of the `test111` user, as he/she will have direct access to the reversible encrypted password.

Reversible Passwords

To drill-down to IoE details:

1. In the **Deviances** tab, click on the IoE tile below the reason for the deviance.

   The **Indicator details** pane opens with a list of deviant objects and the following information:

   - Name of the IoE
   - The severity of the IoE (Critical, High, Medium, Low)

- The IoE status
- The timestamp of the latest detection

2. Click on any of the following tabs:
    - **Information** — Includes internal and external resources on the IoE.
    - **Vulnerability details** — Provides explanations for the weakness detected in your AD.
    - **Deviant objects** — Includes technical details and a search box to filter for objects.
    - **Recommendations** — Includes tips on how to solve the issue.

Attribute Changes

When the value of an attribute changes, the Trail Flow shows a blue dot before the **Attribute** column.

To display the attribute change:

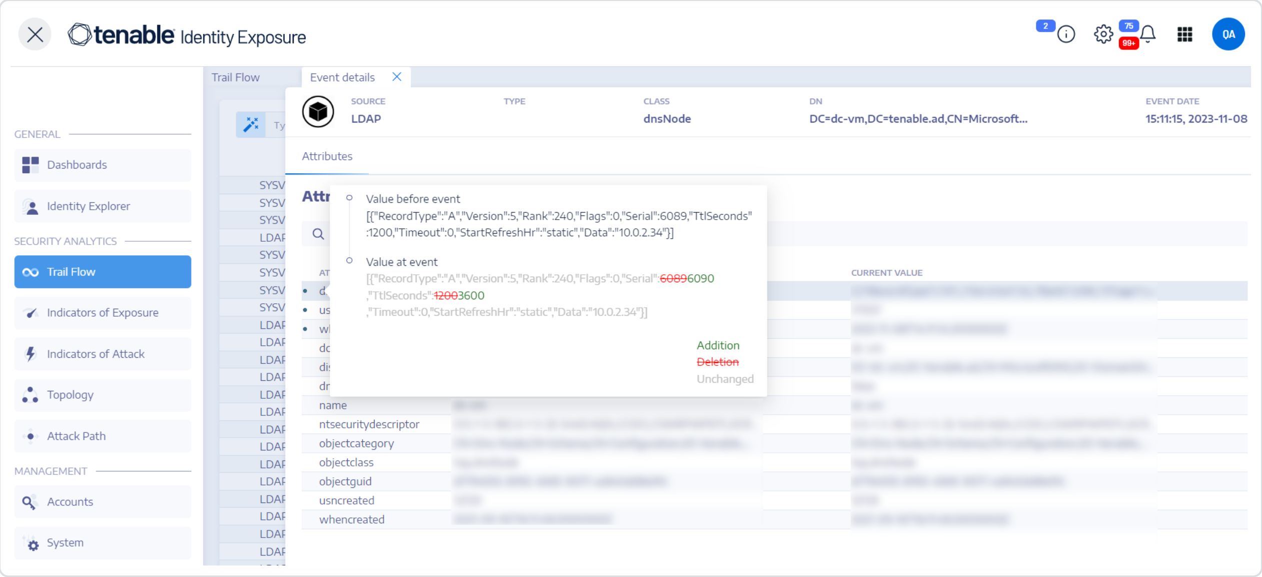
1. In Tenable Identity Exposure, click **Trail Flow** in the navigation bar on the left.

   The **Trail Flow** page opens with a list of events

2. Hover the blue dot in front of the event line to display the changes.

   The color of the **Value at event** label depends on the changes applied to the attribute:

   - Green — **Addition**
   - Red — **Deletion**
   - Gray — **Unchanged**



SOURCE	TYPE	CLASS	DN	EVENT DATE
LDAP		dnsNode	DC=dc-vm,DC=tenable.ad,CN=Microsoft...	15:11:15, 2023-11-08

Value before event
[{"RecordType":"A","Version":5,"Rank":240,"Flags":0,"Serial":6089,"TtlSeconds":1200,"Timeout":0,"StartRefreshHr":"static","Data":"10.0.2.34"}]

Value at event
[{"RecordType":"A","Version":5,"Rank":240,"Flags":0,"Serial":~~6089~~6090,"TtlSeconds":~~1200~~3600,"Timeout":0,"StartRefreshHr":"static","Data":"10.0.2.34"}]

Addition
~~Deletion~~
Unchanged

name
ntsecuritydescriptor
objectcategory
objectclass
objectguid
usncreated
whencreated

Attribute "ntsecuritydescriptor"

A security descriptor is a data structure that contains security information about an AD object such as its ownership and permissions. For more details, see Microsoft's online documentation.

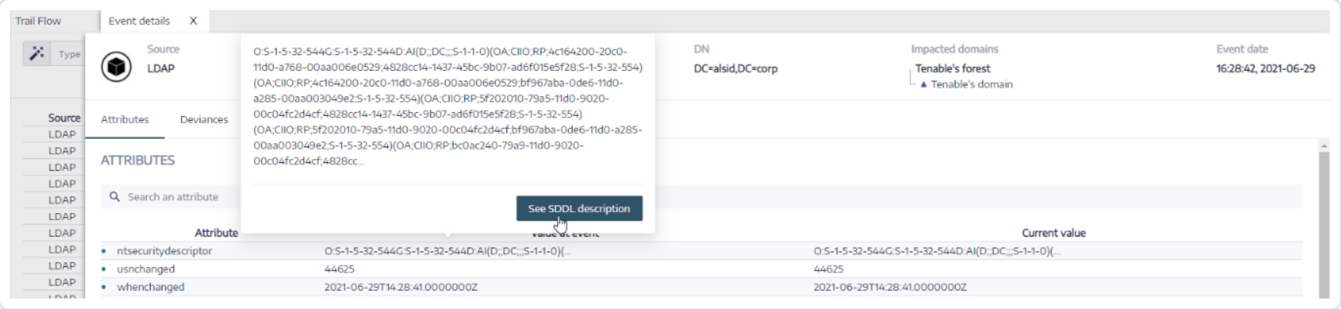
To display details of an object security descriptor:

1. In Tenable Identity Exposure, click **Trail Flow** to open the Trail Flow page.

2. Click to select an entry in the Trail Flow table.

   The **Event details** pane opens.

3. Hover over the `ntsecuritydescriptor` attribute entry (Value at event or Current value column) **.

   O:S-1-5-32-544G:S-1-5-32-544D:AI(D;;DC;;;S-1-1-0)(OA;CIIO;RP;4c164200-20c0-11d0-a768-00aa006e0529;4828cc14-1437-45bc-9b07-ad6f015e5f28;S-1-5-32-554)(OA;CIIO;RP;4c164200-20c0-11d0-a768-00aa006e0529;bf967aba-0de6-11d0-a285-00aa003049e2;S-1-5-32-554)(OA;CIIO;RP;5f202010-79a5-11d0-9020-00c04fc2d4cf;4828cc14-1437-45bc-9b07-ad6f015e5f28;S-1-5-32-554)(OA;CIIO;RP;5f202010-79a5-11d0-9020-00c04fc2d4cf;bf967aba-0de6-11d0-a285-00aa003049e2;S-1-5-32-554)(OA;CIIO;RP;bc0ac240-79a9-11d0-9020-00c04fc2d4cf;4828cc...

   Source: LDAP

   DN: DC=alsid,DC=corp

   Impacted domains: Tenable's forest
   ▲ Tenable's domain

   Event date: 16:28:42, 2021-06-29

Source
LDAP
LDAP
LDAP
LDAP
LDAP
LDAP
LDAP
LDAP
LDAP
LDAP

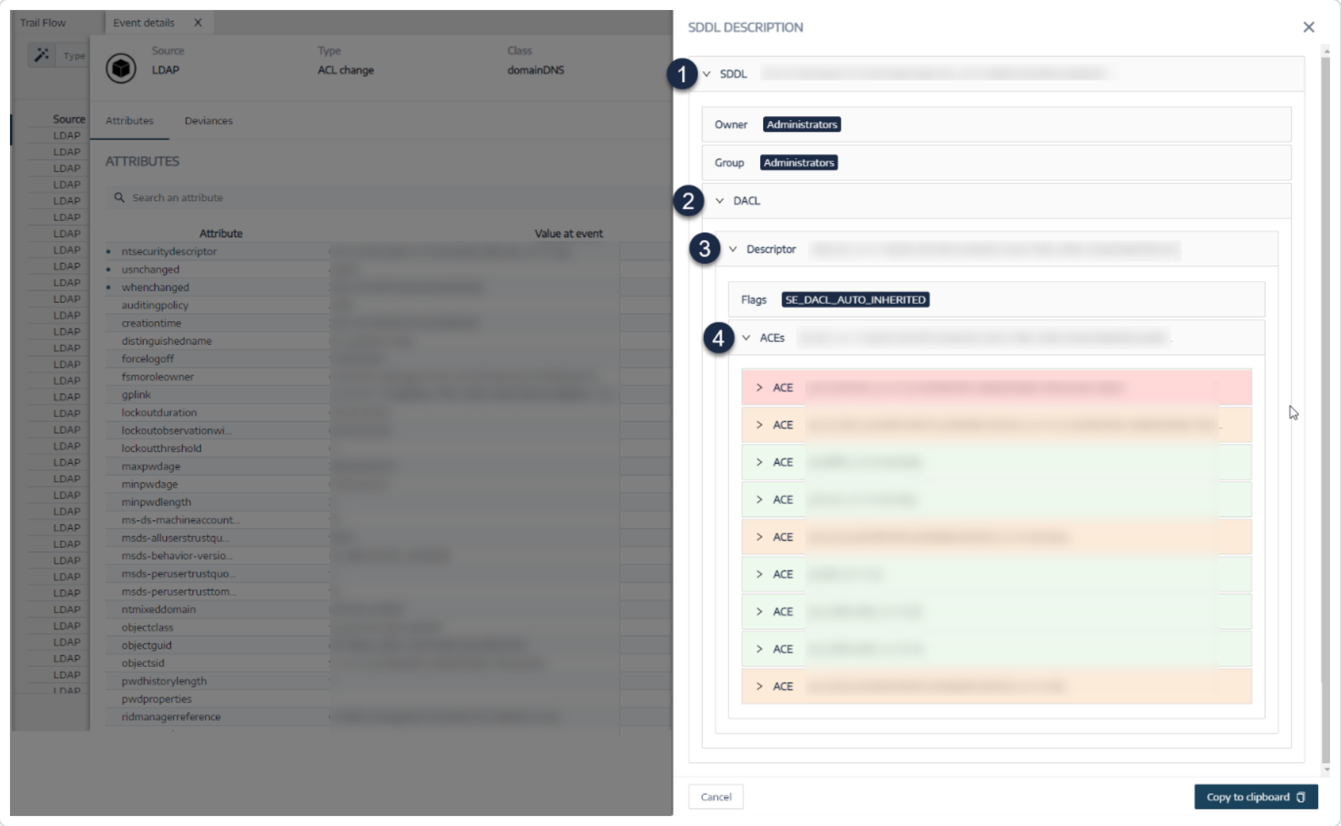
Attribute	Value at event	Current value
• ntsecuritydescriptor	O:S-1-5-32-544G:S-1-5-32-544D:AI(D;;DC;;;S-1-1-0)(...	O:S-1-5-32-544G:S-1-5-32-544D:AI(D;;DC;;;S-1-1-0)(...
• usnchanged	44625	44625
• whenchanged	2021-06-29T14:28:41.0000000Z	2021-06-29T14:28:41.0000000Z

4. Click on **See SDDL Description**.

   The n**SDDL Description** pane opens.

5. Click on the arrows on the left of the SDDL (1), DACL (2), and Descriptor (3) to expand the

description:

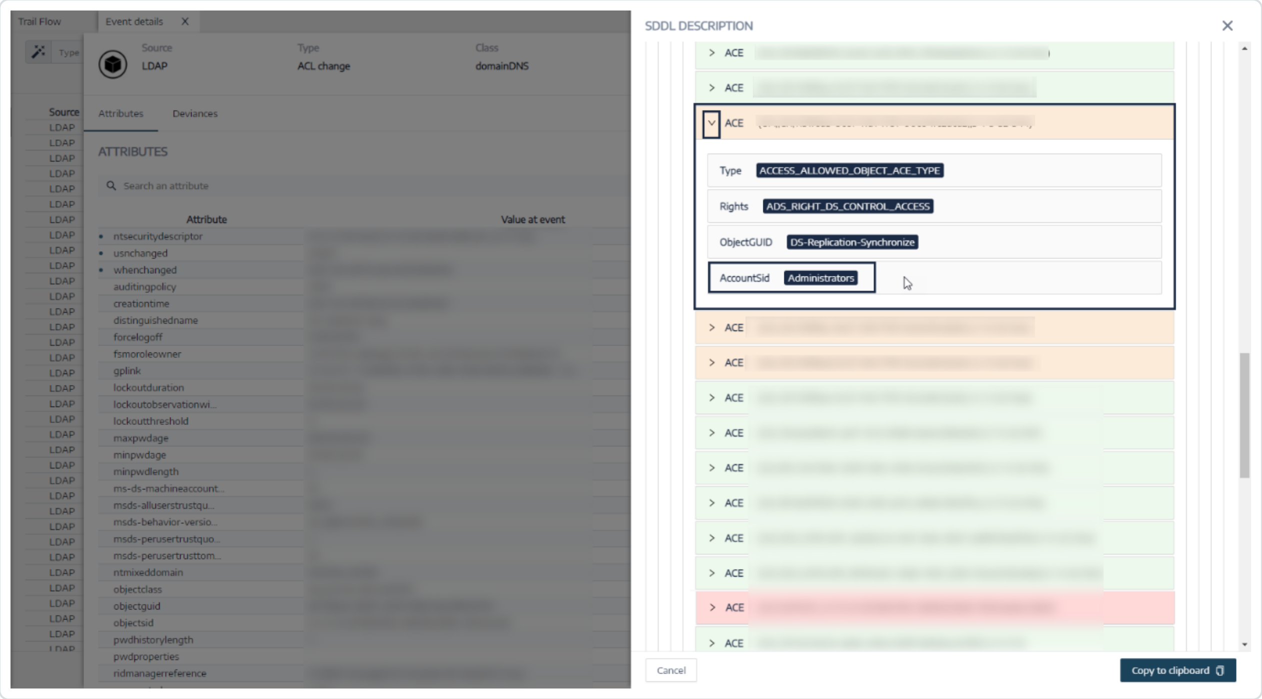


6. Browse to an Access Control Entry (ACE) (4) highlighted in color to display the object's access rights. The color codes indicate:

   - **Red** — Users have dangerous rights assigned to them and they must not have access rights to the object.

   - **Orange** — Privileged users have dangerous rights assigned to them but they generally have this type of right (for example: Domain Admins).

- **Green** — There are no dangerous rights.



Source: LDAP
Type: ACL change
Class: domainDNS

Type: ACCESS_ALLOWED_OBJECT_ACE_TYPE
Rights: ADS_RIGHT_DS_CONTROL_ACCESS
ObjectGUID: DS-Replication-Synchronize
AccountSid: Administrators

7. To copy the SDDL description, click **Copy to clipboard**.

Trail Flow Use Cases

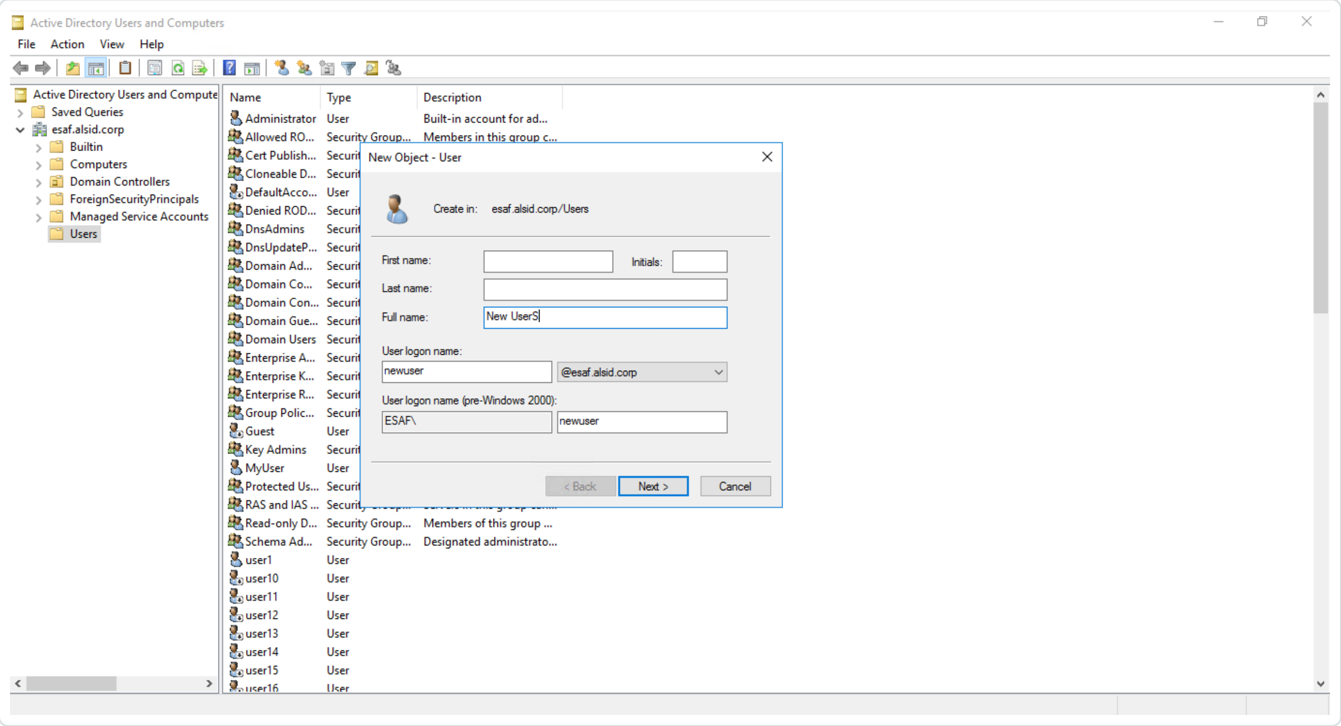
To understand the Trail Flow behavior, two examples illustrate how an operation that you perform in your Active Directory (AD) interface reflects in the Trail Flow page.

Each example compares data from the administrator's side (in the AD interface) with the data from the end user's side (in Tenable Identity Exposure). Whether you use an application, API, or service to carry out an operation on your AD, the result on the Trail Flow is the same.

Note: These examples are not exhaustive and cannot cover every possible situation.

What happens in the Trail Flow when you create a new AD user account?

- On the administrator side, you enter various information on the new user account.



Name	Type	Description
Administrator	User	Built-in account for ad...
Allowed RO...	Security Group...	Members in this group c...
Cert Publish...	Securit	
Cloneable D...	Securit	
DefaultAcco...	User	
Denied ROD...	Securit	
DnsAdmins	Securit	
DnsUpdateP...	Securit	
Domain Ad...	Securit	
Domain Co...	Securit	
Domain Con...	Securit	
Domain Gue...	Securit	
Domain Users	Securit	
Enterprise A...	Securit	
Enterprise K...	Securit	
Enterprise R...	Securit	
Group Polic...	Securit	
Guest	User	
Key Admins	Securit	
MyUser	User	
Protected Us...	Securit	
RAS and IAS ...	Securit	
Read-only D...	Security Group...	Members of this group ...
Schema Ad...	Security Group...	Designated administrato...
user1	User	
user10	User	
user11	User	
user12	User	
user13	User	
user14	User	
user15	User	
user16	User	

New Object - User

Create in: esaf.alsid.corp/Users

First name:

Initials:

Last name:

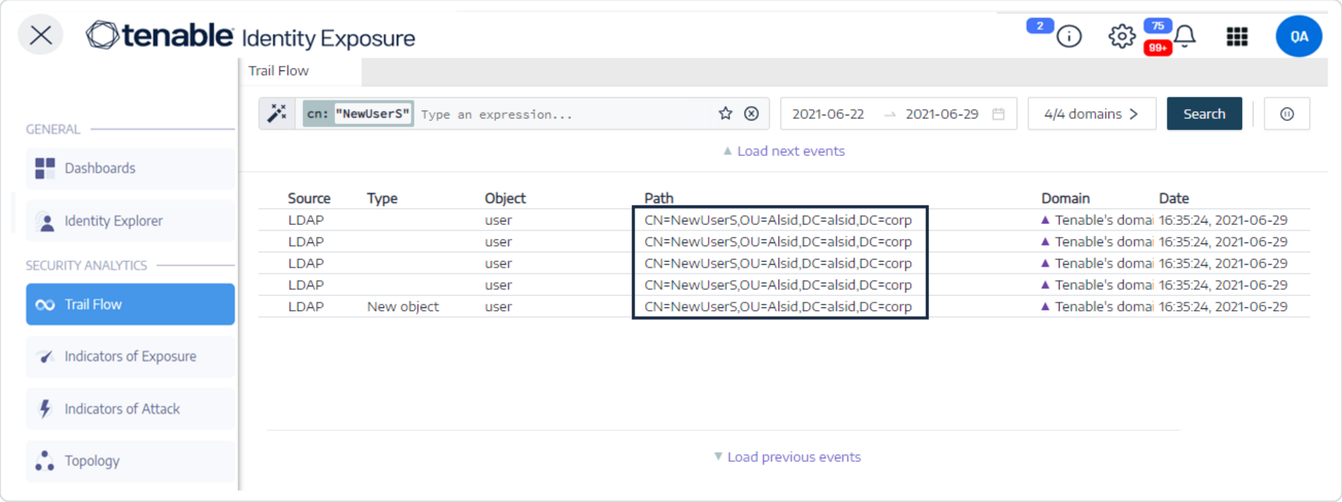
Full name: New UserS

User logon name: newuser @esaf.alsid.corp

User logon name (pre-Windows 2000): ESAF\ newuser

< Back Next > Cancel

- On the end-user side, Tenable Identity Exposure updates the **Trail Flow** page. See the **Type** column indicating *New object*.



cn: "NewUserS" Type an expression...

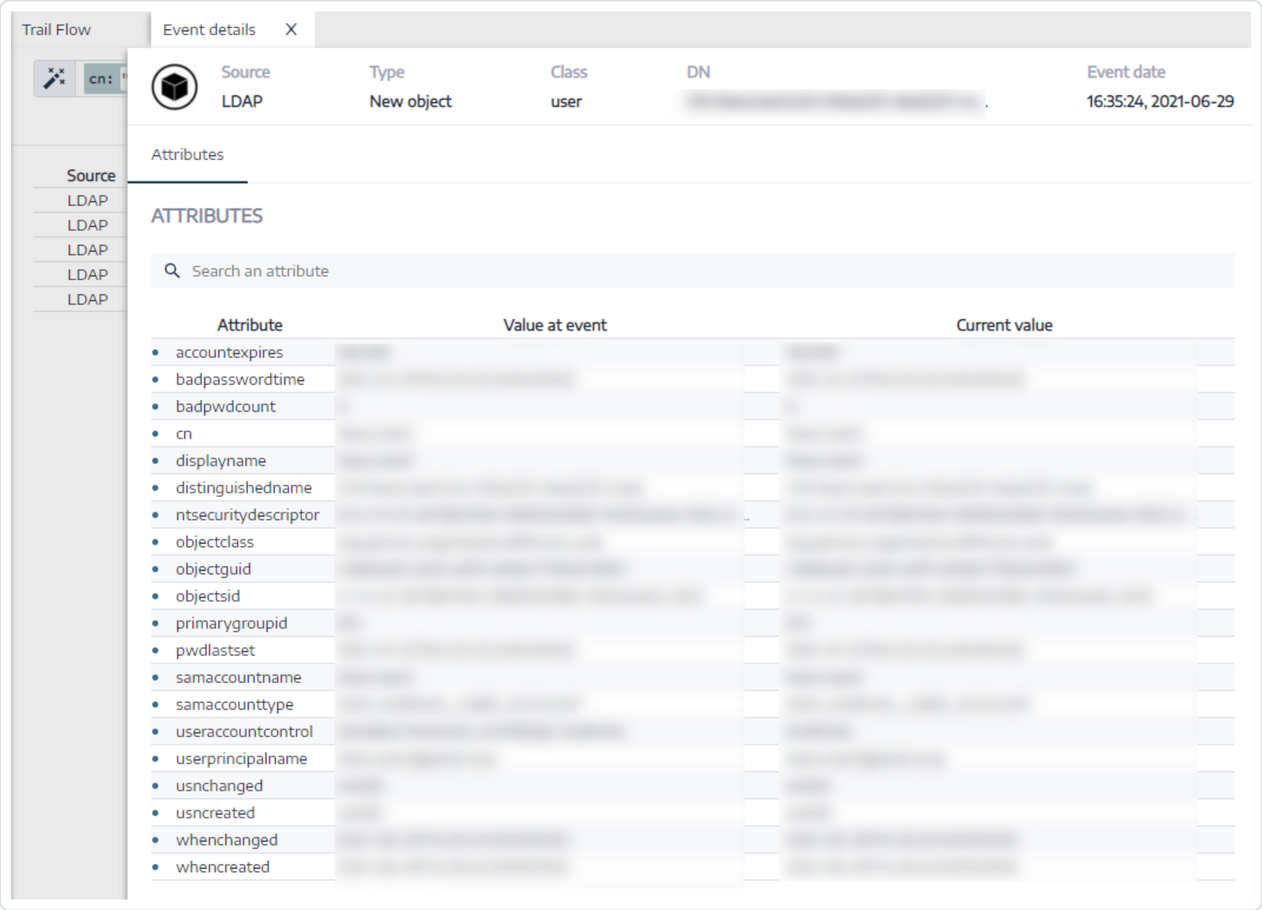
2021-06-22 → 2021-06-29

4/4 domains

Source	Type	Object	Path	Domain	Date
LDAP		user	CN=NewUserS,OU=Alsid,DC=alsid,DC=corp	Tenable's domai	16:35:24, 2021-06-29
LDAP		user	CN=NewUserS,OU=Alsid,DC=alsid,DC=corp	Tenable's domai	16:35:24, 2021-06-29
LDAP		user	CN=NewUserS,OU=Alsid,DC=alsid,DC=corp	Tenable's domai	16:35:24, 2021-06-29
LDAP		user	CN=NewUserS,OU=Alsid,DC=alsid,DC=corp	Tenable's domai	16:35:24, 2021-06-29
LDAP	New object	user	CN=NewUserS,OU=Alsid,DC=alsid,DC=corp	Tenable's domai	16:35:24, 2021-06-29

- The **Event details** page also reflects this change. The blue dots on the left of the attribute names indicate that an update occurred.

  For more details on attributes, see View Event Details.



Source
LDAP
LDAP
LDAP
LDAP
LDAP

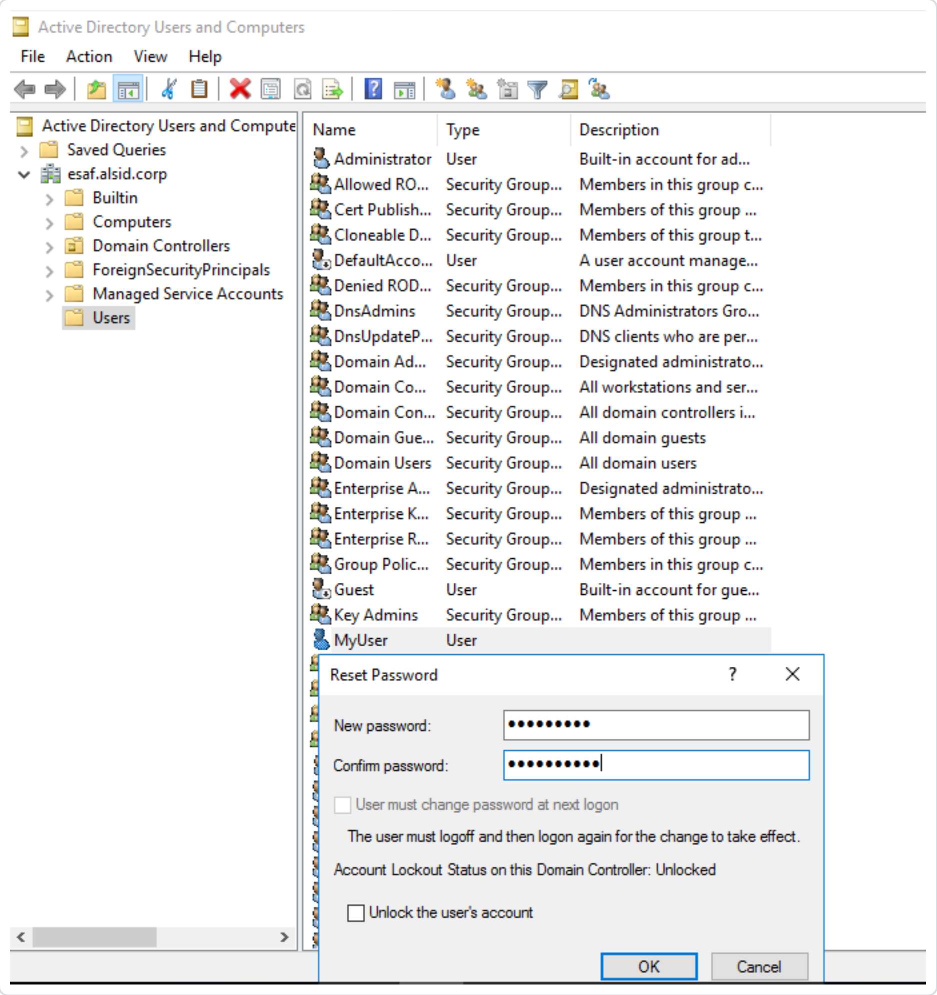
Source	Type	Class	DN	Event date
LDAP	New object	user	[redacted]	16:35:24, 2021-06-29

ATTRIBUTES

Attribute	Value at event	Current value
accountexpires	[redacted]	[redacted]
badpasswordtime	[redacted]	[redacted]
badpwdcount	[redacted]	[redacted]
cn	[redacted]	[redacted]
displayname	[redacted]	[redacted]
distinguishedname	[redacted]	[redacted]
ntsecuritydescriptor	[redacted]	[redacted]
objectclass	[redacted]	[redacted]
objectguid	[redacted]	[redacted]
objectsid	[redacted]	[redacted]
primarygroupid	[redacted]	[redacted]
pwdlastset	[redacted]	[redacted]
samaccountname	[redacted]	[redacted]
samaccounttype	[redacted]	[redacted]
useraccountcontrol	[redacted]	[redacted]
userprincipalname	[redacted]	[redacted]
usnchanged	[redacted]	[redacted]
usncreated	[redacted]	[redacted]
whenchanged	[redacted]	[redacted]
whencreated	[redacted]	[redacted]

What happens in the Trail Flow when you change an AD user's password?

- On the administrator side, you enter various information to reset a user's password.



Name	Type	Description
Administrator	User	Built-in account for ad...
Allowed RO...	Security Group...	Members in this group c...
Cert Publish...	Security Group...	Members of this group ...
Cloneable D...	Security Group...	Members of this group t...
DefaultAcco...	User	A user account manage...
Denied ROD...	Security Group...	Members in this group c...
DnsAdmins	Security Group...	DNS Administrators Gro...
DnsUpdateP...	Security Group...	DNS clients who are per...
Domain Ad...	Security Group...	Designated administrato...
Domain Co...	Security Group...	All workstations and ser...
Domain Con...	Security Group...	All domain controllers i...
Domain Gue...	Security Group...	All domain guests
Domain Users	Security Group...	All domain users
Enterprise A...	Security Group...	Designated administrato...
Enterprise K...	Security Group...	Members of this group ...
Enterprise R...	Security Group...	Members of this group ...
Group Polic...	Security Group...	Members in this group c...
Guest	User	Built-in account for gue...
Key Admins	Security Group...	Members of this group ...
MyUser	User	

Reset Password

New password: ••••••••••

Confirm password: ••••••••••

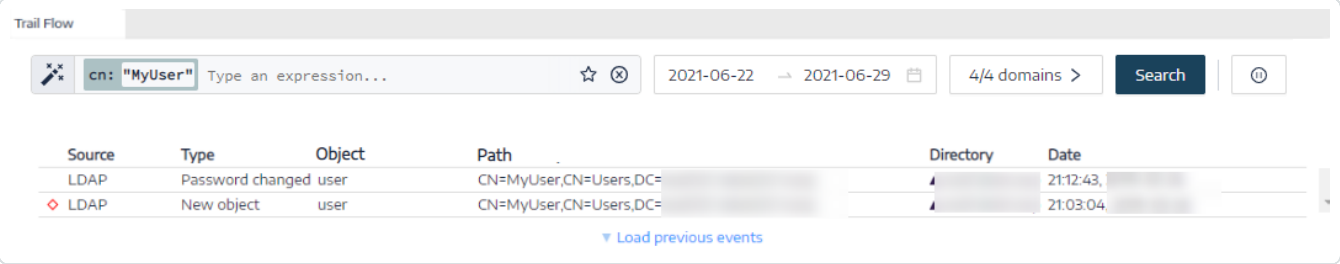
□ User must change password at next logon

The user must logoff and then logon again for the change to take effect.

Account Lockout Status on this Domain Controller: Unlocked

□ Unlock the user's account

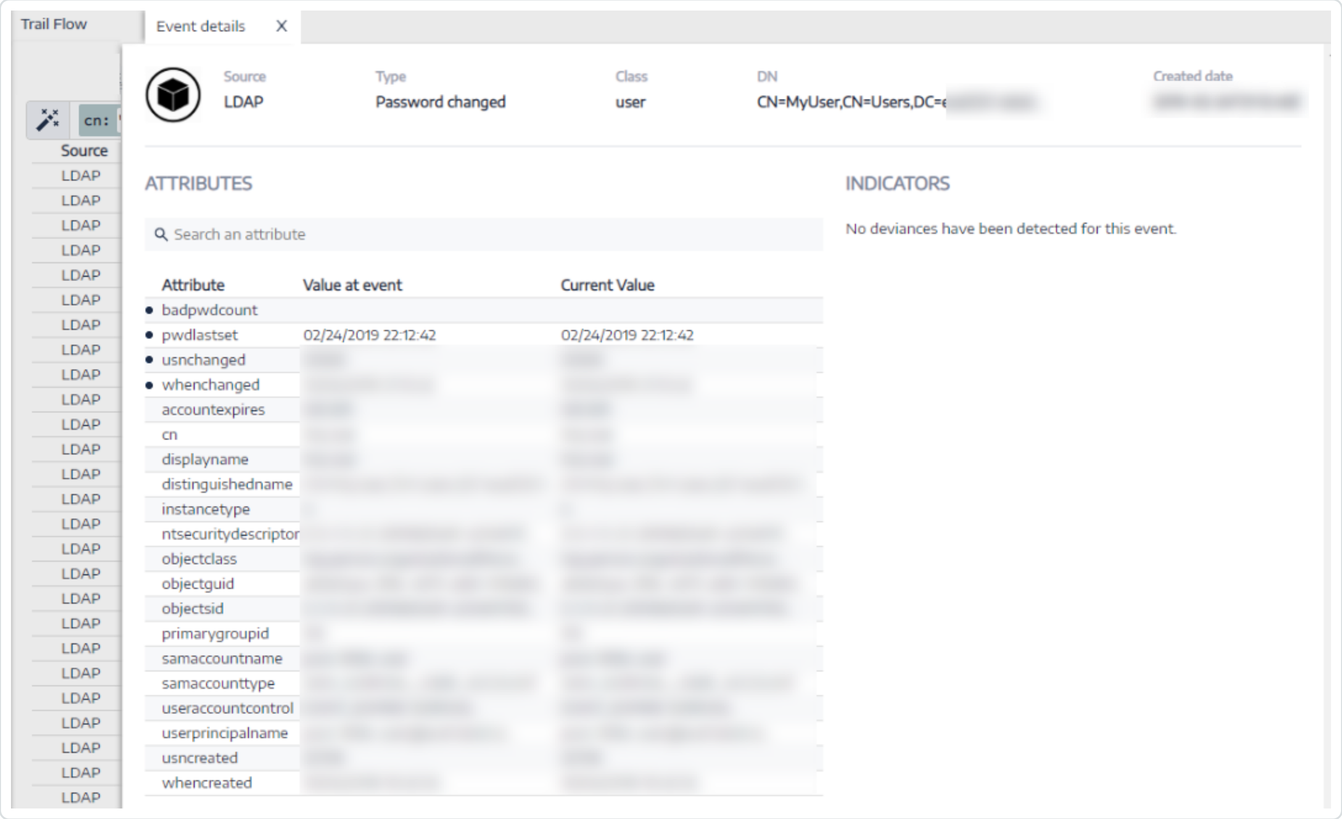
- On the end-user side, Tenable Identity Exposure updates the **Trail Flow** page. See the **Type** column indicating "Password changed."



Source	Type	Object	Path	Directory	Date
LDAP	Password changed	user	CN=MyUser,CN=Users,DC=[redacted]	[redacted]	21:12:43, [redacted]
◇ LDAP	New object	user	CN=MyUser,CN=Users,DC=[redacted]	[redacted]	21:03:04, [redacted]

- The **Event details** page also reflects this change with a blue dot on the left of the `whenchanged` attribute.

For more details on attributes, see Event Details.



Source
LDAP
LDAP
LDAP
LDAP
LDAP
LDAP
LDAP
LDAP
LDAP
LDAP
LDAP
LDAP
LDAP
LDAP
LDAP
LDAP
LDAP
LDAP
LDAP
LDAP
LDAP
LDAP
LDAP
LDAP
LDAP
LDAP

Source	Type	Class	DN	Created date
LDAP	Password changed	user	CN=MyUser,CN=Users,DC=e[redacted]	[redacted]

ATTRIBUTES

Search an attribute

Attribute	Value at event	Current Value
● badpwdcount		
● pwdlastset	02/24/2019 22:12:42	02/24/2019 22:12:42
● usnchanged	[redacted]	[redacted]
● whenchanged	[redacted]	[redacted]
accountexpires	[redacted]	[redacted]
cn	[redacted]	[redacted]
displayname	[redacted]	[redacted]
distinguishedname	[redacted]	[redacted]
instancetype	[redacted]	[redacted]
ntsecuritydescriptor	[redacted]	[redacted]
objectclass	[redacted]	[redacted]
objectguid	[redacted]	[redacted]
objectsid	[redacted]	[redacted]
primarygroupid	[redacted]	[redacted]
samaccountname	[redacted]	[redacted]
samaccounttype	[redacted]	[redacted]
useraccountcontrol	[redacted]	[redacted]
userprincipalname	[redacted]	[redacted]
usncreated	[redacted]	[redacted]
whencreated	[redacted]	[redacted]

INDICATORS

No deviances have been detected for this event.

See also

- Search the Trail Flow Manually
- Search the Trail Flow Using the Wizard
- Customize Trail Flow Queries
- Bookmark Queries
- Query History

Indicators of Exposure

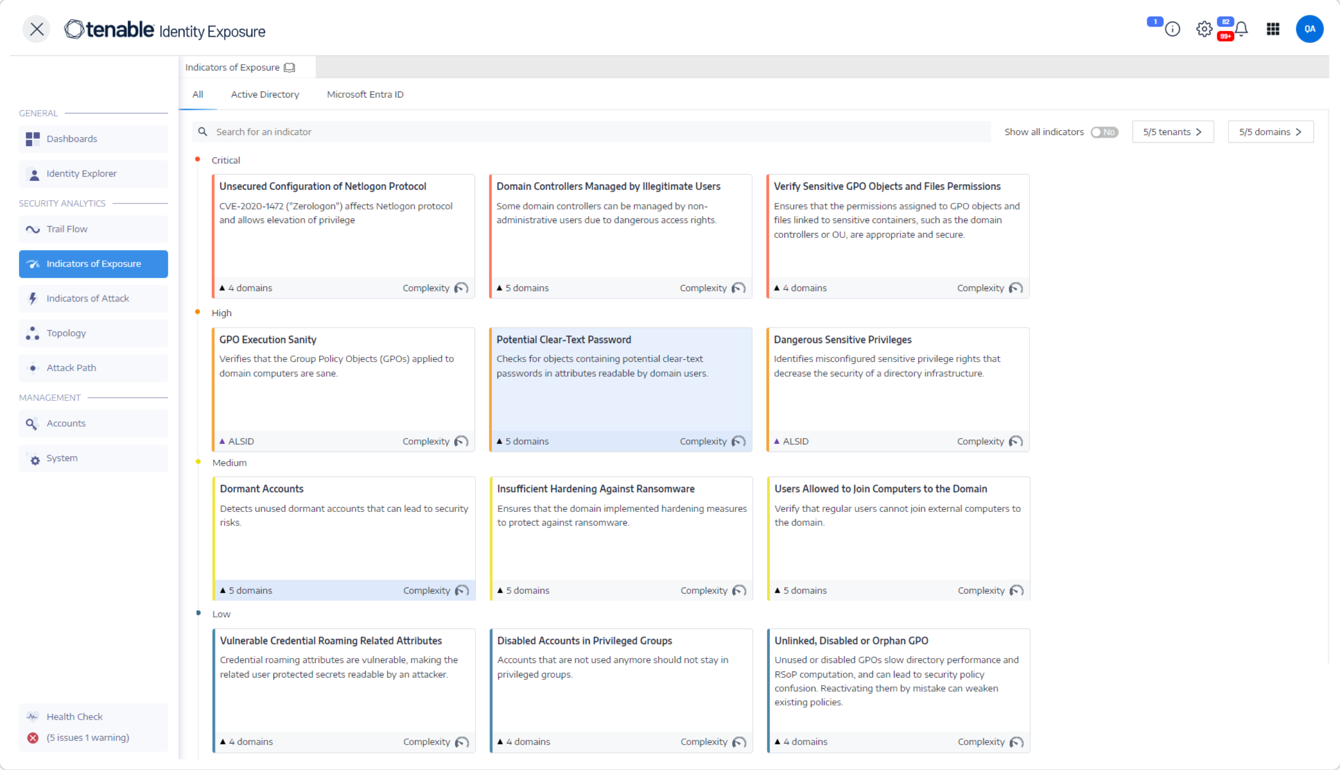
Tenable Identity Exposure measures the security maturity of your AD infrastructures through Indicators of Exposure (IoEs) and assigns severity levels to the flow of events that it monitors and analyzes. Tenable Identity Exposure triggers alerts when it detects security regressions.

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

To search for an IoE:

1. At the top of The **Indicators of Exposure** page, type a string in the Search box. This can be any term related to an IoE such as password, user, logon, etc.

2. Press Enter.

The IoE page updates with the indicators associated with your search term.

To filter IoEs for a specific forest or domain:

1. Click **n/n domain**.

   A **Forest and domains** pane opens.

2. Select the forest or domain.

3. Click **Filter on selection**.

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.

See also

- Indicator of Exposure Details
- Deviant Objects
- Search Deviant Objects
- Ignore a Deviant Object
- Incriminating Attributes

Indicator of Exposure Details

The details on a specific Indicator of Exposure allow you to review technical information on detected vulnerabilities, associated deviant objects, and recommendations on remediation.

To display Indicator of Exposure details:

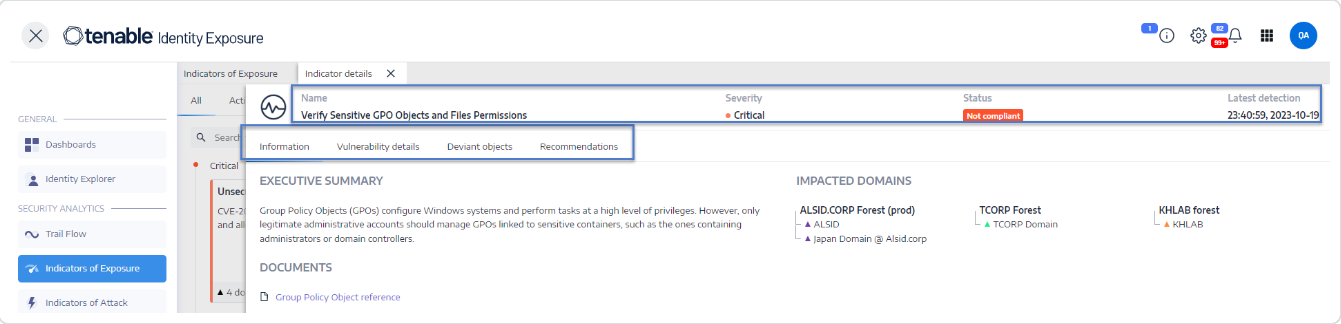
1. In Tenable Identity Exposure, click **Indicators of Exposure** in the navigation pane.

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

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

3. Click on any **Indicators of Exposure** tile on the page.

   The **Indicator details** pane opens.



Name
Verify Sensitive GPO Objects and Files Permissions

Severity
● Critical

Status
Not compliant

Latest detection
23:40:59, 2023-10-19

EXECUTIVE SUMMARY

Group Policy Objects (GPOs) configure Windows systems and perform tasks at a high level of privileges. However, only legitimate administrative accounts should manage GPOs linked to sensitive containers, such as the ones containing administrators or domain controllers.

DOCUMENTS

Group Policy Object reference

IMPACTED DOMAINS

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

TCORP Forest
▲ TCORP Domain

KHLAB forest
▲ KHLAB

At the top, the **Indicator details** pane summarizes the information already provided in the Trail Flow table:

- The **Name** of the IoE.
- Its **Severity** level (Critical, High, Medium, or Low).
- Its compliance **Status** based on the result of the last analysis that Tenable Identity Exposure ran.
- The **Latest detection** indicating the last time that Tenable Identity Exposure ran the analysis.

4. Click on any of the following tabs provide more details for the IoE:

Tab	Description
Information	Includes internal and external resources on the IoE such as: • Executive Summary — an overview on the issue to help you make appropriate decisions. • Documents — links to external resources on the IoE. • Attacker-known tools — name of the hacking tools. • A tree structure of the impacted domains.
Vulnerability details	Provides explanations for the weakness detected in your AD and the risks to your Active Directory (AD) if you do not take remediation actions.
Deviant objects	Deviant objects reveal weaknesses or potentially dangerous behaviors in your AD. You can apply filters to deviant objects to pinpoint critical issues. When an IoE status is not compliant and includes deviant objects, you can take remediation actions to correct the security deficiencies that Tenable Identity Exposure detected. For more information, see Deviant Objects.
Recommendations	Tips on how to restore compliance with your security requirements and improve the security of your AD: • An Executive summary gives an overview on the solution suggested by Tenable Identity Exposure. • The Details sub-section gives advice on how to implement the action plan and helps managers initiate the necessary changes to their AD infrastructures. • The Documents sub-section provides links to external resources on the suggested solution or threat.

See also

- Indicators of Exposure
- Deviant Objects
- Search Deviant Objects
- Ignore a Deviant Object
- Incriminating Attributes

Deviant Objects

Tenable Identity Exposure's Indicators of Exposure (IoE) can flag deviant objects that reveal weaknesses or potentially dangerous behaviors in an Active Directory (AD). Focusing on these deviant objects can help you pinpoint critical issues and remediate them. You can do any of the following:

- Search for a deviant object.
- Ignore a deviant object for a period of time.
- Select the forests and domains to search for deviant objects.
- Get explanations on the incriminating attributes affecting the IoE.
- Download a report showing all deviant objects.

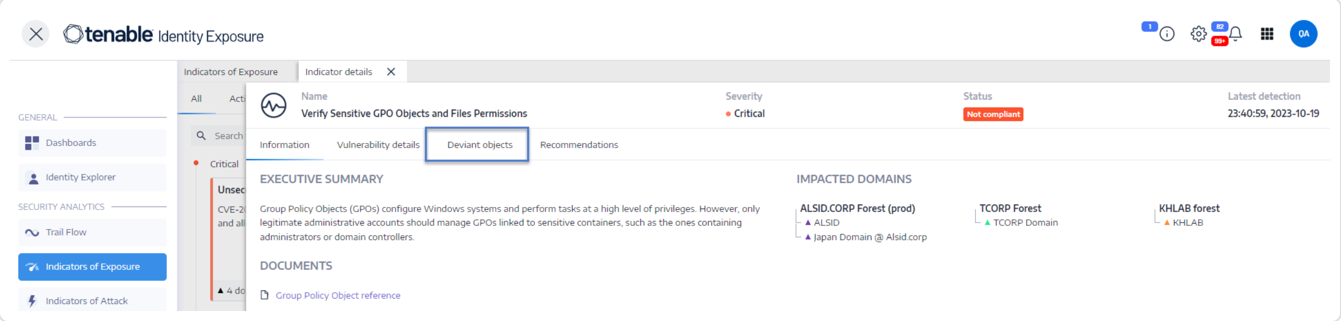
To display deviant objects:

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

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

2. Click on any **Indicators of Exposure** tile on the page.

   The **Indicator details** pane opens.



Name: Verify Sensitive GPO Objects and Files Permissions
Severity: ● Critical
Status: Not compliant
Latest detection: 23:40:59, 2023-10-19

EXECUTIVE SUMMARY

Group Policy Objects (GPOs) configure Windows systems and perform tasks at a high level of privileges. However, only legitimate administrative accounts should manage GPOs linked to sensitive containers, such as the ones containing administrators or domain controllers.

DOCUMENTS

Group Policy Object reference

IMPACTED DOMAINS

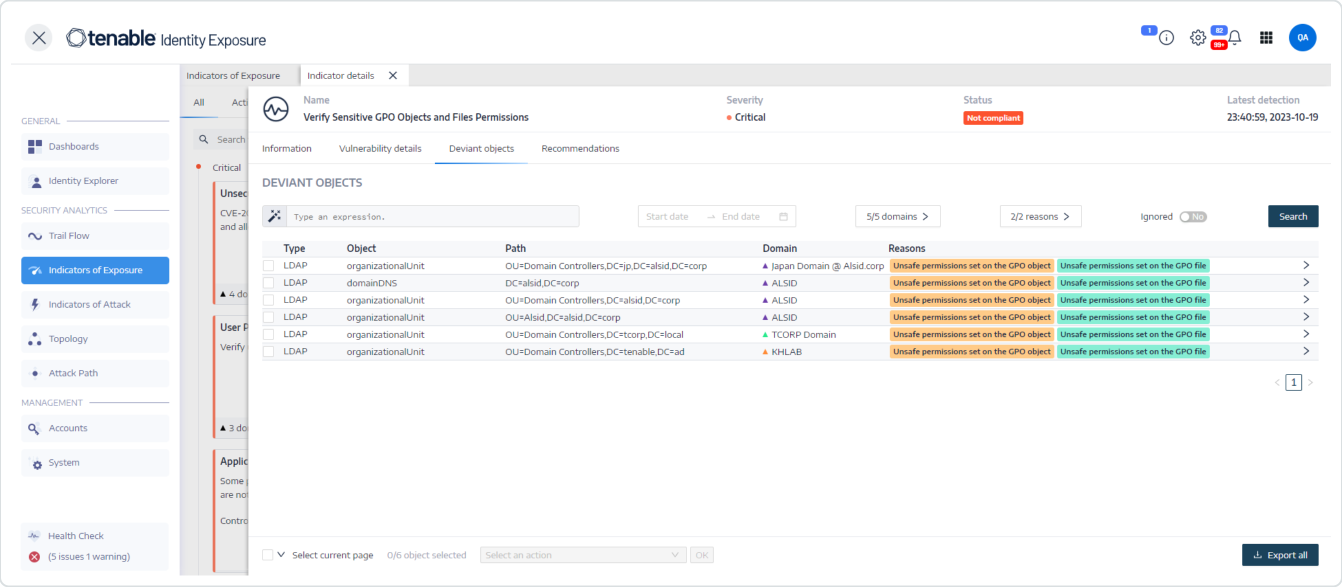
ALSID.CORP Forest (prod)
- ▲ ALSID
- ▲ Japan Domain @ Alsid.corp

TCORP Forest
- ▲ TCORP Domain

KHLAB forest
- ▲ KHLAB

3. Click on the **Deviant objects** tab.

   The list of deviant objects associated with the IoE appears.



Name: Verify Sensitive GPO Objects and Files Permissions

Severity: Critical

Status: Not compliant

Latest detection: 23:40:59, 2023-10-19

DEVIANT OBJECTS

Type	Object	Path	Domain	Reasons
LDAP	organizationalUnit	OU=Domain Controllers,DC=jp,DC=alsid,DC=corp	Japan Domain @ Alsid.corp	Unsafe permissions set on the GPO object Unsafe permissions set on the GPO file
LDAP	domainDNS	DC=alsid,DC=corp	ALSID	Unsafe permissions set on the GPO object Unsafe permissions set on the GPO file
LDAP	organizationalUnit	OU=Domain Controllers,DC=alsid,DC=corp	ALSID	Unsafe permissions set on the GPO object Unsafe permissions set on the GPO file
LDAP	organizationalUnit	OU=Alsid,DC=alsid,DC=corp	ALSID	Unsafe permissions set on the GPO object Unsafe permissions set on the GPO file
LDAP	organizationalUnit	OU=Domain Controllers,DC=tcorp,DC=local	TCORP Domain	Unsafe permissions set on the GPO object Unsafe permissions set on the GPO file
LDAP	organizationalUnit	OU=Domain Controllers,DC=tenable,DC=ad	KHLAB	Unsafe permissions set on the GPO object Unsafe permissions set on the GPO file

The deviant objects table includes the following information:

- **Type** — Indicates the origin of any security-related change in the AD (LDAP or SMB protocols).
- **Object** — Indicates the class or file extension associated with an AD object.
- **Path** — Indicates the full path to an AD object to allow you to identify its unique location in the AD.
- **Domain** — Indicates the domain where the change in your AD comes from.
- **Reasons** — Lists the incriminating attributes affecting deviant objects.

To export the deviant objects report:

1. At the bottom of the **Deviant objects** page, click **Export all**.

   The Export deviant objects pane appears.

2. In the **Export format** box, click the drop-down arrow to select your format.
3. Click **Export all**.

   Tenable Identity Exposure downloads the deviant objects report to your machine.

See also

- Indicators of Exposure
- Indicator of Exposure Details
- Search Deviant Objects
- Ignore a Deviant Object
- Incriminating Attributes

Search Deviant Objects

You can search for deviant objects manually or using the wizard.

Wizard Search

The search wizard allows you to create query expressions.

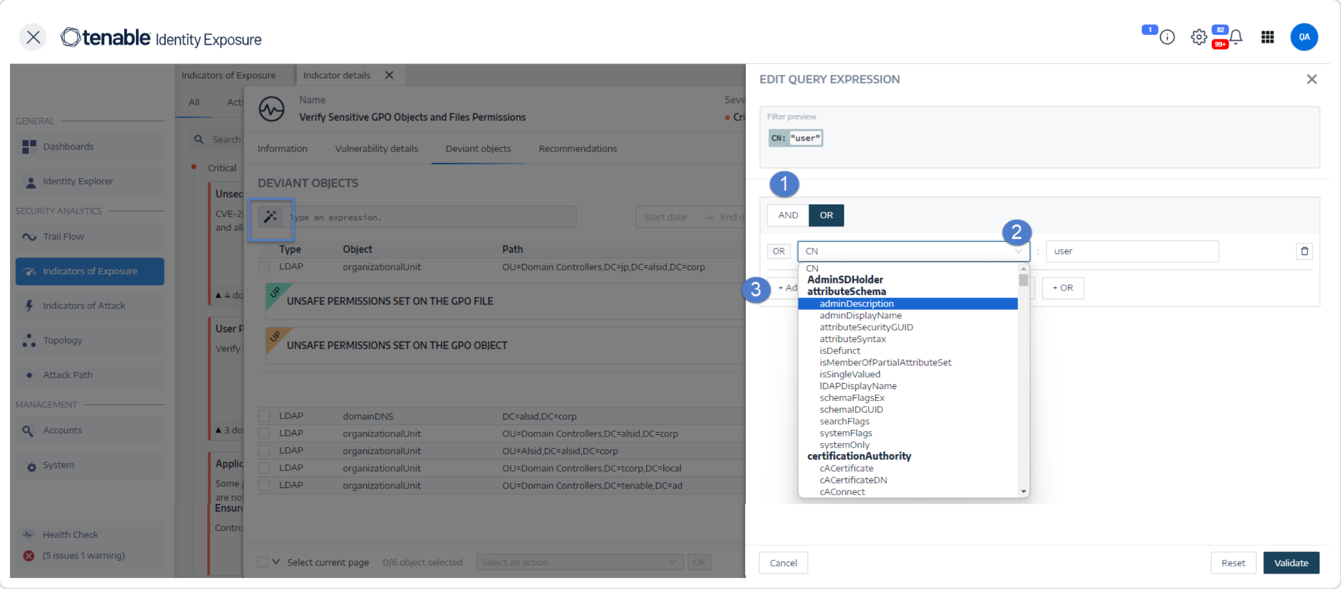
- When you use frequent expressions in the search box, you can add them to a list of bookmarks for later use.
- When you enter an expression in the search box, it Tenable Identity Exposure saves this expression in its History pane for you to reuse.

To search for a deviant object using the wizard:

1. Display the list of Deviant Objects

2. Click on the 🪄 icon.

   The **Edit Query Expression** pane opens.



Filter preview: `CN: "user"`

OR CN : user

CN
AdminSDHolder
attributeSchema
adminDescription
adminDisplayName
attributeSecurityGUID
attributeSyntax
isDefunct
isMemberOfPartialAttributeSet
isSingleValued
lDAPDisplayName
schemaFlagsEx
schemaIDGUID
searchFlags
systemFlags
systemOnly
certificationAuthority
cACertificate
cACertificateDN
cAConnect

Type	Object	Path
LDAP	organizationalUnit	OU=Domain Controllers,DC=jp,DC=alsid,DC=corp
UNSAFE PERMISSIONS SET ON THE GPO FILE		
UNSAFE PERMISSIONS SET ON THE GPO OBJECT		
LDAP	domainDNS	DC=alsid,DC=corp
LDAP	organizationalUnit	OU=Domain Controllers,DC=alsid,DC=corp
LDAP	organizationalUnit	OU=Alsid,DC=alsid,DC=corp
LDAP	organizationalUnit	OU=Domain Controllers,DC=tcorp,DC=local
LDAP	organizationalUnit	OU=Domain Controllers,DC=tenable,DC=ad

3. To define the query expression in the panel, click on the **AND** or the **OR** operator button (1) to apply to the first condition.

4. Select an attribute from the drop-down menu and enter its value (2).

5. Do any of the following:

    - To add an attribute, click **+ Add a new rule** (3).
    - To add another condition, click **Add a new condition+AND** or **+OR** operator. Select an attribute from the drop-down menu and enter its value.
    - To restrict the search to deviant objects, click the **Deviant only** toggle to allow. Select the **+AND** or **+OR** operator to add the condition to the query.
    - To delete a condition or rule, click the 🗑 icon.

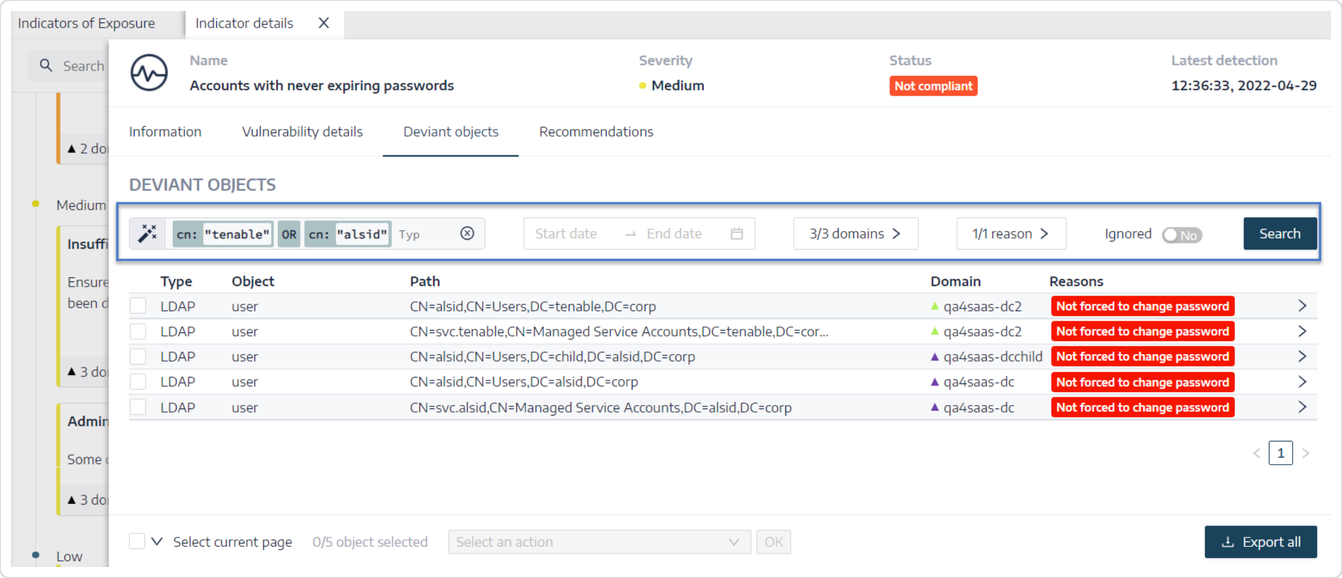
6. Click **Validate** to run the search or **Reset** to modify your query expressions.

Manual Search

To filter deviant objects that match specific character strings or patterns, you can type an expression in the search box to refine results using the Boolean operators *****, **AND**, and **OR**. You can encapsulate **OR** statements with parentheses to modify search priority. The search looks for any specific value in an Active Directory attribute. To search the Trail Flow manually:

To search for a deviant object manually:

1. Display the list of Deviant Objects.



Name: Accounts with never expiring passwords
Severity: Medium
Status: Not compliant
Latest detection: 12:36:33, 2022-04-29

DEVIANT OBJECTS

cn: "tenable" OR cn: "alsid" Typ

	Type	Object	Path	Domain	Reasons
□	LDAP	user	CN=alsid,CN=Users,DC=tenable,DC=corp	▲ qa4saas-dc2	Not forced to change password
□	LDAP	user	CN=svc.tenable,CN=Managed Service Accounts,DC=tenable,DC=cor...	▲ qa4saas-dc2	Not forced to change password
□	LDAP	user	CN=alsid,CN=Users,DC=child,DC=alsid,DC=corp	▲ qa4saas-dcchild	Not forced to change password
□	LDAP	user	CN=alsid,CN=Users,DC=alsid,DC=corp	▲ qa4saas-dc	Not forced to change password
□	LDAP	user	CN=svc.alsid,CN=Managed Service Accounts,DC=alsid,DC=corp	▲ qa4saas-dc	Not forced to change password

2. In the Search box, type a query expression.

3. You can filter the search results as follows:

- Click on the **Calendar** box to select a start date and an end date.
- Click on **n/n Domains** to select forests and domains.

4. Click **Search**.

   Tenable Identity Exposure updates the list with the results matching your search criteria.

Grammar and Syntax

A manual query expression uses the following grammar and syntax:

- Grammar: `EXPRESSION [OPERATOR EXPRESSION]*`
- Syntax: `__KEY__ __SELECTOR__ __VALUE__`

  where:

  - `__KEY__` refers to the AD object attribute to search (such as `CN`, `userAccountControl`, `members`, etc.)
  - `__SELECTOR__` refers to the operator: `:`, `>`, `<`, `>=`, `<=.`
  - `__VALUE__` refers to value to search for.

    You can use more keys to look for specific content:

  - `isDeviant` looks for events that created a deviance.

You can combine multiple Trail Flow query expressions using the **AND** and **OR** operators.

Examples:

- Look for all objects containing the string `alice` into the common name attribute: `cn:"alice"`
- Look for all objects containing the string `alice` in the common name attribute and which created a specific deviance: `isDeviant:"true" and cn:"alice"`
- Look for a GPO named Default Domain Policy: `objectClass:"groupPolicyContainer" and displayname:"Default Domain Policy"`
- Look for all deactivated accounts with a SID containing S-1-5-21: `userAccountControl:"DISABLE" and objectSid:"S-1-5-21"`

- Look for all `script.ini` files in Sysvol: `globalpath:"sysvol" and types:"SCRIPTSini"`

> **Note**: Here, `types` refers to the object attribute and not the column header.

See also

- Indicators of Exposure
- Indicator of Exposure Details
- Deviant Objects
- Ignore a Deviant Object
- Incriminating Attributes

Ignore a Deviant Object

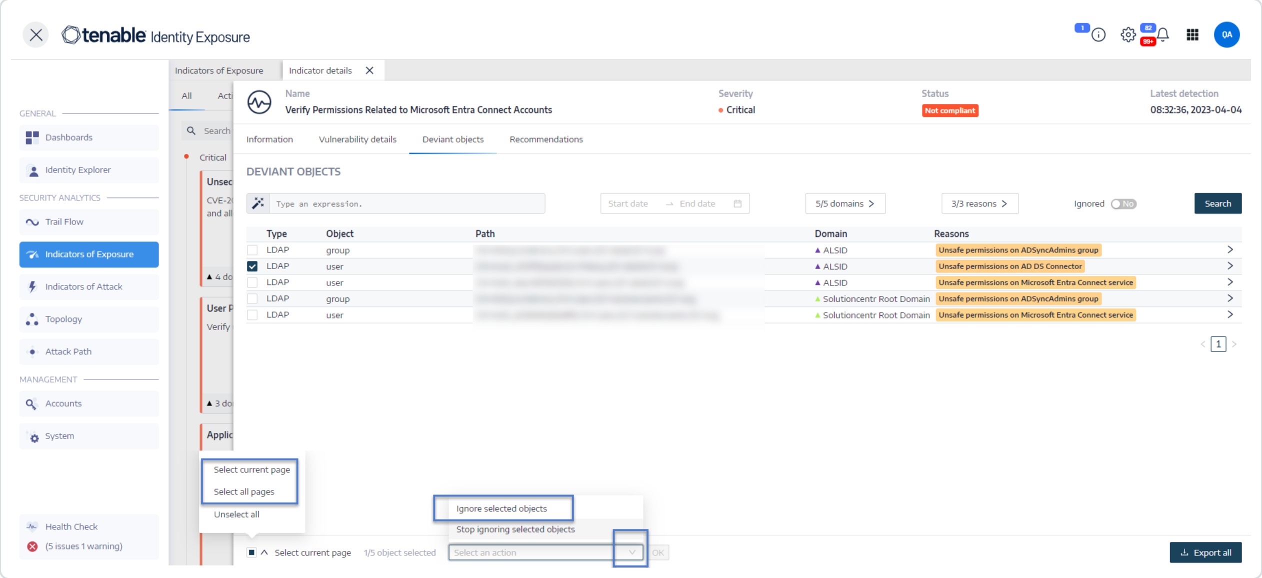
To prevent cluttering the screen for investigation or reporting purposes, you can filter out some deviant objects by forcing Tenable Identity Exposure to ignore them for a selected period of time. You can choose to ignore one or several deviant objects. You can apply a custom filter immediately or to specify a timeframe to activate the filter.

> **Note**: Ignoring an object does not make it resolved in Tenable Identity Exposure.

To ignore deviant objects:

1. In Tenable Identity Exposure, display the list of Deviant Objects
2. Select the checkboxes in front of the deviant object to ignore.
3. Optionally, you can also filter for deviant objects to ignore:
    - Click the **Calendar** box to select a start date and an end date.
    - Click on **n/n Domains** to select forests and domains.

> **Tip**: For faster selection, you can check the **Select all pages** or **Select current page** box at the bottom of the page.



Name: Verify Permissions Related to Microsoft Entra Connect Accounts

Severity: Critical

Status: Not compliant

Latest detection: 08:32:36, 2023-04-04

DEVIANT OBJECTS

Type an expression. | Start date → End date | 5/5 domains | 3/3 reasons | Ignored ○ No

	Type	Object	Path	Domain	Reasons
☐	LDAP	group	[redacted]	ALSID	Unsafe permissions on ADSyncAdmins group
☑	LDAP	user	[redacted]	ALSID	Unsafe permissions on AD DS Connector
☐	LDAP	user	[redacted]	ALSID	Unsafe permissions on Microsoft Entra Connect service
☐	LDAP	group	[redacted]	Solutioncentr Root Domain	Unsafe permissions on ADSyncAdmins group
☐	LDAP	user	[redacted]	Solutioncentr Root Domain	Unsafe permissions on Microsoft Entra Connect service

■ Select current page 1/5 object selected

4. From the drop-down list at the bottom of the page, select **Ignore selected objects**.
5. Click **OK**.

   The **Ignore selected objects** pane appears.
6. Click the **Ignore until** box to display the calendar and select a date until which Tenable Identity Exposure must ignore the deviant object.
7. Click **OK**.

   Tenable Identity Exposure displays a confirmation message and updates the list of remaining deviant objects.

To show ignored deviant objects:

1. Click the **Ignored** toggle to **Yes**.
2. At the bottom of the page, click **Select all pages**.
3. Select **Stop ignoring selected objects** from the drop-down list.
4. Click **OK**.

   A confirmation pane appears.
5. Click **OK** to validate your changes.

   Tenable Identity Exposure displays the ignored deviant objects.

See also

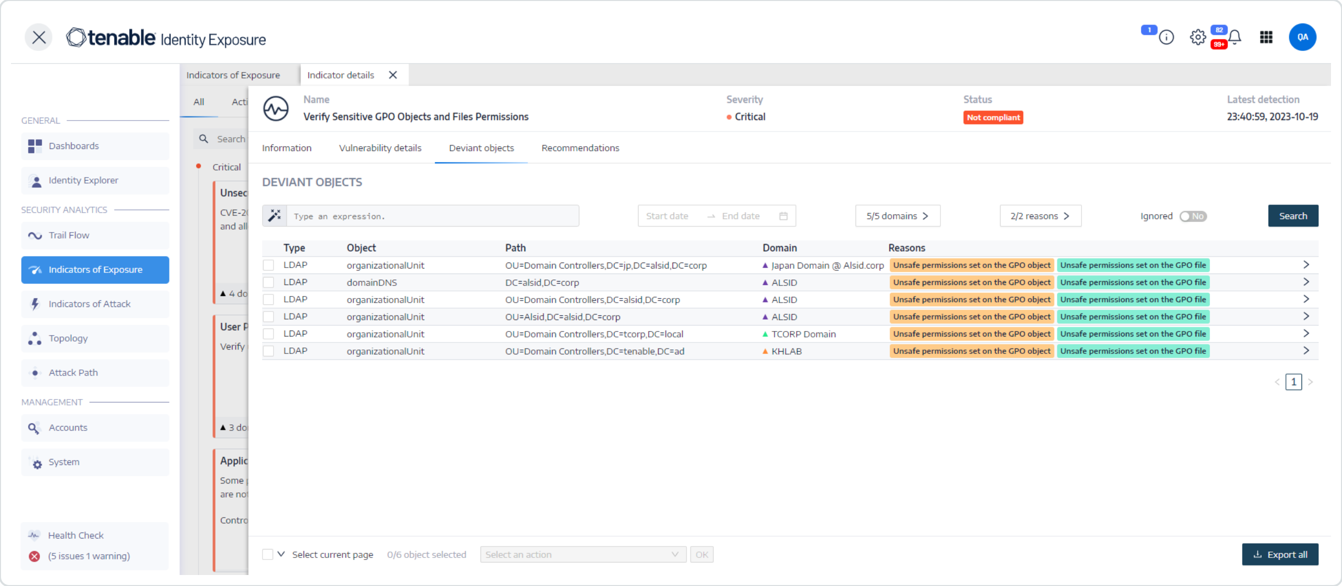
- Indicators of Exposure
- Indicator of Exposure Details
- Deviant Objects
- Search Deviant Objects
- Incriminating Attributes

Incriminating Attributes

Tenable Identity Exposure displays the incriminating attributes that trigger deviant objects in an Indicator of Exposure (IoE) and gives reasons for them to help you understand the deviance and remediate it.

To see incriminating attributes:

1. Display the list of Deviant Objects



Name: Verify Sensitive GPO Objects and Files Permissions

Severity: Critical

Status: Not compliant

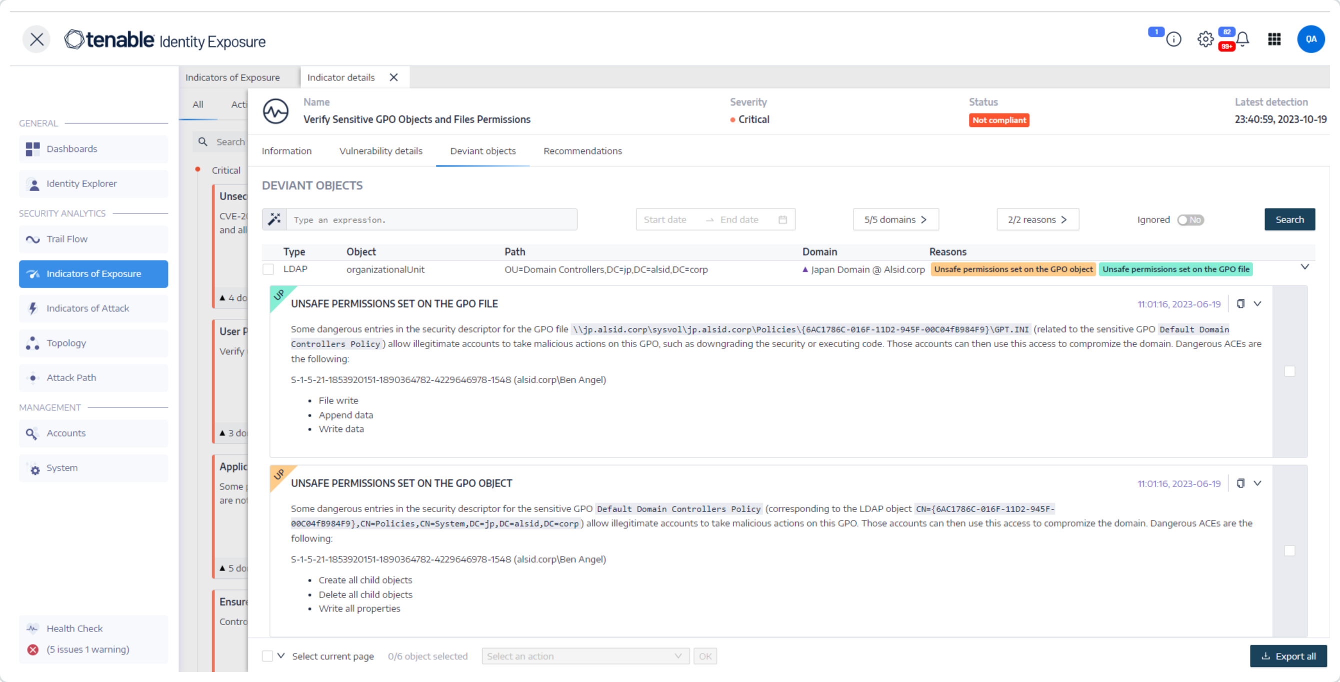
Latest detection: 23:40:59, 2023-10-19

DEVIANT OBJECTS

Type	Object	Path	Domain	Reasons	
LDAP	organizationalUnit	OU=Domain Controllers,DC=jp,DC=alsid,DC=corp	Japan Domain @ Alsid.corp	Unsafe permissions set on the GPO object	Unsafe permissions set on the GPO file
LDAP	domainDNS	DC=alsid,DC=corp	ALSID	Unsafe permissions set on the GPO object	Unsafe permissions set on the GPO file
LDAP	organizationalUnit	OU=Domain Controllers,DC=alsid,DC=corp	ALSID	Unsafe permissions set on the GPO object	Unsafe permissions set on the GPO file
LDAP	organizationalUnit	OU=Alsid,DC=alsid,DC=corp	ALSID	Unsafe permissions set on the GPO object	Unsafe permissions set on the GPO file
LDAP	organizationalUnit	OU=Domain Controllers,DC=tcorp,DC=local	TCORP Domain	Unsafe permissions set on the GPO object	Unsafe permissions set on the GPO file
LDAP	organizationalUnit	OU=Domain Controllers,DC=tenable,DC=ad	KHLAB	Unsafe permissions set on the GPO object	Unsafe permissions set on the GPO file

2. Click on an entry in the list of deviant objects.

Tenable Identity Exposure displays a list of incriminating attributes for that deviant object:



Name: Verify Sensitive GPO Objects and Files Permissions

Severity: Critical

Status: Not compliant

Latest detection: 23:40:59, 2023-10-19

DEVIANT OBJECTS

Type	Object	Path	Domain	Reasons
LDAP	organizationalUnit	OU=Domain Controllers,DC=jp,DC=alsid,DC=corp	Japan Domain @ Alsid.corp	Unsafe permissions set on the GPO object Unsafe permissions set on the GPO file

UNSAFE PERMISSIONS SET ON THE GPO FILE — 11:01:16, 2023-06-19

Some dangerous entries in the security descriptor for the GPO file `\\jp.alsid.corp\sysvol\jp.alsid.corp\Policies\{6AC1786C-016F-11D2-945F-00C04fB984F9}\GPT.INI` (related to the sensitive GPO `Default Domain Controllers Policy`) allow illegitimate accounts to take malicious actions on this GPO, such as downgrading the security or executing code. Those accounts can then use this access to compromize the domain. Dangerous ACEs are the following:

S-1-5-21-1853920151-1890364782-4229646978-1548 (alsid.corp\Ben Angel)

- File write
- Append data
- Write data

UNSAFE PERMISSIONS SET ON THE GPO OBJECT — 11:01:16, 2023-06-19

Some dangerous entries in the security descriptor for the sensitive GPO `Default Domain Controllers Policy` (corresponding to the LDAP object `CN={6AC1786C-016F-11D2-945F-00C04fB984F9},CN=Policies,CN=System,DC=jp,DC=alsid,DC=corp`) allow illegitimate accounts to take malicious actions on this GPO. Those accounts can then use this access to compromize the domain. Dangerous ACEs are the following:

S-1-5-21-1853920151-1890364782-4229646978-1548 (alsid.corp\Ben Angel)

- Create all child objects
- Delete all child objects
- Write all properties

The list includes the following information:

- **Color-coded tags** to distinguish the different reasons when there are several.
- Values:
    - `?` — A missing (empty) attribute value which indicates an abnormal behavior.
    - `No description is available for this deviance`: The detection dates back to version 2.6 and Tenable Identity Exposure no longer manages this attribute.

To copy the incriminating attribute:

- Select the attribute and click the 🗍 icon.

See also

- Indicators of Exposure
- Indicator of Exposure Details
- Deviant Objects

- Search Deviant Objects
- Ignore a Deviant Object

RSoP-Based Indicators of Exposure

Tenable Identity Exposure uses a set of RSoP (Resultant Set of Policy) based Indicators of Exposure (IoEs) to assess and ensure the security and compliance of various aspects. This section provides insights into the current behavior of specific RSoP IoEs and how Tenable Identity Exposure addresses performance concerns associated with their computations.

The following RSoP-dependent IoEs play a role in Tenable Identity Exposure's security framework:

- Logon Restrictions for Privileged Users
- Dangerous Sensitive Privileges
- Application of Weak Password Policies on Users
- Insufficient Hardening Against Ransomware
- Unsecured Configuration of Netlogon Protocol

These IoEs depend on an RSoP computation results cache that is initialized when needed, computing values that are added upon request rather than relying on pre-existing values. Previously, changes to `AdObjects` triggered cache invalidation, leading to frequent re-computation during the IoE's RSoP executions.

Tenable Identity Exposure addresses the performance impact associated with RSoP computations as follows:

1. **Live IoE analysis with potentially obsolete data** — The computation (input/output event) of IoEs that rely on RSoP takes place in real time as they occur, even if the data used for processing may not be the most current. Buffered events that have the potential to invalidate the RSoP cache remain stored until they meet a specific condition, prompting the anticipated computation.

2. **Scheduled RSoP invalidation** — Upon meeting the condition for re-computation, the system invalidates the RSoP cache, taking into account buffered events during the invalidation process.

3. **Re-execution of IoEs with up-to-date cache** — Following the cache invalidation, IoEs undergo re-execution with the most recent version of the `AdObject` from the cache, incorporating buffered events. Tenable Identity Exposure computes each IoE individually for every buffered event.

For these reasons, the optimized computation duration for IoEs dependent on RSoP results in slower computation of deviances related to the RSoP.

Indicators of Exposure Related to Microsoft Entra ID

Indicators of Exposure Specific to Microsoft Entra ID

Tenable Identity Exposure has dedicated Indicators of Exposure (IoEs) that alert to potential vulnerabilities for assets in Microsoft Entra ID.

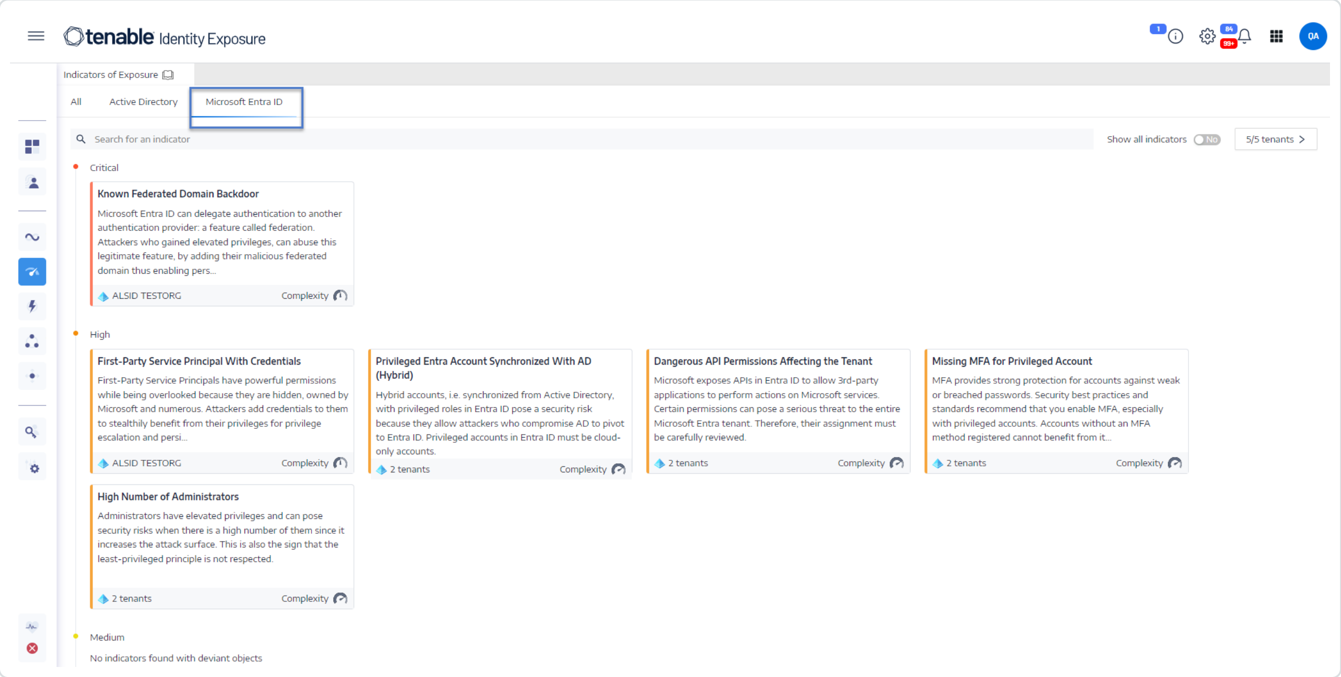
To show Microsoft Entra ID IoEs:

1. In Tenable Identity Exposure, click the IoE icon in the left navigation bar.

   The IoE pane opens.

2. Click on the **Microsoft Entra ID** tab.

   Tenable Identity Exposure shows IoEs related to Microsoft Entra ID that triggered findings.



Known Federated Domain Backdoor
Microsoft Entra ID can delegate authentication to another authentication provider: a feature called federation. Attackers who gained elevated privileges, can abuse this legitimate feature, by adding their malicious federated domain thus enabling pers...
ALSID TESTORG — Complexity

First-Party Service Principal With Credentials
First-Party Service Principals have powerful permissions while being overlooked because they are hidden, owned by Microsoft and numerous. Attackers add credentials to them to stealthily benefit from their privileges for privilege escalation and persi...
ALSID TESTORG — Complexity

Privileged Entra Account Synchronized With AD (Hybrid)
Hybrid accounts, i.e. synchronized from Active Directory, with privileged roles in Entra ID pose a security risk because they allow attackers who compromise AD to pivot to Entra ID. Privileged accounts in Entra ID must be cloud-only accounts.
2 tenants — Complexity

Dangerous API Permissions Affecting the Tenant
Microsoft exposes APIs in Entra ID to allow 3rd-party applications to perform actions on Microsoft services. Certain permissions can pose a serious threat to the entire Microsoft Entra tenant. Therefore, their assignment must be carefully reviewed.
2 tenants — Complexity

Missing MFA for Privileged Account
MFA provides strong protection for accounts against weak or breached passwords. Security best practices and standards recommend that you enable MFA, especially with privileged accounts. Accounts without an MFA method registered cannot benefit from it...
2 tenants — Complexity

High Number of Administrators
Administrators have elevated privileges and can pose security risks when there is a high number of them since it increases the attack surface. This is also the sign that the least-privileged principle is not respected.
2 tenants — Complexity

No indicators found with deviant objects

3. Click on a tile with the IoE that you want to investigate.

4. The Indicator Identity Details pane opens with the following information:

   - **Vulnerability information**: How the exposure to a potential attack can occur.

   - **Findings**: Details about the identity provider type and a description of the risk.

   - **Recommendations**: Steps to remediate the threat.

Remediate Deviances from Indicators of Exposure

Tenable Identity Exposure triggers alerts when an Indicator of Exposure (IoE) encounters deviant objects which require remediation.

The following are examples showing how to perform a remediation procedure for three specific IoEs.

- AdminCount Attribute Set on Standard Users
- Dangerous Kerberos Delegation
- Ensure SDProp Consistency

For complete information about IoEs, see the documentation provided in the Tenable Identity Exposure user interface.

AdminCount Attribute Set on Standard Users

The `adminCount` attribute on a user account indicates its past membership in an administrative group and does not get reset when the account leaves the group. As a result, even old administrative accounts have this attribute, which blocks the inheritance of Active Directory permissions. While originally intended to protect administrators, it can create challenging permission issues.

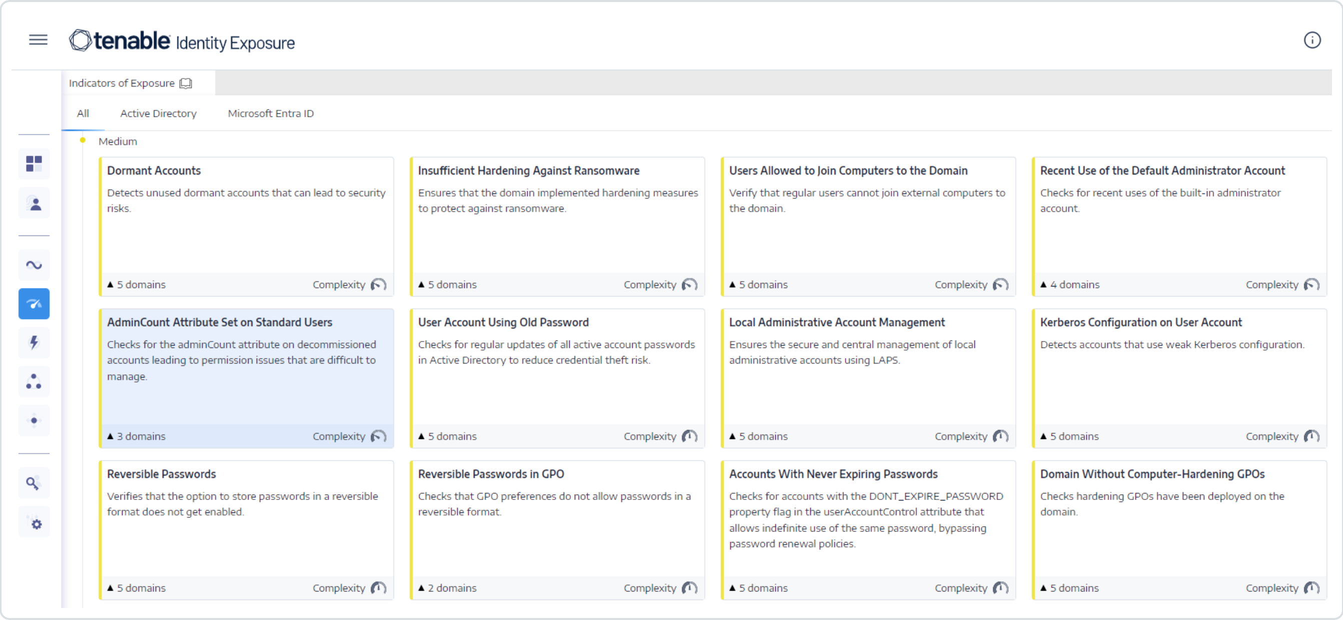
This medium-level IoE only reports on active user accounts and groups with this attribute and excludes privileged groups with legitimate members that have the `adminCount` attribute set to `1`.

To remediate a deviant object from the **AdminCount Attribute Set on Standard Users** IoE:

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

   By default, Tenable Identity Exposure shows only the IoEs that contain deviant objects.

2. Click on the tile for the **AdminCount Attribute Set on Standard Users** IoE.

   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

   Recent Use of the Default Administrator Account
   Checks for recent uses of the built-in administrator account.
   ▲ 4 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.
   ▲ 5 domains Complexity

   Local Administrative Account Management
   Ensures the secure and central management of local administrative accounts using LAPS.
   ▲ 5 domains Complexity

   Kerberos Configuration on User Account
   Detects accounts that use weak Kerberos configuration.
   ▲ 5 domains Complexity

   Reversible Passwords
   Verifies that the option to store passwords in a reversible format does not get enabled.
   ▲ 5 domains Complexity

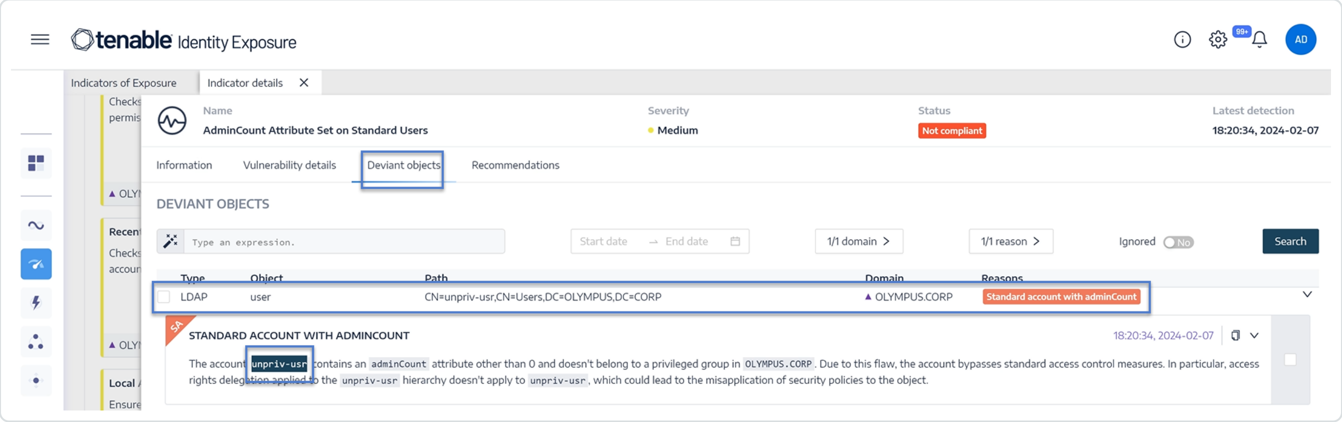
   Reversible Passwords in GPO
   Checks that GPO preferences do not allow passwords in a reversible format.
   ▲ 2 domains Complexity

   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.
   ▲ 5 domains Complexity

   Domain Without Computer-Hardening GPOs
   Checks hardening GPOs have been deployed on the domain.
   ▲ 5 domains Complexity

   The **Indicator details** pane opens.

3. Hover over and click on the deviant object to show its details, and note the domain name and the account. (In this example: Domain = `OLYMPUS.CORP` and the standard account is `unpriv-usr`)



Name: AdminCount Attribute Set on Standard Users | Severity: Medium | Status: Not compliant | Latest detection: 18:20:34, 2024-02-07

DEVIANT OBJECTS

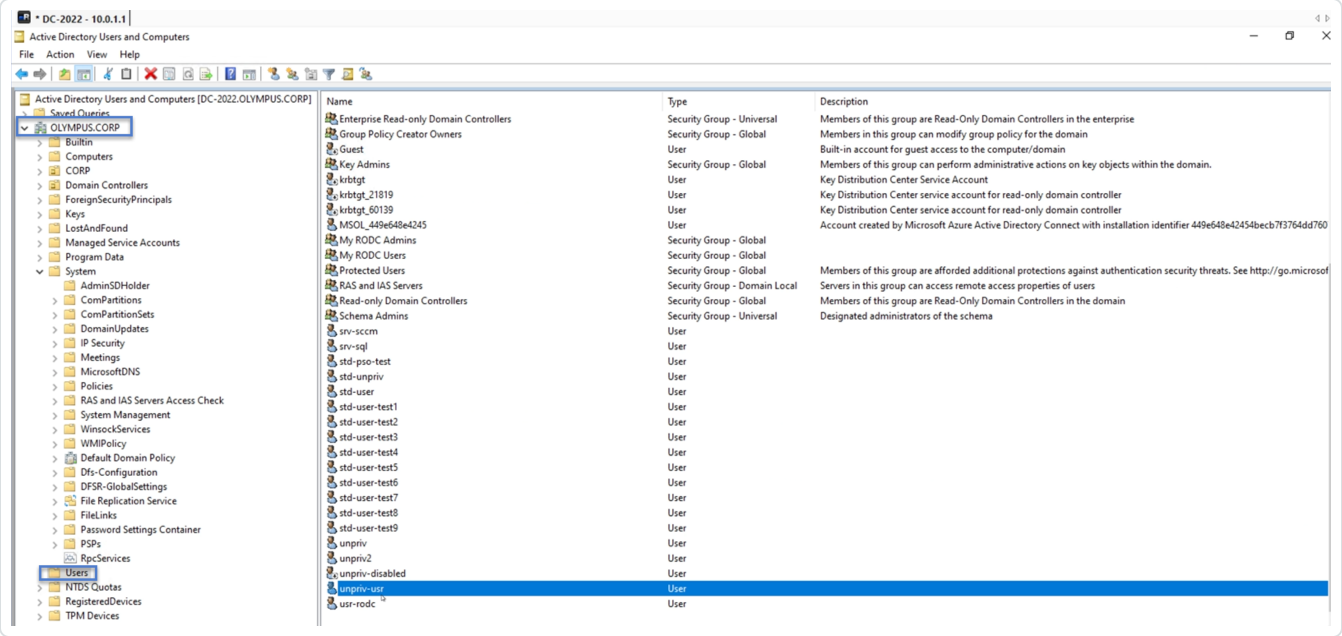
Type	Object	Path	Domain	Reasons
LDAP	user	CN=unpriv-usr,CN=Users,DC=OLYMPUS,DC=CORP	OLYMPUS.CORP	Standard account with adminCount

STANDARD ACCOUNT WITH ADMINCOUNT — 18:20:34, 2024-02-07

The account `unpriv-usr` contains an `adminCount` attribute other than 0 and doesn't belong to a privileged group in `OLYMPUS.CORP`. Due to this flaw, the account bypasses standard access control measures. In particular, access rights delegation applied to the `unpriv-usr` hierarchy doesn't apply to `unpriv-usr`, which could lead to the misapplication of security policies to the object.

4. In Remote Desktop Manager (or similar tool), locate the domain name and navigate to **Users** and the account that Tenable Identity Exposure flagged.

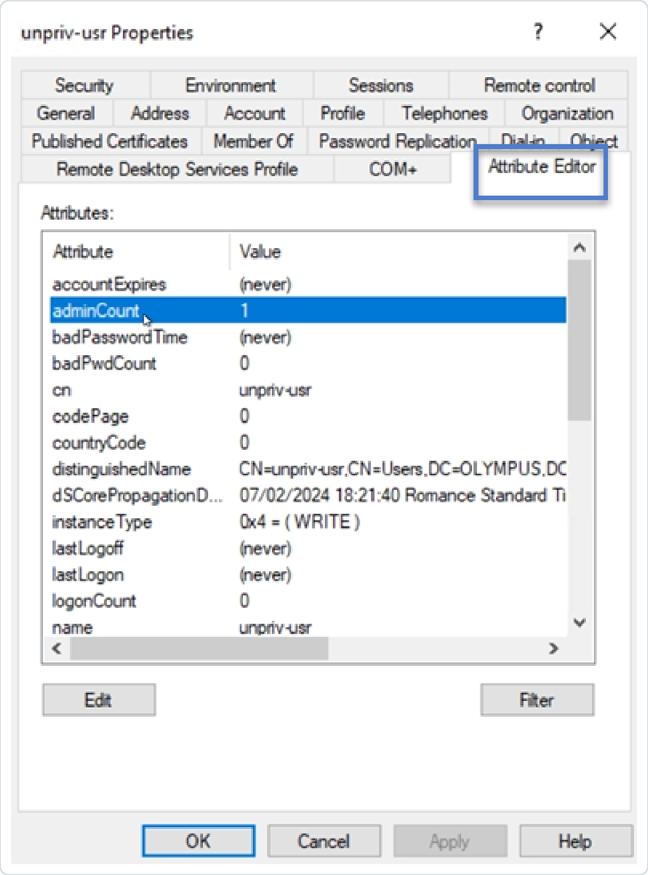
> **Required permission**: You must have an administrator account on the domain to perform the procedure.



Name	Type	Description
Enterprise Read-only Domain Controllers	Security Group - Universal	Members of this group are Read-Only Domain Controllers in the enterprise
Group Policy Creator Owners	Security Group - Global	Members in this group can modify group policy for the domain
Guest	User	Built-in account for guest access to the computer/domain
Key Admins	Security Group - Global	Members of this group can perform administrative actions on key objects within the domain.
krbtgt	User	Key Distribution Center Service Account
krbtgt_21819	User	Key Distribution Center service account for read-only domain controller
krbtgt_60139	User	Key Distribution Center service account for read-only domain controller
MSOL_449e648e4245	User	Account created by Microsoft Azure Active Directory Connect with installation identifier 449e648e42454becb7f3764dd760
My RODC Admins	Security Group - Global	
My RODC Users	Security Group - Global	
Protected Users	Security Group - Global	Members of this group are afforded additional protections against authentication security threats. See http://go.microsof
RAS and IAS Servers	Security Group - Domain Local	Servers in this group can access remote access properties of users
Read-only Domain Controllers	Security Group - Global	Members of this group are Read-Only Domain Controllers in the domain
Schema Admins	Security Group - Universal	Designated administrators of the schema
srv-sccm	User	
srv-sql	User	
std-pso-test	User	
std-unpriv	User	
std-user	User	
std-user-test1	User	
std-user-test2	User	
std-user-test3	User	
std-user-test4	User	
std-user-test5	User	
std-user-test6	User	
std-user-test7	User	
std-user-test8	User	
std-user-test9	User	
unpriv	User	
unpriv2	User	
unpriv-disabled	User	
unpriv-usr	User	
usr-rodc	User	

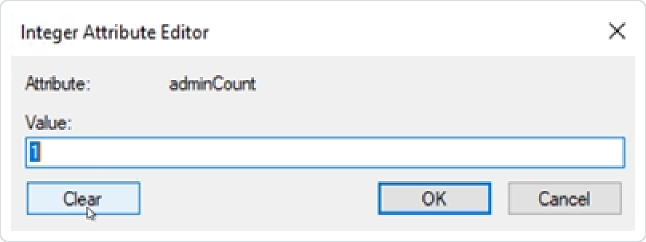
5. Click on the account name to open its **Properties** dialog box and select the **Attribute Editor** tab.

6. From the list of attributes, click on `adminCount` to open the **Integer Attribute Editor** dialog box.



Attribute	Value
accountExpires	(never)
adminCount	1
badPasswordTime	(never)
badPwdCount	0
cn	unpriv-usr
codePage	0
countryCode	0
distinguishedName	CN=unpriv-usr,CN=Users,DC=OLYMPUS,DC
dSCorePropagationD...	07/02/2024 18:21:40 Romance Standard Ti
instanceType	0x4 = (WRITE)
lastLogoff	(never)
lastLogon	(never)
logonCount	0
name	unpriv-usr

7. In the dialog box, click **Clear** and **OK**.



Attribute: adminCount

Value: 1

8. In Tenable Identity Exposure, return to the Indicator details pane and refresh the page.

   The deviant object no longer appears in the list.

Dangerous Kerberos Delegation

The Kerberos protocol, which is central to Active Directory security, permits select servers to reuse user credentials. If an attacker compromises one of these servers, they could steal these credentials and use them to authenticate on other resources.

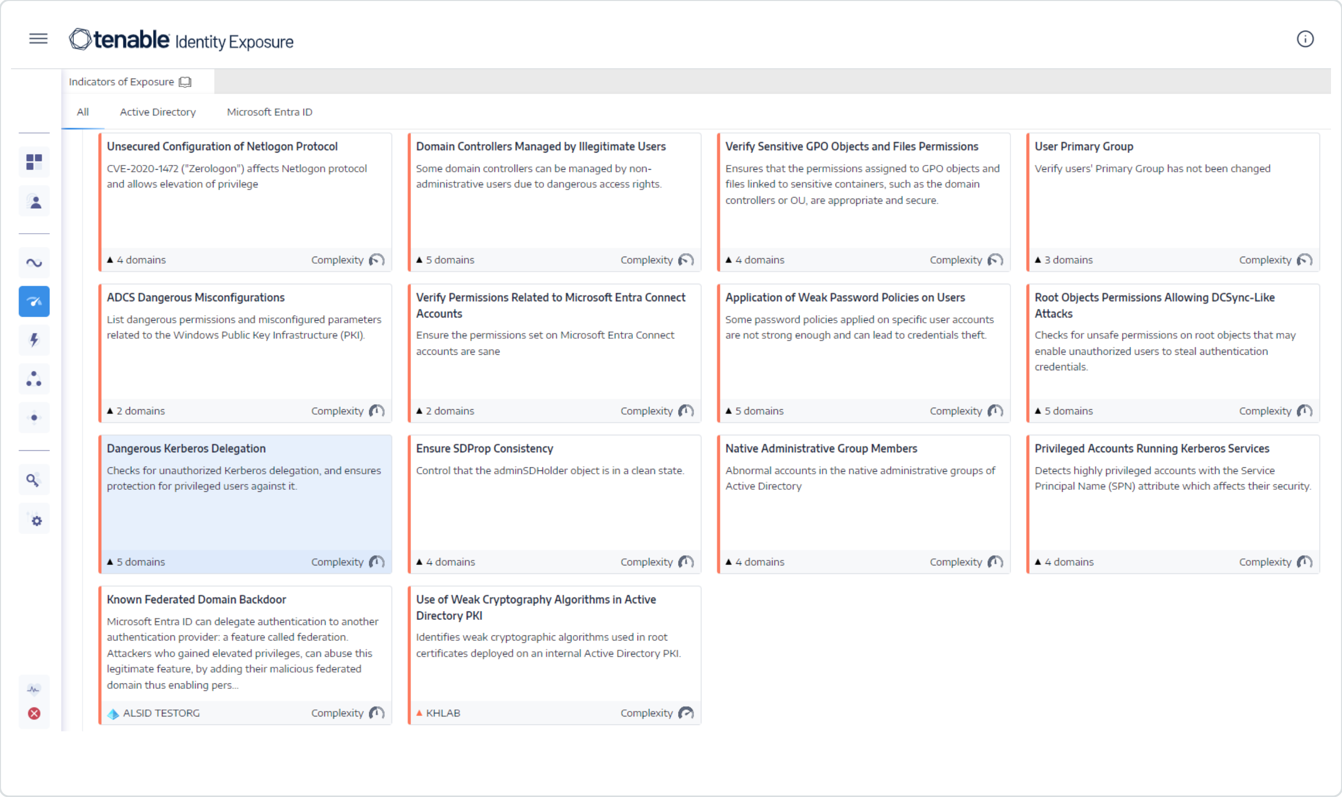
This critical-level IoE reports all accounts with delegation attributes and excludes disabled accounts. Privileged users should not have delegation attributes. To protect these user accounts, add them to the "Protected Users" group or mark them as "Account is sensitive and cannot be delegated".

To add the account to the "Protected Group":

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

   By default, Tenable Identity Exposure shows only the IoEs that contain deviant objects.

2. Click on the tile for the **Dangerous Kerberos Delegation** IoE.



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

User Primary Group
Verify users' Primary Group has not been changed
3 domains — Complexity

ADCS Dangerous Misconfigurations
List dangerous permissions and misconfigured parameters related to the Windows Public Key Infrastructure (PKI).
2 domains — Complexity

Verify Permissions Related to Microsoft Entra Connect Accounts
Ensure the permissions set on Microsoft Entra Connect accounts are sane
2 domains — Complexity

Application of Weak Password Policies on Users
Some password policies applied on specific user accounts are not strong enough and can lead to credentials theft.
5 domains — Complexity

Root Objects Permissions Allowing DCSync-Like Attacks
Checks for unsafe permissions on root objects that may enable unauthorized users to steal authentication credentials.
5 domains — Complexity

Dangerous Kerberos Delegation
Checks for unauthorized Kerberos delegation, and ensures protection for privileged users against it.
5 domains — Complexity

Ensure SDProp Consistency
Control that the adminSDHolder object is in a clean state.
4 domains — Complexity

Native Administrative Group Members
Abnormal accounts in the native administrative groups of Active Directory
4 domains — Complexity

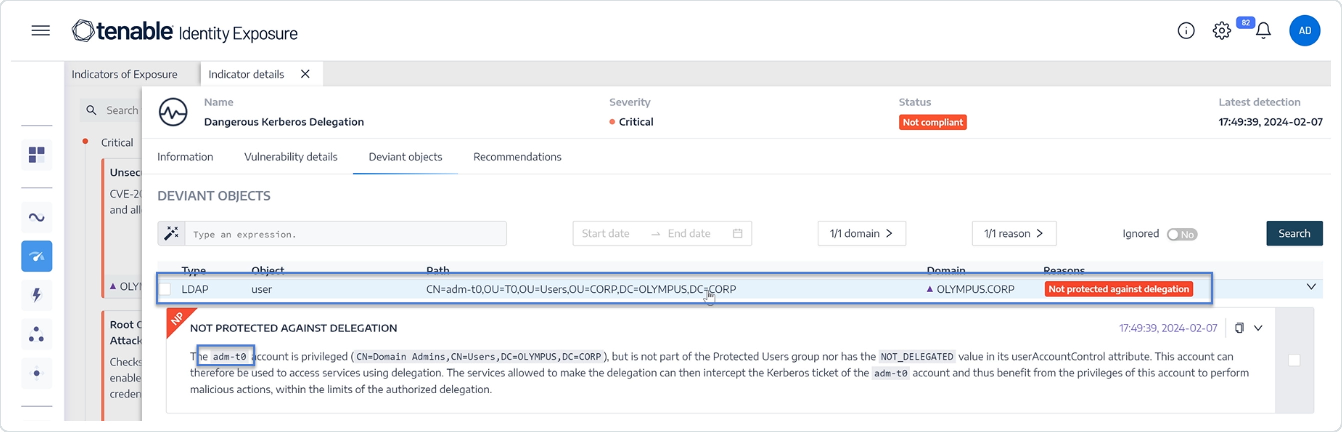
Privileged Accounts Running Kerberos Services
Detects highly privileged accounts with the Service Principal Name (SPN) attribute which affects their security.
4 domains — Complexity

Known Federated Domain Backdoor
Microsoft Entra ID can delegate authentication to another authentication provider: a feature called federation. Attackers who gained elevated privileges, can abuse this legitimate feature, by adding their malicious federated domain thus enabling pers...
ALSID TESTORG — Complexity

Use of Weak Cryptography Algorithms in Active Directory PKI
Identifies weak cryptographic algorithms used in root certificates deployed on an internal Active Directory PKI.
KHLAB — Complexity

The **Indicator details** pane opens.

3. Hover over and click on the deviant object to show its details, note the domain name and the account. (In this example: Domain = OLYMPUS.CORP and account = `adm-t0`)



Name: Dangerous Kerberos Delegation
Severity: Critical
Status: Not compliant
Latest detection: 17:49:39, 2024-02-07

Type	Object	Path	Domain	Reasons
LDAP	user	CN=adm-t0,OU=T0,OU=Users,OU=CORP,DC=OLYMPUS,DC=CORP	OLYMPUS.CORP	Not protected against delegation

NOT PROTECTED AGAINST DELEGATION

17:49:39, 2024-02-07

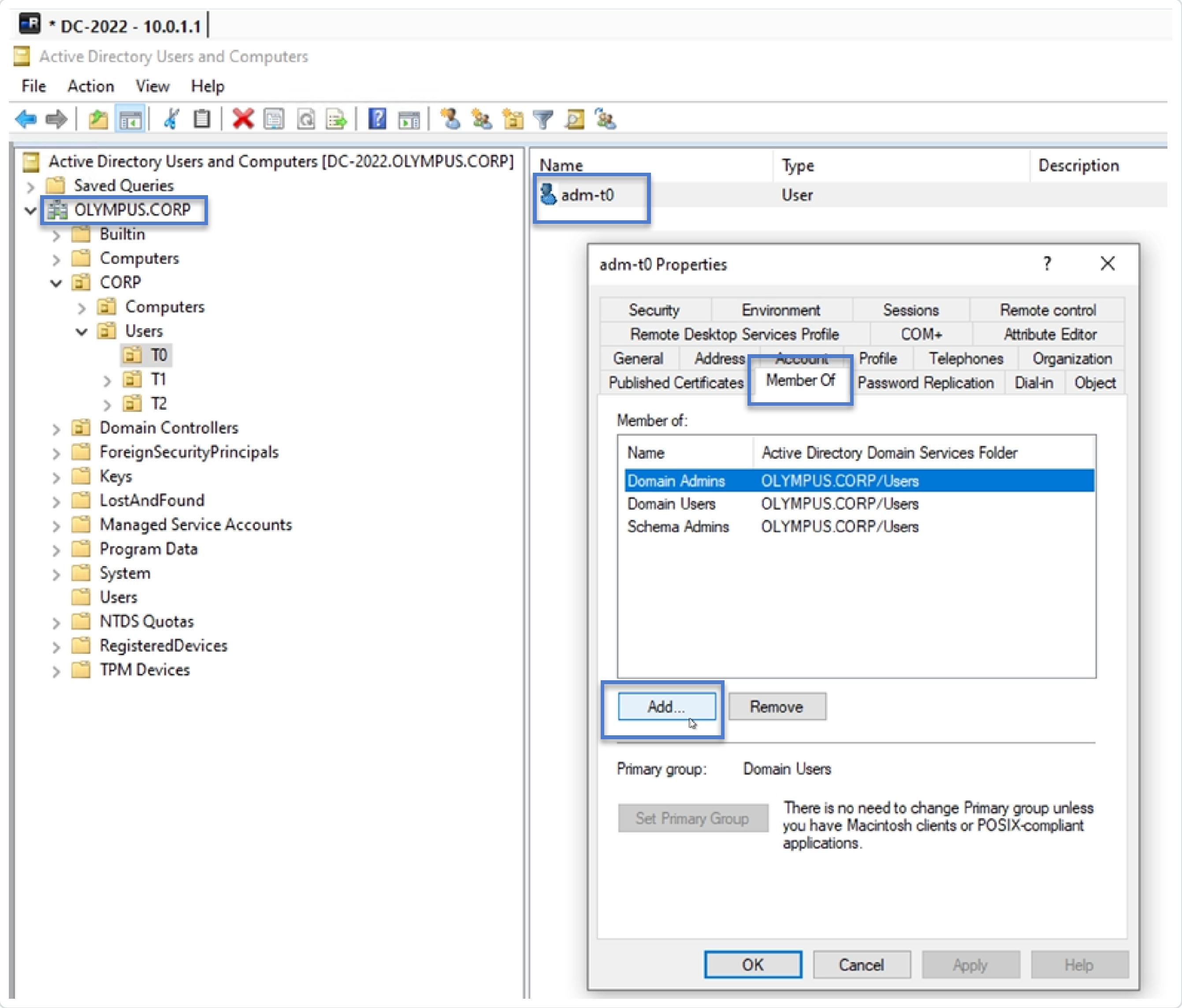
The `adm-t0` account is privileged (`CN=Domain Admins,CN=Users,DC=OLYMPUS,DC=CORP`), but is not part of the Protected Users group nor has the `NOT_DELEGATED` value in its userAccountControl attribute. This account can therefore be used to access services using delegation. The services allowed to make the delegation can then intercept the Kerberos ticket of the `adm-t0` account and thus benefit from the privileges of this account to perform malicious actions, within the limits of the authorized delegation.

4. In Remote Desktop Manager (or similar tool), locate the domain name and navigate to the domain and account that Tenable Identity Exposure flagged.

> **Required permission**: You must have an administrator account on the domain to perform the procedure.

5. Click on the account name to open its **Properties** dialog box and select the **Member Of** tab.

6. From the member list, click **Add**.



Member of:

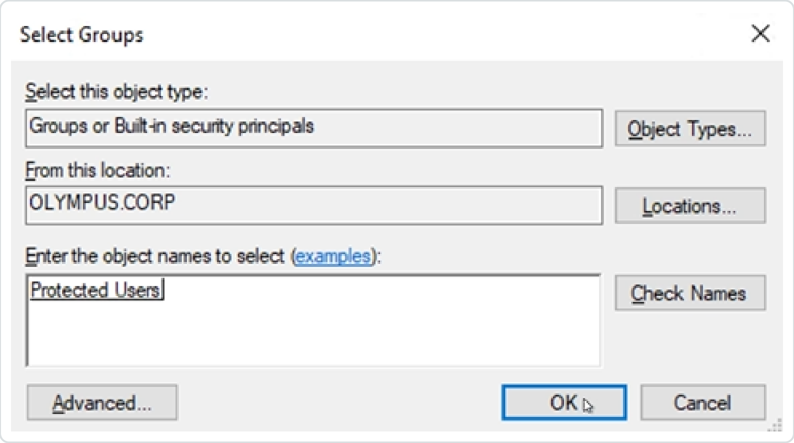
Name	Active Directory Domain Services Folder
Domain Admins	OLYMPUS.CORP/Users
Domain Users	OLYMPUS.CORP/Users
Schema Admins	OLYMPUS.CORP/Users

Primary group: Domain Users

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

The **Select Groups** dialog box appears.

7. Enter the object name "Protected Users" and click **Check Names**.



Select this object type: Groups or Built-in security principals

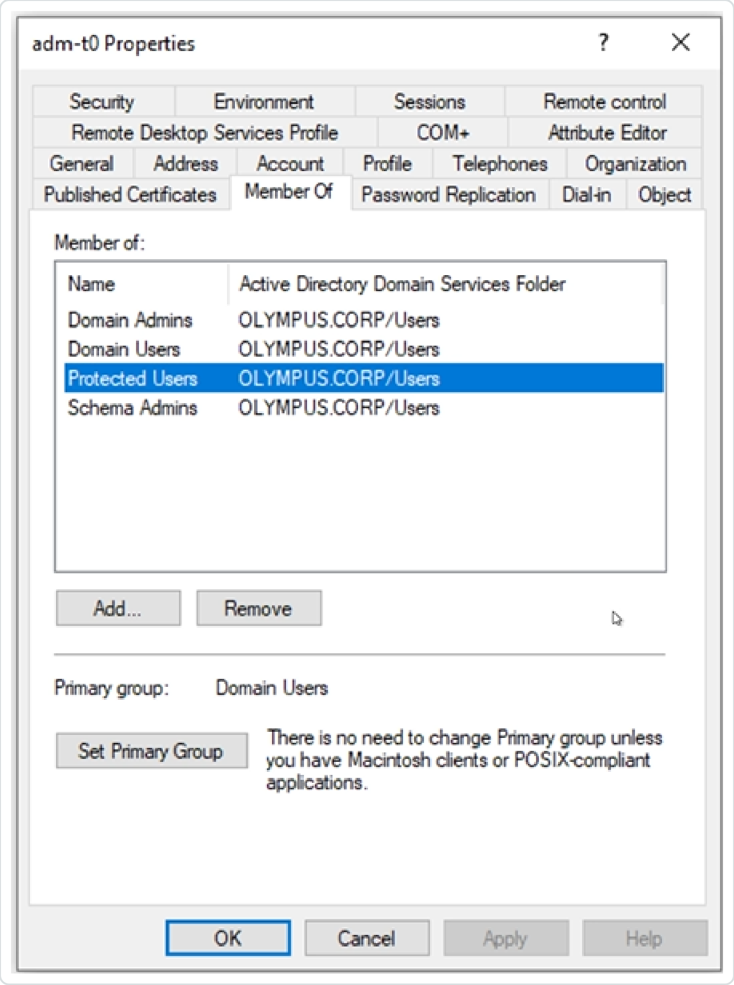
From this location: OLYMPUS.CORP

Enter the object names to select (examples): Protected Users

8. Click **OK** to close the dialog box.

9. In the **Properties** dialog box, click **Apply**.

   The new group appears on the member list.



Member of:

Name	Active Directory Domain Services Folder
Domain Admins	OLYMPUS.CORP/Users
Domain Users	OLYMPUS.CORP/Users
Protected Users	OLYMPUS.CORP/Users
Schema Admins	OLYMPUS.CORP/Users

Primary group: Domain Users

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

10. Click **OK** to close the dialog box.

11. In Tenable Identity Exposure, return to the Indicator details pane and refresh the page.

    The deviant object no longer appears in the list.

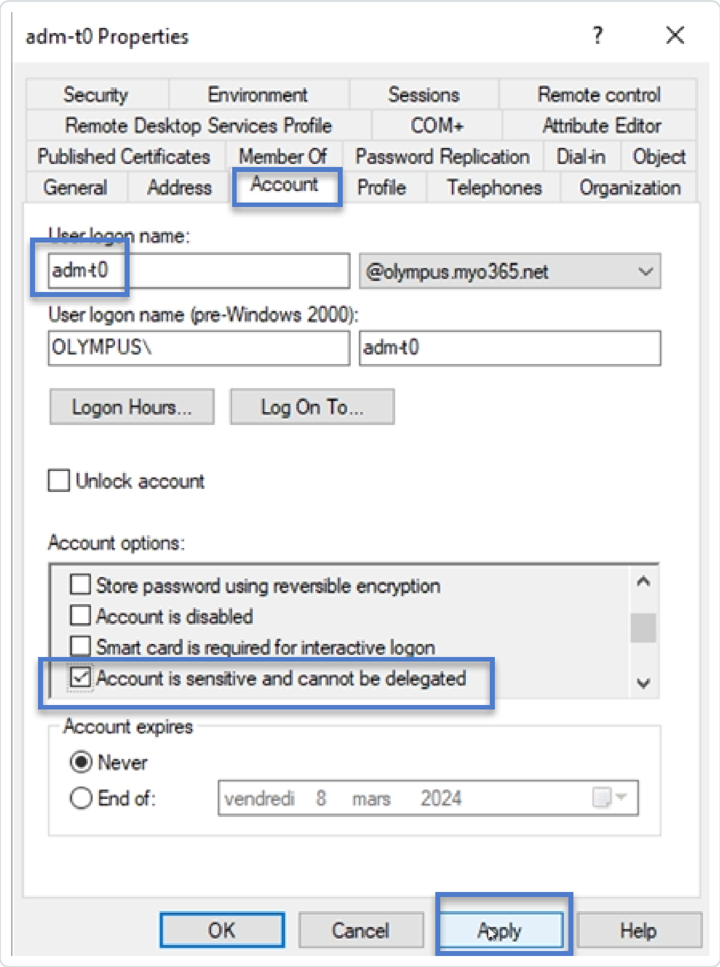
To set the account as "cannot be delegated":

1. In Remote Desktop Manager, locate the domain name and navigate to the domain and account that Tenable Identity Exposure flagged.

   > **Required permission**: You must have an administrator account on the domain to perform the procedure.

2. Click on the account name to open its **Properties** dialog box and select the **Account** tab.

3. From the list of account options, select "Account is sensitive and cannot be delegated" and click **Apply**.



User logon name:
adm-t0 @olympus.myo365.net

User logon name (pre-Windows 2000):
OLYMPUS\ adm-t0

□ Unlock account

Account options:
□ Store password using reversible encryption
□ Account is disabled
□ Smart card is required for interactive logon
☑ Account is sensitive and cannot be delegated

Account expires
● Never
○ End of: vendredi 8 mars 2024

4. Click **OK** to close the dialog box.

5. In Tenable Identity Exposure, return to the Indicator details pane and refresh the page.

   The deviant object no longer appears in the list.

Ensure SDProp Consistency

Attackers who compromise an Active Directory domain commonly change the ACL of the `adminSDHolder` object, and any permission they add to the ACL gets copied to privileged users, making it easy to set up backdoors.

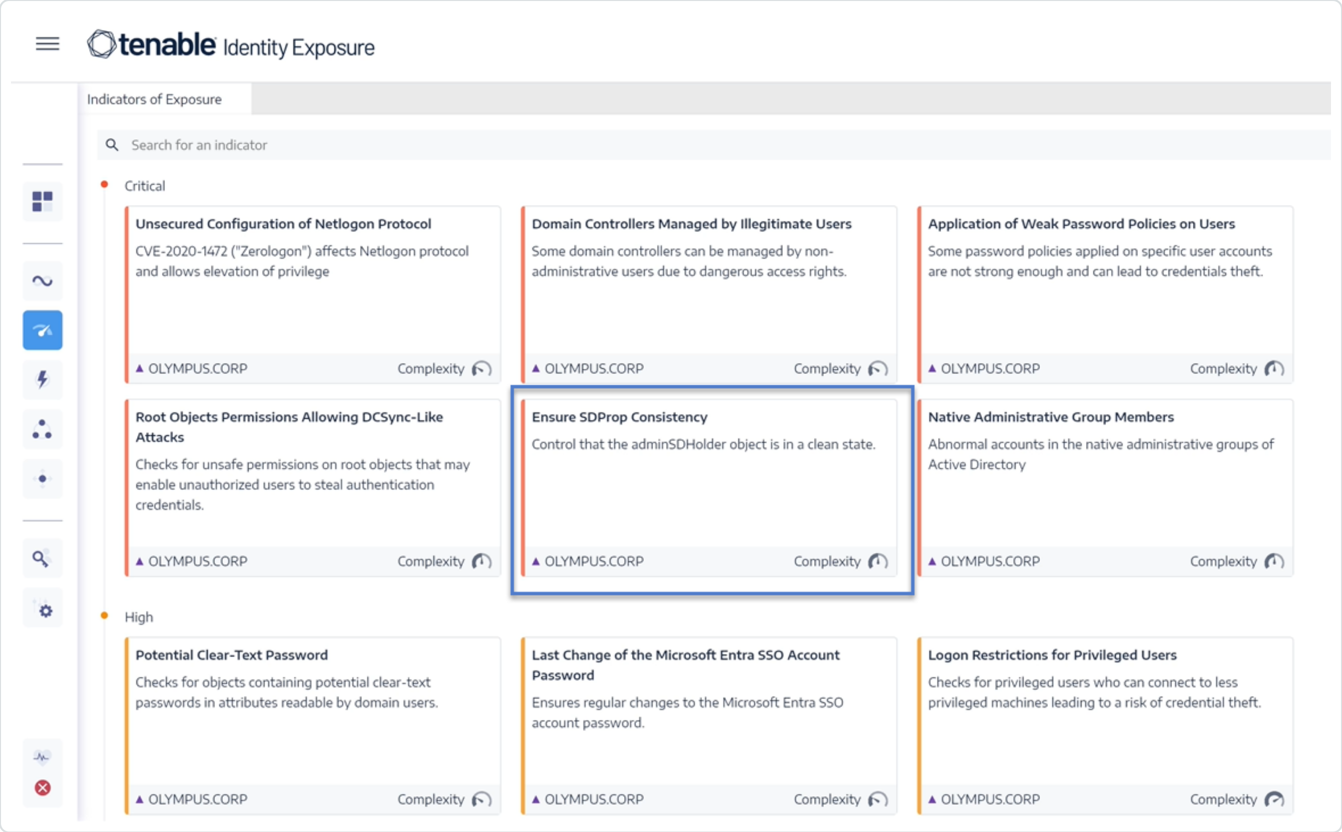
This critical-level IoE checks that the permissions set on the `adminSDHolder` object allow only privileged access to administrative accounts.

To remediate a deviant object from the **Ensure SDProp Consistency** IoE:

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

   By default, Tenable Identity Exposure shows only the IoEs that contain deviant objects.

2. Click on the tile for the **Ensure SDProp Consistency** IoE.



Critical

Unsecured Configuration of Netlogon Protocol
CVE-2020-1472 ("Zerologon") affects Netlogon protocol and allows elevation of privilege
OLYMPUS.CORP Complexity

Domain Controllers Managed by Illegitimate Users
Some domain controllers can be managed by non-administrative users due to dangerous access rights.
OLYMPUS.CORP Complexity

Application of Weak Password Policies on Users
Some password policies applied on specific user accounts are not strong enough and can lead to credentials theft.
OLYMPUS.CORP Complexity

Root Objects Permissions Allowing DCSync-Like Attacks
Checks for unsafe permissions on root objects that may enable unauthorized users to steal authentication credentials.
OLYMPUS.CORP Complexity

Ensure SDProp Consistency
Control that the adminSDHolder object is in a clean state.
OLYMPUS.CORP Complexity

Native Administrative Group Members
Abnormal accounts in the native administrative groups of Active Directory
OLYMPUS.CORP Complexity

High

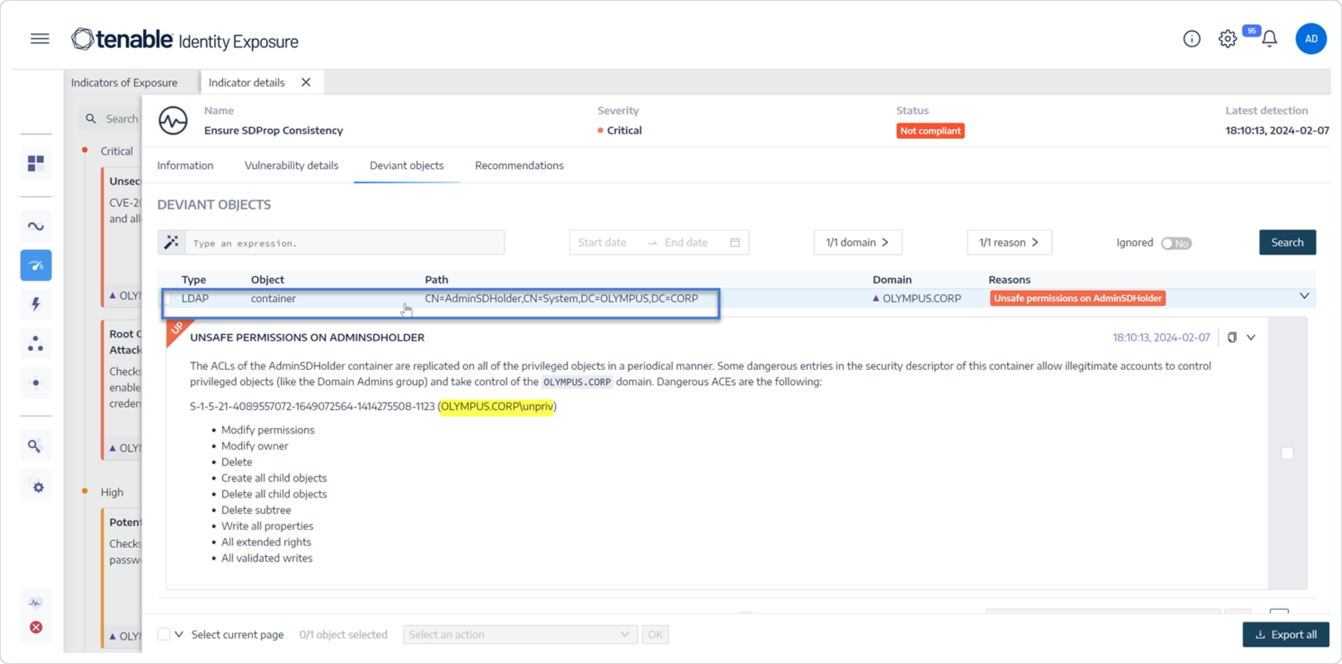
Potential Clear-Text Password
Checks for objects containing potential clear-text passwords in attributes readable by domain users.
OLYMPUS.CORP Complexity

Last Change of the Microsoft Entra SSO Account Password
Ensures regular changes to the Microsoft Entra SSO account password.
OLYMPUS.CORP Complexity

Logon Restrictions for Privileged Users
Checks for privileged users who can connect to less privileged machines leading to a risk of credential theft.
OLYMPUS.CORP Complexity

The **Indicator details** pane opens.

3. Hover over and click on the deviant object to show its details. Note the domain name and the associated permission that Tenable Identity Exposure flagged. (In this example: `OLYMPUS.CORP .\unpriv`)



Name	Severity	Status	Latest detection
Ensure SDProp Consistency	Critical	Not compliant	18:10:13, 2024-02-07

DEVIANT OBJECTS

Type	Object	Path	Domain	Reasons
LDAP	container	CN=AdminSDHolder,CN=System,DC=OLYMPUS,DC=CORP	OLYMPUS.CORP	Unsafe permissions on AdminSDHolder

UNSAFE PERMISSIONS ON ADMINSDHOLDER 18:10:13, 2024-02-07

The ACLs of the AdminSDHolder container are replicated on all of the privileged objects in a periodical manner. Some dangerous entries in the security descriptor of this container allow illegitimate accounts to control privileged objects (like the Domain Admins group) and take control of the `OLYMPUS.CORP` domain. Dangerous ACEs are the following:

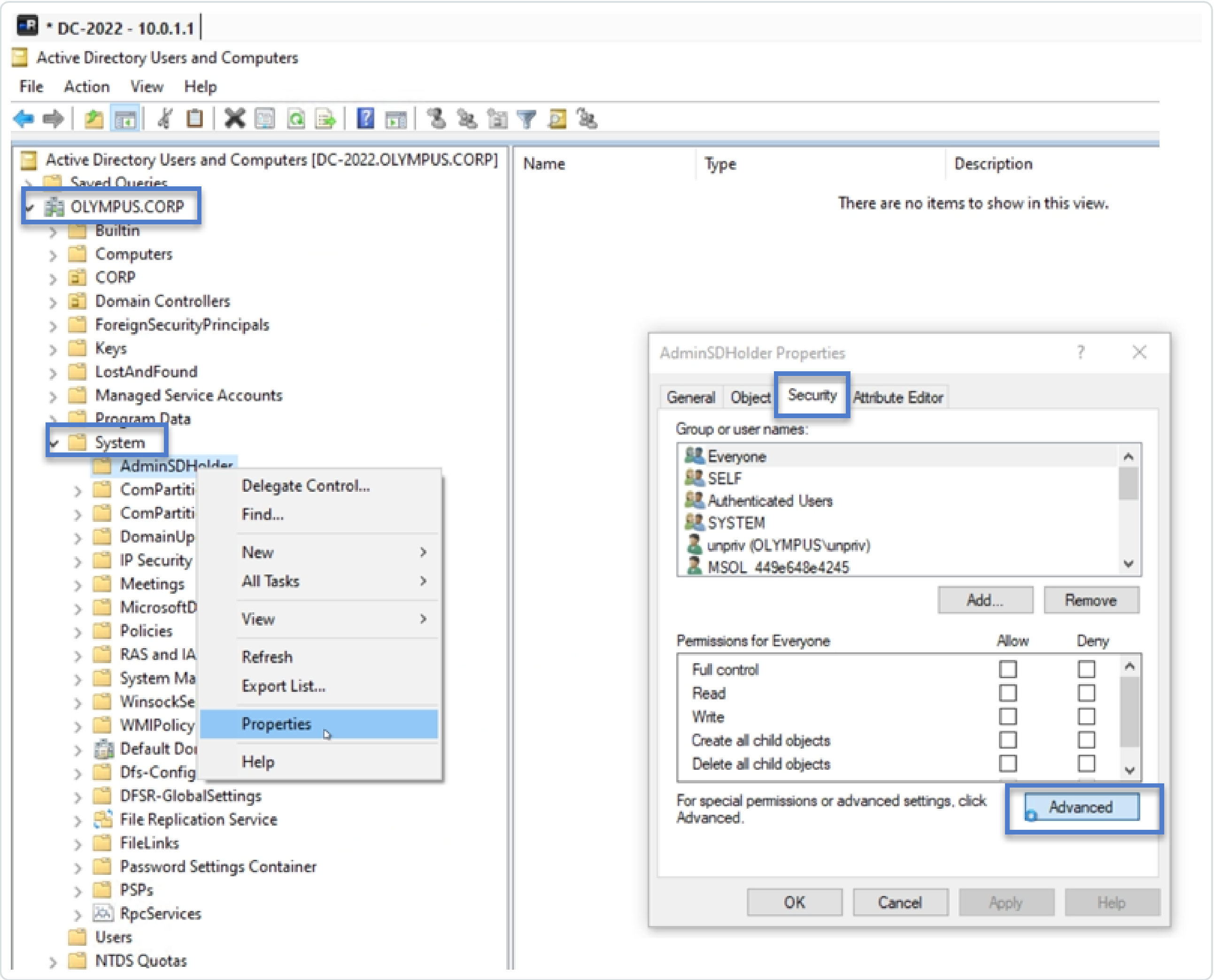
S-1-5-21-4089557072-1649072564-1414275508-1123 (OLYMPUS.CORP\unpriv)

- Modify permissions
- Modify owner
- Delete
- Create all child objects
- Delete all child objects
- Delete subtree
- Write all properties
- All extended rights
- All validated writes

4. In Remote Desktop Manager (or similar tool), locate the domain name and navigate to **System** > **AdminSDHolder**.

> **Required permission**: You must have an administrator account on the domain to perform the procedure.

5. Right-click **AdminSDHolder** and select **Properties** from the contextual menu.



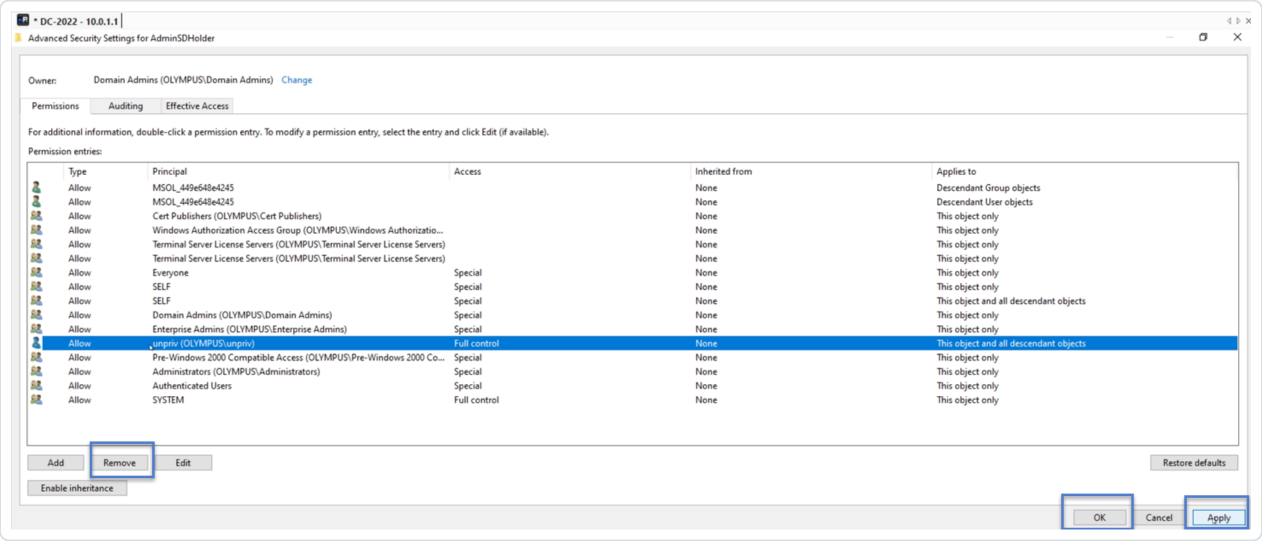
6. In the **Properties** dialog box, select the **Security** tab and click **Advanced**.

7. In the **Advanced Security Settings** window and in the **Permissions** tab, select the permission that raised the alert from the list of permission entries.

8. Click **Remove**.

9. Click **Apply** and **OK** to close the settings window.

10. Click **OK** to close the **Properties** window.



Owner: Domain Admins (OLYMPUS\Domain Admins) Change

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

Type	Principal	Access	Inherited from	Applies to
Allow	MSOL_449e648e4245		None	Descendant Group objects
Allow	MSOL_449e648e4245		None	Descendant User objects
Allow	Cert Publishers (OLYMPUS\Cert Publishers)		None	This object only
Allow	Windows Authorization Access Group (OLYMPUS\Windows Authorizatio...		None	This object only
Allow	Terminal Server License Servers (OLYMPUS\Terminal Server License Servers)		None	This object only
Allow	Terminal Server License Servers (OLYMPUS\Terminal Server License Servers)		None	This object only
Allow	Everyone	Special	None	This object only
Allow	SELF	Special	None	This object only
Allow	SELF	Special	None	This object and all descendant objects
Allow	Domain Admins (OLYMPUS\Domain Admins)	Special	None	This object only
Allow	Enterprise Admins (OLYMPUS\Enterprise Admins)	Special	None	This object only
Allow	unpriv (OLYMPUS\unpriv)	Full control	None	This object and all descendant objects
Allow	Pre-Windows 2000 Compatible Access (OLYMPUS\Pre-Windows 2000 Co...	Special	None	This object only
Allow	Administrators (OLYMPUS\Administrators)	Special	None	This object only
Allow	Authenticated Users	Special	None	This object only
Allow	SYSTEM	Full control	None	This object only

11. In Tenable Identity Exposure, return to the Indicator details pane and refresh the page.

    The deviant object no longer appears in the list.

Indicators of Attack

Required license: Indicators of Attack

Tenable Identity Exposure 's **Indicators of Attack** (IoA) give you the ability to detect attacks on your Active Directory (AD).

A consolidated view of Indicators of Attack shows a timeline and the top 3 incidents that impacted your AD in real time and the attack distribution in a single pane. You can do the following:

- Visualize every threat from an accurate attack timeline.
- Analyze in-depth details about an AD attack.
- Explore MITRE ATT&CK descriptions directly from detected incidents.

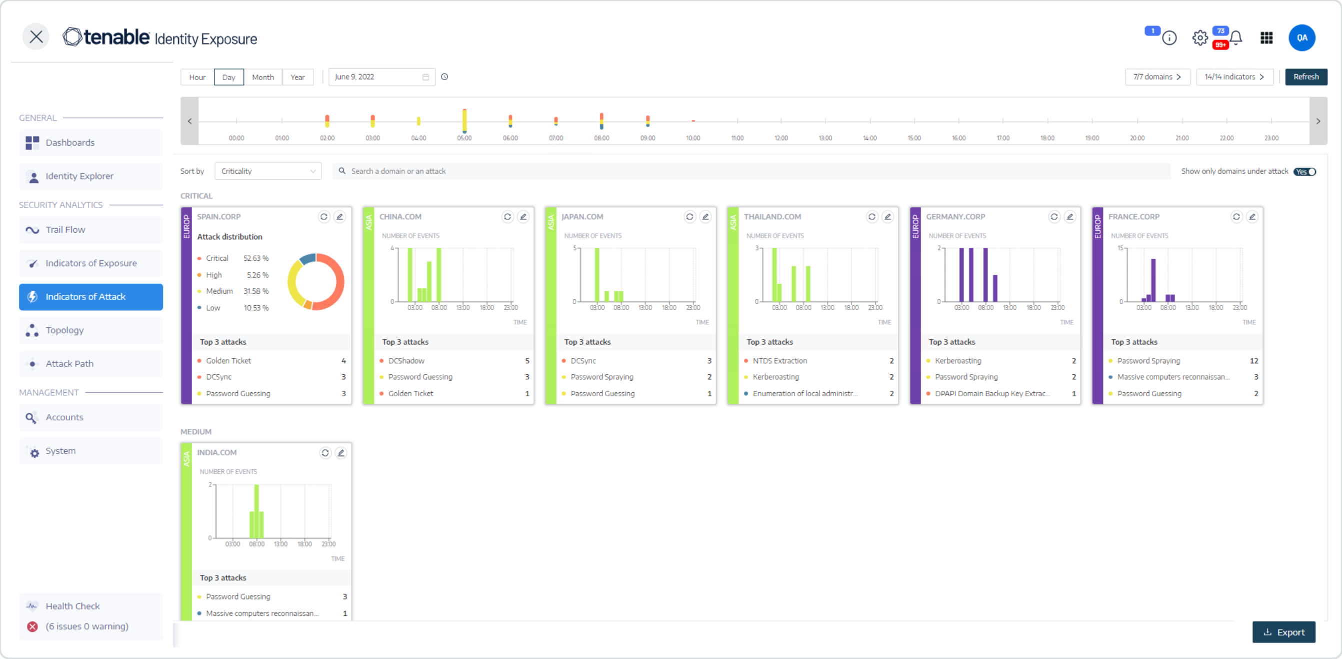
For more information about specific IoAs, see Indicators of Attack and the Active Directory.

Note: If you observe a high number of detected attacks, verify that your administrator correctly calibrated the Indicators of Attack by applying the recommended values for the various IoA options. For more information, see To calibrate IoAs.

To show Indicators of Attack:

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

   The **Indicator of Attacks** pane opens.



2. By default, Tenable Identity Exposure shows all your AD forests and domains. To adjust this view, do any of the following:

   - Select the time period to show — Click on **Hour**, **Day** (default), **Month**, or **Year**.

   - Move along the timeline — Click on the left or right arrow to go forward or backward on the timeline.

   - Select a specific time — Click on the date picker to choose an hour, day, month, or year.

   - Return to current date and time — Click the 🕓 icon next to the date picker.

   - Select the domains — Click on **n/n domains**.

     a. In the **Forest and Domains** pane, select the domains.

     b. Click **Filter on selection**.

        Tenable Identity Exposure updates the view.

- Select the IoAs — Click on **n/n indicators**.

    a. In the Indicators of Attack pane, select the IoAs.

    b. Click **Filter on selection**.

       Tenable Identity Exposure updates the view.

- Sort the IoA tiles — In the **Sort by** box, click the arrow to show a drop-down list of choices: **Domain**, **Criticality**, or **Forest**.

- Search for a domain or attack — In the **Search** box, type the domain name or attack.

- Show only domains under attack — Click the **Show only domains under attack** toggle to **Yes**.

- Export an attack report — Click **Export**.

  The **Export Cards** pane appears.

    a. In the **Export format** box, click the drop-down list arrow to select a format: **PDF**, **CSV**, or **PPTX**.

    b. Click **Export**.

       Tenable Identity Exposure downloads the report to the local machine.

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.

See also

- Indicator of Attack Details
- Indicators of Attack Incidents

Indicator of Attack Details

The Tenable Identity Exposure's Indicator of Attack pane shows information about attacks that occurred in your Active Directory.

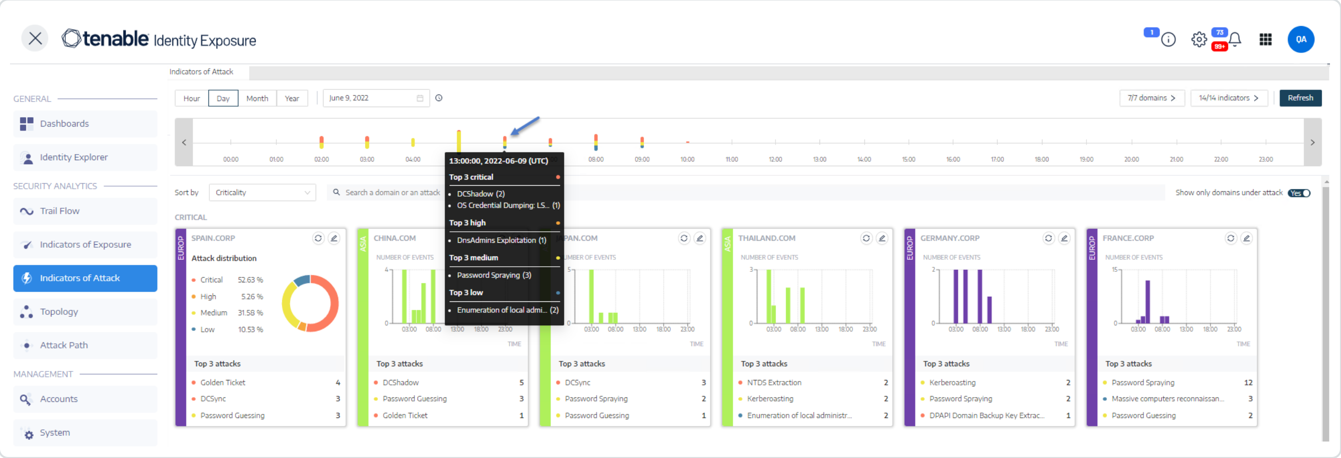
To view Indicators of Attack:

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

  The **Indicator of Attacks** pane opens.

To show attack information on the timeline:

- Click on any event along the timeline to show:
  - The incident detection date and time.
  - The severity level of the top 3 attacks.
  - The total number of attacks detected on this date and time.



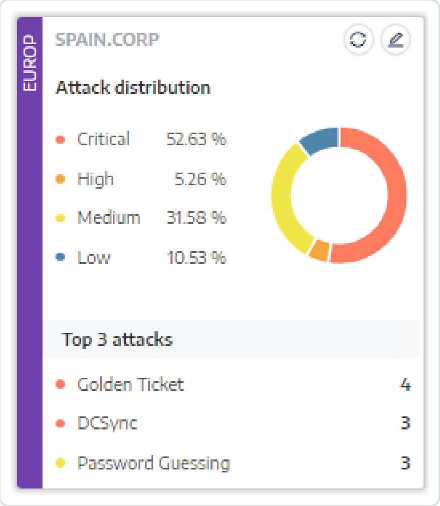
To change the chart type:

1. Click on the ✎ icon to edit the domain tile.

   The **Edit Card Information** pane appears.

2. Select a chart type:

- **Attack distribution**: Shows the distribution of the attack severity.



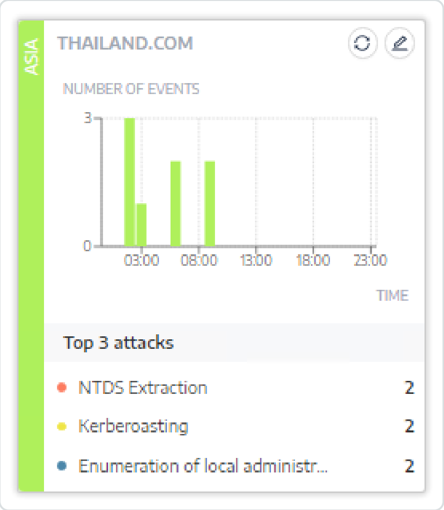
SPAIN.CORP

Attack distribution

● Critical	52.63 %
● High	5.26 %
● Medium	31.58 %
● Low	10.53 %

Top 3 attacks	
● Golden Ticket	4
● DCSync	3
● Password Guessing	3

- **Number of events:** Shows the Top 3 attacks and their number of occurrences.



THAILAND.COM

Top 3 attacks	
● NTDS Extraction	2
● Kerberoasting	2
● Enumeration of local administr...	2

3. Click **Save**.

   Tenable Identity Exposure updates the chart.

See also

- Indicators of Attack
- Indicators of Attack Incidents

Indicators of Attack Incidents

The Indicators of Attack (IoA) list of incidents provides detailed information about specific attacks on your Active Directory (AD). This allows you to take the required action depending on the IoA's severity level.

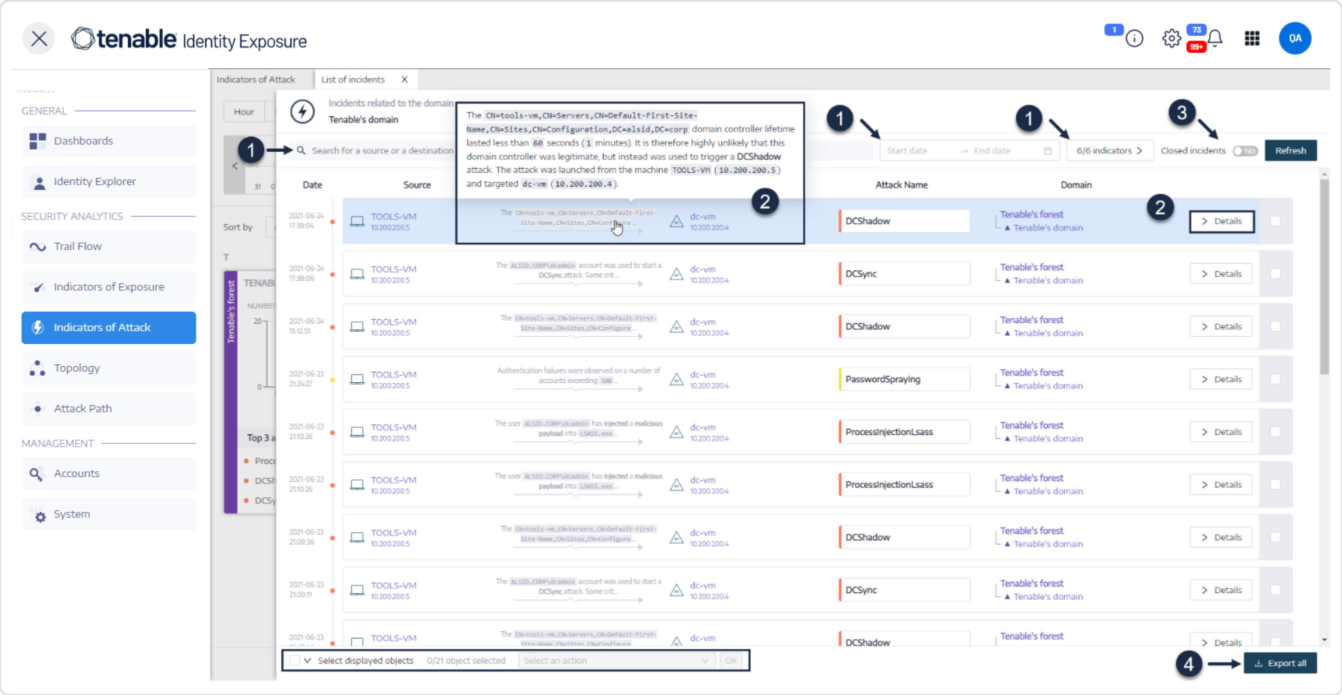
To view attack incidents:

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

   The **Indicator of Attacks** pane opens.

2. Click on any domain tile.

   The **List of incidents** pane appears with a list of incidents that occurred on the domain.



The `CN=tools-vm,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=alsid,DC=corp` domain controller lifetime lasted less than `60` seconds (`1` minutes). It is therefore highly unlikely that this domain controller was legitimate, but instead was used to trigger a DCShadow attack. The attack was launched from the machine `TOOLS-VM` (`10.200.200.5`) and targeted `dc-vm` (`10.200.200.4`).

Date	Source			Attack Name	Domain		
2021-06-24 17:39:04	TOOLS-VM 10.200.200.5	The `CN=tools-vm,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configura` ...	dc-vm 10.200.200.4	DCShadow	Tenable's forest Tenable's domain	> Details	□
2021-06-24 17:38:06	TOOLS-VM 10.200.200.5	The `ALSID.CORP\dcadmin` account was used to start a DCSync attack. Some crit...	dc-vm 10.200.200.4	DCSync	Tenable's forest Tenable's domain	> Details	□
2021-06-24 15:12:51	TOOLS-VM 10.200.200.5	The `CN=tools-vm,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configura` ...	dc-vm 10.200.200.4	DCShadow	Tenable's forest Tenable's domain	> Details	□
2021-06-23 21:24:27	TOOLS-VM 10.200.200.5	Authentication failures were observed on a number of accounts exceeding `500` ...	dc-vm 10.200.200.4	PasswordSpraying	Tenable's forest Tenable's domain	> Details	□
2021-06-23 21:10:26	TOOLS-VM 10.200.200.5	The user `ALSID.CORP\dcadmin` has injected a malicious payload into `LSASS.exe` ...	dc-vm 10.200.200.4	ProcessInjectionLsass	Tenable's forest Tenable's domain	> Details	□
2021-06-23 21:10:26	TOOLS-VM 10.200.200.5	The user `ALSID.CORP\dcadmin` has injected a malicious payload into `LSASS.exe` ...	dc-vm 10.200.200.4	ProcessInjectionLsass	Tenable's forest Tenable's domain	> Details	□
2021-06-23 21:09:36	TOOLS-VM 10.200.200.5	The `CN=tools-vm,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configura` ...	dc-vm 10.200.200.4	DCShadow	Tenable's forest Tenable's domain	> Details	□
2021-06-23 21:09:11	TOOLS-VM 10.200.200.5	The `ALSID.CORP\dcadmin` account was used to start a DCSync attack. Some crit...	dc-vm 10.200.200.4	DCSync	Tenable's forest Tenable's domain	> Details	□
2021-06-23	TOOLS-VM	The `CN=tools-vm,CN=Servers,CN=Default-First-`	dc-vm	DCShadow	Tenable's forest	> Details	□

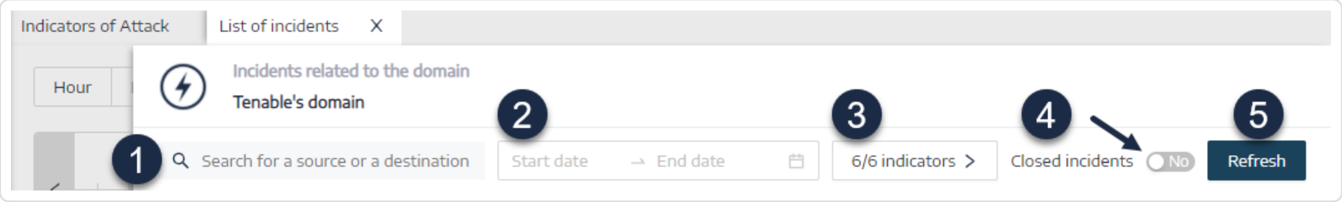
3. From this list, you can do any of the following:

   - Define search criteria to search for specific incidents ❶ .
   - Access detailed explanations on the attacks affecting the AD ❷ .
   - Close or reopen an incident ❸ .
   - Download a report showing all incidents ❹ .

To search for an incident:

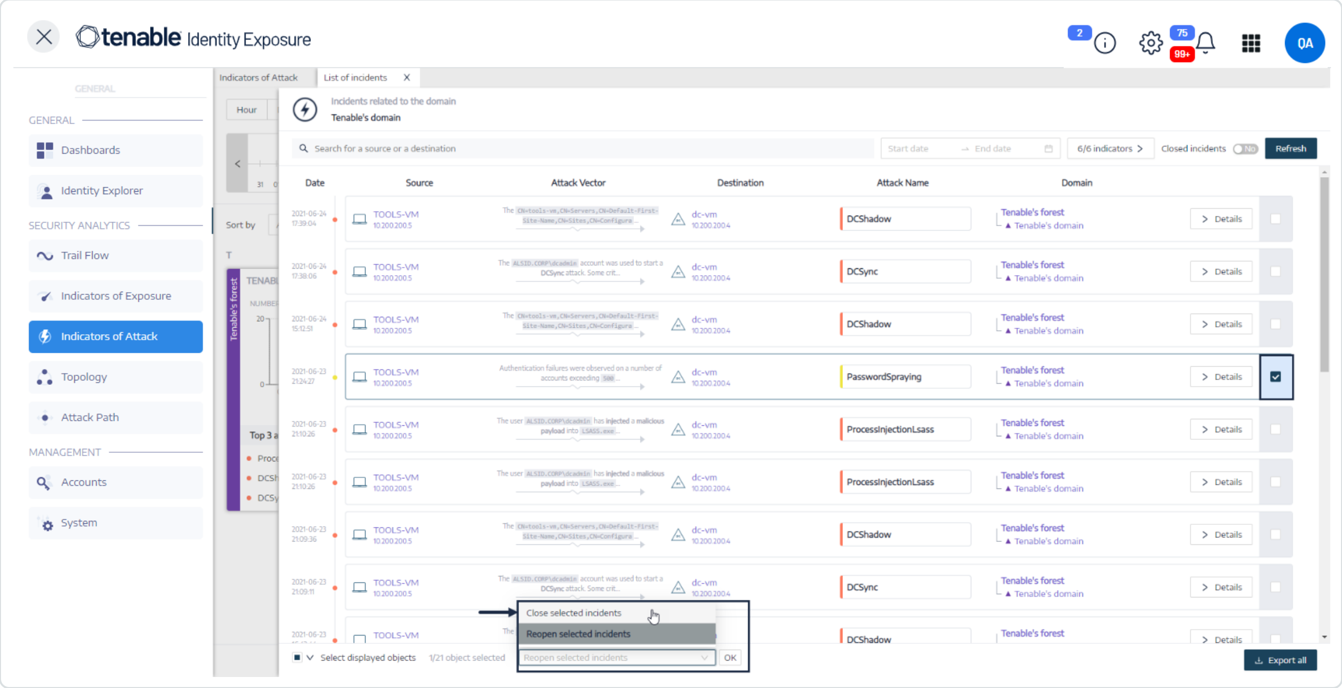
1. In the **Search** box, type the name of a source or destination.
2. Click the date picker to select a start date and end date for the incident.
3. Click **n/n Indicators** to select the related indicators.
4. Click the **Closed Incidents** toggle to **Yes** to limit the search to closed incidents.
5. Click **Refresh**.

   Tenable Identity Exposure updates the list with the matching incidents.



To close an incident:

1. From the list of incidents, select an incident to close or reopen.



Date	Source	Attack Vector	Destination	Attack Name	Domain		
2021-06-24 17:39:04	TOOLS-VM 10.200.200.5	The CN=tools-vm,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configura ...	dc-vm 10.200.200.4	DCShadow	Tenable's forest Tenable's domain	> Details	□
2021-06-24 17:38:06	TOOLS-VM 10.200.200.5	The ALSID.CORP\dcadmin account was used to start a DCSync attack. Some crit...	dc-vm 10.200.200.4	DCSync	Tenable's forest Tenable's domain	> Details	□
2021-06-24 15:12:51	TOOLS-VM 10.200.200.5	The CN=tools-vm,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configura ...	dc-vm 10.200.200.4	DCShadow	Tenable's forest Tenable's domain	> Details	□
2021-06-23 21:24:27	TOOLS-VM 10.200.200.5	Authentication failures were observed on a number of accounts exceeding 500 ...	dc-vm 10.200.200.4	PasswordSpraying	Tenable's forest Tenable's domain	> Details	☑
2021-06-23 21:10:26	TOOLS-VM 10.200.200.5	The user ALSID.CORP\dcadmin has injected a malicious payload into LSASS.exe ...	dc-vm 10.200.200.4	ProcessInjectionLsass	Tenable's forest Tenable's domain	> Details	□
2021-06-23 21:10:26	TOOLS-VM 10.200.200.5	The user ALSID.CORP\dcadmin has injected a malicious payload into LSASS.exe ...	dc-vm 10.200.200.4	ProcessInjectionLsass	Tenable's forest Tenable's domain	> Details	□
2021-06-23 21:09:36	TOOLS-VM 10.200.200.5	The CN=tools-vm,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configura ...	dc-vm 10.200.200.4	DCShadow	Tenable's forest Tenable's domain	> Details	□
2021-06-23 21:09:11	TOOLS-VM 10.200.200.5	The ALSID.CORP\dcadmin account was used to start a DCSync attack. Some crit...	dc-vm 10.200.200.4	DCSync	Tenable's forest Tenable's domain	> Details	□
2021-06-23	TOOLS-VM	The		DCShadow	Tenable's forest	> Details	□

Close selected incidents
Reopen selected incidents
■ Select displayed objects
1/21 object selected
Reopen selected incidents
OK
Export all

2. At the bottom of the pane, click the drop-down menu and select **Close selected incident**.

3. Click **OK**.

   A message asks you to confirm the closure.

4. Click **Confirm**.

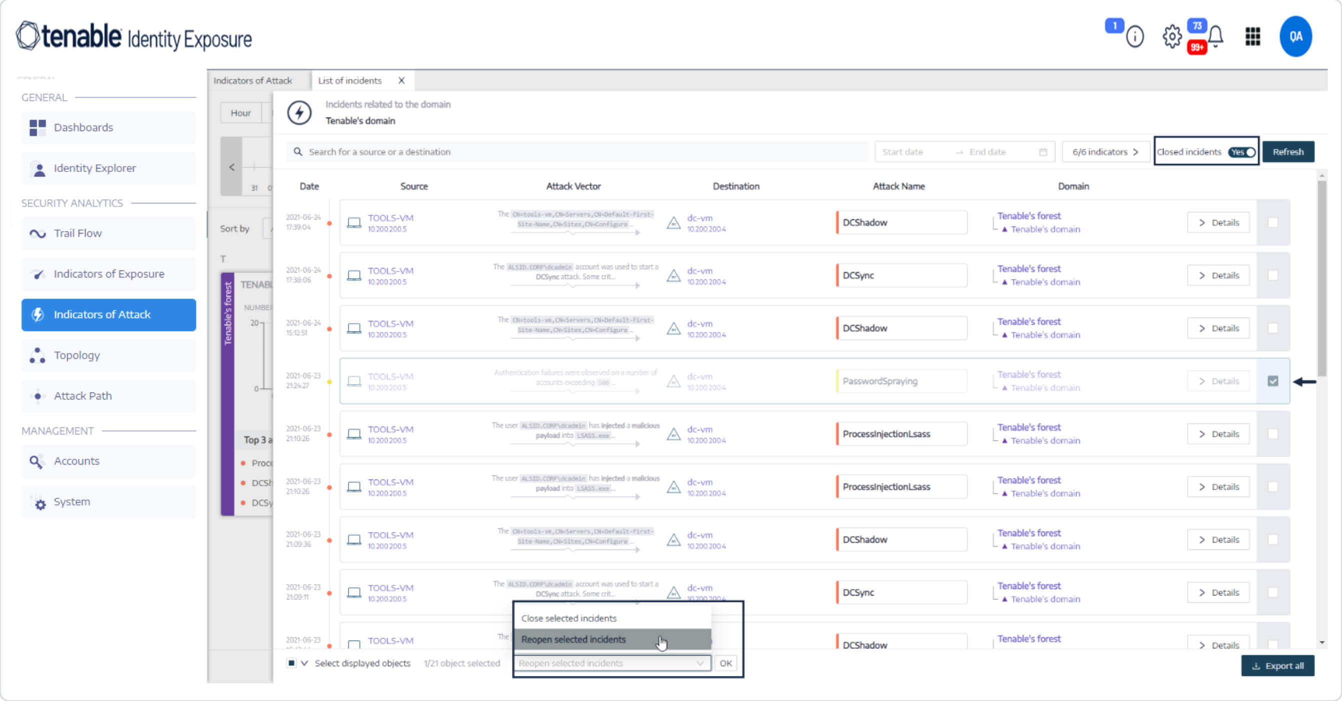
   A message confirms that Tenable Identity Exposure closed the incident and no longer shows it.

To reopen an incident:

1. In the **List of incidents** pane, click the **Closed incidents** toggle to **Yes**.

   Tenable Identity Exposure updates the list with closed incidents.

2. Select the incident to reopen.



Incidents related to the domain
Tenable's domain

Search for a source or a destination

Date	Source	Attack Vector	Destination	Attack Name	Domain		
2021-06-24 17:39:04	TOOLS-VM 10.200.200.5	The CN=tools-vm,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configura ...	dc-vm 10.200.200.4	DCShadow	Tenable's forest Tenable's domain	> Details	□
2021-06-24 17:38:06	TOOLS-VM 10.200.200.5	The ALSID.CORP\dcadmin account was used to start a DCSync attack. Some crit...	dc-vm 10.200.200.4	DCSync	Tenable's forest Tenable's domain	> Details	□
2021-06-24 15:12:51	TOOLS-VM 10.200.200.5	The CN=tools-vm,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configura ...	dc-vm 10.200.200.4	DCShadow	Tenable's forest Tenable's domain	> Details	□
2021-06-23 21:24:27	TOOLS-VM 10.200.200.5	Authentication failures were observed on a number of accounts exceeding 500 ...	dc-vm 10.200.200.4	PasswordSpraying	Tenable's forest Tenable's domain	> Details	☑
2021-06-23 21:10:26	TOOLS-VM 10.200.200.5	The user ALSID.CORP\dcadmin has injected a malicious payload into LSASS.exe ...	dc-vm 10.200.200.4	ProcessInjectionLsass	Tenable's forest Tenable's domain	> Details	□
2021-06-23 21:10:26	TOOLS-VM 10.200.200.5	The user ALSID.CORP\dcadmin has injected a malicious payload into LSASS.exe ...	dc-vm 10.200.200.4	ProcessInjectionLsass	Tenable's forest Tenable's domain	> Details	□
2021-06-23 21:09:36	TOOLS-VM 10.200.200.5	The CN=tools-vm,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configura ...	dc-vm 10.200.200.4	DCShadow	Tenable's forest Tenable's domain	> Details	□
2021-06-23 21:09:11	TOOLS-VM 10.200.200.5	The ALSID.CORP\dcadmin account was used to start a DCSync attack. Some crit...	dc-vm 10.200.200.4	DCSync	Tenable's forest Tenable's domain	> Details	□
2021-06-23	TOOLS-VM	The		DCShadow	Tenable's forest	> Details	□

■ Select displayed objects 1/21 object selected Reopen selected incidents OK

3. At the bottom of the pane, click the drop-down menu and select **Reopen selected incident**.

4. Click **OK**.

   A message confirms that Tenable Identity Exposure reopened the incident.

Tip: You can close or reopen incidents in bulk. At the bottom of the plane, click **Select displayed objects**.

Incident Details

Each entry in the list of incidents shows the following information:

- **Date** — The date when the incident triggering the IoA occurred. Tenable Identity Exposure shows the most recent at the top of the timeline.
- **Source** — The source where the attack originated and its IP address.
- **Attack Vector** — An explanation about what happened during the attack.

> **Tip**: Hover over the attack vector to see more information about the IoA.

- **Destination** — The target of the attack and its IP address.
- **Attack Name** — The technical name of the attack.
- **Domain** — The domains that the attack impacted.

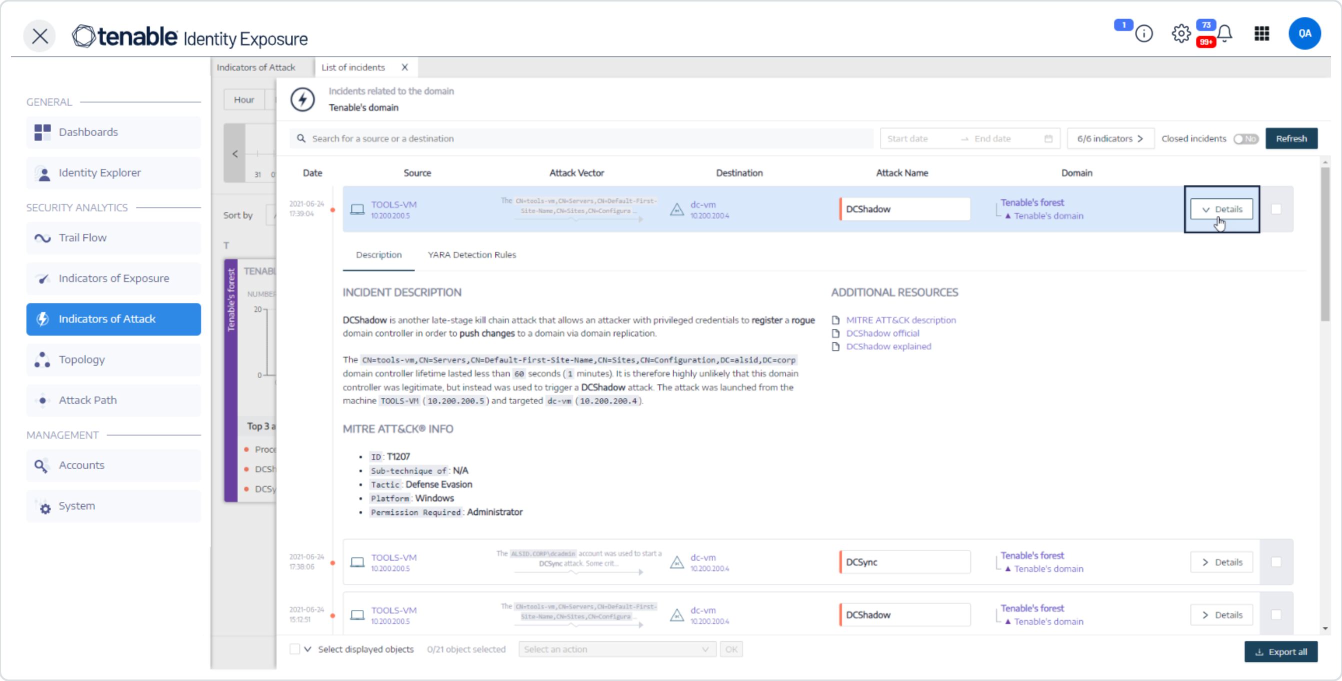
> **Tip**: Tenable Identity Exposure can show a maximum of five panes when you click on several interactive elements (links, action buttons, etc.) in the **List of incidents**. To close all panes simultaneously, click anywhere on the page.

Attack Details

From the list of incidents, you can drill down on a specific attack and take necessary action to remediate.

To show attack details:

1. From the list of incidents, select an incident to drill down for details.
2. Click **Details**.



Incidents related to the domain
Tenable's domain

Date	Source	Attack Vector	Destination	Attack Name	Domain
2021-06-24 17:39:04	TOOLS-VM 10.200.200.5	The CN=tools-vm,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configura ...	dc-vm 10.200.200.4	DCShadow	Tenable's forest Tenable's domain
2021-06-24 17:38:06	TOOLS-VM 10.200.200.5	The ALSID.CORP\dcadmin account was used to start a DCSync attack. Some crit...	dc-vm 10.200.200.4	DCSync	Tenable's forest Tenable's domain
2021-06-24 15:12:51	TOOLS-VM 10.200.200.5	The CN=tools-vm,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configura ...	dc-vm 10.200.200.4	DCShadow	Tenable's forest Tenable's domain

Description | YARA Detection Rules

INCIDENT DESCRIPTION

DCShadow is another late-stage kill chain attack that allows an attacker with privileged credentials to **register** a **rogue** domain controller in order to **push changes** to a domain via domain replication.

The `CN=tools-vm,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=alsid,DC=corp` domain controller lifetime lasted less than `60` seconds (`1` minutes). It is therefore highly unlikely that this domain controller was legitimate, but instead was used to trigger a DCShadow attack. The attack was launched from the machine `TOOLS-VM` (`10.200.200.5`) and targeted `dc-vm` (`10.200.200.4`).

MITRE ATT&CK® INFO

- `ID`: T1207
- `Sub-technique of`: N/A
- `Tactic`: Defense Evasion
- `Platform`: Windows
- `Permission Required`: Administrator

ADDITIONAL RESOURCES

- MITRE ATT&CK description
- DCShadow official
- DCShadow explained

Tenable Identity Exposure displays the details associated with that attack:

Description

The **Description tab** contains the following sections:

- **Incident Description** — Provides a short description of the attack.
- **MITRE ATT&CK Info —** Gives technical information retrieved from the Mitre Att&ck (Adversarial Tactics, Techniques, and Common Knowledge) knowledge base. Mitre Att&ck is a framework that classifies adversary attacks and describes the actions that attackers take after they compromise a network. It also provides standard identifiers for security vulnerabilities to ensure a shared understanding by the cybersecurity community.
- **Additional Resources** — Provides links to websites, articles, and whitepapers for more in-depth information on the attack.

YARA Detection Rules

The **YARA Detection Rules** tab describes the YARA rules that Tenable Identity Exposure uses to detect AD attacks at the network level to strengthen Tenable Identity Exposure's detection chain.

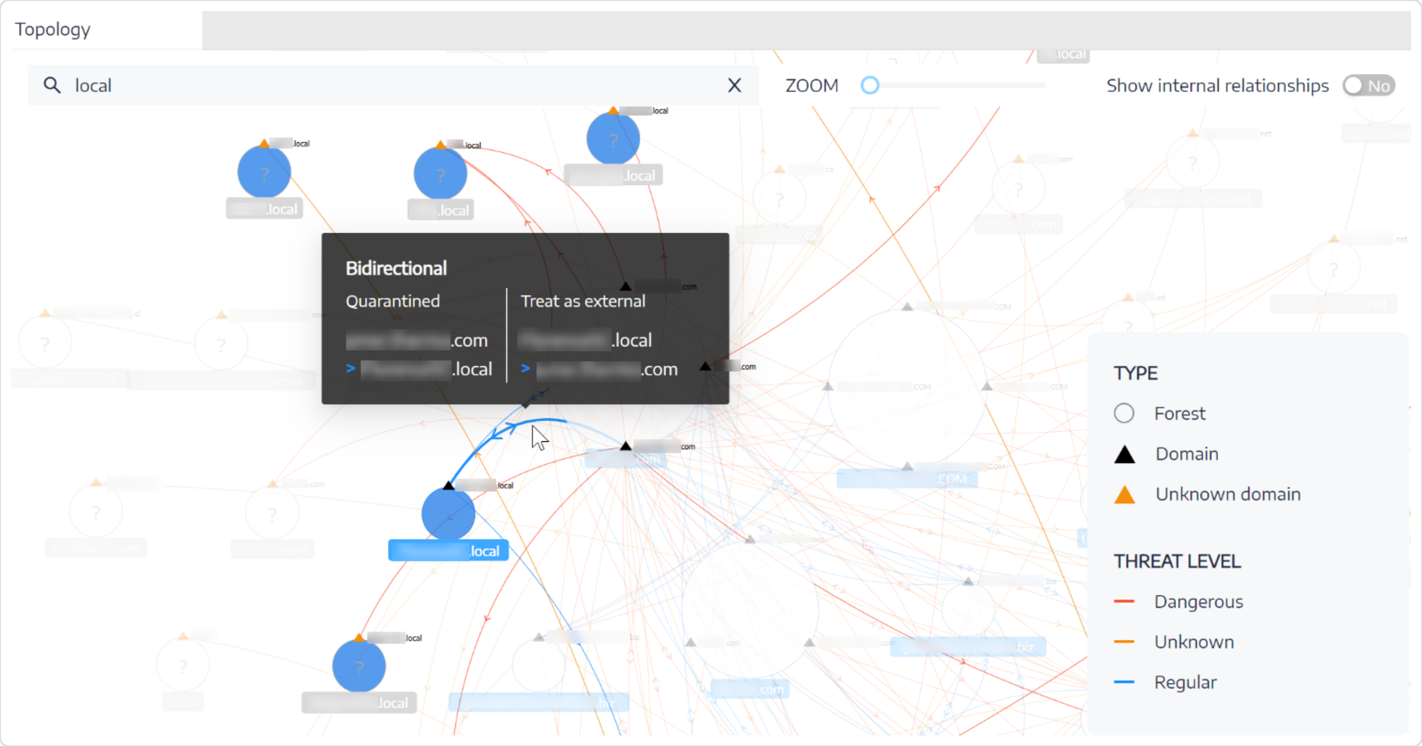
> **Note**: YARA is the name of a tool primarily used in malware research and detection. It provides a rule-based approach to create descriptions of malware families based on textual or binary patterns. A description is essentially a YARA rule name, where these rules consist of sets of strings and a Boolean expression (source: wikipedia.org.)

See also

- Indicators of Attack
- Indicator of Attack Details

Topology

The Topology page provides an interactive graphic visualization of your Active Directory. The **Topology Graph** displays the forests, domains, and trust relationships that exist between them.



Topology

local

ZOOM

Show internal relationships No

Bidirectional

Quarantined	Treat as external
[redacted].com	[redacted].local
> [redacted].local	> [redacted].com

TYPE

○ Forest

▲ Domain

▲ Unknown domain

THREAT LEVEL

— Dangerous

— Unknown

— Regular

To open the Topology page:

- In Tenable Identity Exposure, click on **Topology** on the left navigation menu.

  The Topology pane opens with a graphical representation of your AD.

To search for a domain:

- In the **Topology** pane, type a domain name in the **Search** box.

  Tenable Identity Exposure highlights the domain.

To zoom in on the graph:

- In the **Topology** pane, click on the **Zoom** slider to adjust the graph size.

To display the link between two domains:

- In the **Topology** pane, click the **Show internal relationships** toggle to **Yes**.

To display details about a domain:

- In the **Topology** pane, click on the ▲ for the domain name.

  The **Domain details** pane opens with the Indicators of Exposure (IoE) detected and the compliance score for the domain. You can click on the tile for the IoE to drill down for more information.

See also

- Trust Relationships
- Dangerous Trusts

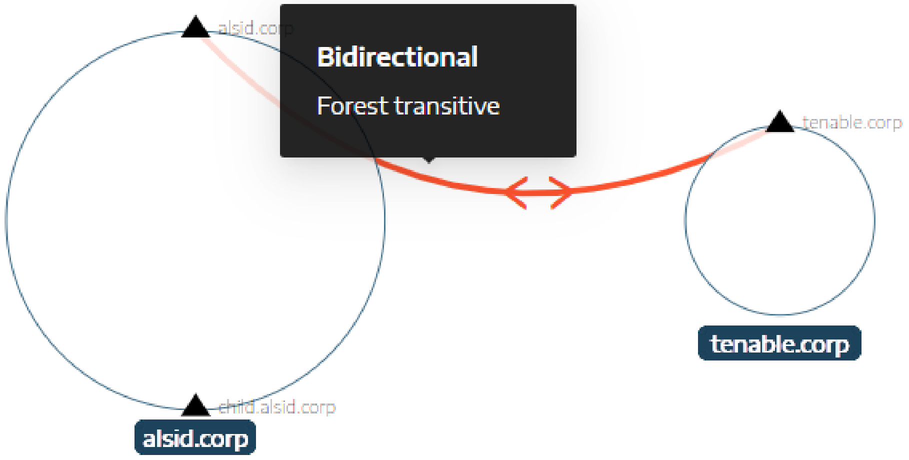
Trust Relationships

The curved arrows between domains on the topology graph represent trust relationships.

To display trust relationships:

- On the topology graph, hover over the curved arrows.

  Tenable Identity Exposure displays the trust relationships display specific attributes between two entities.



Bidirectional

Forest transitive

The color of a trust relationship depends on its threat level:

- **Red** for dangerous trusts
- **Orange** for regular trusts
- **Blue** for unknown trusts

For more information, see Dangerous Trusts.

The trust attribute information indicates the trust direction as **unidirectional** or **bidirectional** (incoming/outgoing) and displays one of the following values:

Value	Description
Non-transitive	By default, intra-forest trusts are transitive trusts. Tenable Identity Exposure uses this flag to convert them into non-transitive trusts. On the

	other hand, inter-forest trusts are non-transitive by default, hence the presence of the forest transitive flag. Tenable Identity Exposure displays this value if an intra-forest inter-domain trust exists. The trust grants no access and delegates no authority to interconnected domains beyond the forest.
Forest transitive	Indicates that a transitive trust exists between two forests. The trust granted to another domain can pass to the trusted forest.
Within forest	Indicates that an inter-domain trust exists within the same forest. If `WITHIN_FOREST` and `QUARANTINED_DOMAIN` are both present, the trust is referred to as **QuarantinedWithinForest**.
Up level only	Indicates that only clients running Windows 2000 operating systems and later can use this trust.
Treat as external	(Only when `FOREST_TRANSITIVE` applies) Indicates an external type of trust. Tenable Identity Exposure modifies the security identifier (SID) filtering on the trust and authorizes the SIDs whose relative identifier (RID) is greater than or equal to 1000 to pass across the forest.
Quarantined	Indicates that Tenable Identity Exposure enabled the filtering of the SIDs whose RID is greater than or equal to 1000 for the trust. By default, Tenable Identity Exposure only enables it for an external trust but it can also apply to a parent/child trust or a forest trust.
Cross-organization authentication	Indicates that Tenable Identity Exposure enabled selective authentication and can use it across domain or forest trusts.
Selective authentication	See Cross-organization authentication.
Cross organization without TGT delegation	Displays if the delegation on a trusted domain is fully disabled (never sets the ok-as-delegate option in the issued service tickets).
RC4 encryption:	Indicates that the trust supports RC4-encryption keys for Kerberos

	exchanges. This flag is present only if the `trustType` applies to `TRUST_TYPE_MIT`.
AES keys	Indicates that the trust supports AES-encryption keys for Kerberos exchanges.
PIM trust	If the `FOREST_TRANSITIVE` and `TREAT_AS_EXTERNAL` flags apply and the `QUARANTINED_DOMAIN` flag is not on, the PIM trust flag indicates that the trusted forest manages privileged identities (Privileged Identity Management) regarding SID filtering (local SIDs can pass across this trust). PIM trust act to implement bastion forests.
No attribute	Indicates that the external trust has no specific attribute.

Dangerous Trusts

The color of a trust relationship depends on its threat level:

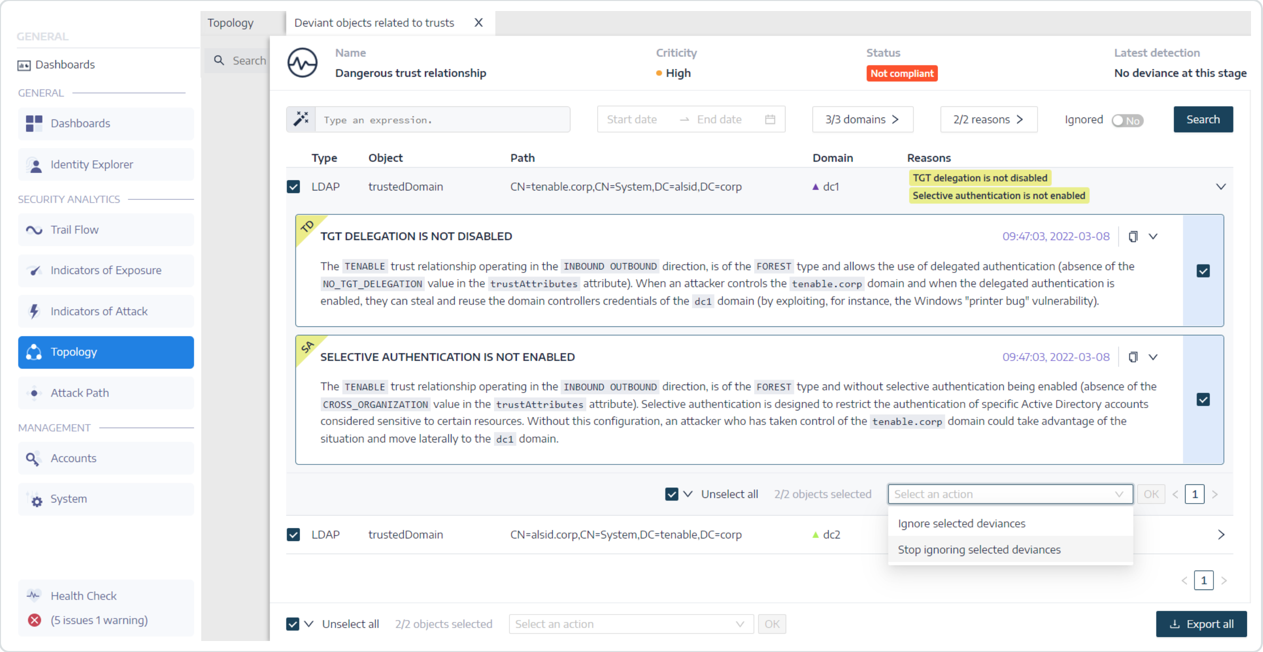
- **Red** for dangerous trusts
- **Orange** for regular trusts
- **Blue** for unknown trusts

To investigate a dangerous trust:

1. On the topology graph, click on the curved arrows.

   The **Deviant objects related to trusts** pane opens.

   > **Tip**: The details of the events displayed on this dangerous trust relationships pane are all linked to the **Dangerous Trust Relationship** Indicator of Exposure which you can also access from the **Indicators of Exposure** navigation menu.



Name	Criticity	Status	Latest detection
Dangerous trust relationship	● High	Not compliant	No deviance at this stage

	Type	Object	Path	Domain	Reasons
☑	LDAP	trustedDomain	CN=tenable.corp,CN=System,DC=alsid,DC=corp	▲ dc1	TGT delegation is not disabled Selective authentication is not enabled

TD TGT DELEGATION IS NOT DISABLED 09:47:03, 2022-03-08 ☑

The `TENABLE` trust relationship operating in the `INBOUND OUTBOUND` direction, is of the `FOREST` type and allows the use of delegated authentication (absence of the `NO_TGT_DELEGATION` value in the `trustAttributes` attribute). When an attacker controls the `tenable.corp` domain and when the delegated authentication is enabled, they can steal and reuse the domain controllers credentials of the `dc1` domain (by exploiting, for instance, the Windows "printer bug" vulnerability).

SA SELECTIVE AUTHENTICATION IS NOT ENABLED 09:47:03, 2022-03-08 ☑

The `TENABLE` trust relationship operating in the `INBOUND OUTBOUND` direction, is of the `FOREST` type and without selective authentication being enabled (absence of the `CROSS_ORGANIZATION` value in the `trustAttributes` attribute). Selective authentication is designed to restrict the authentication of specific Active Directory accounts considered sensitive to certain resources. Without this configuration, an attacker who has taken control of the `tenable.corp` domain could take advantage of the situation and move laterally to the `dc1` domain.

☑ Unselect all 2/2 objects selected Select an action OK < 1 >
Ignore selected deviances
Stop ignoring selected deviances

	Type	Object	Path	Domain
☑	LDAP	trustedDomain	CN=alsid.corp,CN=System,DC=tenable,DC=corp	▲ dc2

2. Hover over and click on a deviant object from the list to display the details.

To export deviant objects:

1. On the topology graph, click on the curved arrows.

   The **Deviant objects related to trusts** pane opens.

2. Click **Export all**.

   The **Export deviant objects** pane opens.

3. In the **Export format** box, click the drop-down arrow to select a format.

4. Click **Export all**.

   Tenable Identity Exposure downloads a file in the selected format to your computer.

5. Click **X** to close the pane.

Attack Path

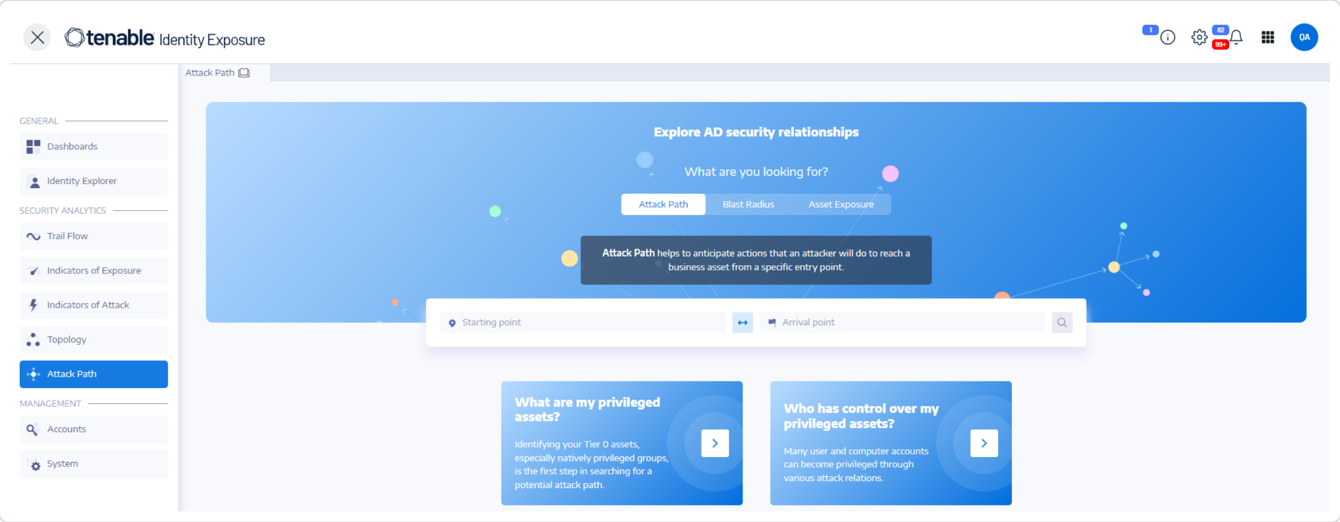
Tenable Identity Exposure offers several ways to visualize the potential vulnerability of a business asset through graphical representations.

- **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.

To display the Attack Path:

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

   The **Attack Path** pane appears.



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?

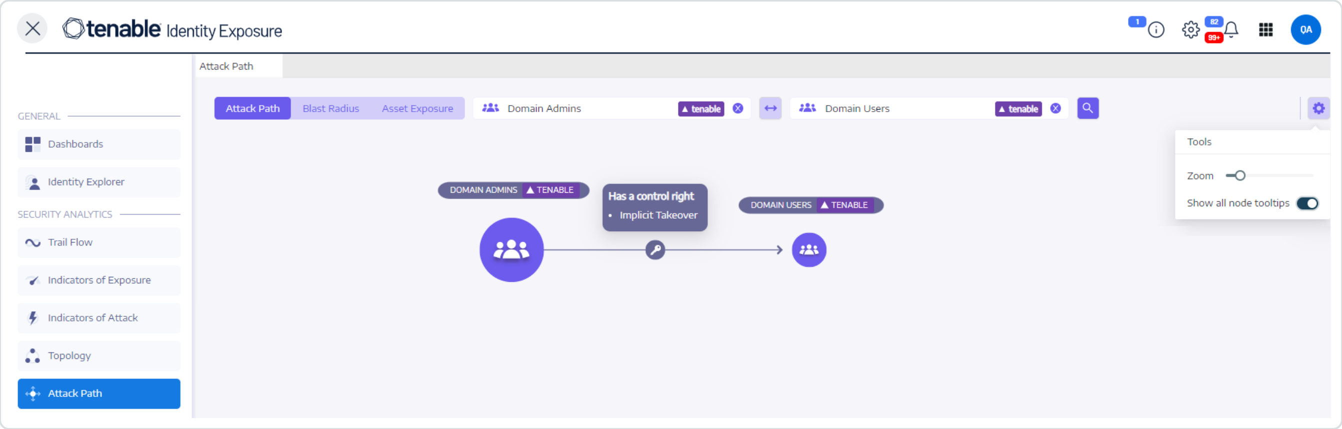
Identifying your Tier 0 assets, especially natively privileged groups, is the first step in searching for a potential attack path.

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.



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:

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

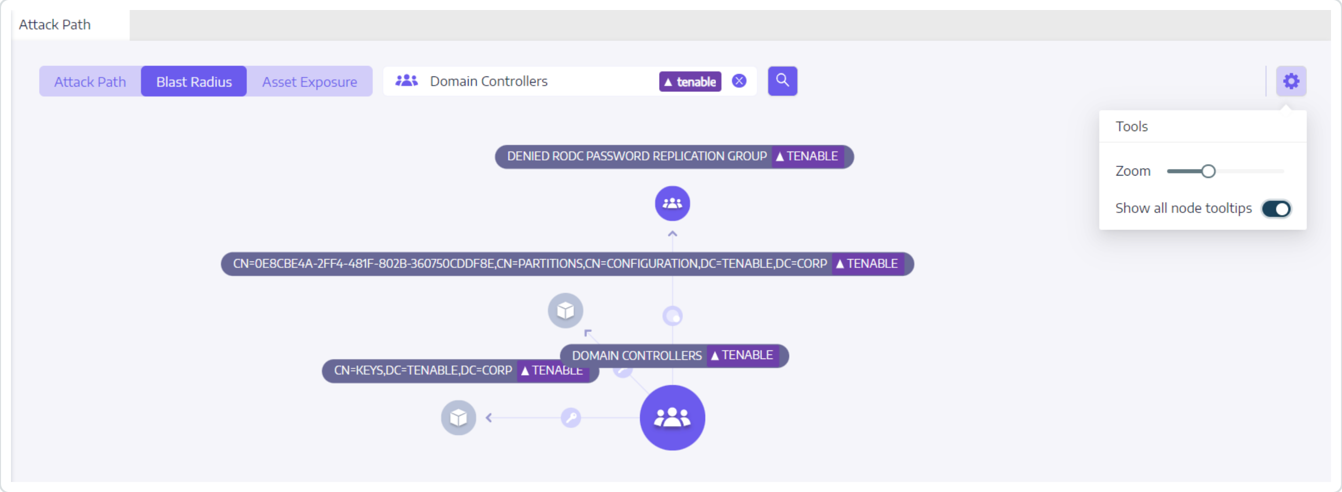
   The **Attack Path** pane appears.

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

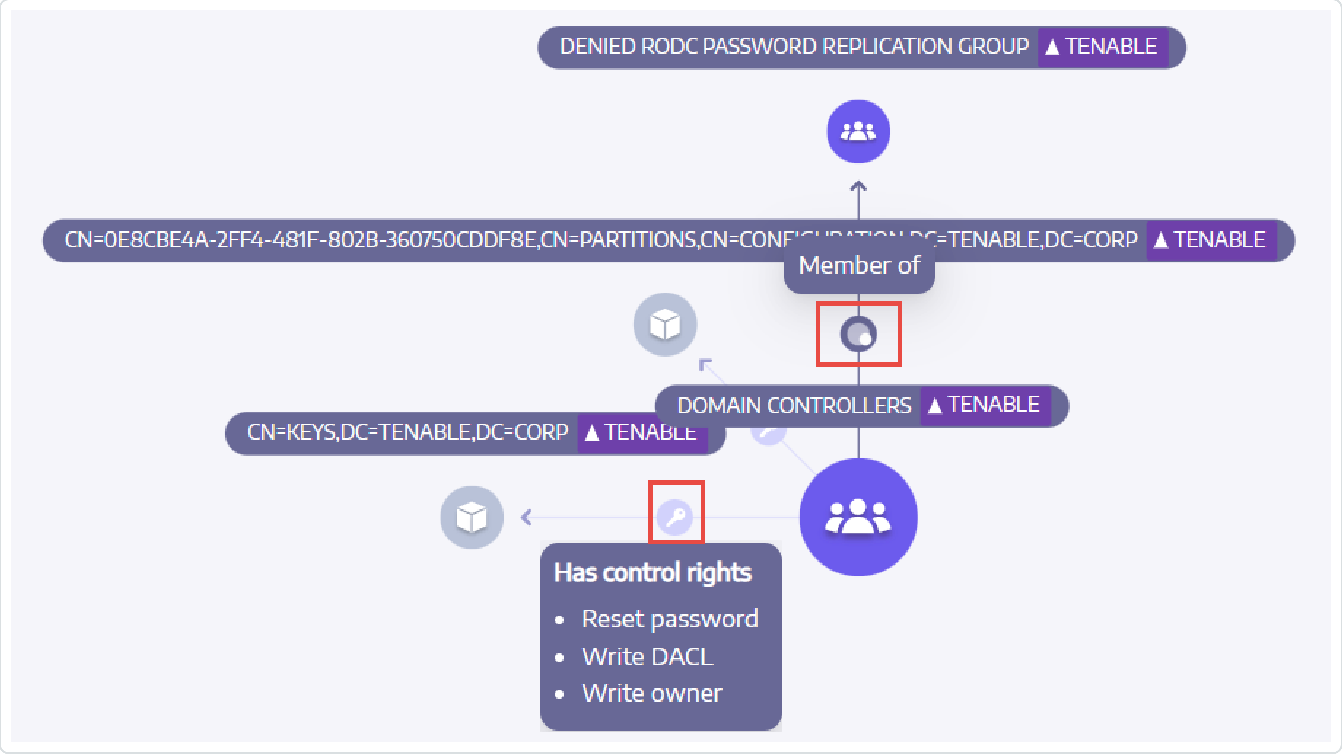
3. In the **Search for an object** box, type the name of an asset.

4. Click the 🔍 icon.

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


Attack Path
Attack Path
Blast Radius
Asset Exposure
Domain Controllers
tenable
Tools
Zoom
Show all node tooltips
DENIED RODC PASSWORD REPLICATION GROUP
TENABLE
CN=0E8CBE4A-2FF4-481F-802B-360750CDDF8E,CN=PARTITIONS,CN=CONFIGURATION,DC=TENABLE,DC=CORP
TENABLE
DOMAIN CONTROLLERS
TENABLE
CN=KEYS,DC=TENABLE,DC=CORP
TENABLE

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=CONFIGURATION,DC=TENABLE,DC=CORP ▲TENABLE
Member of
DOMAIN CONTROLLERS ▲TENABLE
CN=KEYS,DC=TENABLE,DC=CORP ▲TENABLE
Has control rights
Reset password
Write DACL
Write owner

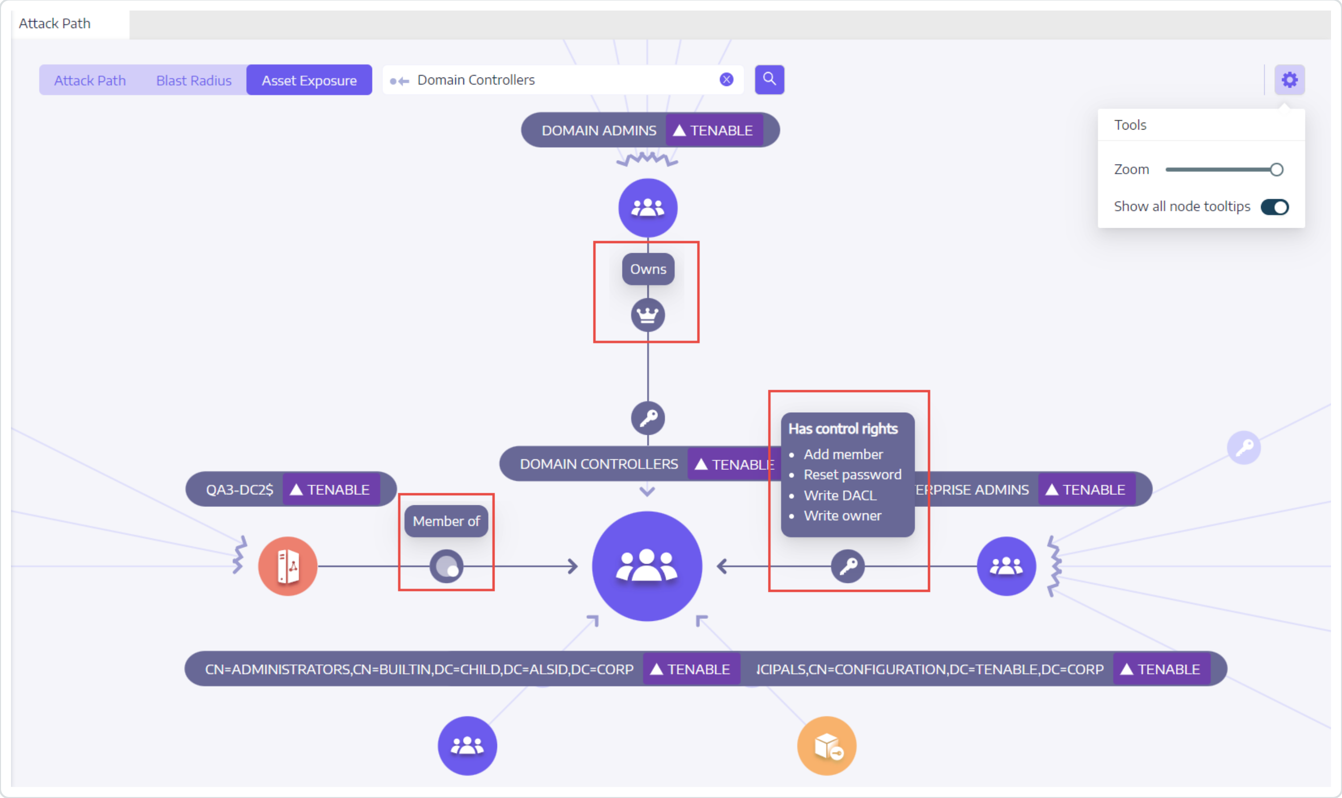
To display the Asset Exposure:

1. To display the Blast Radius:
2. In Tenable Identity Exposure, click **Attack Path** on the sidebar menu.

   The **Attack Path** pane appears.
3. In the banner, click **Asset Exposure**.
4. In the **Search for an object** box, type the name of an asset.
5. Click the 🔍 icon.

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

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

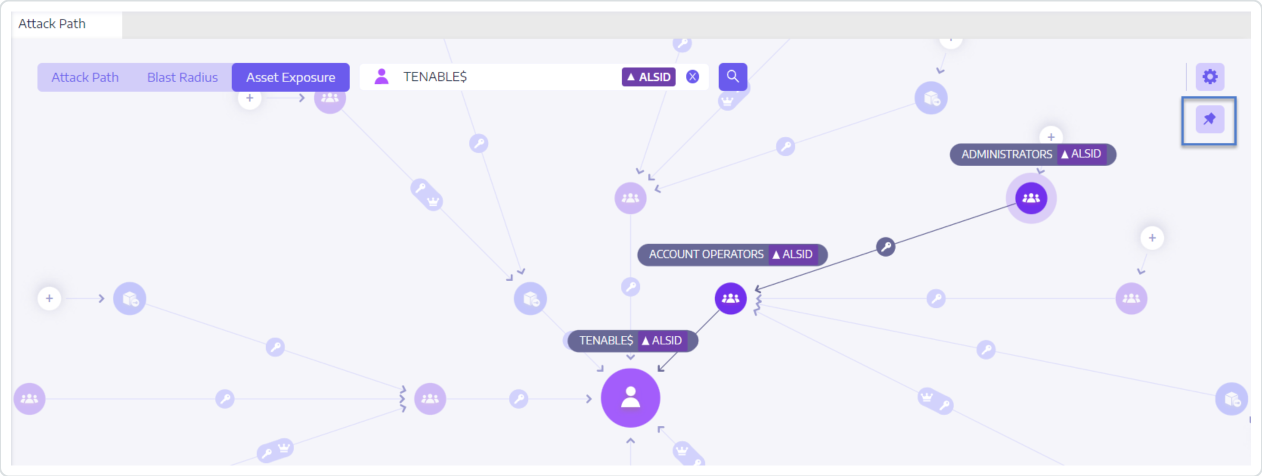


To pin an attack path:

1. Click on a node on the attack path that you want to highlight.

   Tenable Identity Exposure pins that attack path on the screen.

2. To unpin the attack path, click the 📌 icon or another node on a different attack path.

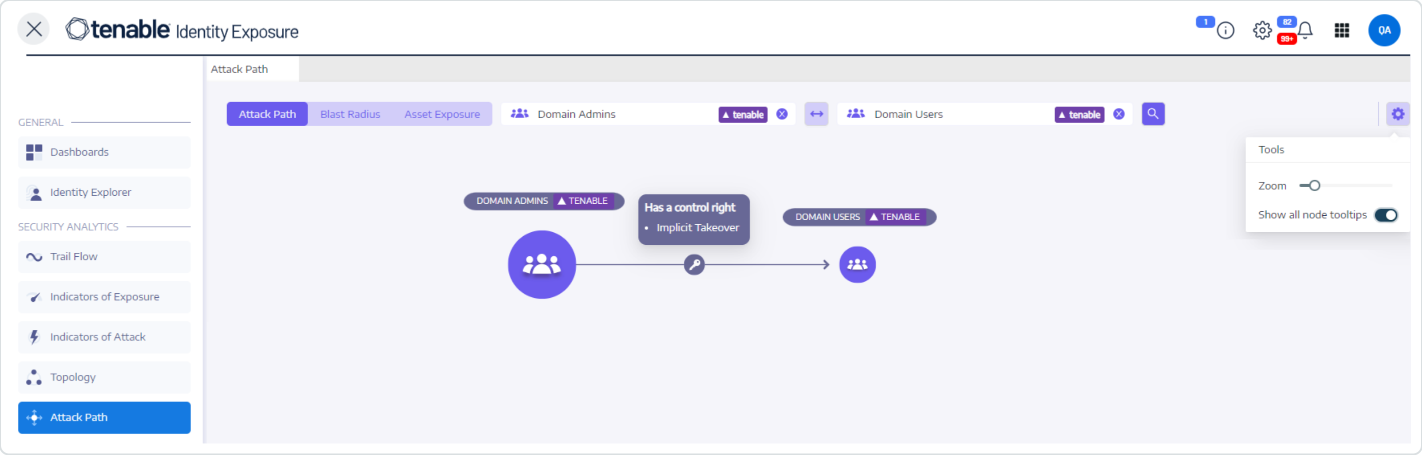


See also

- Attack Relations

Attack Relations

Attack relations are unidirectional from a Source node to a Target node. Since relations are transitive, attackers can chain them together to create an "attack path":



Tenable Identity Exposure has the following attack relations:

- Add Key Credential
- Add Member
- Allowed To Act
- Allowed To Delegate
- Belongs To GPO
- DCSync
- Grant Allowed To Act
- Has SID History
- Implicit Takeover
- Inherit GPO
- Linked GPO
- Member Of
- Owns

- Reset Password
- RODC Manage
- Write DACL
- Write Owner

Add Key Credential

Description

The Source security principal can impersonate the Target by exploiting key trust account mappings, also known as key credentials or "shadow credentials".

This is possible because the Source has permission to edit the `msDS-KeyCredentialLink` attribute of the Target.

Windows Hello for Business (WHfB) normally uses this feature, but it is available for attackers to exploit it even if it is not in use.

Exploitation

Attackers who compromise the Source security principal must edit the `msDS-KeyCredentialLink` attribute of the Target computer by using specialized hacker tools such as Whisker or DSInternals.

The attackers' goal is to add a new certificate to this target's attribute, for which they have the private key. They can then authenticate as the Target with the known private key using the Kerberos PKINIT protocol to obtain a TGT. This protocol also allows attackers to fetch the target's NTLM hash.

Remediation

Several natively privileged security principals have this permission by default, namely Account Operators, Administrators, Domain Admins, Enterprise Admins, Enterprise Key Admins, Key Admins, and SYSTEM. These legitimate security principals do not require remediation.

For Source security principals without a legitimate need to modify this attribute, you must remove this permission. Search for permissions such as "Write all properties", "Write msDS-AllowedToActOnBehalfOfOtherIdentity", "Full control", etc.

See also

- Add Member
- Allowed To Act

- Allowed To Delegate
- Belongs To GPO
- DCSync
- Grant Allowed To Act
- Has SID History
- Implicit Takeover
- Inherit GPO
- Linked GPO
- Member Of
- Owns
- Reset Password
- RODC Manage
- Write DACL
- Write Owner

Add Member

Description

The Source security principal can add itself (validated write right), or anyone (write property right), to the members of the Target group and benefit from the access rights given to the group.

A malicious security principal performing this operation would create a "Member of" attack relation.

Exploitation

Attackers who compromise the Source security principal only have to edit the "members" attribute of the Target group through native Windows commands such as "net group /domain", PowerShell such as "Add-ADGroupMember", administration tools such as "Active Directory Users and Computers", or dedicated hacker tools such as PowerSploit.

Remediation

If the Source security principal does not need the right to add a member to the Target group, then you must remove this permission.

To modify the security descriptor of the Target group:

1. In "Active Directory Users and Computers", right-click **Properties** > **Security**.
2. Remove permissions such as "Write Members", "Write all properties", "Full control", "All validated writes", "Add/remove self as member", etc.

Note: A group can inherit permission from an object higher in the Active Directory tree.

See also

- Add Key Credential
- Allowed To Act
- Allowed To Delegate
- Belongs To GPO

- DCSync
- Grant Allowed To Act
- Has SID History
- Implicit Takeover
- Inherit GPO
- Linked GPO
- Member Of
- Owns
- Reset Password
- RODC Manage
- Write DACL
- Write Owner

Allowed To Act

Description

The Source security principal is allowed to perform Kerberos Resource-Based Constrained Delegation on the Target computer. This means that it can impersonate any user when it authenticates with Kerberos to any service running on the Target computer.

Therefore, it often leads to a total compromise of the Target computer.

This attack is also known as Resource-Based Constrained Delegation (RBCD), Kerberos Resource-Based Constrained Delegation (KRBCD), Resource-Based Kerberos Constrained Delegation (RBKCD), and "allowed to act on behalf of other identity".

Exploitation

Attackers who compromise the Source security principal can use dedicated hacker tools such as Rubeus to exploit legitimate Kerberos protocol extensions (S4U2self and S4U2proxy) in order to forge Kerberos service tickets and impersonate the targeted user. Attackers will likely choose to impersonate a privileged user to obtain privileged access.

Once attackers forge the service ticket, they can use any native administration tool or specialized hacker tool compatible with Kerberos to execute remotely arbitrary commands.

A successful exploitation attempt must meet the following constraints:

- The Source and Target security principals must have a ServicePrincipalName. Tenable Identity Exposure does not create this attack relation without this condition.
- The account targeted for spoofing must neither be marked "is sensitive and cannot be delegated" (`ADS_UF_NOT_DELEGATED` in UserAccountControl) nor be a member of the "Protected Users" group because Active Directory protects such accounts from delegation attacks.

Remediation

If the Source security principal does not need permission to perform Kerberos Resource-Based Constrained Delegation (RBCD) on the Target computer, then you must remove it. You must make the modification on the Target side, as opposed to the "Allowed to delegate" delegation attack relation.

You cannot manage RBCD with existing graphical administration tools such as "Active Directory Users and Computers". You must instead use PowerShell to modify the content of the `msDS-AllowedToActOnBehalfOfOtherIdentity` attribute.

Use the following commands to list the Source security principals allowed to act on the Target (in the "Access:" section):

```
Get-ADComputer target -Properties msDS-AllowedToActOnBehalfOfOtherIdentity | Select-Object -
ExpandProperty msDS-AllowedToActOnBehalfOfOtherIdentity | Format-List
```

If you do not want any of the listed security principals is desired, you can clear all of them with this command:

```
Set-ADComputer target -Clear "msDS-AllowedToActOnBehalfOfOtherIdentity"
```

If you only need to remove one security principal from the list, Microsoft unfortunately does not provide a direct command. You must overwrite the attribute with the same list minus the one to remove. For example, if "sourceA", "sourceB" and "sourceC" were all allowed and you want to remove just "sourceB", run:

```
Set-ADComputer target -PrincipalsAllowedToDelegateToAccount (Get-ADUser sourceA),(Get-ADUser sourceC)
```

Finally, as a general recommendation, in order to limit the exposure of sensitive privileged accounts to such delegation attacks, Tenable Identity Exposure recommends that you mark them as "is sensitive and cannot be delegated" (`ADS_UF_NOT_DELEGATED`) or add them to the "Protected Users" group, after careful verification of the associated operational impacts.

See also

- Add Key Credential
- Add Member
- Allowed To Delegate

- Belongs To GPO
- DCSync
- Grant Allowed To Act
- Has SID History
- Implicit Takeover
- Inherit GPO
- Linked GPO
- Member Of
- Owns
- Reset Password
- RODC Manage
- Write DACL
- Write Owner

Allowed To Delegate

Description

The Source security principal is allowed to perform Kerberos Constrained Delegation (KCD) with protocol transition on the Target computer. This means that it can impersonate any user when it authenticates with Kerberos to any service running on the Target computer.

Therefore, it often leads to a total compromise of the Target computer.

Exploitation

Attackers who compromise the Source security principal can use dedicated hacker tools such as Rubeus to exploit legitimate Kerberos protocol extensions (S4U2self and S4U2proxy) in order to forge Kerberos service tickets and impersonate the targeted user. Attackers are likely to choose to impersonate a privileged user to obtain privileged access.

Once attackers forge the service ticket, they can use any native administration tool or specialized hacker tool compatible with Kerberos to execute remotely arbitrary commands.

A successful exploitation attempt must meet the following constraints:

- The Source security principal must be enabled for protocol transition (`ADS_UF_TRUSTED_TO_AUTHENTICATE_FOR_DELEGATION` in UserAccountControl / "Use any authentication protocol" in the Delegation GUI). More precisely, the attack could work without protocol transition ("Use Kerberos only" in the Delegation GUI), but attackers must first coerce a Kerberos authentication from the targeted user to the Source security principal, which makes the attack harder. Therefore, Tenable Identity Exposure does not create an attack relation in this case.

- The Source and Target security principals must have a ServicePrincipalName. Tenable Identity Exposure does not create this attack relation without this condition.

- The account targeted for spoofing must neither be marked "is sensitive and cannot be delegated" (`ADS_UF_NOT_DELEGATED` in UserAccountControl) nor be a member of the "Protected Users" group because Active Directory protects such accounts from delegation attacks

On the contrary, the Target computer where delegation is allowed is designated by a Service Principal Name (SPN) and thus contains a specific service such as SMB with "cifs/host.example.net", HTTP with "http/host.example.net", etc. However, attackers can actually target any other SPN and service running under the same Target account using a "sname substitution attack". Therefore, this is not a limitation.

Remediation

If the Source security principal does not need permission to perform Kerberos Constrained Delegation (KCD) on the Target computer, then you must remove it. You must make the modification on the Source side, as opposed to an "Allowed to act" delegation attack relation.

To remove the Source security principal:

1. In "Active Directory Users and Computers" administration GUI, go to the Source object's **Properties** > **Delegation** tab.
2. Remove the Service Principal Name corresponding to the Target.
3. If you do not want any delegation from this Source, remove all SPNs and select "Do not trust this computer for delegation".

Alternatively, you can use PowerShell to modify the content of the Source's "msDS-AllowedToDelegateTo" attribute.

- For example, in Powershell, run this command to replace all values:

```
Set-ADObject -Identity "CN=Source,OU=corp,DC=example,DC=net" -Replace @{ "msDS-
AllowedToDelegateTo" = @("cifs/desiredTarget.example.net") }
```

- If you do not want any delegation from this Source, run the following command to clear the attribute:

```
Set-ADObject -Identity "CN=Source,OU=corp,DC=example,DC=net" -Clear "msDS-
AllowedToDelegateTo"
```

It is also possible to reduce the risk while not completely closing this attack path by disabling protocol transition. This requires that all security principals connect to the Source using only Kerberos instead of NTLM.

To disable protocol transition:

1. In "Active Directory Users and Computers" administration GUI, go to the Source object's **Properties** > **Delegation** tab.
2. Select "Use Kerberos only" instead of "Use any authentication protocol".

Alternatively, you can run the following command in PowerShell to disable protocol transition:

```
Set-ADAccountControl -Identity "CN=Source,OU=corp,DC=example,DC=net" -TrustedToAuthForDelegation
$false
```

Finally, as a general recommendation, in order to limit the exposure of sensitive privileged accounts to such delegation attacks, Tenable Identity Exposure recommends that you mark them as "Is sensitive and cannot be delegated" (`ADS_UF_NOT_DELEGATED`) or add them to the "Protected Users" group after careful verification of the associated operational impacts.

See also

- Add Key Credential
- Add Member
- Allowed To Act
- Belongs To GPO
- DCSync
- Grant Allowed To Act
- Has SID History
- Implicit Takeover
- Inherit GPO
- Linked GPO
- Member Of
- Owns
- Reset Password

- RODC Manage
- Write DACL
- Write Owner

Belongs To GPO

Description

The Source GPO file or folder in the SYSVOL share belongs to the target GPC (GPO), which means that it defines the settings or programs/scripts that the GPO applies.

Exploitation

This is not an attack relation that an attacker would use in isolation. However, as an example, it can show complete attack paths where attackers who have control over a GPO file/folder belonging to a GPO can force arbitrary settings or launch scripts on the users/computers at the end of the attack path.

Remediation

This relation shows how GPO files and folders found in SYSVOL are related to the corresponding GPC (GPO) object. This is normal and by design.

Therefore, there is no need for remediation.

See also

- Add Key Credential
- Add Member
- Allowed To Act
- Allowed To Delegate
- DCSync
- Grant Allowed To Act
- Has SID History
- Implicit Takeover
- Inherit GPO

- Linked GPO
- Member Of
- Owns
- Reset Password
- RODC Manage
- Write DACL
- Write Owner

DCSync

Description

DCSync is a legitimate Active Directory feature that domain controllers only use for replicating changes, but illegitimate security principals can also use it.

The Source security principal can request sensitive secrets (password hashes, Kerberos keys, etc.) from the Target domain using the DCSync feature, ultimately leading to a total compromise of the domain.

To fetch secrets, two security permissions are required: "Replicating Directory Changes" (`DS-Replication-Get-Changes`) and "Replicating Directory Changes All" (`DS-Replication-Get-Changes-All`). The relation occurs only if you give both of these permissions to the Source, either directly or through nested group membership.

Exploitation

Attackers who compromise the Source security principal can fetch secrets using dedicated hacker tools such as *mimikatz* or *impacket*.

- **Golden ticket**: Results from obtaining the password hash of the "krbtgt" account, which makes it possible to forge a Kerberos TGT and allows the impersonation of anyone on any computer/service. This notably gives administrative privileges over any computer in the domain.
- **Silver ticket**: Results from obtaining the password hash of a computer/service account, which makes it possible to forge a Kerberos service ticket and allows the impersonation of anyone on the given computer/service.

Remediation

Legitimate security principals allowed by default to leverage DCSync are:

- Administrators
- Domain Admins

- Enterprise Admins
- SYSTEM

In addition, the Microsoft Entra ID Connect configuration allows its password hash synchronization service account (MSOL_...) to leverage DCSync.

Finally, it is possible to discover service accounts for certain security tools, notably password auditing solutions. Verify their legitimacy with the people in charge.

For Source security principals without a legitimate need to perform DCSync, you must remove this permission.

To modify the security descriptor of the Target domain:

1. In "Active Directory Users and Computers", right-click the domain name and select Properties > Security.
2. Remove the "Replicating Directory Changes" and "Replicating Directory Changes All" permissions for illegitimate security principals.

> **Note**: DCSync relations can occur through permissions from nested group membership. Hence depending on the exact situation, you must remove the groups themselves or only some of their members.

See also

- Add Key Credential
- Add Member
- Allowed To Act
- Allowed To Delegate
- Belongs To GPO
- Grant Allowed To Act
- Has SID History
- Implicit Takeover
- Inherit GPO

- Linked GPO
- Member Of
- Owns
- Reset Password
- RODC Manage
- Write DACL
- Write Owner

Grant Allowed To Act

Description

The Source security principal is allowed to grant itself or someone else an Allowed To Act relation to the Target computer. It often leads to a total compromise of the Target computer via a Kerberos RBCD delegation attack.

This is possible because the Source has the permission to edit the Target's "msDS-AllowedToActOnBehalfOfOtherIdentity" attribute.

A malicious security principal performing this operation can create an "Allowed To Act" attack relation.

Exploitation

Attackers who compromise the Source security principal must edit the Target computer's `msDS-AllowedToActOnBehalfOfOtherIdentity` attribute using PowerShell (for example "Set-ADComputer <target> -PrincipalsAllowedToDelegateToAccount ...").

Remediation

Several natively privileged security principals have this permission by default, namely Account Operators, Administrators, Domain Admins, Enterprise Admins and SYSTEM. These security principals are legitimate and do not require remediation.

Kerberos RBCD is designed so that a computer's administrators can give the rights to perform delegation on the computer to anyone who needs it. This is different from other modes of Kerberos delegation that require Domain Admins level permission. This allows lower-level administrators to manage these security settings themselves, which is a principle also called delegation. In this case, the relation is legitimate.

However, if the Source security principal is not a legitimate administrator of the Target computer, the relation is not legitimate and you must remove this permission.

To modify the security descriptor of the Target computer:

1. In "Active Directory Users and Computers", right-click **Properties** > **Security**.
2. Remove the permission given to the Source security principal. Look for permissions such as "Write msDS-AllowedToActOnBehalfOfOtherIdentity", "Write all properties", "Write account restrictions", "Full control", etc.

> **Note**: The Source security principal can inherit the permission from an object higher in the Active Directory tree.

See also

- Add Key Credential
- Add Member
- Allowed To Act
- Allowed To Delegate
- Belongs To GPO
- DCSync
- Has SID History
- Implicit Takeover
- Inherit GPO
- Linked GPO
- Member Of
- Owns
- Reset Password
- RODC Manage
- Write DACL
- Write Owner

Has SID History

Description

The Source security principal has the SID of the Target security principal in its SIDHistory attribute, which means that the Source has the same rights as the Target.

SID History is a legitimate mechanism used when migrating security principals between domains to keep all authorizations referencing their previous SID functional.

However, this is also a persistence mechanism that attackers use, as it allows a discreet backdoor account to have the same rights as the desired target such as an Administrator account.

Exploitation

Attackers who compromise the Source security principal can directly authenticate as the Target security principal since the Target's SID is transparently added into the token that Active Directory authentication mechanisms generate (NTLM & Kerberos).

Remediation

If the Source and Target security principals are related to an approved domain migration, you can consider the relation to be legitimate and not perform any action. This relation remains visible as a reminder of a potential attack path.

If the domain of origin was deleted after the migration or is not configured in Tenable Identity Exposure, the Target security principal is marked as unresolved. Since the risk lies with the Target and that Target does not exist, there is no risk and hence no remediation required.

On the contrary, SID History relations to natively privileged users or groups are very likely malicious since Active Directory prevents their creation. This means that they were probably created using hacker techniques such as a "DCShadow" attack. You can also find these cases in the IoE related to "SID History".

If this is the case, Tenable Identity Exposure recommends a forensic examination of the entire Active Directory forest. The reason is that attackers must have obtained high privileges — domain administrator or equivalent — to edit maliciously the Source's SID history. The forensic examination helps you analyze the attack with corresponding remediation guidance, and identifies potential backdoors to remove.

Finally, Microsoft recommends that you modify all access rights in all services (SMB shares, Exchange, etc.) to use the new SIDs and remove unnecessary SIDHistory values after this migration is complete. This is a housekeeping best practice, although identifying exhaustively and fixing all ACLs is very difficult.

A user who has the right to edit the SIDHistory attribute on the Source object itself can remove SIDHistory values. Contrary to creation, this operation does not require domain administrator rights.

To do this, you can only use PowerShell because graphical tools such as Active Directory Users and Computers will fail. Example:

```
Set-ADUser -Identity <user> -Remove @{sidhistory="S-1-..."}
```

Caution: While removing a SIDHistory value is easy, reverting this operation is very complicated. This is because you must recreate the SIDHistory value which requires the presence of the other domain that may be decommissioned. For this reason, Microsoft also recommends that you prepare snapshots or backups.

See also

- Add Key Credential
- Add Member
- Allowed To Act
- Allowed To Delegate
- Belongs To GPO
- DCSync
- Grant Allowed To Act
- Implicit Takeover
- Inherit GPO
- Linked GPO
- Member Of
- Owns

- Reset Password
- RODC Manage
- Write DACL
- Write Owner

Implicit Takeover

Description

The Source is a Tier0 security principal. Tier0 is the set of Active Directory objects that have the highest privileges in the domain, such as the members of the Domain Admins or Domain Controllers group. All Tier0 assets can implicitly compromise any other object in the domain, even if there is no explicit other relation.

This relation makes it possible to model implicit rights built-in to Active Directory. These rights are by design and documented, and thus known to attackers. However, Tenable Identity Exposure cannot collect these rights by standard means. Moreover, this relation simplifies attack path graphs, because as soon as attackers compromise a Tier0 node, they can attack any other object directly without going through other explicit relations.

In summary, Source Tier0 assets are considered to all have "Implicit Takeover" relations to any Target node in the graph.

Exploitation

The exact exploitation method depends on the type of the Source Tier0 asset targeted, but these are well-documented techniques that attackers efficiently master.

Remediation

This relation is by design and you cannot remediate it. It is almost impossible to stop an attacker who reaches a Tier0 asset from attacking further.

Remediation efforts must focus on upstream relations in attack paths.

See also

- Add Key Credential
- Add Member
- Allowed To Act
- Allowed To Delegate

- Belongs To GPO
- DCSync
- Grant Allowed To Act
- Has SID History
- Inherit GPO
- Linked GPO
- Member Of
- Owns
- Reset Password
- RODC Manage
- Write DACL
- Write Owner

Inherit GPO

Description

A Source linkable container such as an Organizational Unit (OU) or Domain – but not Sites – contains the Target OU, User, Device, DC, or Read-Only Domain Controller (RODC) in the LDAP tree. This is because the children objects of the linkable container inherit the GPO where it is linked (see "Linked GPO" relations).

Tenable Identity Exposure takes into account whenever an OU blocks inheritance.

Exploitation

Attackers have nothing to do to exploit this relation as long as they manage to compromise the GPO upstream in the attack path. By design, the relation applies to linkable containers and objects below them, as shown by Inherit GPO relations.

Remediation

In most cases, it is normal and legitimate for GPOs to apply to linkable children containers from their parent containers. However, this linkage exposes additional attack paths.

Therefore, in order to reduce risks, you should link GPOs to the lowest level in the organizational units hierarchy, whenever possible.

Moreover, GPOs require protection from unauthorized modifications by attackers, in order not to expose them to other attack relations.

Finally, OUs can disable GPO inheritance from higher levels through their "block inheritance" option. However, use this option only as a last resort because it blocks all GPOs -- including the potential security hardening GPOs defined at the highest domain level. It also makes the reasoning about applied GPOs more difficult.

See also

- Add Key Credential
- Add Member

- Allowed To Act
- Allowed To Delegate
- Belongs To GPO
- DCSync
- Grant Allowed To Act
- Has SID History
- Implicit Takeover
- Linked GPO
- Member Of
- Owns
- Reset Password
- RODC Manage
- Write DACL
- Write Owner

Linked GPO

Description

The Source GPO is linked to the Target linkable container, such as a Domain or Organizational Unit (OU). This means that the Source GPO can assign settings and run programs on the devices and users contained in the Target. The Source GPO also applies to objects in containers below it through "Inherit GPO" relations.

Ultimately, the GPO can compromise the devices and users on which it applies.

Exploitation

Attackers must first compromise the Source GPO through another attack relation.

From there, they employ several techniques to perform malicious actions on devices and users contained in the Target and those below it. Examples are:

- Abusing the legitimate "immediate scheduled tasks" to execute arbitrary scripts on devices.
- Adding a new local user with administrative rights on all devices
- Installing an MSI program
- Disabling the firewall or antivirus
- Granting further rights
- etc.

Attackers can modify a GPO by manually editing its content using administration tools such as "Group Policy Management" or dedicated hacker tools such as PowerSploit.

Remediation

In most cases, linking a GPO to a linkable container is normal and legitimate. However, this linkage increases the attack surface where it occurs as well as in the containers below it.

Therefore, in order to reduce risks, you should link GPOs to the lowest level in the organizational units hierarchy, whenever possible.

Moreover, GPOs require protection from unauthorized modifications by attackers, in order not to expose them to other attack relations.

See also

- Add Key Credential
- Add Member
- Allowed To Act
- Allowed To Delegate
- Belongs To GPO
- DCSync
- Grant Allowed To Act
- Has SID History
- Implicit Takeover
- Inherit GPO
- Member Of
- Owns
- Reset Password
- RODC Manage
- Write DACL
- Write Owner

Member Of

Description

The Source security principal is a member of the Target group. Therefore, it benefits from all the access rights that the group holds, such as accessing file shares, assuming roles in business applications, etc.

Exploitation

Attackers do not have to do anything to exploit this attack relation. They only need to authenticate as the Source security principal to get the Target group in their local or remote security token, or Kerberos ticket.

Remediation

If the Source security principal is an illegitimate member of the Target group, then you must remove it.

You can use any standard Active Directory administration tool such as "Active Directory Users and Computers" or PowerShell such as Remove-ADGroupMember.

See also

- Add Key Credential
- Add Member
- Allowed To Act
- Allowed To Delegate
- Belongs To GPO
- DCSync
- Grant Allowed To Act
- Has SID History
- Implicit Takeover

- Inherit GPO
- Linked GPO
- Owns
- Reset Password
- RODC Manage
- Write DACL
- Write Owner

Owns

Description

The Source security principal is the declared owner of the Target object because it likely created the Target object. Owners have implicit rights – "Read Control" and "Write DACL" – that allow them to obtain additional rights, for themselves or someone else, and ultimately compromise the Target object.

Exploitation

Attackers who compromise the Source security principal only have to edit the Target object's security descriptor using native Windows commands such as "dsacls", PowerShell such as "Set-ACL", administration tools such as "Active Directory Users and Computers", or dedicated hacker tools such as PowerSploit.

When an object gets created, there is a risk of privilege escalation if a low privileged user creates it and thus owns it – for example, a standard helpdesk technician – and later that object gets elevated to higher privileges – for example, administrator. The original owner remains and can now compromise the newly privileged object to take advantage of its privileges.

Remediation

If the Source security principal is not a legitimate owner of the Target object, then you must change it.

To change the owner of the Target object:

1. In "Active Directory Users and Computers", right-click **Properties** > **Security** > **Advanced**.
2. On the **Owner** line at the top, click **Change**.

Safe Target object owners used by default for most sensitive Active Directory objects are:

- Objects in the Domain partition: "Administrators" or "Domain Admins"
- Objects in the Configuration partition: "Enterprise Admins"
- Objects in the Schema partition: "Schema Admins"

See also

- Add Key Credential
- Add Member
- Allowed To Act
- Allowed To Delegate
- Belongs To GPO
- DCSync
- Grant Allowed To Act
- Has SID History
- Implicit Takeover
- Inherit GPO
- Linked GPO
- Member Of
- Reset Password
- RODC Manage
- Write DACL
- Write Owner

Reset Password

Description

The Source security principal can reset the password of the Target, which allows it to authenticate as the Target using the new attributed password and benefit from the Target's privileges.

Resetting a password is not the same as changing a password, which anyone who knows the current password can do. A password change typically occurs when a password expires.

Exploitation

Attackers who compromise the Source security principal can reset the password of the Target using native Windows commands such as "net user /domain", PowerShell such as "Set-ADAccountPassword -Reset", administration tools such as "Active Directory Users and Computers", or dedicated hacker tools such as PowerSploit.

Attackers then only have to authenticate to the Active Directory or the targeted resource using legitimate authentication methods with their new chosen password to impersonate fully the Target.

However, attackers do not usually know the previous password to revert to it after the attack. Therefore, the attack is often visible for the legitimate person behind the Target and can even cause a denial of service, especially for service accounts.

Remediation

IT administrators and helpdesk staff are legitimately allowed to reset passwords. But you must put in place the appropriate delegations to let them perform this action only within their allowed perimeter.

Also, according to the tiering model, you must ensure that a lower level staff such as a helpdesk for normal users cannot reset the password of a higher level account, such as a domain administrator, because this is an opportunity for privilege escalation.

To modify the Target's security descriptor and remove illegitimate permissions:

1. In "Active Directory Users and Computers", right-click Properties > Security.
2. Remove "Reset password" permission for the Source security principal.

Note: Do not confuse this permission with "Change password".

See also

- Add Key Credential
- Add Member
- Allowed To Act
- Allowed To Delegate
- Belongs To GPO
- DCSync
- Grant Allowed To Act
- Has SID History
- Implicit Takeover
- Inherit GPO
- Linked GPO
- Member Of
- Owns
- RODC Manage
- Write DACL
- Write Owner

RODC Manage

Description

The Source security principal is found in the "ManagedBy" attribute of the Target Read-Only Domain Controller (RODC). This means that the Source has administrative rights over the Target RODC.

> **Note**: Other Active Directory object types use the same "ManagedBy" attribute for informational purposes only, and do not give any administrative rights to the declared manager. Therefore, this relation exists only for Target nodes of the RODC type.

RODCs are less sensitive than the more common writable Domain Controllers, but they are still a high-value target for attackers because they can steal credentials from RODCs to allow them to pivot further to other systems. This depends on the level of hardening in the RODC's configuration – for example, the number of objects with secrets that it can synchronize.

Exploitation

The exploitation method is identical to that of the "AdminTo" relation.

Attackers who compromise the Source security principal can use its identity to connect remotely and execute commands on the Target RODC with administrative rights. They can exploit available native protocols such as Server Message Block (SMB) with administrative shares, Remote Desktop Protocol (RDP), Windows Management Instrumentation (WMI), Remote Procedure Call (RPC), Windows Remote Management (WinRM), etc.

Attackers can use native remote administration tools such as PsExec, services, scheduled tasks, Invoke-Command, etc., or specialized hacker tools such as wmiexec, smbexec, Invoke-DCOM, SharpRDP, etc.

The attack's final goal can either be to compromise the Target RODC or to use credential dumping tools such as mimikatz to obtain more credentials and secrets to pivot to other machines.

Remediation

If the Source security principal is not a legitimate administrator of the Target Read-Only Domain Controller (RODC), then you must replace it with a proper administrator.

Note that Domain Admins do not generally administer RODCs, hence the dedicated "managed by" setting. This is because RODCs have a lower trust level and high-privilege Domain Admins should not expose their credentials by authenticating on them.

Therefore, you must select a proper "middle-level" administrator for RODCs according to your Active Directory RODC rules – for example, the IT administrator of an organization's local branch where they are located.

To change the "ManagedBy" attribute:

1. In "Active Directory Users and Computers", select the RODC > **Properties** > "**ManagedBy**" tab.
2. Click **Change**.

You can also run the following command in PowerShell:

```
Set-ADComputer <rodc> -ManagedBy (Get-ADUser <rodc_admin>)
```

See also

- Add Key Credential
- Add Member
- Allowed To Act
- Allowed To Delegate
- Belongs To GPO
- DCSync
- Grant Allowed To Act
- Has SID History
- Implicit Takeover
- Inherit GPO
- Linked GPO
- Member Of

- Owns
- Reset Password
- Write DACL
- Write Owner

Write DACL

Description

The Source security principal has the permission to change the permissions of the Target object in the Discretionary Access Control List (DACL). This allows the Source to obtain for themselves, or give to someone else, additional rights and ultimately compromise the Target object.

Exploitation

Attackers who compromise the Source security principal only have to edit the Target object's security descriptor using native Windows commands such as "dsacls", PowerShell such as "Set-ACL", administration tools such as "Active Directory Users and Computers", or dedicated hacker tools such as PowerSploit.

Remediation

If the Source security principal does not have legitimate permission to change the permissions of the Target object, then you must remove this permission.

To modify the Target object's security descriptor:

1. In "Active Directory Users and Computers", right-click the object then **Properties** > **Security** > **Advanced**.
2. Remove the "Modify permissions" permission for the Source security principal.

> **Note**: An object can inherit this permission from an object higher in the Active Directory tree.

See also

- Add Key Credential
- Add Member
- Allowed To Act
- Allowed To Delegate

- Belongs To GPO
- DCSync
- Grant Allowed To Act
- Has SID History
- Implicit Takeover
- Inherit GPO
- Linked GPO
- Member Of
- Owns
- Reset Password
- RODC Manage
- Write Owner

Write Owner

Description

The Source security principal has the permission to change the owner of the Target object, including assigning themselves as the owner. Owners have implicit rights, "Read Control" and "Write DACL", that allow them to obtain additional rights for themselves or for someone else, and ultimately compromise the Target object.

For more information, see the Owns relation.

Exploitation

Attackers who compromise the Source security principal can assign themselves as the owner of the Target using native Windows commands such as "dsacls /takeownership", PowerShell such as "Set-ACL", administration tools such as "Active Directory Users and Computers", or dedicated hacker tools such as PowerSploit.

They can then edit the Target object's security descriptor using similar methods.

Remediation

If the Source security principal does not have legitimate permission to change the Target object's owner, then you must remove this permission.

To modify the Target object's security descriptor:

1. In "Active Directory Users and Computers", right-click the object and select **Properties** > **Security** > **Advanced**.
2. Remove the "Modify owner" permission for the Source security principal.

> **Note**: An object can inherit this permission from an object higher in the Active Directory tree.

See also

- Add Key Credential
- Add Member

- Allowed To Act
- Allowed To Delegate
- Belongs To GPO
- DCSync
- Grant Allowed To Act
- Has SID History
- Implicit Takeover
- Inherit GPO
- Linked GPO
- Member Of
- Owns
- Reset Password
- RODC Manage
- Write DACL

Identifying Tier 0 Assets

Tier 0 assets include accounts, groups, and other assets that have direct or indirect administrative control of the Active Directory forests and domains.

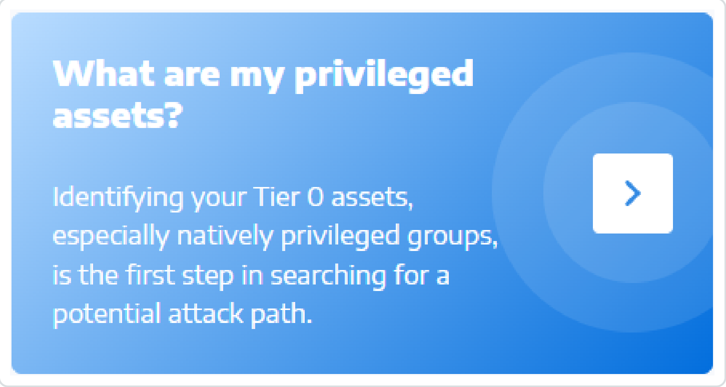
Tenable Identity Exposure lists your Tier 0 assets and accounts with potential attack paths leading to that asset.

To list Tier 0 assets:

1. In Tenable Identity Exposure, click on the Attack Path icon ✥ in the left navigation bar.

   The **Attack Path** pane opens.

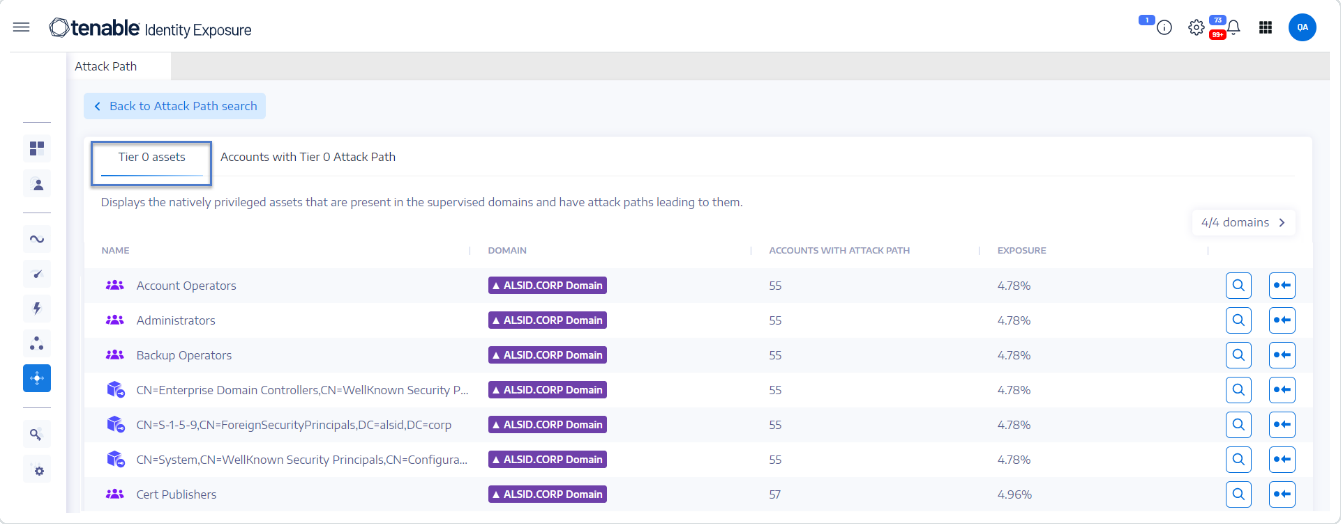
2. Click on the tile "**What are my privileged assets?**".

   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.

   Tenable Identity Exposure shows a list of Tier 0 assets in your AD.

   tenable Identity Exposure
QA
Attack Path
Back to Attack Path search
Tier 0 assets
Accounts with Tier 0 Attack Path

   Displays the natively privileged assets that are present in the supervised domains and have attack paths leading to them.

   4/4 domains

NAME	DOMAIN	ACCOUNTS WITH ATTACK PATH	EXPOSURE
Account Operators	▲ ALSID.CORP Domain	55	4.78%
Administrators	▲ ALSID.CORP Domain	55	4.78%
Backup Operators	▲ ALSID.CORP Domain	55	4.78%
CN=Enterprise Domain Controllers,CN=WellKnown Security P...	▲ ALSID.CORP Domain	55	4.78%
CN=S-1-5-9,CN=ForeignSecurityPrincipals,DC=alsid,DC=corp	▲ ALSID.CORP Domain	55	4.78%
CN=System,CN=WellKnown Security Principals,CN=Configura...	▲ ALSID.CORP Domain	55	4.78%
Cert Publishers	▲ ALSID.CORP Domain	57	4.96%

   Each line gives the **asset name**, its **domain**, and the following information:

  - **Accounts with Attack Path**: The number of assets that have an attack path leading to the Tier 0 asset.
  - **Exposure**: The accounts that have an attack path leading to the Tier 0 asset as a percentage of the total number of accounts in the domain.

To filter the assets for any specific domain:

1. Click the **n/n** button.

   The **Forest and Domains** pane opens. You can do either of the following:

   - In the **Search** box, type the name of a forest or domain.
   - Select the **Expand all** box and select the forest or domain that you want.

2. Click **Filter on selection**.

   Tenable Identity Exposure updates the list of assets.

To list the accounts with attack paths leading to the Tier 0 asset:

- At the end of line of the Tier 0 asset name, click the 🔍 icon.

  Tenable Identity Exposure shows a list of accounts with attack paths leading to that Tier 0 asset.

To see the asset exposure of the Tier 0 asset:

- At the end of line with the Tier 0 asset name, click the •← icon.

  Tenable Identity Exposure opens the Asset Exposure page for that Tier 0 asset. For more information, see Attack Relations

Accounts with Attack Paths

Tenable Identity Exposure shows accounts with attack paths leading to Tier 0 assets to give you a comprehensive view of a potential security threat, because user and computer accounts can become privileged through various attack relations.

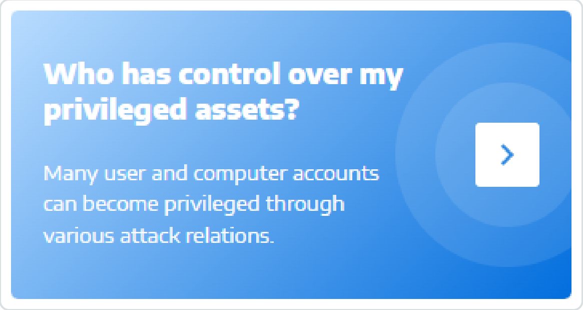
For more information, see Identifying Tier 0 Assets.

To show assets with attack paths:

1. In Tenable Identity Exposure, click on the Attack Path icon in the left navigation bar.

   The **Attack Path** pane opens.

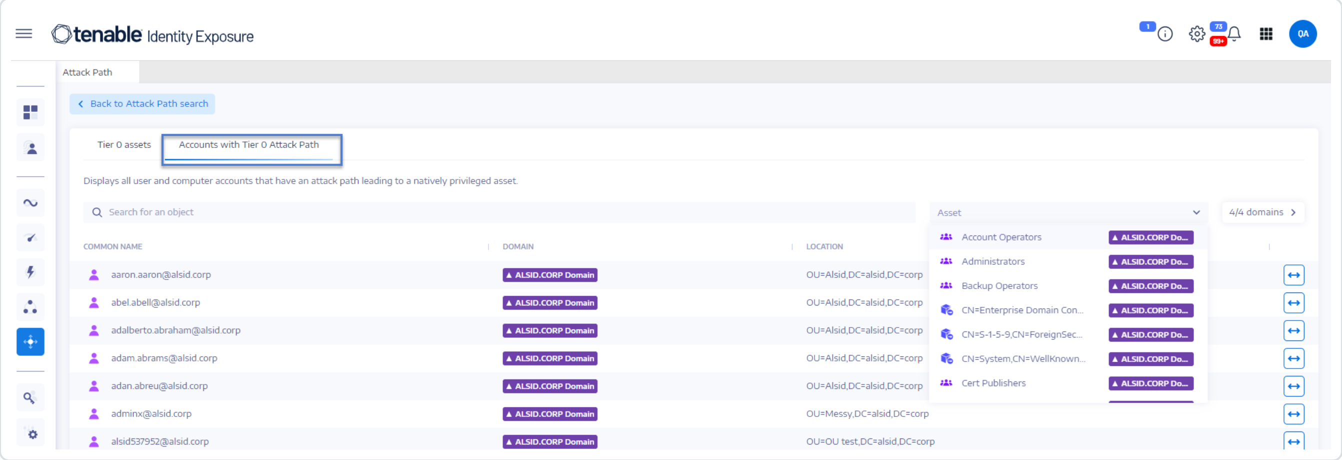
2. Click on the tile "**Who has control over my privileged assets?**".



Who has control over my privileged assets?

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

   Tenable Identity Exposure shows all user and computer accounts that have an attack path leading to a Tier 0 asset.



tenable Identity Exposure
Attack Path
Back to Attack Path search
Tier 0 assets
Accounts with Tier 0 Attack Path

Displays all user and computer accounts that have an attack path leading to a natively privileged asset.

Search for an object
Asset
4/4 domains

COMMON NAME	DOMAIN	LOCATION
aaron.aaron@alsid.corp	ALSID.CORP Domain	OU=Alsid,DC=alsid,DC=corp
abel.abell@alsid.corp	ALSID.CORP Domain	OU=Alsid,DC=alsid,DC=corp
adalberto.abraham@alsid.corp	ALSID.CORP Domain	OU=Alsid,DC=alsid,DC=corp
adam.abrams@alsid.corp	ALSID.CORP Domain	OU=Alsid,DC=alsid,DC=corp
adan.abreu@alsid.corp	ALSID.CORP Domain	OU=Alsid,DC=alsid,DC=corp
adminx@alsid.corp	ALSID.CORP Domain	OU=Messy,DC=alsid,DC=corp
alsid537952@alsid.corp	ALSID.CORP Domain	OU=OU test,DC=alsid,DC=corp

Account Operators	ALSID.CORP Do...
Administrators	ALSID.CORP Do...
Backup Operators	ALSID.CORP Do...
CN=Enterprise Domain Con...	ALSID.CORP Do...
CN=S-1-5-9,CN=ForeignSec...	ALSID.CORP Do...
CN=System,CN=WellKnown...	ALSID.CORP Do...
Cert Publishers	ALSID.CORP Do...

To search for a specific asset:

1. In the **Search** box, type the name of the asset.
2. In the **Asset** box, click the arrow **>** to show a drop-down list of Tier 0 assets and select one.

   Tenable Identity Exposure updates the list with the matching results.

To filter the assets for any specific domain:

1. Click the **n/n** button.

   The **Forest and Domains** pane opens. You can do either of the following:

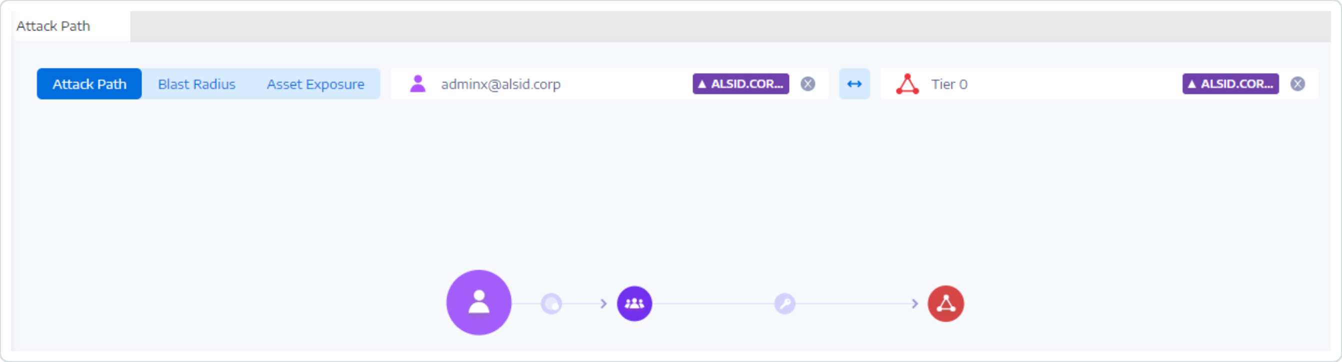
   - In the **Search** box, type the name of a forest or domain.
   - Select the **Expand all** box and select the forest or domain that you want.
2. Click **Filter on selection**.

   Tenable Identity Exposure updates the list of assets.

To explore the attack path:

- At the end of the line of the asset name, click the ↔ icon.

  Tenable Identity Exposure opens the Attack Path page from that asset to all Tier 0 assets. For more information, see Attack Path and Attack Relations



Attack Path Node Types

The attack path feature in Tenable Identity Exposure shows you a graph visualizing attack paths open to attackers within your Active Directory environment. The graph comprises **edges** that represent attack relations and **nodes** that represent Active Directory (LDAP/SYSVOL) objects.

The following list describes all the possible node types that you can expect to see in attack path graphs.

Node Type	Location	Icon	Description
User	LDAP	👤	LDAP object that has its `objectClass` attribute containing the class `user` but not `computer`.
Group	LDAP	👥	LDAP object that has its `objectClass` attribute containing the `class` group.
Device	LDAP	🖥	LDAP object that has its `objectClass` attribute containing the class `computer` but not `msDS-GroupManagedServiceAccount`. Its `primaryGroupID` attribute does not equal 516 (DC) or 521 (RODC). **Note**: To differentiate Tenable products, this category is called "Device" instead of "Computer" to be more generic.
Organizational Unit (OU)	LDAP	📂	LDAP object that has its `objectClass` attribute containing the class `organizationalUnit`. Avoid confusion between objects of the `container` class and the fact that any Active Directory (AD) object can serve as a container, allowing it to contain other objects.
Domain	LDAP	△	LDAP object that has its `objectClass` attribute containing the class `domainDNS` and certain attributes.
Domain Controller	LDAP	🚪	LDAP object that has its `objectClass` attribute containing the class `computer` and its `primaryGroupID`

(DC)			attribute equal to 516 (therefore not an RODC).
Read-Only Domain Controller (RODC)	LDAP	🔒	LDAP object that has its `objectClass` attribute containing the class `computer` and its `primaryGroupID` attribute equal to 521 (therefore not a normal DC).
Group Policy (GPC)	LDAP	⚙	LDAP object that has its `objectClass` attribute containing the class `groupPolicyContainer`.
GPO file	SYSVOL	⚙	File found in the SYSVOL share of a specific GPO (for example "`\\example.net\sysvol\example.net\Policies\{A8370D7F-8AC0-452E-A875-2A6A52E9D392}\{Machine,User}\Preferences\ScheduledTasks\ScheduledTasks.xml`")
GPO folder	SYSVOL	📁	Folder found in the SYSVOL share of a specific GPO. There is one for each GPO (for example "`\\example.net\sysvol\example.net\Policies\{A8370D7F-8AC0-452E-A875-2A6A52E9D392}\Machine\Scripts\Startup`")
Group-Managed Service Account (gMSA)	LDAP	🤖	LDAP object that has its `objectClass` attribute containing the class `msDS-GroupManagedServiceAccount`.
Enterprise NtAuth store	LDAP	✓	LDAP object that has its `objectClass` attribute containing the class `certificationAuthority`.
PKI certificate template	LDAP	📝	LDAP object that has its `objectClass` attribute containing the class `pKICertificateTemplate`.

Unresolved security principal	LDAP	?	LDAP object that has its `objectSid` or `DistinguishedName` attribute used at some point when building relations, but for which there is an unknown corresponding LDAP security principal object (classic case of "unresolved SID"). Also lacking information about the specific security principal type (User, Computer, Group, etc.) associated with them; only their SID/DN is known.
Special Identity	LDAP		Windows and Active Directory use well-known identities internally. These identities function similarly to groups, but AD does not declare them as such. For more information, see Special Identity Groups.
Others			Currently all AD/SYSVOL objects that do not fall into the mentioned categories.

Activity Logs

The activity logs in Tenable Identity Exposure allow you to view the traces of all activities that occurred on the Tenable Identity Exposure platform related to specific IP addresses, users, or actions.

> **Note**: Due to technical limitations, activity logs concerning specific views, such as Tenant Management (including adding, editing, or removing), are not currently visible.

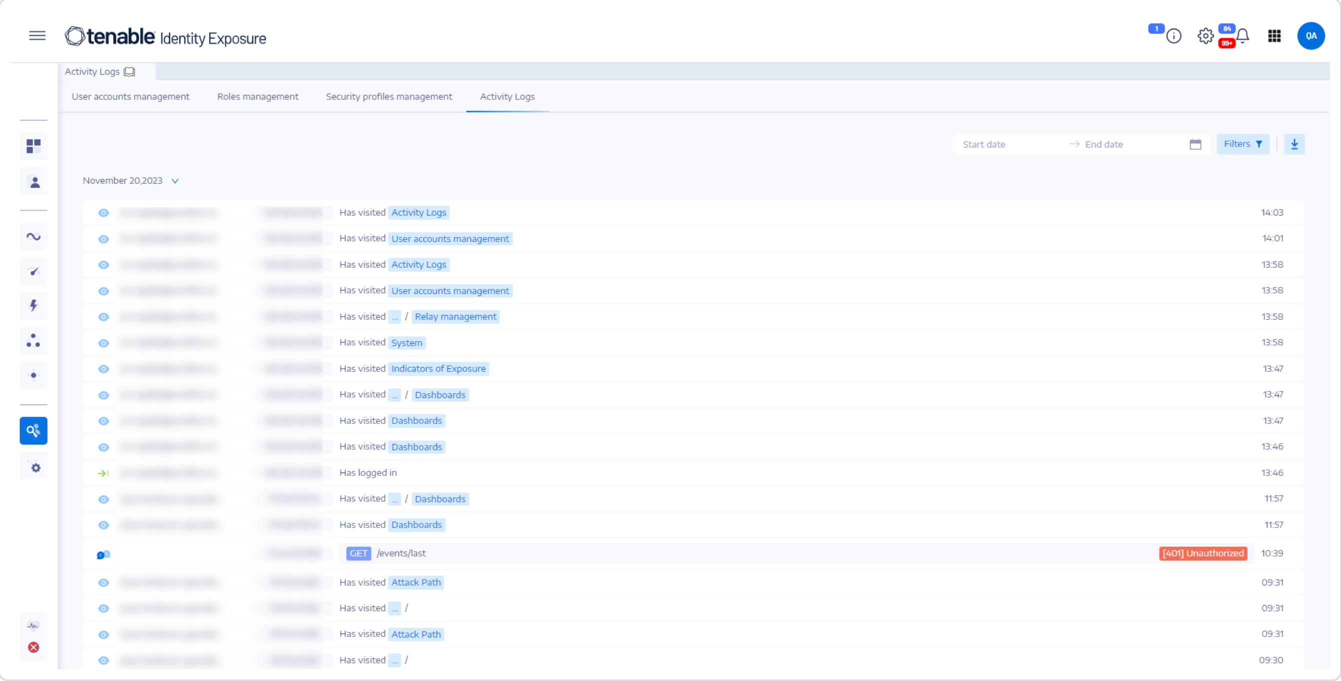
To view the activity logs:

1. In Tenable Identity Exposure, click on the **Accounts** icon in the left navigation menu.

   The **User account management** pane appears.

2. Select the **Activity Logs** tab.

   The Activity Logs pane opens.



November 20,2023

```
[redacted] [redacted] Has visited Activity Logs                          14:03
[redacted] [redacted] Has visited User accounts management               14:01
[redacted] [redacted] Has visited Activity Logs                          13:58
[redacted] [redacted] Has visited User accounts management               13:58
[redacted] [redacted] Has visited ... / Relay management                 13:58
[redacted] [redacted] Has visited System                                 13:58
[redacted] [redacted] Has visited Indicators of Exposure                 13:47
[redacted] [redacted] Has visited ... / Dashboards                       13:47
[redacted] [redacted] Has visited Dashboards                             13:47
[redacted] [redacted] Has visited Dashboards                             13:46
[redacted] [redacted] Has logged in                                      13:46
[redacted] [redacted] Has visited ... / Dashboards                       11:57
[redacted] [redacted] Has visited Dashboards                             11:57
           [redacted] GET /events/last          [401] Unauthorized       10:39
[redacted] [redacted] Has visited Attack Path                            09:31
[redacted] [redacted] Has visited ... /                                  09:31
[redacted] [redacted] Has visited Attack Path                            09:31
[redacted] [redacted] Has visited ... /                                  09:30
```

To display activity logs for a specific time frame:

1. At the top of the activity log pane, click on the date picker.
2. Select a start date and an end date for the period that you want.
3. (Optional) Use the scroll bar to select the time (default: current time)
4. Click **OK**.

   Tenable Identity Exposure shows the activity log for that time period.

To filter activity logs:

1. At the top of the activity log pane, click the Filters ▼ button.

   The **Filters** pane appears.

2. Click > in the following boxes:
   - IP Address
   - User
   - Action
3. Click **Validate**.

   Tenable Identity Exposure shows the activity log for the filter you defined.

To clear filters:

- At the bottom of the **Filters** pane, click **Erase filters**.

  Tenable Identity Exposure shows the unfiltered activity log.

To export the activity logs:

- At the top of the activity log pane, click the ⤓ icon.

  Tenable Identity Exposure downloads the activity log in CSV format to your computer.

Tenable Identity Exposure Administrator Guide

Last updated: March 25, 2024

The Administrator's Guide provides information about administration tasks for Tenable Identity Exposure (formerly known as Tenable.ad).

Tenable recommends some of the following to get started as an administrator in Tenable Identity Exposure:

- Prepare and Install
- Configure Profile and Users
- Detect and Monitor

Tip: For additional information on Tenable Identity Exposure, review the following customer education materials:

- Tenable Identity Exposure Self Help Guide
- Tenable Identity Exposure Introduction (Tenable University)

Prepare and Install

To prepare for and complete Tenable Identity Exposure installation:

- Install Tenable Identity Exposure as described in the *Tenable Identity Exposure Installation Guide*.
- Connect and sign in to Tenable Identity Exposure.

Configure Profile and Users

Next, we recommend interacting with the following to configure and navigate the Tenable Identity Exposure interface:

- Set profile preferences: Configure your default language, change your password, and set other preferences for your profile
- Create and add users to your Tenable Identity Exposure instance.

- Configure role-based access control (RBAC) to secure access to data and functions within your organization.

Detect and Monitor

Once you have configured and tuned Tenable Identity Exposure to your business needs, you can begin working with your data:

- Deploy the Indicators of Attack module.
- Manage and receive relevant information about the security state of the monitored infrastructure using the Tenable Identity Exposure portal.
- Define attack scenarios by selecting the types of attack for Tenable Identity Exposure to monitor on specific domains.

Note: Tenable Identity Exposure can be purchased alone or as part of the Tenable One package. For more information, see Tenable One.

Tenable One Exposure Management Platform

Tenable One is an Exposure Management Platform to help organizations gain visibility across the modern attack surface, focus efforts to prevent likely attacks and accurately communicate cyber risk to support optimal business performance.

The platform combines the broadest vulnerability coverage spanning IT assets, cloud resources, containers, web apps and identity systems, builds on the speed and breadth of vulnerability coverage from Tenable Research and adds comprehensive analytics to prioritize actions and communicate cyber risk. Tenable One allows organizations to:

- Gain comprehensive visibility across the modern attack surface
- Anticipate threats and prioritize efforts to prevent attacks
- Communicate cyber risk to make better decisions

Tenable Identity Exposure exists as a standalone product, or can be purchased as part of the Tenable One Exposure Management platform.

Tip: For additional information on getting started with Tenable One products, check out the Tenable One Deployment Guide.

For more information, see the following:

Active Directory Configuration

Tenable Identity Exposure requires some configuration on the monitored Active Directory to allow certain features to work:

- Access to AD Objects or Containers
- Access for Privileged Analysis
- Indicators of Attack Deployment

Access to AD Objects or Containers

> **Note**: This section only applies for a Tenable Identity Exposure license for the Indicator of Exposure module.

Tenable Identity Exposure does not require administrative privileges to achieve its security monitoring.

This approach relies on the ability of the user account that Tenable Identity Exposure uses to read all Active Directory objects stored in a domain (including user accounts, organizational units, groups, etc.).

By default, most objects have a read access for the group Domain Users that the Tenable Identity Exposure service account uses. However, you must manually configure some containers to allow read access for the Tenable Identity Exposure user account.

The following table details the Active Directory objects and containers that require manual configuration for read access on each domain that Tenable Identity Exposure monitors.

Location of the Container	Description
`CN=Deleted Objects,DC=<DOMAIN>,DC=<TLD>`	A container that hosts deleted objects.
`CN=Password Settings Container,CN=System, DC=<DOMAIN>,DC=<TLD>`	(Optional) A container that hosts Password Settings Objects.

To grant access to AD objects and containers:

- In the domain controller's command line interface, run the following command to grant access to Active Directory objects or containers:

  > **Note**: You must run this command on each domain that Tenable Identity Exposure monitors.

  ```
  dsacls "<__CONTAINER__>" /takeownership
  dsacls "<__CONTAINER__>" /g <__SERVICE_ACCOUNT__>:LCRP /I:T
  ```

where:

- `<__CONTAINER__>` refers to the container that requires access.
- `<__SERVICE_ACCOUNT__>` refers to the service account that Tenable Identity Exposure uses.

Access for Privileged Analysis

The optional Privileged Analysis feature requires administrative privileges. You must assign permissions for the service account that Tenable Identity Exposure uses.

For more information, see Privileged Analysis.

Note: You must assign permissions on each domain where you enable Privileged Analysis.

To assign permissions using the command line:

Requirement: To assign permissions, you need an account with Domain Admins rights or equivalent.

- In the domain controller's command-line interface, run the following command to add both permissions:

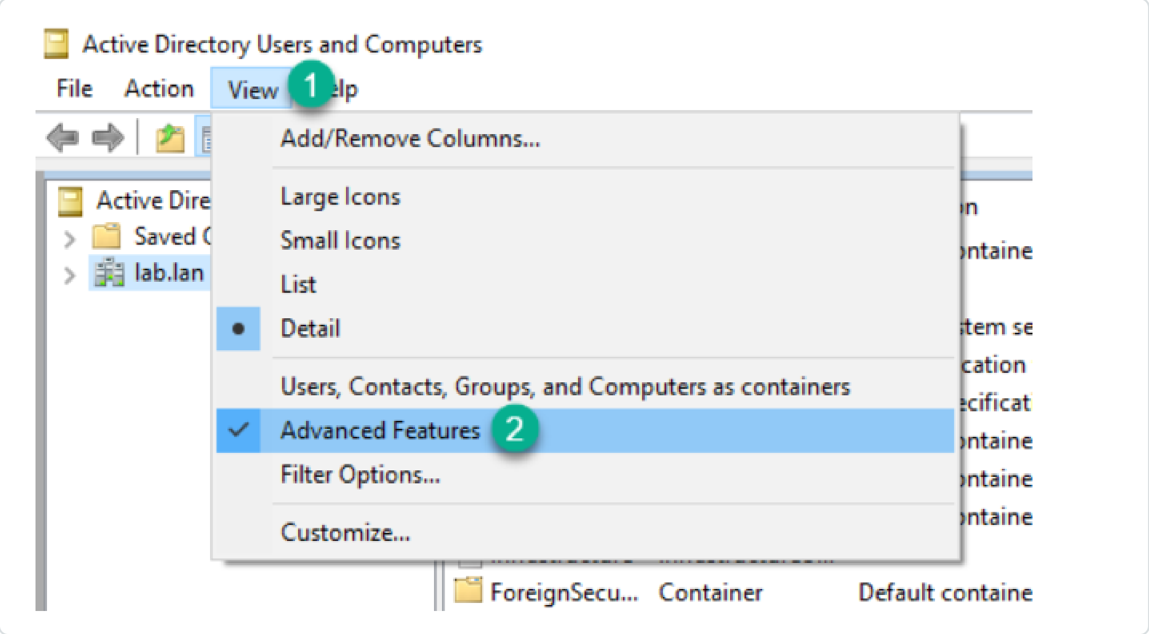
  ```
  dsacls "<__DOMAIN_ROOT__>"  /g "<__SERVICE_ACCOUNT__>:CA;Replicating Directory Changes" "<__
  SERVICE_ACCOUNT__>:CA;Replicating Directory Changes All"
  ```

  Where:

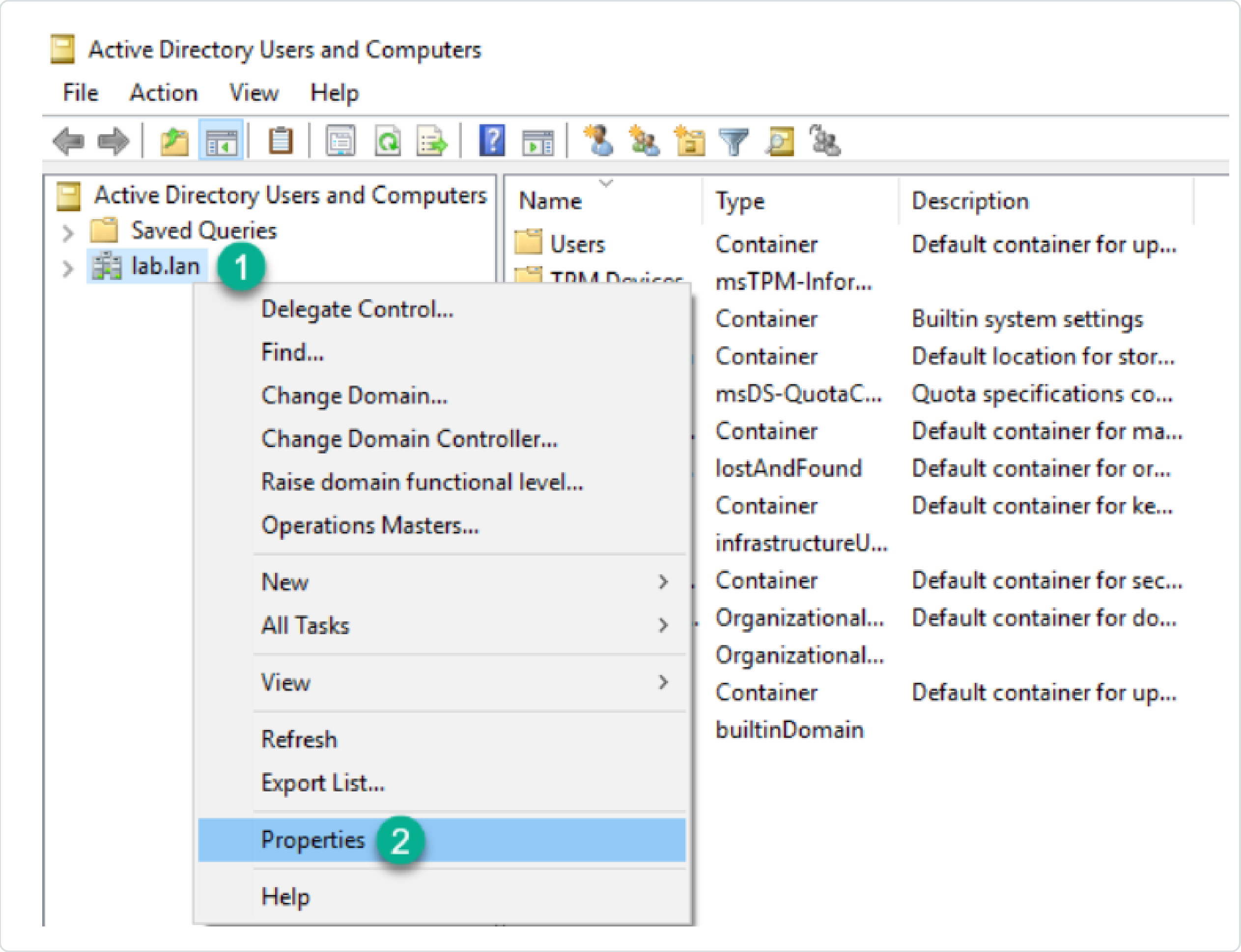
  - `<__DOMAIN_ROOT__>` refers to the Distinguished Name of the root of the domain. Example: “`DC=<DOMAIN>,DC=<TLD>`”
  - `<__SERVICE_ACCOUNT__>` refers to the service account that Tenable Identity Exposure uses. Example: “`DOMAIN\tenablead`”.

To assign permissions using the graphical user interface:

1. From the **Start** menu in Windows, open **Active Directory Users and Computers**.
2. From the **View** menu, select **Advanced Features**.



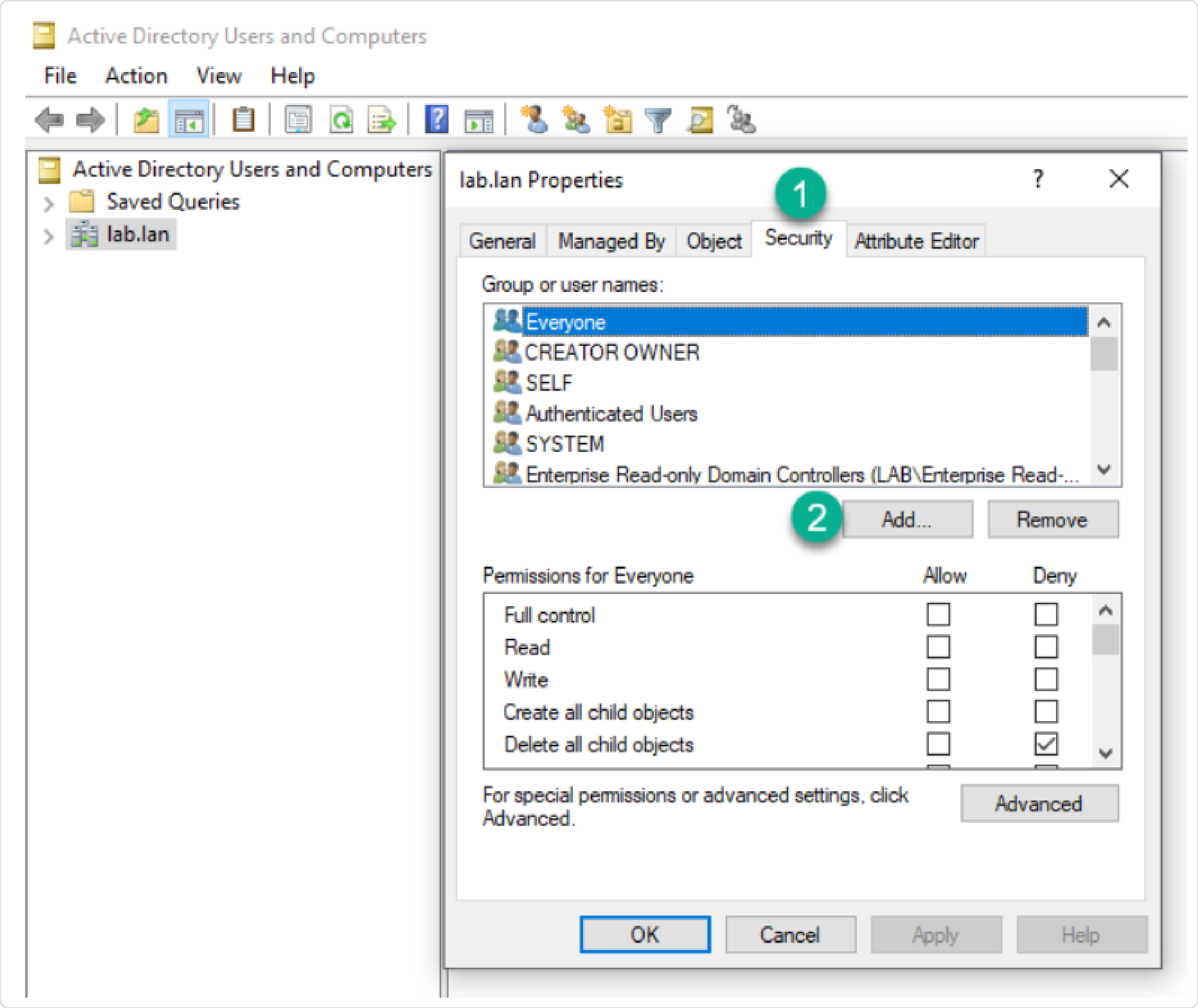
3. Right-click on the domain root and select **Properties**.



Name	Type	Description
Users	Container	Default container for up...
TPM Devices	msTPM-Infor...	
	Container	Builtin system settings
	Container	Default location for stor...
	msDS-QuotaC...	Quota specifications co...
	Container	Default container for ma...
	lostAndFound	Default container for or...
	Container	Default container for ke...
	infrastructureU...	
	Container	Default container for sec...
	Organizational...	Default container for do...
	Organizational...	
	Container	Default container for up...
	builtinDomain	

The domain root's properties pane opens.

4. Click the **Security** tab and click **Add**.



Group or user names:

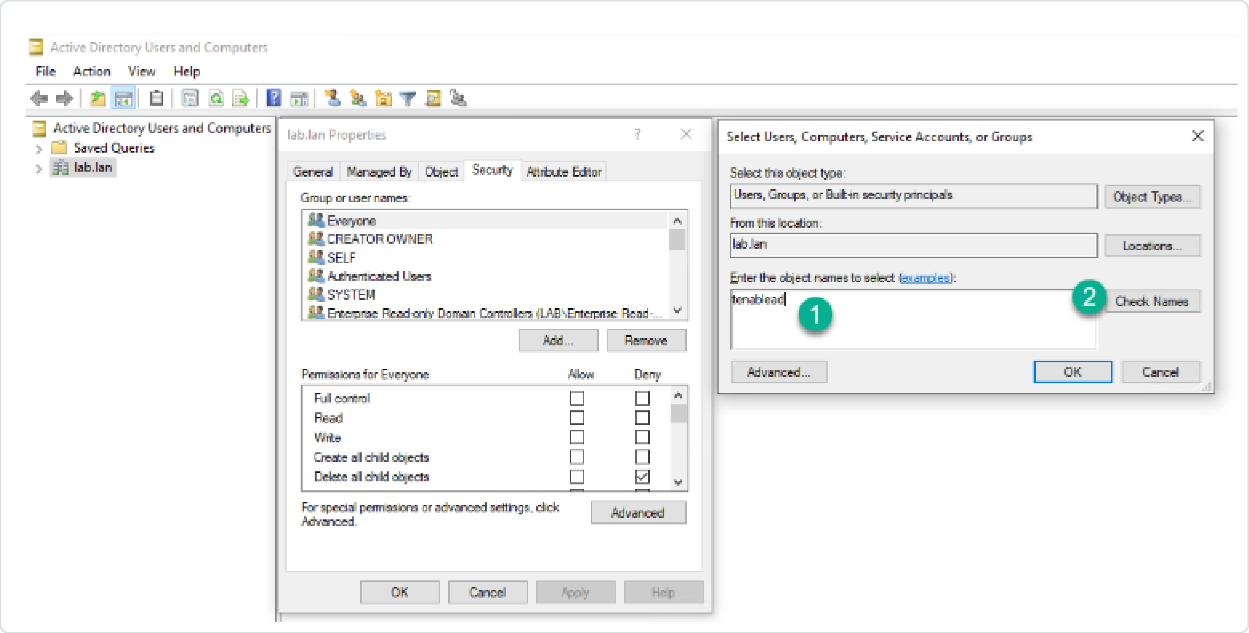
- Everyone
- CREATOR OWNER
- SELF
- Authenticated Users
- SYSTEM
- Enterprise Read-only Domain Controllers (LAB\Enterprise Read-...

Permissions for Everyone	Allow	Deny
Full control	☐	☐
Read	☐	☐
Write	☐	☐
Create all child objects	☐	☐
Delete all child objects	☐	☑

For special permissions or advanced settings, click Advanced.

5. Locate the Tenable Identity Exposure service account:

> **Note**: in a forest with multiple domains environment, the service account may be in a different Active Directory domain.



Group or user names:

- Everyone
- CREATOR OWNER
- SELF
- Authenticated Users
- SYSTEM
- Enterprise Read-only Domain Controllers (LAB\Enterprise Read-...

Permissions for Everyone	Allow	Deny
Full control	□	□
Read	□	□
Write	□	□
Create all child objects	□	□
Delete all child objects	□	☑

For special permissions or advanced settings, click Advanced.

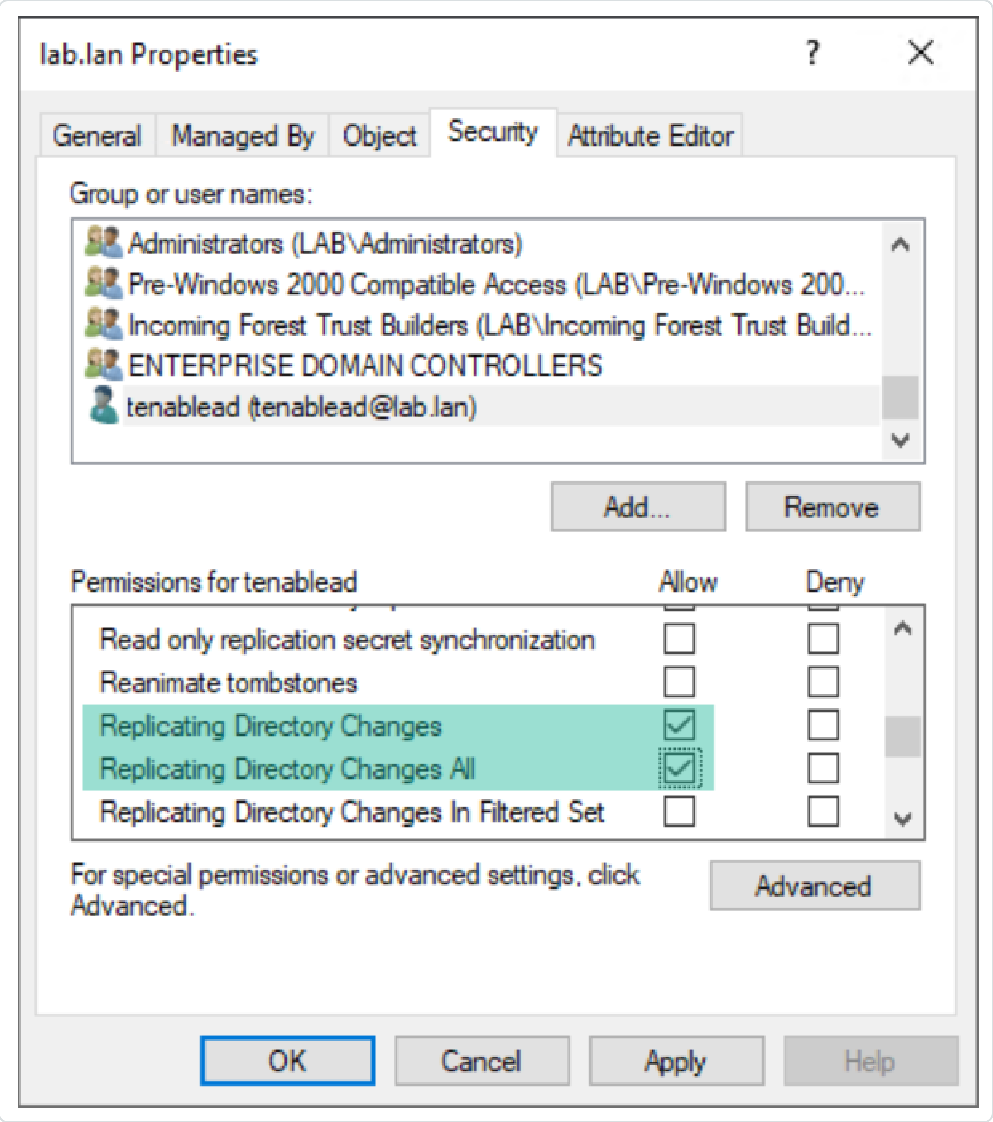
Select this object type:
Users, Groups, or Built-in security principals

From this location:
lab.lan

Enter the object names to select (examples):
tenablead

6. Scroll down the list and deselect all permissions set by default.

7. In the **Allow** column, select permissions for both *Replicating Directory Changes* and *Replicating Directory Changes All*.



Group or user names:

- Administrators (LAB\Administrators)
- Pre-Windows 2000 Compatible Access (LAB\Pre-Windows 200...
- Incoming Forest Trust Builders (LAB\Incoming Forest Trust Build...
- ENTERPRISE DOMAIN CONTROLLERS
- tenablead (tenablead@lab.lan)

Permissions for tenablead	Allow	Deny
Read only replication secret synchronization	☐	☐
Reanimate tombstones	☐	☐
Replicating Directory Changes	☑	☐
Replicating Directory Changes All	☑	☐
Replicating Directory Changes In Filtered Set	☐	☐

For special permissions or advanced settings, click Advanced.

8. Click **OK**.

Important Notes

> Tenable Identity Exposure only requires one service account per forest, so when you assign permissions in a domain you may need to **search for the service account from another domain**.

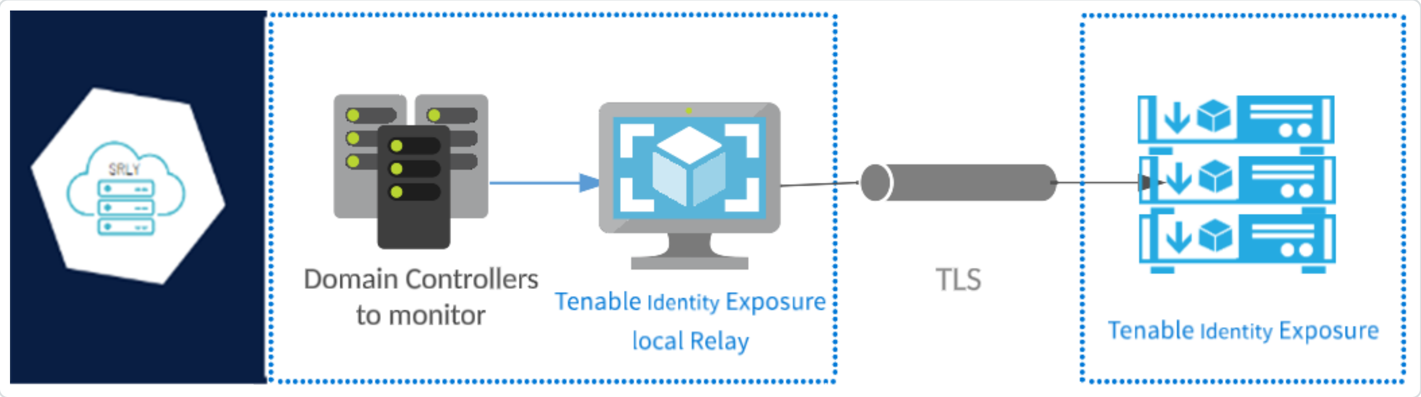
> You must assign additional permissions **at the domain root level**. The Active Directory does not support permissions assigned to an organizational unit or a specific user — for example to restrict Privileged Analysis to the OU or user — and therefore these do not have any effect.

These permissions grant the Tenable Identity Exposure service account much more power over the Active Directory domain. You must then consider it as **a privileged account (Tier 0)** and protect it as similarly as a domain administrator account. For the complete procedure, see Protecting Service Accounts.

Secure Relay

Secure Relay is a mode of transfer for your Active Directory data from your network to Tenable Identity Exposure using Transport Layer Security (TLS) instead of a VPN, as shown in this diagram. The Relay feature also supports HTTP proxy with or without authentication if your network requires a proxy server to reach the internet.

Tenable Identity Exposure can support multiple Secure Relays which you can map to domains according to your needs.

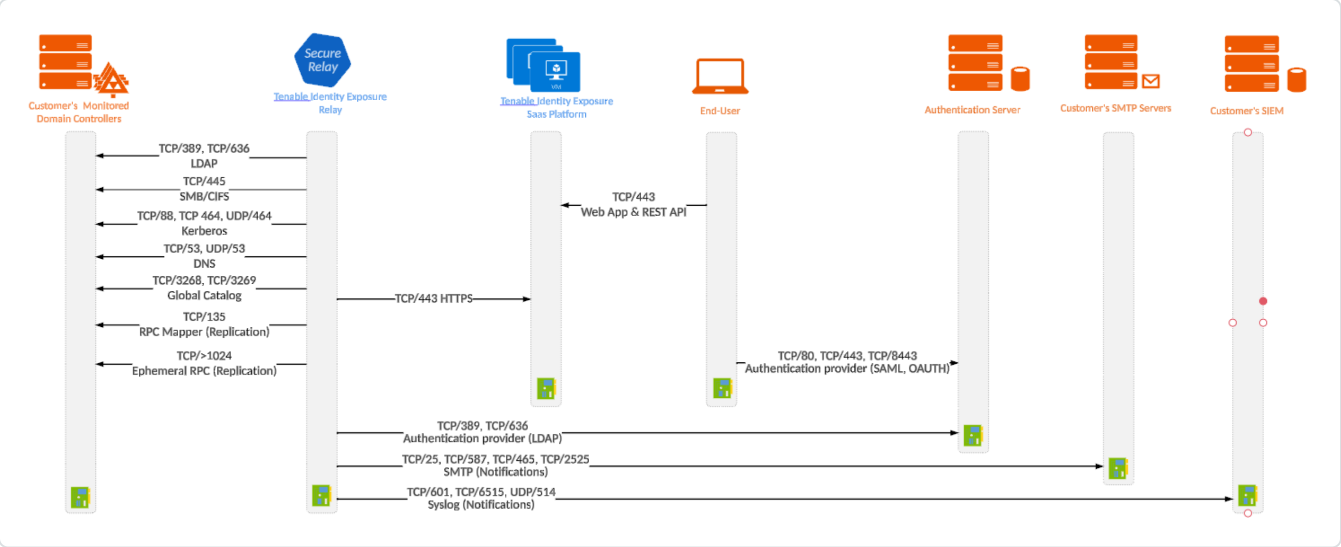

SRLY
Domain Controllers to monitor
Tenable Identity Exposure local Relay
TLS
Tenable Identity Exposure

Note: The Secure Relay feature currently only applies if Tenable Identity Exposure provisions your platform to use Secure Relay. It is not possible to switch the provisioning manually from VPN to Secure Relay. For assistance in the migration of your platform from VPN to Secure Relay, contact your Tenable Identity Exposure customer support representative.

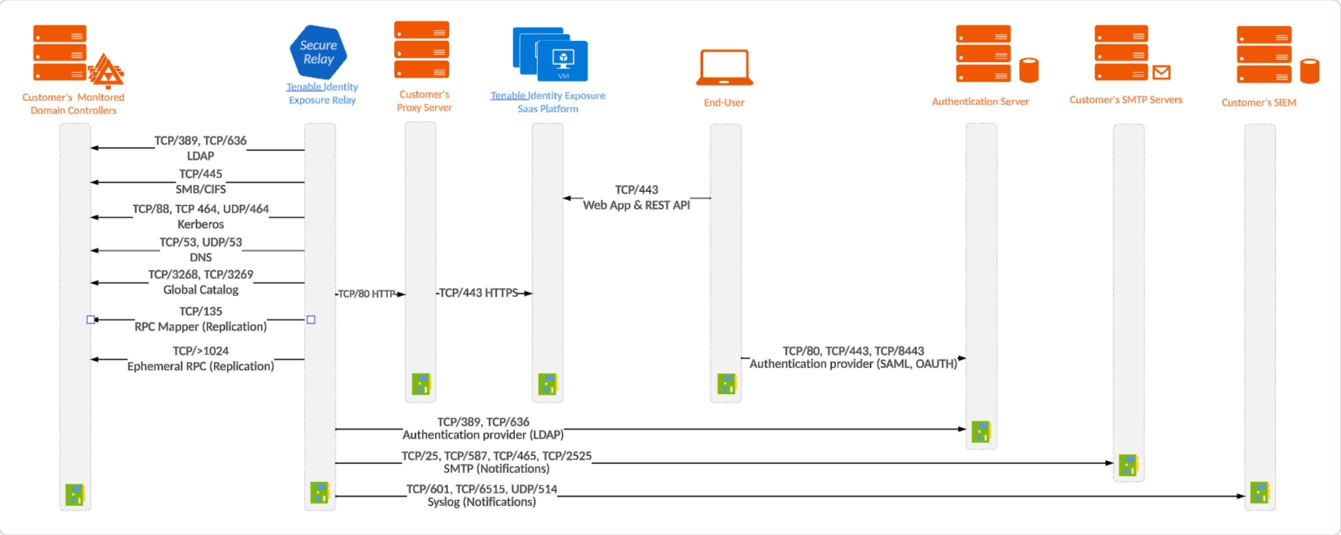
Network Flows

Required Ports for Secure Relay

- For a classic setup **without a proxy server**, the Relay requires the following ports:



- For a setup **using a proxy server**, the Relay requires the following ports:



TLS Requirements

To use TLS 1.2, your Relay server must support at least one of the following cipher suites as of 24 January 2024:

- `TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256`
- `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384`
- `TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256`

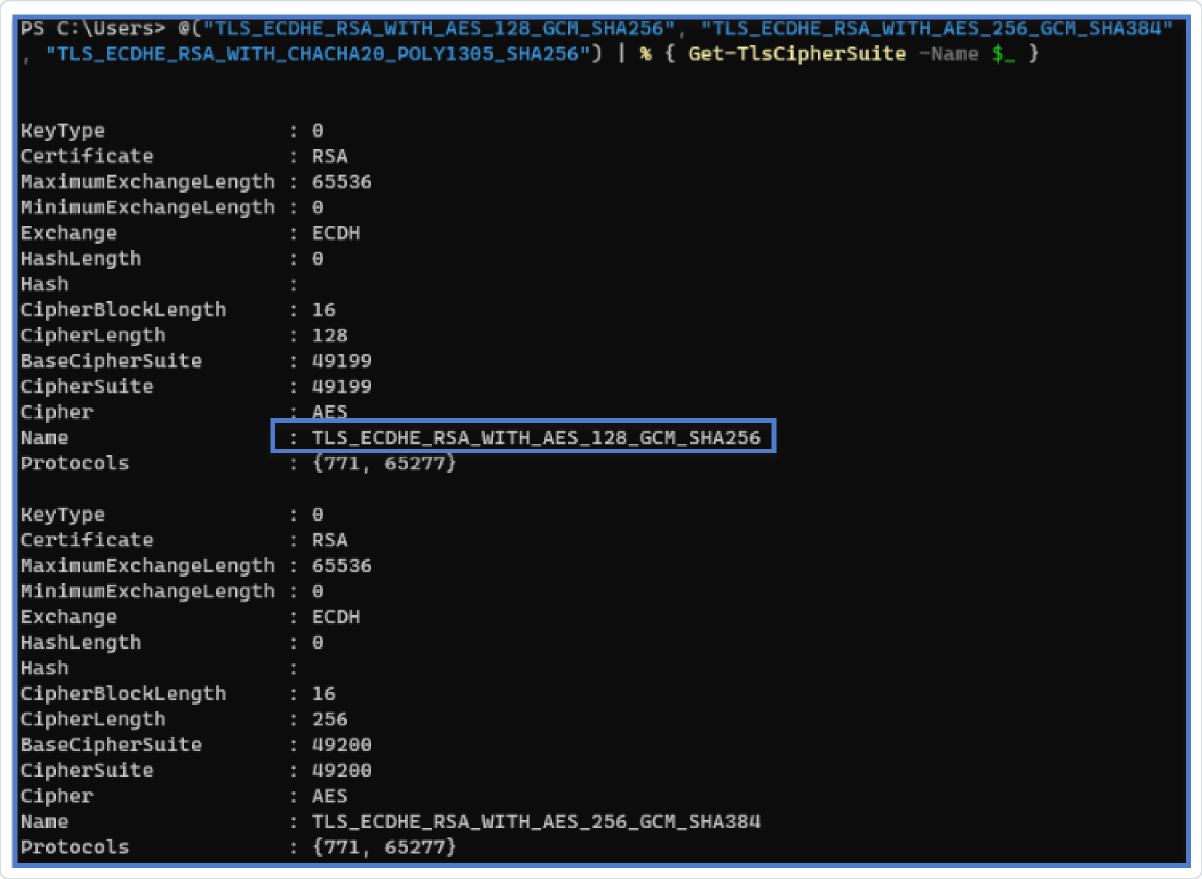
Also, ensure that your Windows configuration aligns with the specified cipher suites for compatibility with the Relay feature.

To check for cipher suites:

1. In PowerShell, run the following command:

```
@("TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256", "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384", "TLS_ECDHE_
RSA_WITH_CHACHA20_POLY1305_SHA256") | % { Get-TlsCipherSuite -Name $_ }
```

2. Check the output: `TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256`.



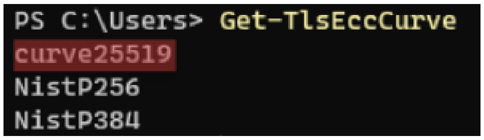
```
PS C:\Users> @("TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256", "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384"
, "TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256") | % { Get-TlsCipherSuite -Name $_ }


KeyType               : 0
Certificate           : RSA
MaximumExchangeLength : 65536
MinimumExchangeLength : 0
Exchange              : ECDH
HashLength            : 0
Hash                  :
CipherBlockLength     : 16
CipherLength          : 128
BaseCipherSuite       : 49199
CipherSuite           : 49199
Cipher                : AES
Name                  : TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
Protocols             : {771, 65277}

KeyType               : 0
Certificate           : RSA
MaximumExchangeLength : 65536
MinimumExchangeLength : 0
Exchange              : ECDH
HashLength            : 0
Hash                  :
CipherBlockLength     : 16
CipherLength          : 256
BaseCipherSuite       : 49200
CipherSuite           : 49200
Cipher                : AES
Name                  : TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
Protocols             : {771, 65277}
```

3. An empty output indicates that none of the required cipher suites is enabled for the Relay's TLS connection to work. Enable at least one cipher suite.

4. Verify the Elliptic Curve Cryptography (ECC) curve from the Relay server. This verification is mandatory for using Elliptic Curve Diffie-Hellman Ephemeral (ECDHE) cipher suites. In PowerShell, run the following command:

```
Get-TlsEccCurve
```

5. Check that you have curve **25519**. If not, enable it.

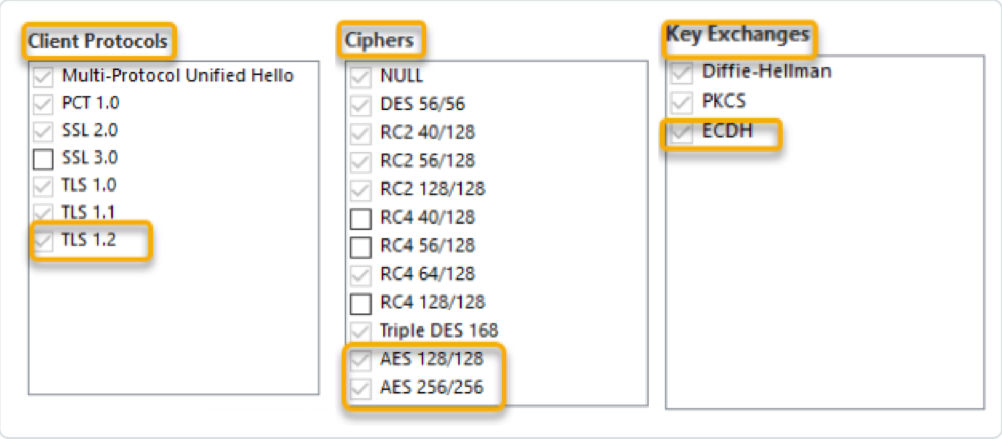


```
PS C:\Users> Get-TlsEccCurve
curve25519
NistP256
NistP384
```

To verify Windows cryptographic settings:

1. In an IIS Crypto tool, check that you have the following options enabled:

   - Client Protocols: **TLS 1.2**
   - Ciphers: **AES 128/128** and **AES 256/256**
   - Key Exchanges: **ECDH**



Client Protocols

☑ Multi-Protocol Unified Hello
☑ PCT 1.0
☑ SSL 2.0
□ SSL 3.0
☑ TLS 1.0
☑ TLS 1.1
☑ TLS 1.2

Ciphers

☑ NULL
☑ DES 56/56
☑ RC2 40/128
☑ RC2 56/128
☑ RC2 128/128
□ RC4 40/128
□ RC4 56/128
☑ RC4 64/128
□ RC4 128/128
☑ Triple DES 168
☑ AES 128/128
☑ AES 256/256

Key Exchanges

☑ Diffie-Hellman
☑ PKCS
☑ ECDH

2. After you modify the cryptographic settings, restart the machine.

> **Note**: Modifying Windows cryptographic settings affects all applications running on the machine and using the Windows TLS library, known as "Schannel." Therefore, ensure that any adjustment you make does not cause unintended side effects. Verify that the chosen configurations align with the organization's overall hardening objectives or compliance mandates.

Before you start

Prerequisites

Virtual machine

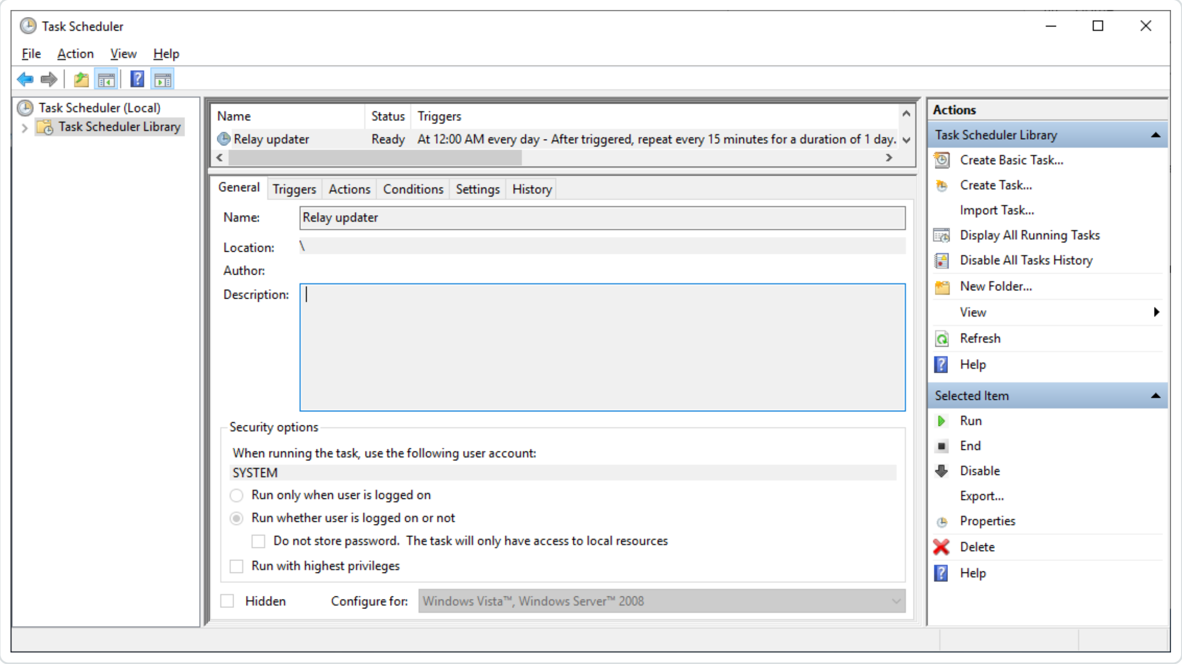
The requirements for the virtual machine (VM) hosting the Secure Relay are the following:

Customer Size	Tenable Identity Exposure Services	Instance Required	Memory (per instance)	vCPU (per instance)	Disk Topology	Available Disk Space (per instance)
Any size	• `tenable_Relay` • `tenable_envoy`	1	8 GB of RAM	2 vCPU	Partition for logs separate from the system partition	30 GB

The VM must also have:

- A Windows Server 2016+ operating system (no Linux)
- Resolved internet-facing DNS queries and internet access for at least `cloud.tenable.com` and `*.tenable.ad` (TLS 1.2).
- Local administrator privileges
- EDR, antivirus, and GPO configuration:
  - Sufficient CPU remaining on the VM — for example, the Windows Defender Real-Time feature consumes a considerable amount of CPU and can saturate the machine.
  - Automatic updates:
    - Allow calls toward `*.tenable.ad` so that the automatic update feature can download a Relay executable file.

- Check that there is no Group Policy Object (GPO) blocking the automatic update feature.
- Do not delete or alter the 'Relay updater' scheduled task:



Name	Status	Triggers
Relay updater	Ready	At 12:00 AM every day - After triggered, repeat every 15 minutes for a duration of 1 day.

Name: Relay updater

Location: \

Author:

Description:

Security options

When running the task, use the following user account:

SYSTEM

○ Run only when user is logged on

● Run whether user is logged on or not

□ Do not store password. The task will only have access to local resources

□ Run with highest privileges

□ Hidden Configure for: Windows Vista™, Windows Server™ 2008

Role Permissions

You must be a user with role-based permissions to configure the Relay. The required permissions are the following:

- **Data entities**: Entity Relay
- **Interface entities**:
  - Management > System > Configuration > Application Services > Relay
  - Management > System > Relay management

For more information, see Set Permissions for a Role.

Allowed Files and Processes

For the Relay to operate smoothly, allow certain files and processes for third-party security tools such as antivirus and/or EDR (Endpoint Detection and Response) and XDR (Extended Detection and Response).

Allow the following files and processes:

Note: Adapt the C:\ path to your Relay installation drive.

Windows
Files
C:\Tenable\*
C:\tools\*
C:\ProgramData\Tenable\*
Processes
nssm.exe --> Path: C:\tools\nssm.exe
Tenable.Relay.exe --> Path: C:\Tenable\Tenable.ad\SecureRelay\Tenable.Relay.exe
envoy.exe --> Path: C:\Tenable\Tenable.ad\SecureRelay\envoy.exe
updater.exe --> Path: C:\Tenable\Tenable.ad\updater.exe
powershell.exe --> Path: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe (may be different depending on the OS version)
Scheduled Tasks
C:\Windows\System32\Tasks\Relay updater
C:\Windows\System32\Tasks\Manual Renew Apikey
C:\Windows\System32\Tasks\Tenable\Tenable.ad\SecureRelay\CompressLogsSecureRelay
C:\Windows\System32\Tasks\Tenable\Tenable.ad\SecureRelay\RemoveLogsSecureRelay

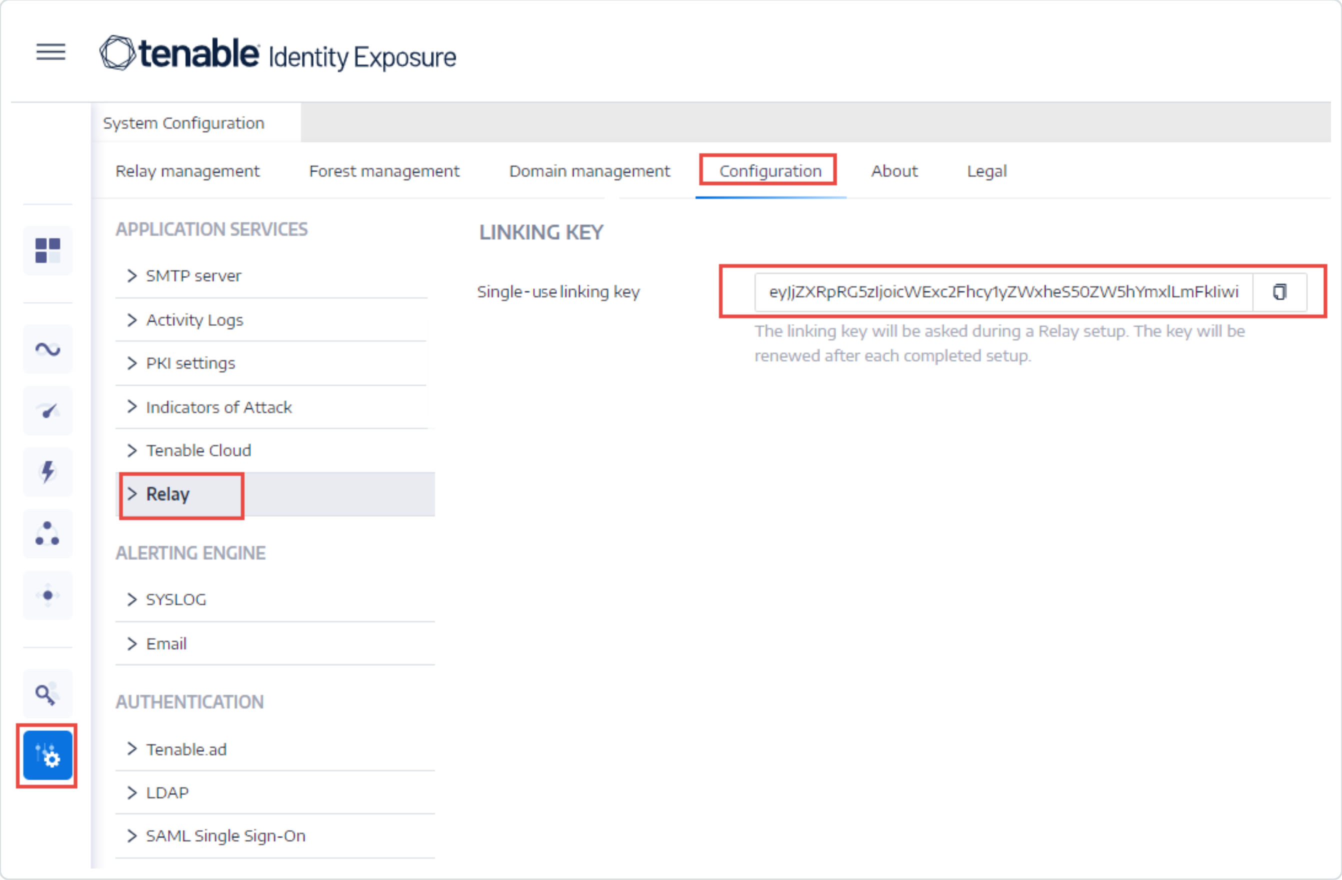
Registry Key
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Tenable\Tenable.ad Secure Relay

Linking key

The Secure Relay installation requires a single-use linking key that contains the address of your network and an authentication token. Tenable Identity Exposure regenerates a new key after each successful Secure Relay installation.

To retrieve the linking key:

1. In Tenable Identity Exposure, click **System** on the left menu bar and select the **Configuration** tab > **Relay**.



Single-use linking key: eyJjZXRpRG5zIjoicWExc2Fhcy1yZWxheS50ZW5hYmxlLmFkIiwi

The linking key will be asked during a Relay setup. The key will be renewed after each completed setup.

2. Click ⧉ to copy the linking key.

Installation

To install the Secure Relay:

- Choose an installation method:
  - Install the Secure Relay (GUI)
  - Install the Secure Relay (Tenable Nessus Agent)

Uninstallation

To uninstall a Secure Relay:

1. In Windows, go to **Settings** > **Apps & Features** > **Tenable Identity Exposure Secure Relay**.
2. Click **Uninstall**.

   When the uninstallation completes, Tenable Identity Exposure Secure Relay services and environment variables no longer appear in your system.

3. In Tenable Identity Exposure, click **Systems** on the left menu bar and select the **Relay Management** tab.
4. Select the relay you just uninstalled and click 🗑 to remove it from the list of available relays.

Automatic Updates

After you install Secure Relay, Tenable Identity Exposure checks regularly for new versions. This process is fully automated and requires HTTPS access to your domain (TCP/443). An icon in the network tray indicates when Tenable Identity Exposure is updating Secure Relay. Once the process completes, Tenable Identity Exposure services restart and data collection resumes.

See also

For complete information about Secure Relay, see Secure Relay in the Tenable Identity Exposure Administrator Guide.

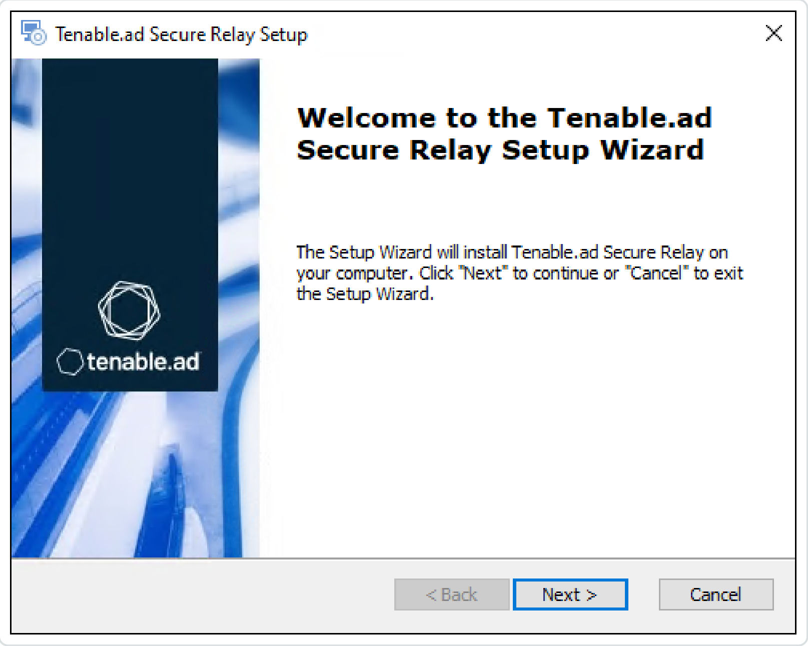
Install the Secure Relay (GUI)

The following procedure installs the Secure Relay using a Windows installer. Before you begin, check that you have the necessary prerequisites and **required linking key** as described in Secure Relay

To install the Secure Relay:

1. Download the installer from the Tenable Identity Exposure Downloads Portal to your virtual machine.
2. Double-click on the file `tenable.ad_SecureRelay_v3.xx.x` to start the installation wizard.

   The **Welcome** screen appears.

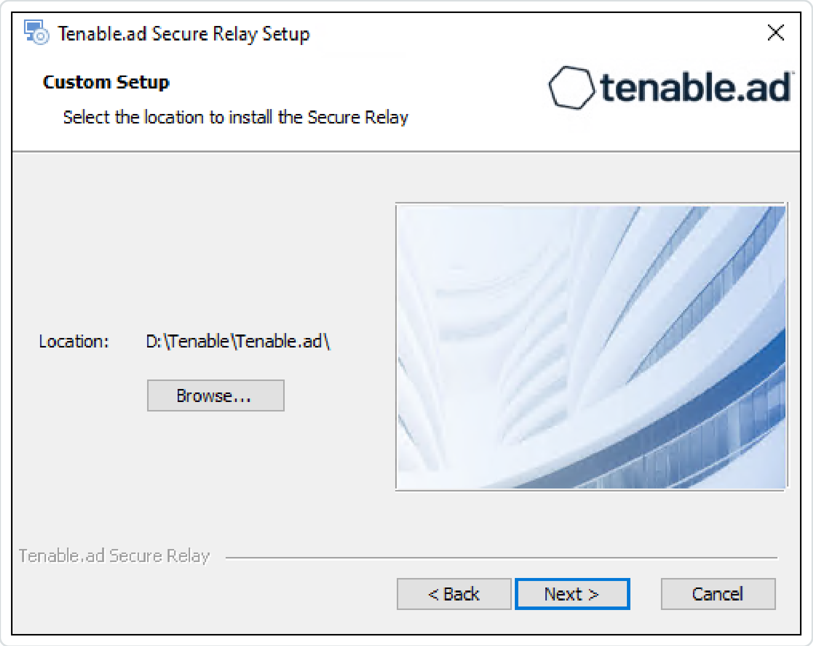
   Tenable.ad Secure Relay Setup

   Welcome to the Tenable.ad Secure Relay Setup Wizard

   The Setup Wizard will install Tenable.ad Secure Relay on your computer. Click "Next" to continue or "Cancel" to exit the Setup Wizard.

3. Click **Next**.

   The **Custom Setup** window appears.



Tenable.ad Secure Relay Setup

Custom Setup

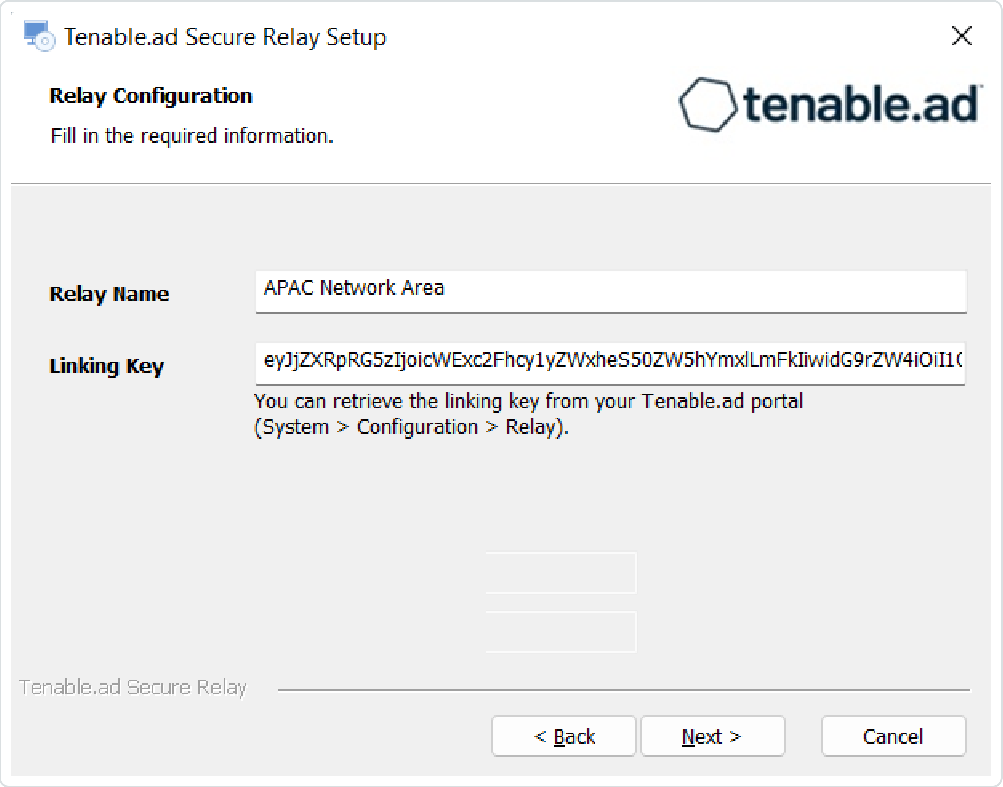
Select the location to install the Secure Relay

Location: D:\Tenable\Tenable.ad\

4. Click **Browse** to select the disk partition you reserved for Secure Relay (separate from the system partition).

5. Click **Next**.

   The **Relay Configuration** window appears.



Tenable.ad Secure Relay Setup

Relay Configuration

Fill in the required information.

Relay Name: APAC Network Area

Linking Key: eyJjZXRpRG5zIjoicWExc2Fhcy1yZWxheS50ZW5hYmxlLmFkIiwidG9rZW4iOiI1(

You can retrieve the linking key from your Tenable.ad portal (System > Configuration > Relay).

6. Provide the following information:

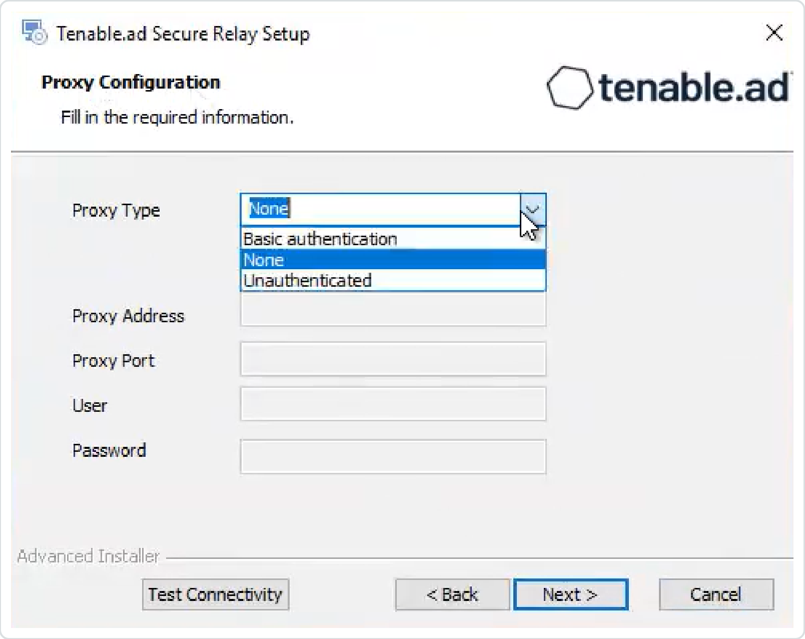
   a. In the **Relay Name** box, type a name for your Secure Relay.

   b. In the **Linking key** box, paste the linking key that you retrieved from the Tenable Identity Exposure portal.

   c. If you choose to use a proxy server, select the option **Use an HTTP Proxy for your Relay calls** and provide the proxy address and port number.

7. Click **Next**.

   The Proxy Configuration window appears:



Tenable.ad Secure Relay Setup

Proxy Configuration

Fill in the required information.

Proxy Type: None

8. Select one of the following options:

   a. **None**: Do not use a proxy server.

   b. **Unauthenticated**: Type the address and port for the proxy server.

   c. **Basic authentication**: In addition to the address and port, type the user and password for the proxy server.

> **Caution**: To configure a proxy using "Unauthenticated" or "Basic authentication", the relay only supports IPv4 addresses (such as `192.168.0.1`) or a proxy URI without `http://` or `https://` (such as `myproxy.mycompany.com`.) The relay does not support IPv6 addresses (such as `2001:0db8:85a3:0000:0000:8a2e:0370:7334`.)

9. Click **Test Connectivity**. The following can occur:

   - **Green light** — The connection succeeded.
   - **Invalid linking key** — Retrieve the linking key from the Tenable Identity Exposure portal.
   - **Invalid Relay Name** — This box cannot remain empty. Provide a name for the relay.
   - **Connection failed** — Check your internet access.

10. Click **Next**.

    The **Ready to Install** window appears.

11. Click **Install**.

12. After the installation completes, click **Finish**.

What to do next

- Post-installation Checks

See also

- Secure Relay
- Install the Secure Relay (Tenable Nessus Agent)
- Post-installation Checks
- Configure the Relay

Install the Secure Relay (Tenable Nessus Agent)

The following procedure installs the Secure Relay using Tenable Nessus Agent.

Before you start

- Check that you have downloaded and installed Tenable Nessus Agent.

  > **Note**: The Tenable Nessus Agent installation program asks for an Agent Key. This key is **not required** for the Secure Relay feature.

- Meet the necessary prerequisites and have the **required linking key** as described in Secure Relay.

To install the Secure Relay:

1. On a machine hosting Tenable Nessus Agent and acting as a Relay, open an administrator command prompt window in the Tenable Nessus Agent directory (`c:\Program Files\Tenable\Nessus Agent`) and type the following command:

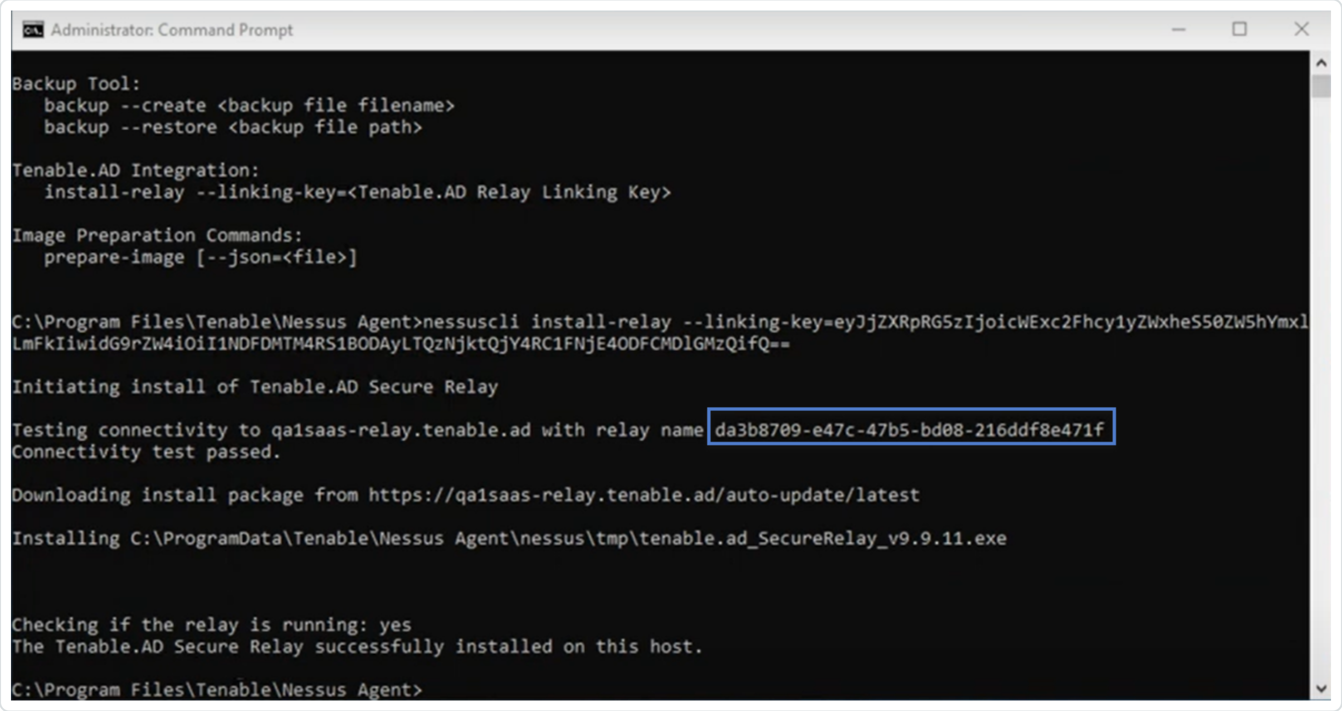
   Secure Relay Installation

   ```
   nessuscli install-relay --linking-key=<Relay Linking Key> --proxy-host=<Customer Proxy IP or
   DNS> --proxy-port=<Customer Proxy Port>
   ```

2. Replace <Tenable Identity Exposure Relay Linking Key> with the value you copied previously from your Tenable Identity Exposure instance, and provide a proxy address and port number if you use a proxy server.

   The installation begins. It requires a few minutes to run connectivity checks and the installation process.

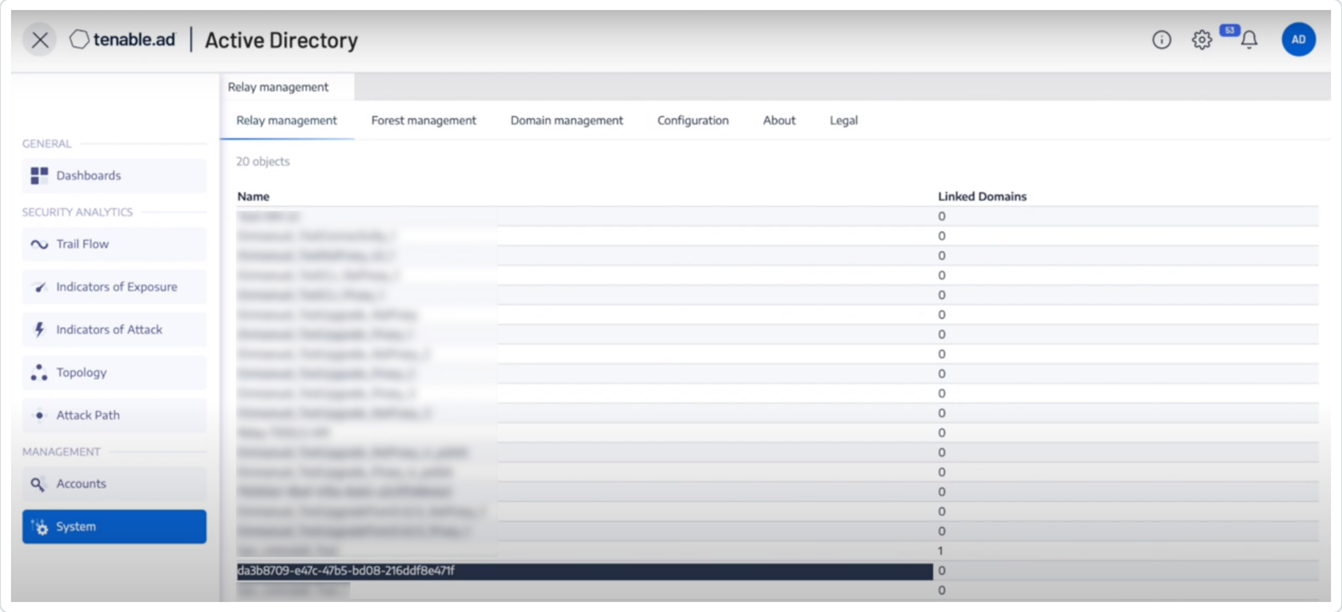
   When the installation completes successfully, it shows a message that the Relay is running on the host machine.



Administrator: Command Prompt

```
Backup Tool:
   backup --create <backup file filename>
   backup --restore <backup file path>

Tenable.AD Integration:
   install-relay --linking-key=<Tenable.AD Relay Linking Key>

Image Preparation Commands:
   prepare-image [--json=<file>]


C:\Program Files\Tenable\Nessus Agent>nessuscli install-relay --linking-key=eyJjZXRpRG5zIjoicWExc2Fhcy1yZWxheS50ZW5hYmxl
LmFkIiwidG9rZW4iOiI1NDFDMTM4RS1BODAyLTQzNjktQjY4RC1FNjE4ODFCMDlGMzQifQ==

Initiating install of Tenable.AD Secure Relay

Testing connectivity to qa1saas-relay.tenable.ad with relay name da3b8709-e47c-47b5-bd08-216ddf8e471f
Connectivity test passed.

Downloading install package from https://qa1saas-relay.tenable.ad/auto-update/latest

Installing C:\ProgramData\Tenable\Nessus Agent\nessus\tmp\tenable.ad_SecureRelay_v9.9.11.exe


Checking if the relay is running: yes
The Tenable.AD Secure Relay successfully installed on this host.

C:\Program Files\Tenable\Nessus Agent>
```

3. In Tenable Identity Exposure, click **System** > **Relay Management**. The newly installed Relay appears in the list of Relays with the identifier shown in the installation window.



20 objects

Name	Linked Domains
[redacted]	0
[redacted]	0
[redacted]	0
[redacted]	0
[redacted]	0
[redacted]	0
[redacted]	0
[redacted]	0
[redacted]	0
[redacted]	0
[redacted]	0
[redacted]	0
[redacted]	0
[redacted]	0
[redacted]	0
[redacted]	0
[redacted]	0
[redacted]	1
da3b8709-e47c-47b5-bd08-216ddf8e471f	0
[redacted]	0

What to do next

- Post-installation Checks

See also

- Secure Relay
- Install the Secure Relay (GUI)
- Post-installation Checks
- Configure the Relay

Post-installation Checks

After the Secure Relay installation completes, check for the following:

List of installed Relays in Tenable Identity Exposure

To see the list of installed relays:

- In Tenable Identity Exposure, click **Systems** on the left menu bar and select the **Relay Management** tab.

  The pane shows a list of secure relays and their linked domains.

Services

After a successful installation, the following services are running:

- `Tenable_Relay`
- `tenable_envoy`

> **Note**: You can locate the Envoy license in Tenable Identity Exposure at **Systems** > **Legal** > **Envoy license**.

Environment variables

The installation also added 4 new environment variables related to Secure Relay with names beginning with "ALSID." If you selected to use a proxy server, there are 2 additional variables related to the proxy IP and port.

Logs for Troubleshooting

You can find logs in the following locations:

- **Installation logs**: `C:\Users\<your user>\AppData\Local\Temp`
- **Relay logs**: On the VM hosting Secure Relay in the folder specified at the time of installation.

What to do next

- Configure the Relay

See also

- Secure Relay
- Install the Secure Relay (GUI)
- Install the Secure Relay (Tenable Nessus Agent)

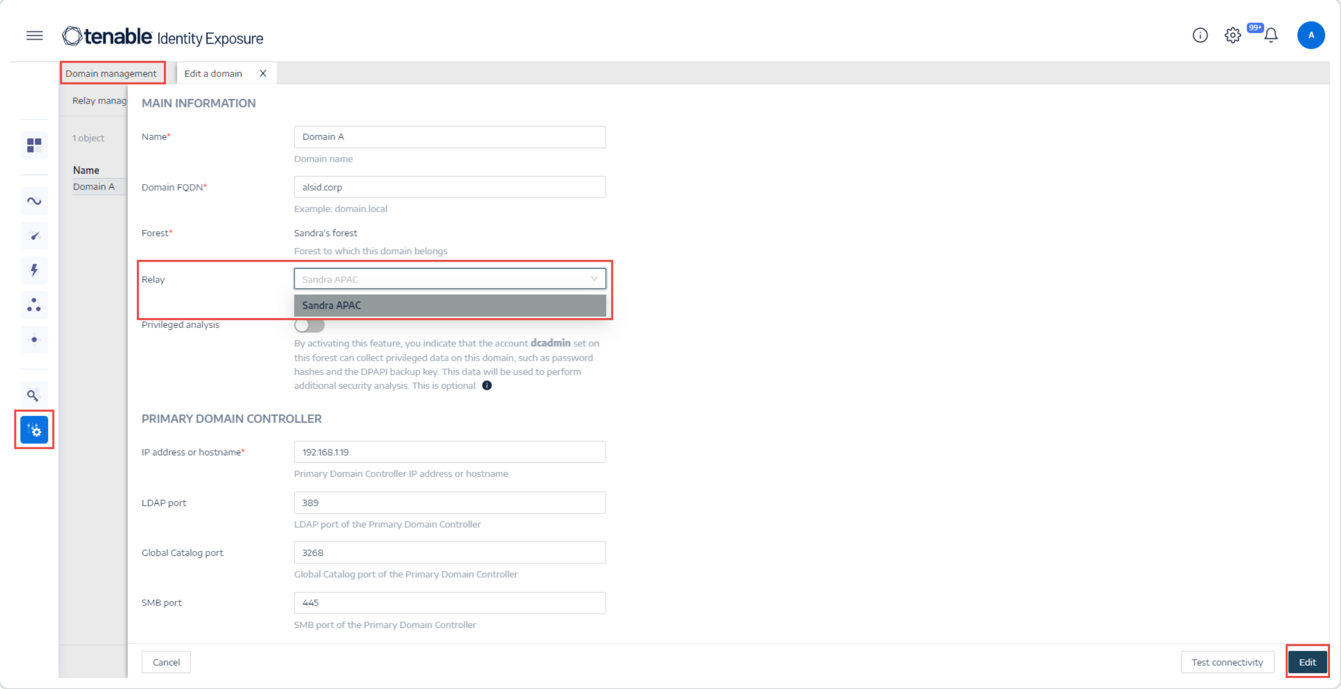
Configure the Relay

After installation and post-installation checks, you configure your Relay in Tenable Identity Exposure to link it to a domain and to set up alerts.

To link a domain to a Secure Relay:

1. In Tenable Identity Exposure, click **Systems** on the left menu bar and select the **Domain Management** tab.
2. In the list of domains, select a domain to link and click on ✎ at the end of the line.

   The **Edit a domain** pane opens.
3. In the **Relay** box, click the arrow to show a drop-down list of installed relays and select a relay to link to the domain.

   MAIN INFORMATION

   Name* Domain A
   Domain name

   Domain FQDN* alsid.corp
   Example: domain.local

   Forest* Sandra's forest
   Forest to which this domain belongs

   Relay Sandra APAC
   Sandra APAC

   Privileged analysis
   By activating this feature, you indicate that the account **dcadmin** set on this forest can collect privileged data on this domain, such as password hashes and the DPAPI backup key. This data will be used to perform additional security analysis. This is optional.

   PRIMARY DOMAIN CONTROLLER

   IP address or hostname* 192.168.1.19
   Primary Domain Controller IP address or hostname

   LDAP port 389
   LDAP port of the Primary Domain Controller

   Global Catalog port 3268
   Global Catalog port of the Primary Domain Controller

   SMB port 445
   SMB port of the Primary Domain Controller
4. Click **Edit**.

   A message confirms that Tenable Identity Exposure updated the domain. Sysvol and LDAP synchronize to include the modification. The Trail Flow begins to receive new events.

See also

- Secure Relay
- Install the Secure Relay (GUI)
- Install the Secure Relay (Tenable Nessus Agent)
- Post-installation Checks

Indicators of Attack Deployment

Note: This information only applies to licenses benefiting from the Indicator of Attack module.

Tenable Identity Exposure 's **Indicators of Attack** (IoA) give you the ability to detect attacks on your Active Directory (AD). Each IoA requires specific audit policies that the installation script automatically enables. For a complete list of Tenable Identity Exposure IoAs and their implementation, see the Tenable Identity Exposure Indicators of Attack Reference Guide in the Tenable downloads portal.

Indicators of Attack and the Active Directory

Tenable Identity Exposure works as a non-intrusive solution that monitors an Active Directory infrastructure without deploying agents and with minimal configuration change in your environment.

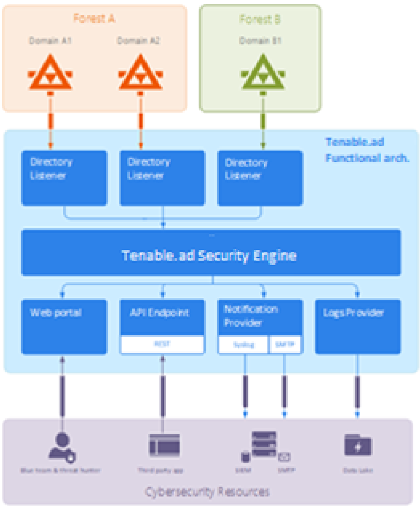
Tenable Identity Exposure uses a regular user account with no administrative permissions to connect to standard APIs for its security monitoring feature.

Tenable Identity Exposure uses the Active Directory replication mechanisms to retrieve the relevant information, which incurs only limited bandwidth costs between each domain's PDC and Tenable Identity Exposure's Directory Listener.

To detect efficiently security incidents using indicators of attack, Tenable Identity Exposure uses the Event Tracing for Windows (ETW) information and the replication mechanisms available on each Domain Controller. To collect this set of information, you deploy a dedicated Group Policy Object (GPO) using a script from Tenable Identity Exposure as described in Install Indicators of Attack.

This GPO activates an event logs listener using Windows EvtSubscribe APIs on all domain controllers which writes to the system volume (SYSVOL) to benefit from the AD replication engine and Tenable Identity Exposure's ability to listen to SYSVOL events. The GPO creates a file in SYSVOL for each domain controller and flushes its contents periodically.

To initiate security monitoring, Tenable Identity Exposure must contact standard directory APIs from Microsoft.



Domain Controller

Tenable Identity Exposure only requires communication with the Primary Domain Controller emulator (PDCe) using the network protocols described in the Network Flow Matrix.

In the case of multiple monitored domains or forests, Tenable Identity Exposure must reach each domain's PDCe. For best performance, Tenable recommends that you host Tenable Identity Exposure on a physical network close to the PDCe to monitor.

User Account

Tenable Identity Exposure authenticates to the monitored infrastructure using a non-administrator user account to access the replication flow.

A simple Tenable Identity Exposure user can access all collected data. Tenable Identity Exposure does not access secret attributes such as credentials, password hashes, or Kerberos keys.

Tenable recommends that you create a service account that is a member of the group “Domain Users” as follows:

- The service account is on the main monitored domain.
- The service account is in any Organizational Unit (OU), preferably where you create other security service accounts.
- The service account has standard user group membership (such as member of the Domain Users AD default group).

Before you begin

- Review the limitations and potential impacts of installing IoAs, as described in Technical Changes and Potential Impact.
- Check that the DC has the PowerShell modules for Active Directory and GroupPolicy installed and available.
- Check that the DC has the Distributed File System Tools feature RSAT-DFS-Mgmt-Con enabled so that the deployment script can check for replication status because it cannot create a GPO while the DC is replicating.
- Tenable Identity Exposure recommends that you install/upgrade IoAs during off-peak hours to limit disruptions to your platform.
- Check permissions — To install IoAs, you must have a user role with the following permissions:
  - In **Data Entities**, "Read" access for:
    - All Indicators of Attack
    - All domains
  - In **Interface Entities**, access for:
    - Management > System > Configuration
    - Management > System > Configuration > Application Services > Indicators of Attack
    - Management > System > Configuration > Application Services > Indicators of Attack > Download installation file

  For more information about role-based permissions, see Set Permissions for a Role.

See also

- Install Indicators of Attack
- Indicators of Attack Installation Script
- Technical Changes and Potential Impact

- Install Microsoft Sysmon, a Windows system tool that some of Tenable Identity Exposure’s indicators of attack require to get relevant system data.

- Troubleshoot Indicators of Attack

Install Indicators of Attack

Required User Role: Organizational user with permission to modify the Indicators of Attack configuration in Tenable Identity Exposure. For more information, see Set Permissions for a Role.

Tenable Identity Exposure's Indicators of Attack (IoA) module requires you to run a PowerShell installation script with an administrative account that can create and link a new Group Policy Object (GPO) to an organizational unit (OU). You can run this script from any machine joined to your Active Directory domain that Tenable Identity Exposure monitors and that can reach domain controllers via the network.

You only have to execute this installation script once for each AD domain, since the GPO created automatically deploys the event listener to all existing and new domain controllers (DCs).

Moreover, enabling the "Automatic Updates" option avoids having to re-execute the installation script, even if you change the IoA configuration.

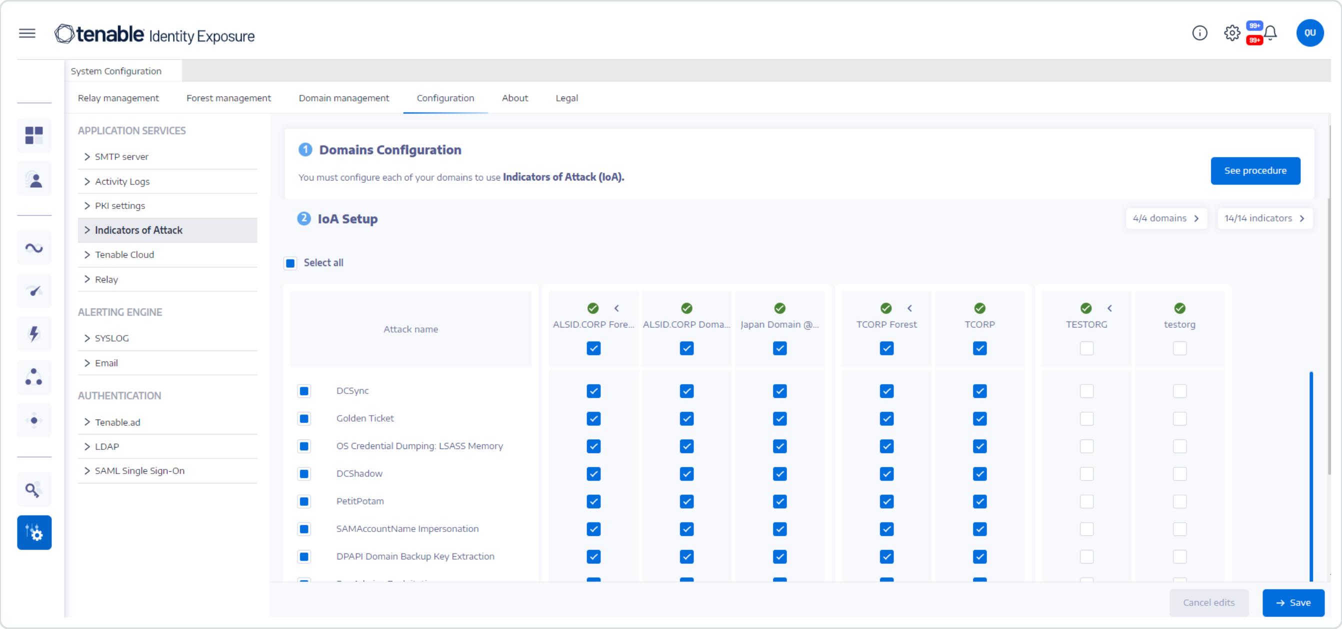
To configure domains for IoAs:

1. In Tenable Identity Exposure, click **System** on the left menu bar and the **Configuration** tab.

   The **Configuration** pane appears.

2. Click **Indicators of Attack**.

   The IoA configuration pane appears.



1 Domains Configuration

You must configure each of your domains to use **Indicators of Attack (IoA).**

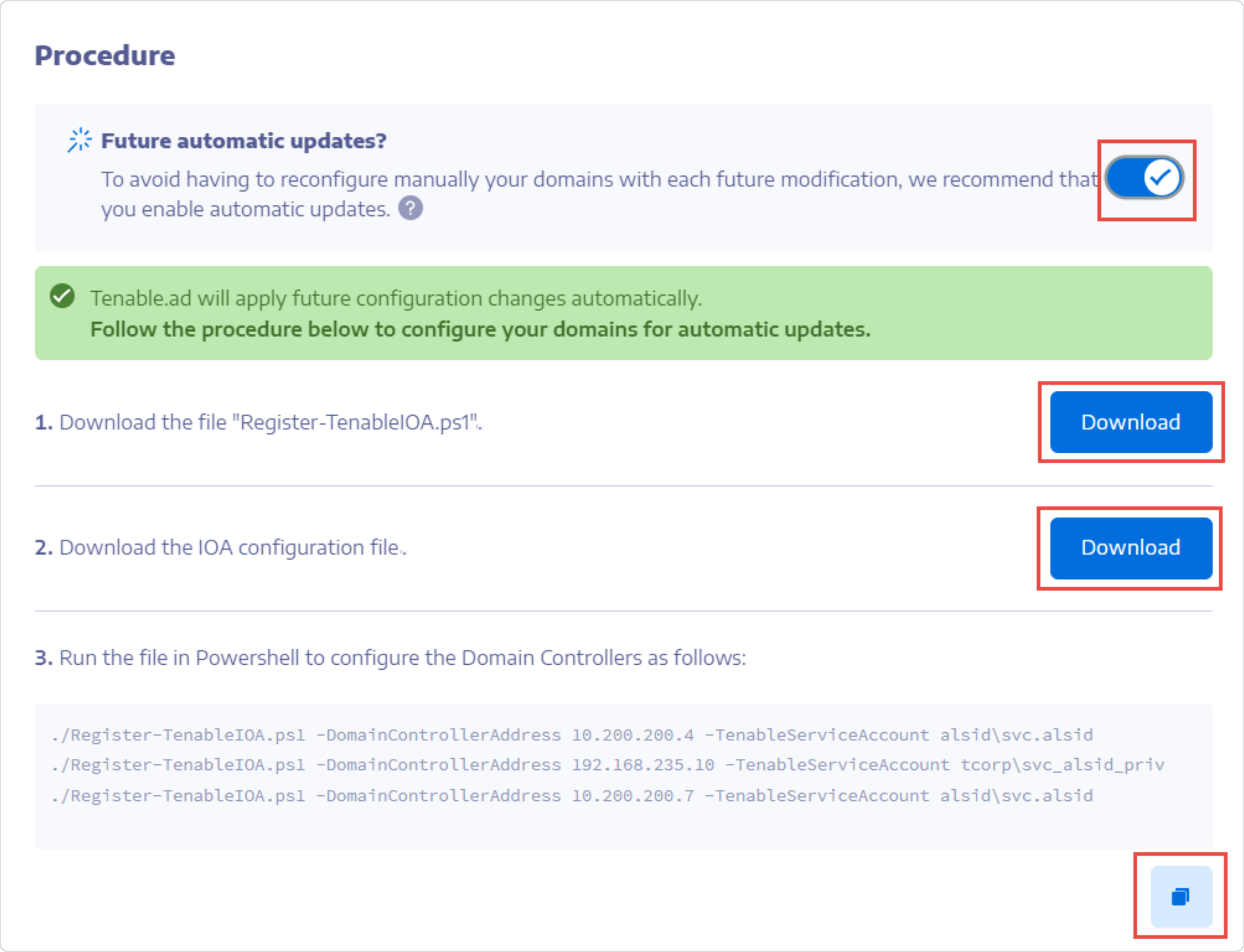
2 IoA Setup

■ Select all

	Attack name	ALSID.CORP Fore...	ALSID.CORP Doma...	Japan Domain @...	TCORP Forest	TCORP	TESTORG	testorg
		☑	☑	☑	☑	☑	□	□
■	DCSync	☑	☑	☑	☑	☑	□	□
■	Golden Ticket	☑	☑	☑	☑	☑	□	□
■	OS Credential Dumping: LSASS Memory	☑	☑	☑	☑	☑	□	□
■	DCShadow	☑	☑	☑	☑	☑	□	□
■	PetitPotam	☑	☑	☑	☑	☑	□	□
■	SAMAccountName Impersonation	☑	☑	☑	☑	☑	□	□
■	DPAPI Domain Backup Key Extraction	☑	☑	☑	☑	☑	□	□

3. In **(1) Domains Configuration**, click **See Procedure**.

   A procedure window opens.



Procedure

Future automatic updates?

To avoid having to reconfigure manually your domains with each future modification, we recommend that you enable automatic updates. ?

Tenable.ad will apply future configuration changes automatically.
Follow the procedure below to configure your domains for automatic updates.

1. Download the file "Register-TenableIOA.ps1".

2. Download the IOA configuration file.

3. Run the file in Powershell to configure the Domain Controllers as follows:

```
./Register-TenableIOA.ps1 -DomainControllerAddress 10.200.200.4 -TenableServiceAccount alsid\svc.alsid
./Register-TenableIOA.ps1 -DomainControllerAddress 192.168.235.10 -TenableServiceAccount tcorp\svc_alsid_priv
./Register-TenableIOA.ps1 -DomainControllerAddress 10.200.200.7 -TenableServiceAccount alsid\svc.alsid
```

4. Under **Future automatic updates?**:

    - The default option **Enable** allows Tenable Identity Exposure to update automatically your IoA configuration whenever you modify it in Tenable Identity Exposure in the future. This also ensures continuous security analysis.

    - If you turn off this option, a message asks you to turn it on to get automatic future updates. Click **See procedure** and toggle to **Enable**.

5. Click **Download** to download the script to run for each domain (`Register-TenableIOA.ps1`).

6. Click **Download** to download the configuration file for the domains (`TadIoaConfig-AllDomains.json`).

7. Click ❐ to copy the Powershell command to configure your domains.

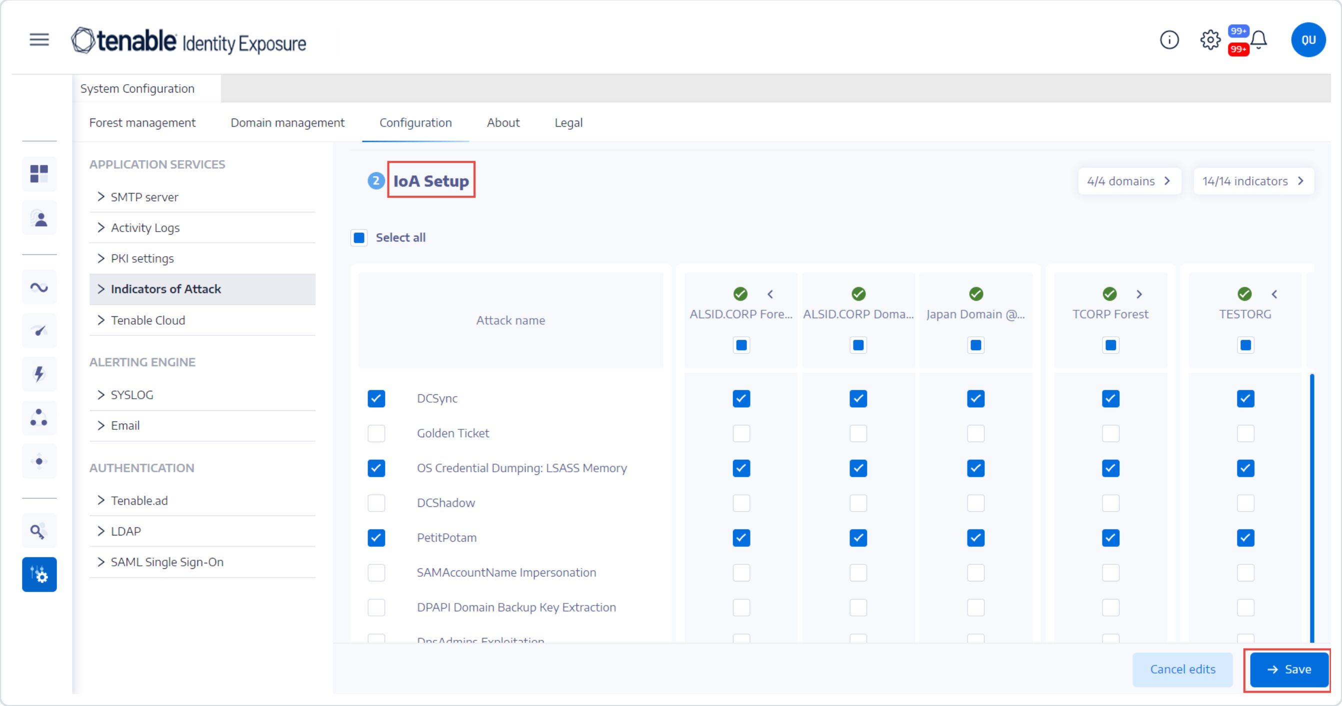
8. Click outside the procedure window to close it.

9. Open a PowerShell terminal with administrative rights and run the commands to configure your domain controllers for IoAs.

> **Note**: The service account you use to install IoAs and to query the domains must have write permissions in Tenable Identity Exposure (formerly known as Tenable.ad) GPO folder. The installation script adds this permission automatically. If you remove this permission, Tenable Identity Exposure shows an error message and automatic updates no longer work. For more information, see Indicators of Attack Installation Script.

To set up your IoAs:

1. In the IoA configuration pane, under **IoA Setup,** select the IoAs you want in your configuration.



Attack name	ALSID.CORP Fore...	ALSID.CORP Doma...	Japan Domain @...	TCORP Forest	TESTORG
☑ DCSync	☑	☑	☑	☑	☑
□ Golden Ticket	□	□	□	□	□
☑ OS Credential Dumping: LSASS Memory	☑	☑	☑	☑	☑
□ DCShadow	□	□	□	□	□
☑ PetitPotam	☑	☑	☑	☑	☑
□ SAMAccountName Impersonation	□	□	□	□	□
□ DPAPI Domain Backup Key Extraction	□	□	□	□	□
□ DnsAdmins Exploitation	□	□	□	□	□

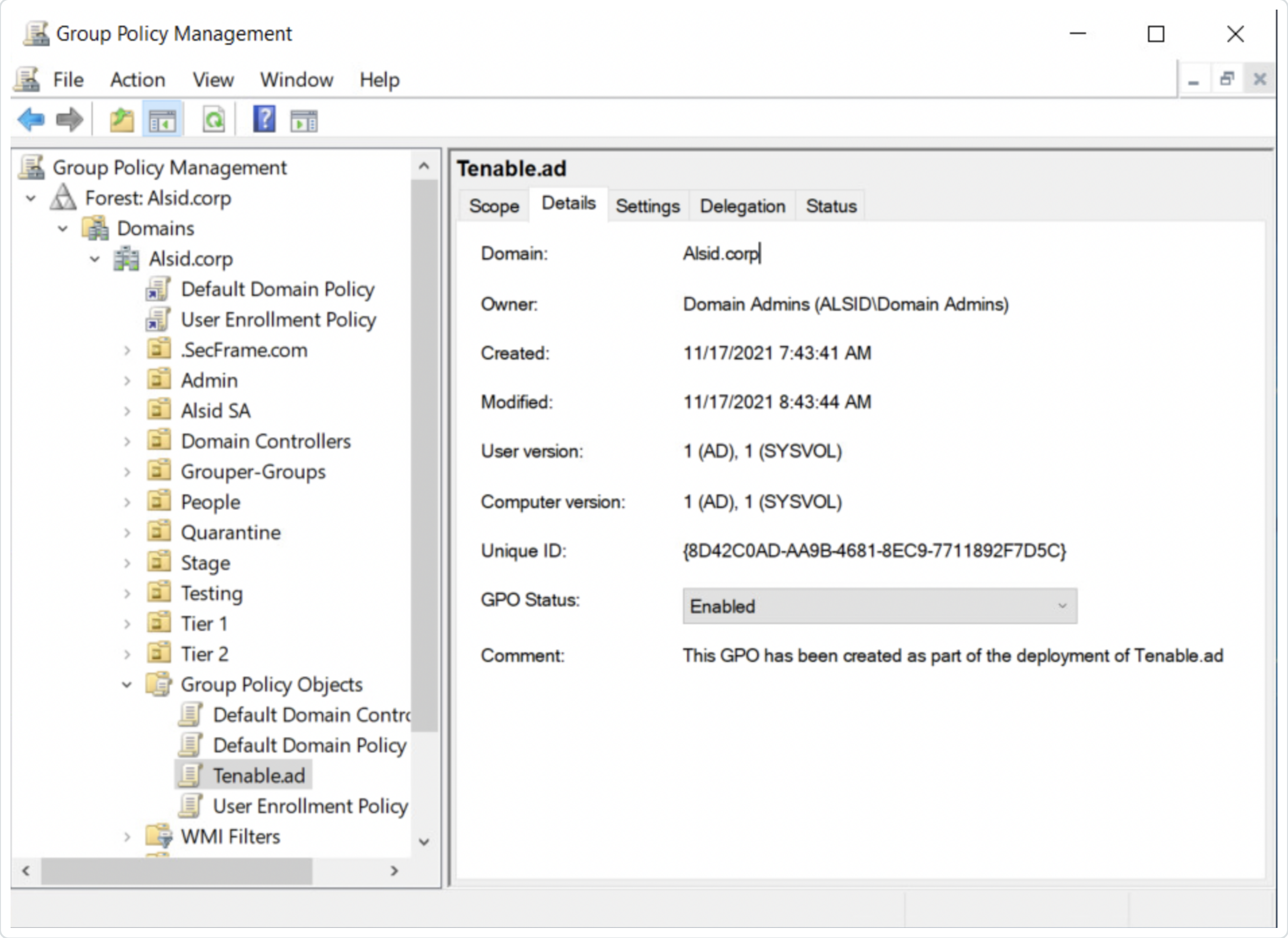
> **Tip**: The **Zerologon Exploitation** Indicator of Attack (IoA) dates from 2020. If all of your domain controllers (DCs) received updates within the past three years, they are protected from this vulnerability. To determine the required patches for securing your DCs against this vulnerability, consult the information in Netlogon Elevation of Privilege Vulnerability from Microsoft. Once you've confirmed your DCs' security, you can safely deactivate this IoA to avoid unnecessary alerts.

2. Click **Save**.

- If you enabled **Future automatic updates**, Tenable Identity Exposure saves and automatically updates your new configuration. Allow a few minutes for this update to take effect.
- If you did not enable **Future automatic updates**, a procedure window appears to guide you To configure domains for IoAs:

To check the IoA installation:

1. In Group Policy Management, check that the new Tenable Identity Exposure GPO exists and it links to the `Domain Controllers` OU:



Tenable.ad

Domain: Alsid.corp

Owner: Domain Admins (ALSID\Domain Admins)

Created: 11/17/2021 7:43:41 AM

Modified: 11/17/2021 8:43:44 AM

User version: 1 (AD), 1 (SYSVOL)

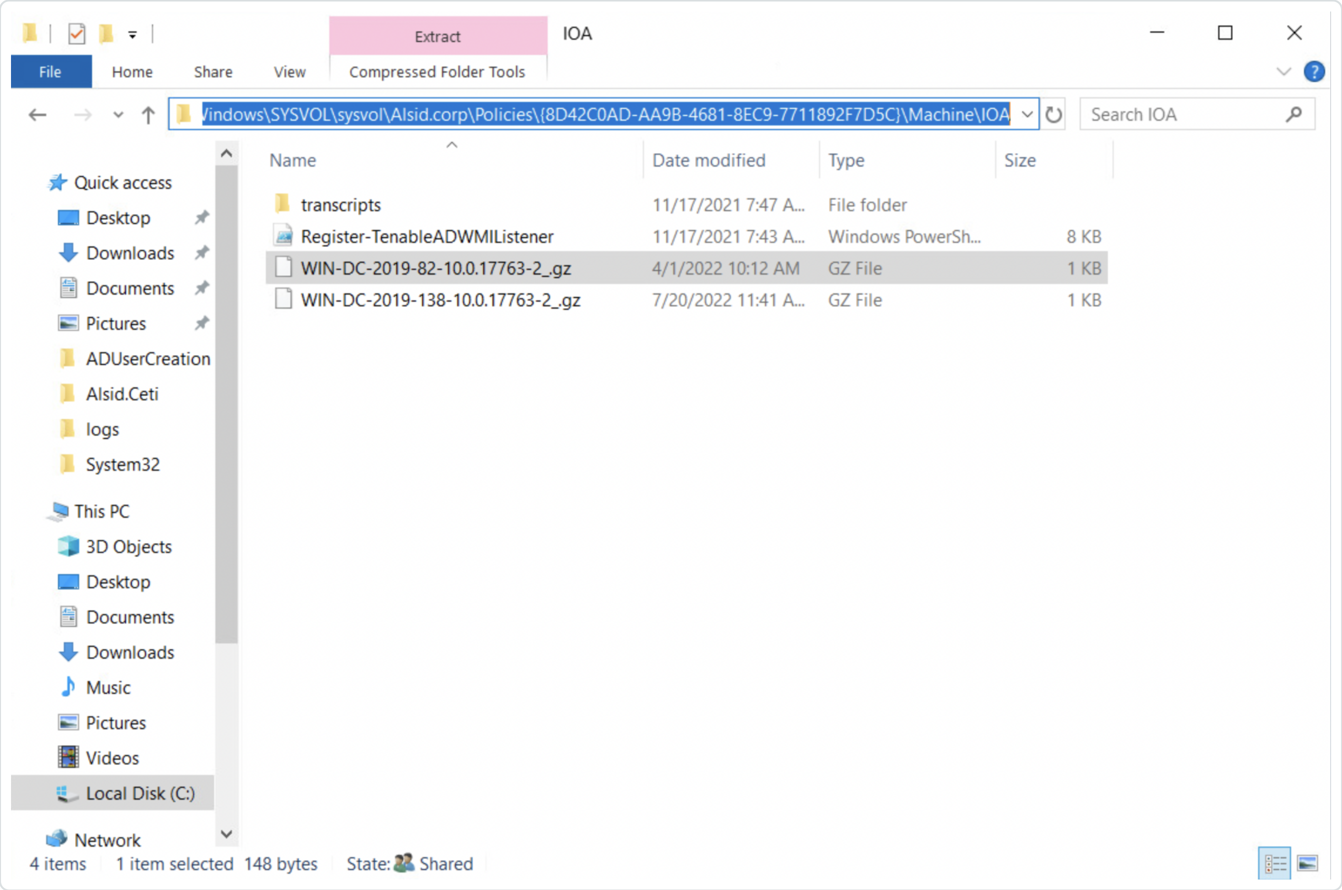
Computer version: 1 (AD), 1 (SYSVOL)

Unique ID: {8D42C0AD-AA9B-4681-8EC9-7711892F7D5C}

GPO Status: Enabled

Comment: This GPO has been created as part of the deployment of Tenable.ad

2. Go to the path `C:\Windows\SYSVOL\sysvol\alsid.corp\Policies\{GUID}\Machine\IOA` and check that the `.gz` file exists for **all domain controllers** before you test the IoAs:



Windows\SYSVOL\sysvol\Alsid.corp\Policies\{8D42C0AD-AA9B-4681-8EC9-7711892F7D5C}\Machine\IOA

Name	Date modified	Type	Size
transcripts	11/17/2021 7:47 A...	File folder	
Register-TenableADWMIListener	11/17/2021 7:43 A...	Windows PowerSh...	8 KB
WIN-DC-2019-82-10.0.17763-2_.gz	4/1/2022 10:12 AM	GZ File	1 KB
WIN-DC-2019-138-10.0.17763-2_.gz	7/20/2022 11:41 A...	GZ File	1 KB

4 items 1 item selected 148 bytes State: Shared

To check the "Write" permission access for the Tenable Identity Exposure service account:

1. In the file manager, go to `\\<DNS-NAME>\sysvol\<DNS-NAME>\Policies\{<GPO-ID>}\Machine\`.
2. Right-click on the "IOA" folder and select **Properties**.
3. Select the **Security** tab and click **Advanced**.
4. Click the **Effective Access** tab.
5. Click **Select a user**.
6. Type `<TENABLE-SERVICE-ACCOUNT-NAME>` and click **OK**.
7. Click on **View effective access**.
8. Check that the "Write" permission is activated.

Alternately, you can use Powershell:

- Run the following commands:

```
Install-Module -Name NTFSSecurity -RequiredVersion 4.2.3
```

```
Get-NTFSEffectiveAccess -Path \\<DNS-NAME>\sysvol\<DNS-NAME>\Policies\{<GPO-ID>}\IOA\ -
Account <TENABLE-SERVICE-ACCOUNT-NAME>
```

To calibrate IoAs

To avoid false positive attacks or lack of detection of legitimate attacks, you must calibrate your IoAs according to your environment by adapting them to the size of your Active Directory, whitelisting known tools, etc.

1. See the Tenable Identity Exposure Indicators of Attack Reference Guide for information about the options and recommended values to select.
2. In the security profile, apply the options and values to each IoA as described in Customize an Indicator.

Troubleshooting

The following error messages can appear during the deployment:

Message	Remediation
"Tenable Identity Exposure cannot write to the configuration file because the target folder `<targetFolder>` does not exist. This indicates that the IoA module deployment may have failed."	Uninstall the script and click "See procedure" for instructions to re-install the script.
"Tenable Identity Exposure could not write to the configuration file located on `<targetFile>` to update it. This can be due to another process locking the file or permission changes."	• Ensure that no other process besides the IoA module is using the configuration file. • Check that the service account has permission to modify the file contents.

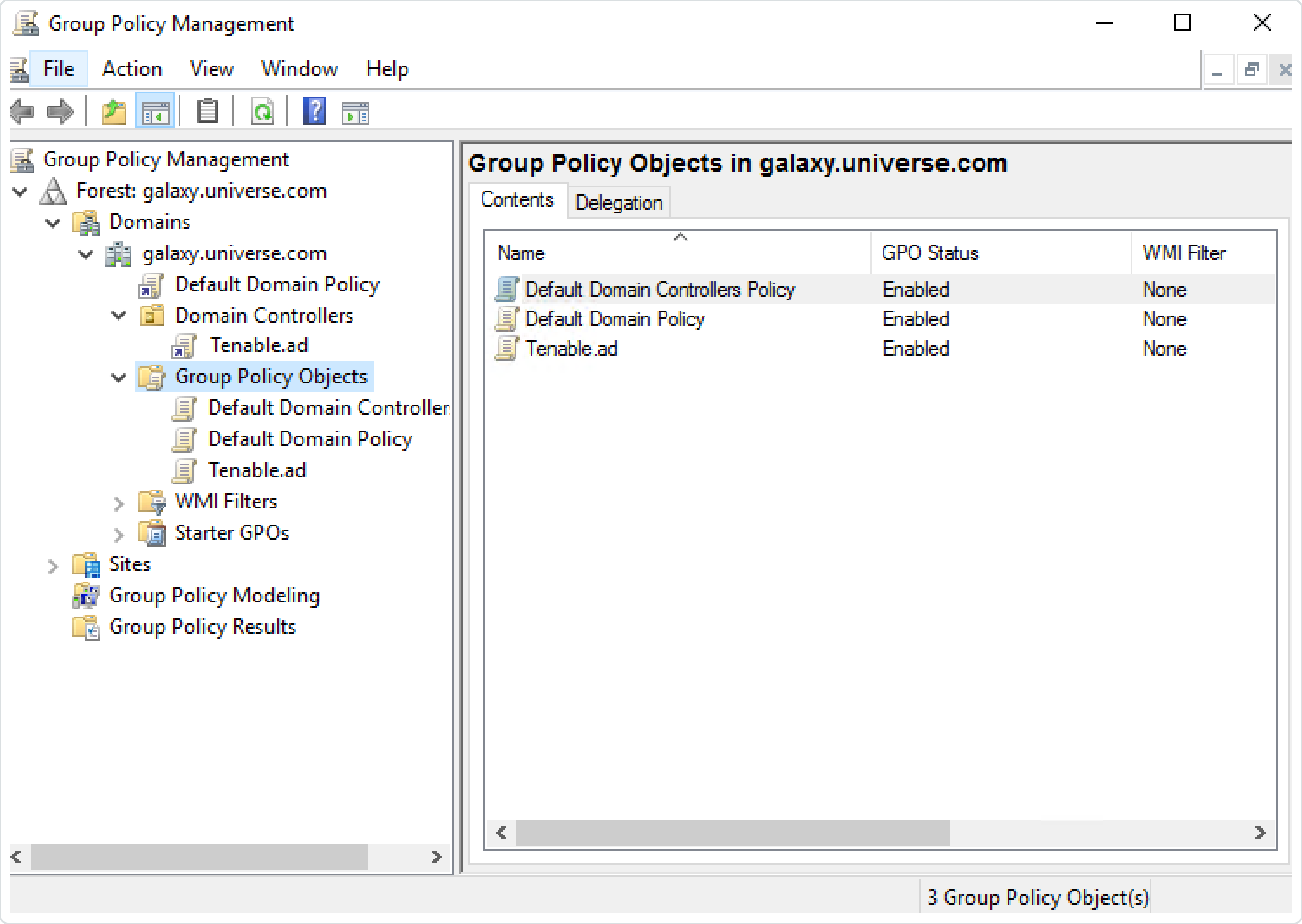
	• If you do not want to grant permission to the service account, disable the "Automatic Updates" toggle and click "See Procedure" for instructions on how to do a manual update whenever you modify your IoA configuration.
"The target folder `<targetFolder>` contains a version of Tenable Identity Exposure that cannot run automatic updates."	The currently installed script is an old version using WMI. Uninstall the current version, download a new installation script, and run this script.
"The configuration file deployment ran into an unexpected error."	Uninstall the script and click "See procedure" for instructions to re-install the script. If this does not work, contact your customer support representative.

For more information, see:

- Indicators of Attack Installation Script
- Technical Changes and Potential Impact
- Antivirus Detection
- Advanced Audit Policy Configuration Precedence

Indicators of Attack Installation Script

After you download and run the Indicators of Attack (IoA) installation file, the IoA script creates a new Group Policy Object (GPO) named by default `Tenable.ad` in the Active Directory (AD) database. The system links the Tenable Identity Exposure GPO only to the Domain Controllers' Organizational Unit (OU) that contains all domain controllers (DCs). The new policy automatically replicates between all DCs using the GPO mechanism.



Name	GPO Status	WMI Filter
Default Domain Controllers Policy	Enabled	None
Default Domain Policy	Enabled	None
Tenable.ad	Enabled	None

Installation Script (Tenable Identity Exposure v. 3.29)

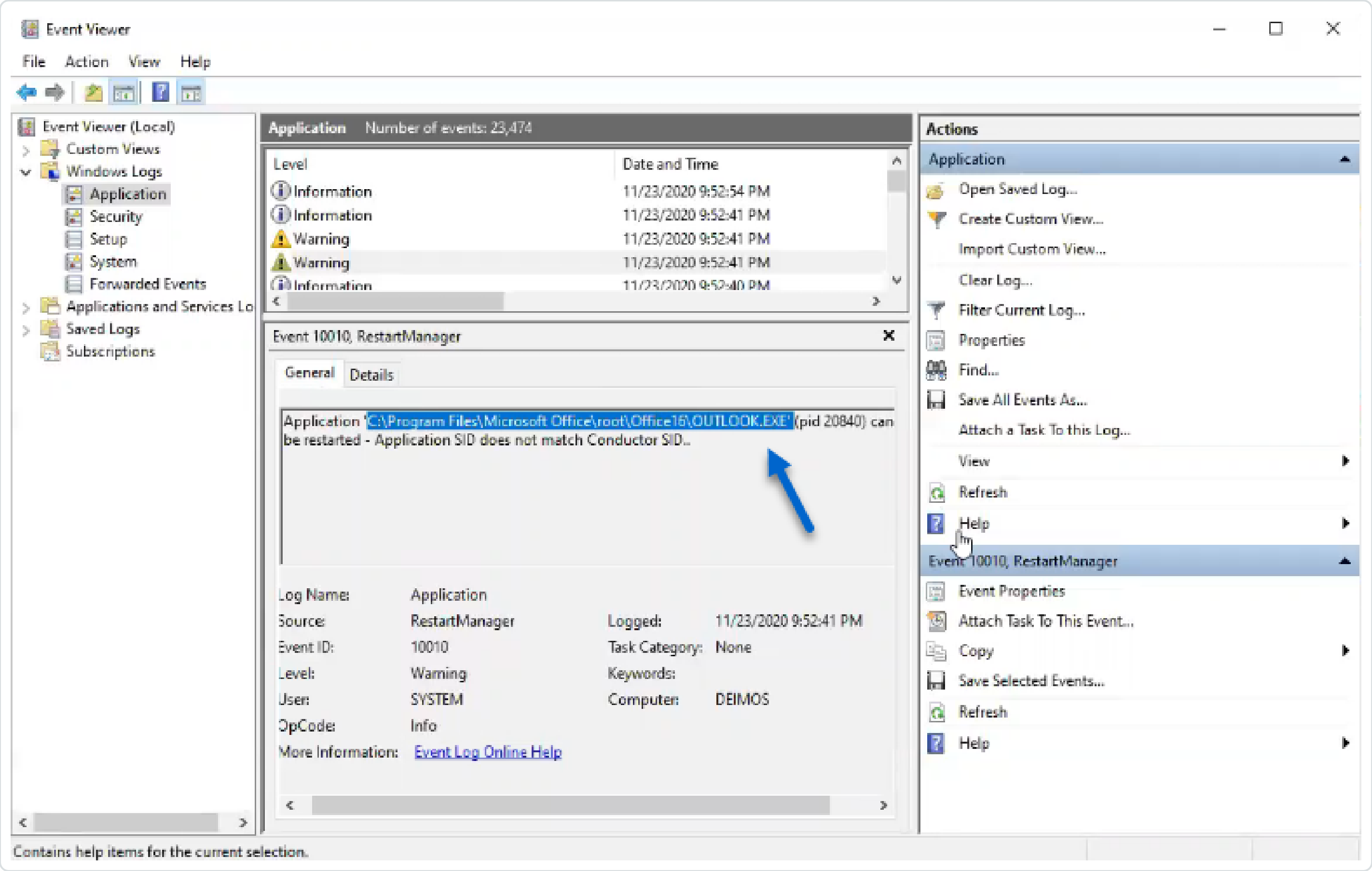
The GPO contains PowerShell scripts that all DCs execute locally to collect data of interest, as follows:

- The script configures an event logs listener on each domain controller using Windows EvtSubscribe API. The script makes a subscription for each necessary event log channel, as specified in the `TenableADEventsListenerConfiguration.json` configuration file, by submitting a request and a callback triggered by EvtSubscribe for each matching event log.
- The event listener receives event logs and buffers them before periodically flushing them to a file stored in a network share called Sysvol. Each DC flushes to a single Sysvol file that stores collected events and replicates it to other domain controllers.
- The script also creates a WMI consumer to ensure that this mechanism is persistent by re-registering the event subscriber when a DC restarts. WMI notifies the consumer each time a DC restarts to allow the consumer to register the event listener again.
- At this point, Distributed File System (DFS) replication occurs and automatically synchronizes files between domain controllers. Tenable Identity Exposure's platform listens for incoming DFS replication traffic and uses this data to gather events, run a security analysis, and then generate IoA alerts.

Local Data Retrieval

Windows event logs record all the events that occur in the operating system and its applications. Event logs rely on a framework of components integrated in Windows.

Using the EvtSubscribe API, the Tenable Identity Exposure IoA events log listener collects only useful event logs data segments in the form of insertion strings that it extracts from the event logs. Tenable Identity Exposure writes these insertion strings in a file stored in the Sysvol folder and replicates them via the DFS engine. This allows Tenable Identity Exposure to gather just the right amount of security data from event logs to run a security analysis and detect attacks.



Application Number of events: 23,474

Level	Date and Time
Information	11/23/2020 9:52:54 PM
Information	11/23/2020 9:52:41 PM
Warning	11/23/2020 9:52:41 PM
Warning	11/23/2020 9:52:41 PM
Information	11/23/2020 9:52:40 PM

Event 10010, RestartManager

Application 'C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE' (pid 20840) can be restarted - Application SID does not match Conductor SID..

Log Name:	Application		
Source:	RestartManager	Logged:	11/23/2020 9:52:41 PM
Event ID:	10010	Task Category:	None
Level:	Warning	Keywords:	
User:	SYSTEM	Computer:	DEIMOS
OpCode:	Info		
More Information:	Event Log Online Help		

Contains help items for the current selection.

IoA Script Summary

The following table gives an overview of the Tenable Identity Exposure script deployment.

Steps	Description	Component Involved	Technical Action
1	Register Tenable Identity Exposure's IoA deployment	GPO Management	Creates the `Tenable.ad` (default name) GPO and links it to the Domain Controllers OU.

2	Start Tenable Identity Exposure's IoA deployment on DC	DC local system	Each DC detects the new GPO to apply, depending on the AD replication and Group Policy refresh intervals.
3	Control Advanced Logging Policy state	DC local system	The system activates the advanced logging policy by setting the registry key `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\SCENoApplyLegacyAuditPolicy`.
4	Update Local Logging policy	DC local system	Depending on the IoAs to detect, Tenable Identity Exposure dynamically generates and activates specific audit policies. This policy does not deactivate any existing logging policy — it only enriches them if necessary. If it detects a conflict, the GPO installation script stops and shows the message "Tenable Identity Exposure requires the audit policy '...' but the current AD configuration prevents its usage."
5	Register an event listener and a WMI producer	DC local system	The system registers and executes the script contained in the GPO. This script runs a PowerShell process to subscribe to event logs using EvtSubscribe API and to create an instance of `ActiveScriptEventConsumer` for persistence purposes. Tenable Identity Exposure uses these objects to receive and store event logs contents.
6	Collect event logs messag	DC local system	Tenable Identity Exposure captures relevant event log messages, buffers them periodically, and saves them to files (one per DC) stored in the Sysvol folder associated to the Tenable Identity Exposure GPO (`...{GPO_`

	es		`GUID}\Machine\IOA<DC_name>`).
7	Replicate files to the declared DC SYSVOL folder	Active Directory	Using DFS, the AD replicates files across the domain, and specifically in the declared DC. The Tenable Identity Exposure platform gets notification for each file and reads their content.
8	Overwrite these files	Active Directory	Each DC automatically and continuously writes the periodically buffered events in the same file.

Installation Script (Tenable Identity Exposure v. 3.19.11 and earlier)

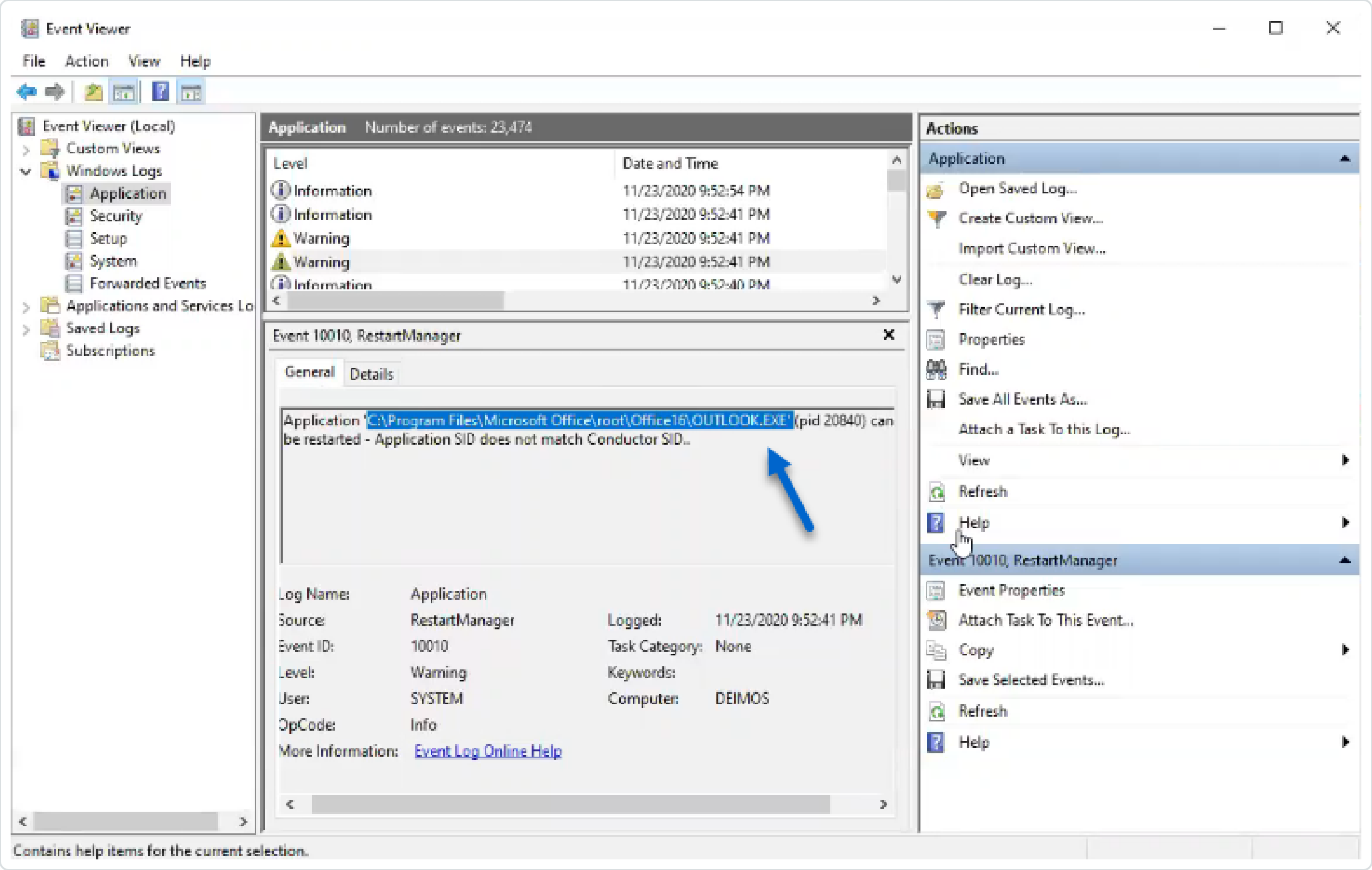
The GPO contains PowerShell scripts that all DCs execute locally to collect data of interest, as follows:

- The scripts configure an event watcher and a Windows Management Instrumentation (WMI) Producer/Consumer in the machine's memory. WMI is a Windows component that provides you with information about the status of local or remote computer systems.
- The event watcher receives event logs and periodically buffers them before flushing them to a file stored in a network share called Sysvol. Each DC flushes to a single Sysvol file that stores collected events and replicates it to other domain controllers.
- The WMI consumer makes this mechanism persistent by registering again the event watcher when a DC restarts. The producer wakes up and notifies the consumer each time a DC restarts. As a result, the consumer registers the event watcher again.
- At this point, Distributed File System or DFS replication occurs and automatically synchronizes files between domain controllers. Tenable Identity Exposure's platform listens for incoming DFS replication traffic and uses this data to gather events, run a security analysis, and then generate IoA alerts.

Local Data Retrieval

Windows event logs record all the events that occur in the operating system and its applications. Event logs called Event Tracing for Windows (ETW) rely on a framework of components integrated in Windows. ETW is in the kernel and produces data stored locally on DCs and not replicated by AD protocols.

Using the WMI engine, Tenable Identity Exposure collects only useful ETW data segments in the form of insertion strings that it extracts from the event logs. Tenable Identity Exposure writes these insertion strings in a file stored in the Sysvol folder and replicates them via the DFS engine. This allows Tenable Identity Exposure to gather just the right amount of security data from ETW to run a security analysis and detect attacks.



Application Number of events: 23,474

Level	Date and Time
Information	11/23/2020 9:52:54 PM
Information	11/23/2020 9:52:41 PM
Warning	11/23/2020 9:52:41 PM
Warning	11/23/2020 9:52:41 PM
Information	11/23/2020 9:52:40 PM

Event 10010, RestartManager

Application 'C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE' (pid 20840) can be restarted - Application SID does not match Conductor SID..

Log Name:	Application		
Source:	RestartManager	Logged:	11/23/2020 9:52:41 PM
Event ID:	10010	Task Category:	None
Level:	Warning	Keywords:	
User:	SYSTEM	Computer:	DEIMOS
OpCode:	Info		
More Information:	Event Log Online Help		

Contains help items for the current selection.

IoA Script Summary

The following table gives an overview of the Tenable Identity Exposure script deployment.

Ste	Description	Compon	Technical Action

ps		ent Involved	
1	Register Tenable Identity Exposure's IoA deployment	GPO Manage ment	Creates the `Tenable.ad` (default name) GPO and links it to the Domain Controllers OU.
2	Start Tenable Identity Exposure's IoA deployment on DC	DC local system	Each DC detects the new GPO to apply, depending on the AD replication and Group Policy refresh intervals.
3	Register an event watcher and a WMI producer/co nsumer	DC local system	The system registers and executes an Immediate Task. This task runs a PowerShell process to create instances of the following classes: `ManagementEventWatcher` and `ActiveScriptEventConsumer`. Tenable Identity Exposure uses these objects to receive and store ETW messages.
4	Control Advanced Logging Policy state	DC local system	The system activates the advanced logging policy by setting the registry key `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\SCENoApplyLegacyAuditPolicy`.
5	Update Local Logging policy	DC local system	Depending on the IoAs to detect, Tenable Identity Exposure dynamically generates and activates an advanced logging policy. This policy does not deactivate any existing logging policy — it only enriches them if necessary. If it detects a conflict, the GPO installation script stops and shows the message "Tenable Identity

			Exposure requires the audit policy '...' but the current AD configuration prevents its usage."
6	Collect ETW messages	DC local system	Tenable Identity Exposure captures relevant ETW messages, buffers them periodically, and saves them to files (one per DC) stored in the Sysvol folder associated to the Tenable Identity Exposure GPO (`...{GPO_GUID}\Machine\IOA<DC_name>`).
7	Replicate files to the Tenable Identity Exposure platform	Active Directory	Using DFS, the AD replicates files across the domain. The Tenable Identity Exposure platform also receives the files.
8	Overwrite these files	Active Directory	Each DC automatically and continuously writes the periodically buffered events in the same file.

See also

- Indicators of Attack and the Active Directory
- Install Indicators of Attack
- Technical Changes and Potential Impact

Technical Changes and Potential Impact

The installation script for the Indicators of Attack (IoA) module creates a GPO that applies the following changes transparently on the monitored DCs:

- A new GPO named “Tenable.ad” by default linked to the domain controller's organization unit (OU) by default.
- Modification of a registry key to activate the Microsoft Advanced logging policy.
- Activation of a new Event Log policy to force Domain Controllers to generate the ETW information that IoAs require.

  > **Note**: The Event Log policy is mandatory so that the ETW engine can generate the insertion strings that Tenable Identity Exposure requires. This policy does not disable any existing logging policy but adds to them. If there is a conflict, the deployment script stops with an error message.

- Addition of a write permission for the Tenable Identity Exposure service account that allows "Automatic updates" of the IoA configuration stored in the GPO folder.

Limitation and Potential Impacts

The **Indicator of Attack** (IoA) module can pose the following limitations:

- The IoA module relies on the ETW data and operates within the limitations that Microsoft defines.
- The installed GPO must replicate over the entire domain, and the GPO refresh interval must elapse for the installation process to complete. During this replication period, false positives and false negatives can happen, even though Tenable Identity Exposure minimizes this effect by not starting the checks in the Indicator of Attack engine immediately.
- Tenable uses the SYSVOL file share to retrieve ETW information from domain controllers. As SYSVOL replicates to every domain controller in the domain, a significant increase of the replication activity appears during a high peak of Active Directory activity.
- Replicating files between domain controllers and Tenable Identity Exposure also consumes some network bandwidth. Tenable Identity Exposure controls these impacts with the automatic removal of the files it collects, and limits the size of these files (500 MB maximum

by default.)

- Issues with slow or broken Distributed File System (DFS) replication. For more information, see DFS Replication Issues Mitigation .

See also

- Indicators of Attack and the Active Directory
- Install Indicators of Attack
- Indicators of Attack Installation Script
- Troubleshoot Indicators of Attack

Attack Scenarios (< v. 3.36)

Caution: This configuration update feature for Indicator of Attack no longer applies to Tenable Identity Exposure versions > 3.36.

Required User Role: Organizational user with permissions to modify the Indicators of Attack configuration.

You define an attack scenario by selecting the types of attack for Tenable Identity Exposure to monitor on specific domains.

Before you begin

In order to modify the attack scenario, you must have a user role with the following permissions:

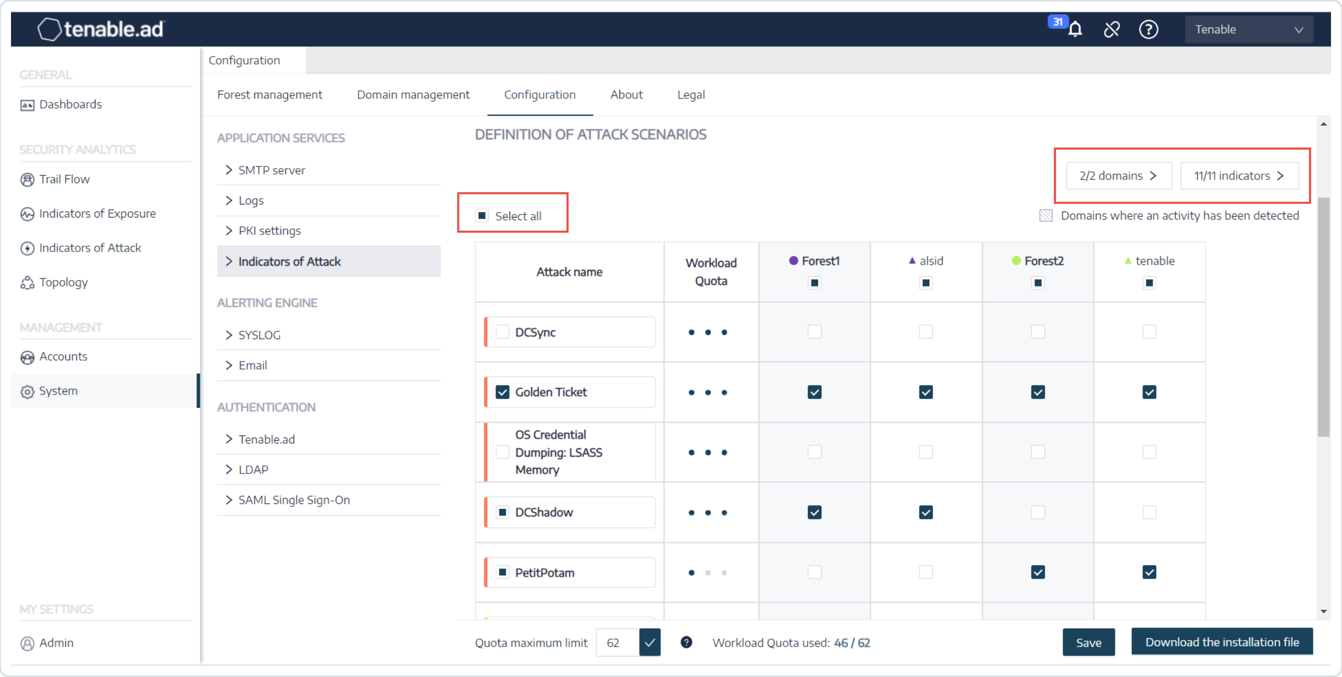
- In **Data Entities**, "Read" access for:
  - All Indicators of Attack
  - All domains
- In **Interface Entities**, access for:
  - Management > System > Configuration
  - Management > System > Configuration > Application Services > Indicators of Attack
  - Management > System > Configuration > Application Services > Indicators of Attack > Download installation file

For more information about role-based permissions, see Set Permissions for a Role.

To define an attack scenario:

1. In Tenable Identity Exposure, click on **Systems** > **Configuration** > **Indicators of Attack**.

   The **Definition of Attack Scenarios** pane opens.



DEFINITION OF ATTACK SCENARIOS

■ Select all

▨ Domains where an activity has been detected

Attack name	Workload Quota	● Forest1 ■	▲ alsid ■	● Forest2 ■	▲ tenable ■
□ DCSync	• • •	□	□	□	□
☑ Golden Ticket	• • •	☑	☑	☑	☑
□ OS Credential Dumping: LSASS Memory	• • •	□	□	□	□
■ DCShadow	• • •	☑	☑	□	□
■ PetitPotam	• • •	□	□	☑	☑

Quota maximum limit 62 ✓

Workload Quota used: 46 / 62

2. Under **Attack Name**, select the attack to monitor.

3. Select the domain on which to monitor for the selected attack.

4. Optionally, you can do one of the following:

   - Click on **Select all** to monitor for all attacks on all domains.

   - Click on **n/n domains** or **n/n indicators** to filter for specific domains to monitor for specific attacks.

5. Click **Save**.

   A confirmation message informs you that Tenable Identity Exposure clears the activity status of each attack after you save the configuration.

6. Click **Confirm**.

   A message confirms that Tenable Identity Exposure updated the Indicator of Attack configuration.

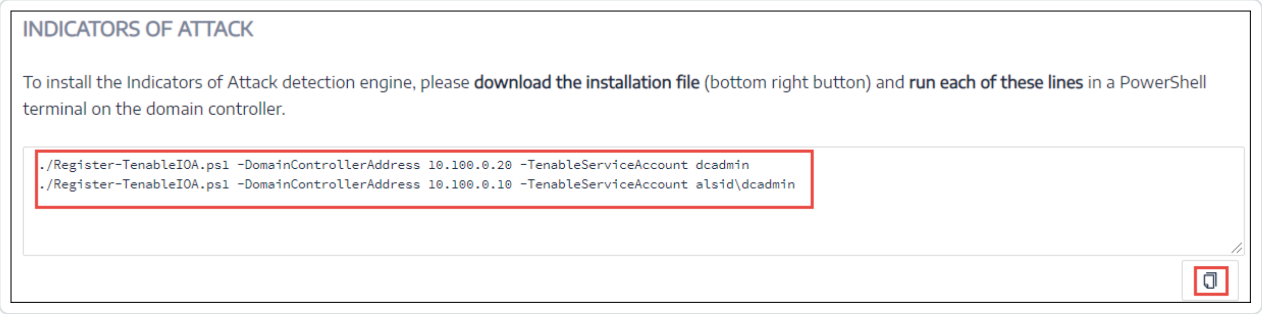
7. Click **Download the installation file**.

8. For the new attack configuration to take effect, run the installation file:

a. Copy and paste the downloaded installation file to the DC in the monitored domain.

b. Open a PowerShell terminal with administrative rights.

c. In Tenable Identity Exposure, copy the commands under the Indicators of Attack section at the bottom of the window.



INDICATORS OF ATTACK

To install the Indicators of Attack detection engine, please **download the installation file** (bottom right button) and **run each of these lines** in a PowerShell terminal on the domain controller.

```
./Register-TenableIOA.ps1 -DomainControllerAddress 10.100.0.20 -TenableServiceAccount dcadmin
./Register-TenableIOA.ps1 -DomainControllerAddress 10.100.0.10 -TenableServiceAccount alsid\dcadmin
```

d. In the PowerShell window, paste the commands to run the script.

Workload Quota

Caution: The workload quota feature only no longer applies to Tenable Identity Exposure versions > 3.36.

Required User Role: Organizational user with permissions to edit the workload quota.

Each Indicator of Attack in Tenable Identity Exposure has an associated workload quota that takes into account the resources required to analyze data from an attack.

Tenable Identity Exposure calculates the workload quota to limit the number of Indicators of Attack (IoAs) running simultaneously which has an impact on bandwidth and CPU usage for event generation on domain controllers.

After you modify the workload quota limit, do the following:

- Increase: Monitor statistics following the increase to ensure a comfortable margin.
- Decrease: Deactivate some IoAs to stay under this quota, which reduces security coverage against attacks.

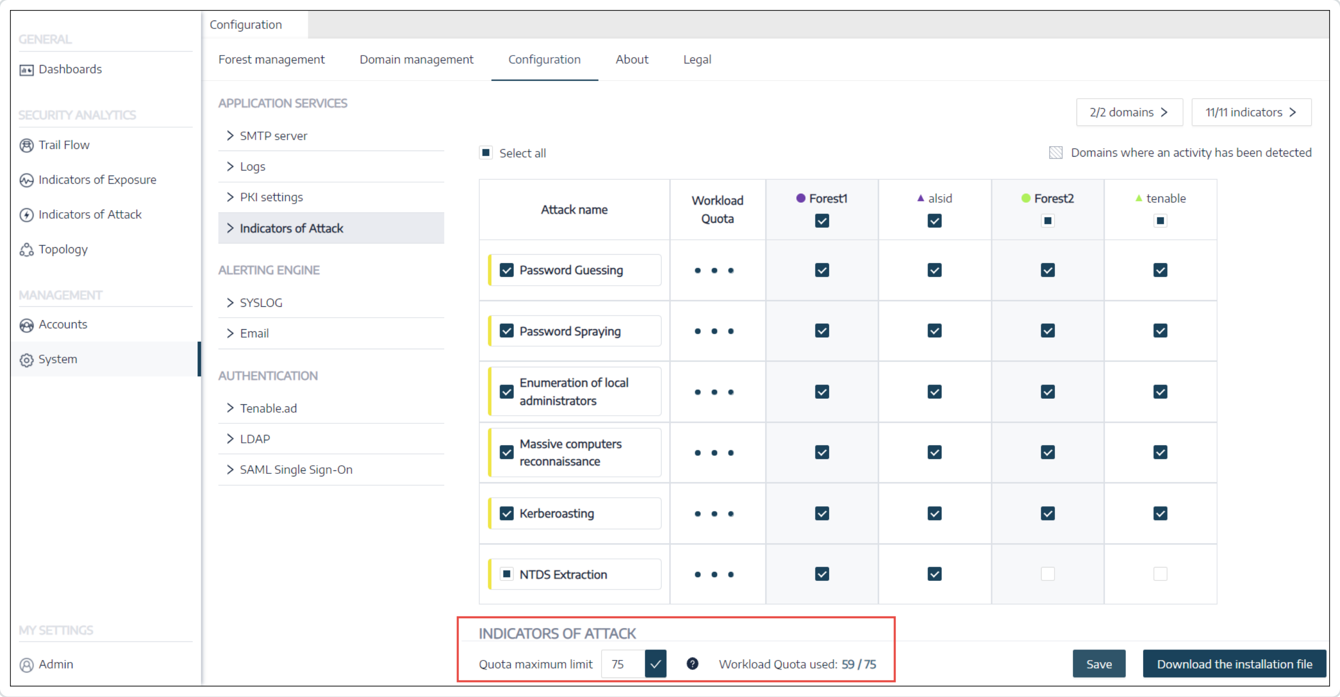
To modify the workload quota limit:

1. In Tenable Identity Exposure, click on **Systems** > **Configuration** > **Indicators of Attack**.

   The **IoA configuration** pane opens.

2. Select the IoAs you want for your configuration.

3. Under **Indicators of Attack**, in the **Quota maximum limit** box, type a value for the workload quota limit.



Attack name	Workload Quota	Forest1 ☑	alsid ☑	Forest2 ■	tenable ■
☑ Password Guessing	• • •	☑	☑	☑	☑
☑ Password Spraying	• • •	☑	☑	☑	☑
☑ Enumeration of local administrators	• • •	☑	☑	☑	☑
☑ Massive computers reconnaissance	• • •	☑	☑	☑	☑
☑ Kerberoasting	• • •	☑	☑	☑	☑
■ NTDS Extraction	• • •	☑	☑	□	□

INDICATORS OF ATTACK

Quota maximum limit 75 ✓

Workload Quota used: 59 / 75

4. Click the checkmark next to the value you entered.

   A message informs you of the modification's impacts on Tenable Identity Exposure.

> **Note**: If you type a quota maximum limit that is smaller than what the current attack configuration requires, you must adjust the number of active Indicators of Attack or raise the limit.

5. Click **Confirm**.

   A message confirms that Tenable Identity Exposure updated the quota maximum limit.

6. Click **Save**.

   A confirmation message informs you that Tenable Identity Exposure clears the activity status of each attack after you save the configuration.

7. Click **Confirm**.

   A message confirms that Tenable Identity Exposure updated the Indicator of Attack configuration.

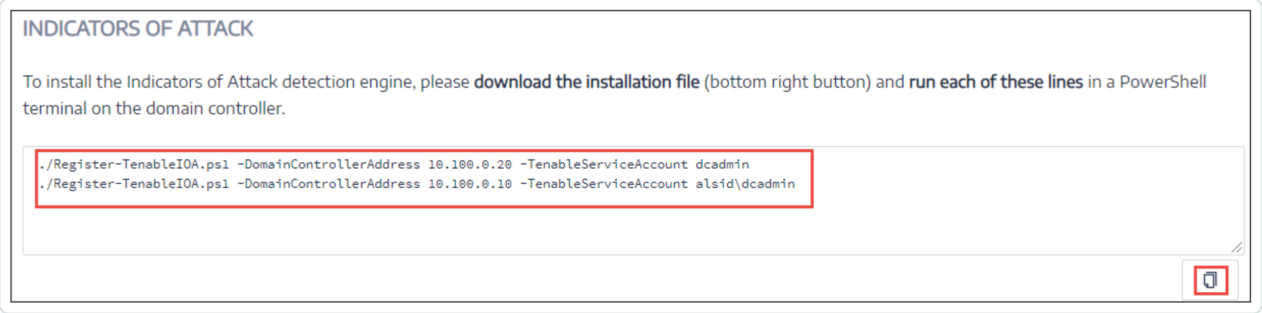
8. Click **Download the installation file**.

9. For the new attack configuration to take effect, run the installation file:

   a. Copy and paste the downloaded installation file to the DC in the monitored domain.

   b. Open a PowerShell terminal with administrative rights.

   c. In Tenable Identity Exposure, copy the commands under the Indicators of Attack section at the bottom of the window.



INDICATORS OF ATTACK

To install the Indicators of Attack detection engine, please **download the installation file** (bottom right button) and **run each of these lines** in a PowerShell terminal on the domain controller.

```
./Register-TenableIOA.ps1 -DomainControllerAddress 10.100.0.20 -TenableServiceAccount dcadmin
./Register-TenableIOA.ps1 -DomainControllerAddress 10.100.0.10 -TenableServiceAccount alsid\dcadmin
```

   d. In the PowerShell window, paste the commands to run the script.

Install Microsoft Sysmon

Some Tenable Identity Exposure's Indicators of Attack (IoAs) require the Microsoft System Monitor (Sysmon) service to activate.

Sysmon monitors and logs system activity to the Windows event log to provide more security-oriented information in the Event Tracing for Windows (ETW) infrastructure.

Because installing an additional Windows service and driver can affect performances of the domain controllers hosting the Active Directory infrastructure. Tenable does not deploy automatically Microsoft Sysmon. You must install it manually or use a dedicated GPO.

The following IoAs require Microsoft Sysmon.

Name	Reason
OS Credential Dumping: LSASS Memory	Detects Process Injection

Note: If you choose to install Sysmon, then you must install it on all domain controllers and not just the PDC to collect all necessary events.

Note: Test your Sysmon installation for compatibility issues before a full deployment of Tenable Identity Exposure.

Tip: Make sure to update Sysmon regularly after installation to take advantage of any patches that address possible vulnerabilities. The oldest version compatible with Tenable Identity Exposure is Sysmon 12.0.

To install Sysmon:

1. Download Sysmon from the Microsoft website.

2. In the command-line interface, run the following command to install Microsoft Sysmon on the local machine:

   ```
   .\Sysmon64.exe -accepteula -i C:\TenableSysmonConfigFile.xml
   ```

   Note: See the commented Sysmon configuration file for configuration explanations.

3. Run the following command to add a registry key to indicate to WMI filters that Sysmon is installed:

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Microsoft-Windows-
Sysmon/Operational"
```

To uninstall Sysmon:

1. Open a PowerShell terminal.
2. Browse to the folder that contains `Sysmon64.exe`.
3. Type the following command:

```
PS C:\> .\Sysmon64.exe -u
```

To delete the registry key:

- In the command-line interface, type the following command on all machines running Sysmon:

```
reg delete "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Microsoft-Windows-
Sysmon/Operational"
```

Sysmon Configuration File

Notes:
- Copy and save the Sysmon configuration file as an XML file before you use it. In case of error, you can also download the configuration file directly here.
- Unblock the file in the file properties before you run it.

```
<Sysmon schemaversion="4.40">
  <EventFiltering>

    <!--SYSMON EVENT ID 1 : PROCESS CREATION [ProcessCreate]-->
    <RuleGroup name="" groupRelation="or">
      <ProcessCreate onmatch="exclude">
        <!--NOTE: Using "exclude" with no rules means everything in this section will be logged-->
      </ProcessCreate>
    </RuleGroup>

    <!--SYSMON EVENT ID 2 : FILE CREATION TIME RETROACTIVELY CHANGED IN THE FILESYSTEM
```

```
[FileCreateTime]-->
    <RuleGroup name="" groupRelation="or">
      <FileCreateTime onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </FileCreateTime>
    </RuleGroup>

    <!--SYSMON EVENT ID 3 : NETWORK CONNECTION INITIATED [NetworkConnect]-->
    <RuleGroup name="" groupRelation="or">
      <NetworkConnect onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </NetworkConnect>
    </RuleGroup>

    <!--SYSMON EVENT ID 4 : RESERVED FOR SYSMON SERVICE STATUS MESSAGES-->
      <!--Cannot be filtered.-->

    <!--SYSMON EVENT ID 5 : PROCESS ENDED [ProcessTerminate]-->
    <RuleGroup name="" groupRelation="or">
      <ProcessTerminate onmatch="exclude">
        <!--NOTE: Using "exclude" with no rules means everything in this section will be logged-->
      </ProcessTerminate>
    </RuleGroup>

    <!--SYSMON EVENT ID 6 : DRIVER LOADED INTO KERNEL [DriverLoad]-->
    <RuleGroup name="" groupRelation="or">
      <DriverLoad onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </DriverLoad>
    </RuleGroup>

    <!--SYSMON EVENT ID 7 : DLL (IMAGE) LOADED BY PROCESS [ImageLoad]-->
    <RuleGroup name="" groupRelation="or">
      <ImageLoad onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </ImageLoad>
    </RuleGroup>

    <!--SYSMON EVENT ID 8 : REMOTE THREAD CREATED [CreateRemoteThread]-->
    <RuleGroup name="" groupRelation="or">
      <CreateRemoteThread onmatch="include">
        <TargetImage name="lsass" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
      </CreateRemoteThread>
    </RuleGroup>

    <!--SYSMON EVENT ID 9 : RAW DISK ACCESS [RawAccessRead]-->
    <RuleGroup name="" groupRelation="or">
      <RawAccessRead onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </RawAccessRead>
    </RuleGroup>

    <!--SYSMON EVENT ID 10 : INTER-PROCESS ACCESS [ProcessAccess]-->
    <RuleGroup name="" groupRelation="or">
        <ProcessAccess onmatch="include">
          <!-- Detect Access to LSASS-->
          <Rule groupRelation="and">
            <TargetImage name="technique_id=T1003,technique_name=Credential Dumping"
condition="is">C:\Windows\system32\lsass.exe</TargetImage>
```

```
            <GrantedAccess>0x1FFFFF</GrantedAccess>
          </Rule>
          <Rule groupRelation="and">
            <TargetImage name="technique_id=T1003,technique_name=Credential Dumping"
condition="is">C:\Windows\system32\lsass.exe</TargetImage>
            <GrantedAccess>0x1F1FFF</GrantedAccess>
          </Rule>
          <Rule groupRelation="and">
            <TargetImage name="technique_id=T1003,technique_name=Credential Dumping"
condition="is">C:\Windows\system32\lsass.exe</TargetImage>
            <GrantedAccess>0x1010</GrantedAccess>
          </Rule>
          <Rule groupRelation="and">
            <TargetImage name="technique_id=T1003,technique_name=Credential Dumping"
condition="is">C:\Windows\system32\lsass.exe</TargetImage>
            <GrantedAccess>0x143A</GrantedAccess>
          </Rule>

          <!-- Detect process hollowing to LSASS-->
          <Rule groupRelation="and">
            <TargetImage name="technique_id=T1003,technique_name=Credential Dumping"
condition="is">C:\Windows\system32\lsass.exe</TargetImage>
            <GrantedAccess>0x0800</GrantedAccess>
          </Rule>
          <Rule groupRelation="and">
            <TargetImage name="technique_id=T1003,technique_name=Credential Dumping"
condition="is">C:\Windows\system32\lsass.exe</TargetImage>
            <GrantedAccess>0x800</GrantedAccess>
          </Rule>

          <!-- Detect process process injection to LSASS-->
          <Rule groupRelation="and">
            <TargetImage name="technique_id=T1055,technique_name=Process Injection"
condition="is">C:\Windows\system32\lsass.exe</TargetImage>
            <GrantedAccess>0x0820</GrantedAccess>
          </Rule>
          <Rule groupRelation="and">
            <TargetImage name="technique_id=T1055,technique_name=Process Injection"
condition="is">C:\Windows\system32\lsass.exe</TargetImage>
            <GrantedAccess>0x820</GrantedAccess>
          </Rule>
        </ProcessAccess>
    </RuleGroup>

    <!--SYSMON EVENT ID 11 : FILE CREATED [FileCreate]-->
    <RuleGroup name="" groupRelation="or">
      <FileCreate onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </FileCreate>
    </RuleGroup>

    <!--SYSMON EVENT ID 12 & 13 & 14 : REGISTRY MODIFICATION [RegistryEvent]-->
    <RuleGroup name="" groupRelation="or">
      <RegistryEvent onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </RegistryEvent>
    </RuleGroup>

    <!--SYSMON EVENT ID 15 : ALTERNATE DATA STREAM CREATED [FileCreateStreamHash]-->
    <RuleGroup name="" groupRelation="or">
      <FileCreateStreamHash onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </FileCreateStreamHash>
    </RuleGroup>

    <!--SYSMON EVENT ID 16 : SYSMON CONFIGURATION CHANGE-->
      <!--Cannot be filtered.-->

    <!--SYSMON EVENT ID 17 & 18 : PIPE CREATED / PIPE CONNECTED [PipeEvent]-->
    <RuleGroup name="" groupRelation="or">
      <PipeEvent onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </PipeEvent>
    </RuleGroup>

    <!--SYSMON EVENT ID 19 & 20 & 21 : WMI EVENT MONITORING [WmiEvent]-->
    <RuleGroup name="" groupRelation="or">
      <WmiEvent onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </WmiEvent>
    </RuleGroup>

    <!--SYSMON EVENT ID 22 : DNS QUERY [DnsQuery]-->
    <RuleGroup name="" groupRelation="or">
      <DnsQuery onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </DnsQuery>
    </RuleGroup>

    <!--SYSMON EVENT ID 23 : FILE DELETED [FileDelete]-->
    <RuleGroup name="" groupRelation="or">
      <FileDelete onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </FileDelete>
    </RuleGroup>

  </EventFiltering>
</Sysmon>
```

Uninstall Indicators of Attack

Required Role: Administrator on the local machine.

To uninstall the Indicators of Attack (IoA) module, you run a command that creates a new Group Policy Object (GPO) called Tenable Identity Exposure cleaning.

The uninstallation process uses this new GPO by default to clean out previously installed GPOs and its SYSVOL files, the registry setting, the advanced logging policy, and the WMI filters.

Note: If you changed the name of the initial GPO, you must pass it to the uninstaller so that it knows which GPO to uninstall. To pass the new GPO name, use the parameter `-GpoDisplayName`.

To uninstall the IoA module:

1. In the command-line interface, run the following command to uninstall the IoA module:

   ```
   Register-TenableIOA.ps1 -Uninstall
   ```

2. Replicate this new GPO over the entire domain. The script enforces a 4-hour delay for the replication to complete.

3. Run the following command to delete the cleaning GPO:

   ```
   Remove-GPO -Guid <GUID> -Domain "<DOMAIN>"
   ```

4. Optional: Run the following command to verify that the GPO no longer exists:

   ```
   (Get-ADDomainController -Filter *).Name | Foreach-Object {Get-GPO -Name "Tenable.ad cleaning"}
   | Select Displayname| measure
   ```

Troubleshoot Indicators of Attack

- Advanced Audit Policy Configuration Precedence
- Antivirus Detection
- Tenable Identity Exposure Log Files
- Event Logs Listener Validation
- DFS Replication Issues Mitigation

Antivirus Detection

Tenable and Microsoft do not recommend installing antivirus, Endpoint Protection Platform (EPP), or Endpoint Detection and Response (EDR) software on domain controllers (or any other tool with a central management console). If you choose to do so, your antivirus/EPP/EDR might detect and even block or delete required items for the collection of Indicator of Attack (IoA) events on domain controllers.

Tenable Identity Exposure's deployment script for Indicators of Attack does not include malicious code, nor is it even obfuscated. However, occasional detections are normal, given its usage of PowerShell and WMI and the agentless nature of the implementation.

If you encounter issues such as:

- Error messages during installation
- False-positive or false-negative in detection

To troubleshoot installation scripts antivirus detection:

1. Review your antivirus/EPP/EDR security logs to check for any detection, blocking, or deletion of Tenable Identity Exposure components. Antivirus/EPP/EDR can affect the following components:
   - The `ScheduledTasks.xml` file in the Tenable Identity Exposure GPO applied to domain controllers.
   - The Tenable Identity Exposure scheduled task on domain controllers that launches PowerShell.exe.
   - The Tenable Identity Exposure `Register-TenableADEventsListener.exe` process launched on domain controllers.
2. Add security exceptions in your tools for the affected components.
   - In particular, Symantec Endpoint Protection can raise `CL.Downloader!gen27` detections during the IoA installation process. You can add this specific known risk to your exceptions policy.

- Once the Task Scheduler is set up, run PowerShell to initiate the `Register-TenableADEventsListener.exe` process. The antivirus/EPP/EDR software may potentially obstruct this PowerShell script, hindering the proper execution of Indicators of Attack. Track this process closely and ensure that it runs only once across all monitored domain controllers.

  Examples of file path exclusions for Antivirus/EPP/EDR:

  ```
  Register-TenableADEventsListener.exe process
   "\\"domain"\sysvol\"domain"\Policies\{"GUID_Tenable.ad}\Machine\IOA\Register-
  TenableADEventsListener.exe"
  ```

  ```
  ScheduledTasks.xml file
      C:\Users\<User Name>\AppData\Local\Temp\4\Tenable.ad\
  {GUID}\DomainSysvol\GPO\Machine\Preferences\ScheduledTasks\ScheduledTasks.xml
      C:\Windows\[SYSVOL]\POLICIES\
  {[GUID]}\Machine\Preferences\ScheduledTasks\ScheduledTasks.xml
      \\[DOMAIN.FQDN]\[SYSVOL]\POLICIES\
  {[GUID]}\Machine\Preferences\ScheduledTasks\ScheduledTasks.xml
  ```

Advanced Audit Policy Configuration Precedence

The group policy object (GPO) that Tenable Identity Exposure creates to enable required events logging is linked to the organization unit (OU) domain controllers with Enforced mode enabled.

This gives the GPO a high priority, but an enforced GPO configured at a higher level (such as domain or site) takes precedence over it.

If the higher priority GPO that defines the Advanced Audit Policy Configuration settings conflicts with Tenable Identity Exposure’s needs, it takes precedence and Tenable Identity Exposure misses required events for attack detection.

Since Windows merges Advanced Audit Policy Configuration settings defined by GPOs, different GPOs can define different settings.

However, at each setting level, it only uses the GPO-defined value with the higher precedence. For example, Tenable Identity Exposure needs the Success and Failure value for the Audit Credential Validation setting. However, if a GPO with higher precedence only defines Success for Audit Credential Validation, then Windows only collects Success events and Tenable Identity Exposure misses the required Failure events.

To check for GPO precedence:

1. In the command-line interface, run the following command on a domain controller.

   It outputs the effective Advanced Audit Policy Configuration after considering all GPOs and precedence.

   ```
   auditpol.exe /get /category:*
   ```

2. Compare the output with the Tenable Identity Exposure advanced audit policy requirements. For each setting that Tenable Identity Exposure requires, check that the effective policy also covers it.

   - It is not an issue if the effective policy is more exhaustive, such as when Tenable Identity Exposure needs "Success" or "Failure" and the setting is "Success and Failure".

   - If the effective policy is insufficient, it means that a GPO with a higher precedence defines conflicting settings.

To fix the GPO precedence:

1. Look for GPOs linked to higher levels (domain or site) in "enforced" mode that define the Advanced Audit Policy Configuration.

2. In the command-line interface, run the following command on a domain controller to pinpoint the winning GPO:

   ```
   gpresult /scope:computer /h gpo.html
   ```

3. Modify the corresponding Advanced Audit Policy Configuration setting in the GPO to meet Tenable Identity Exposure's minimum requirements. For example:

   - If Tenable Identity Exposure requires "Success" and the higher priority GPO defines "Failure," then modify the setting to "Success and Failure."

   - If Tenable Identity Exposure requires "Success and Failure" and the higher priority GPO defines "Success," then modify the setting to "Success and Failure."

4. After you modify the setting, you can either wait for the updated GPO to apply or force it with the `gpupdate` command.

5. Repeat the procedure To check for GPO precedence: to check the new effective policy.

Event Logs Listener Validation

The Indicator of Attack installation script configures an event watcher and a Windows Management Instrumentation (WMI) Producer/Consumer in the machine's memory. WMI is a Windows component that provides you with information about the status of local or remote computer systems.

To check for correct WMI registration:

- In PowerShell, run the following command:

```
Get-WmiObject -Class '__FilterToConsumerBinding' -Namespace 'root\subscription' -Filter "Filter
= ""__EventFilter.name='AlsidForAD-Launcher'"""
```

- If at least one consumer exists, you obtain this type of output:

```
> Get-WmiObject -Class '__FilterToConsumerBinding' -Namespace 'root\subscription' -Filter
"Filter = ""__EventFilter.name='AlsidForAD-Launcher'"""


__GENUS                  : 2
__CLASS                  : __FilterToConsumerBinding
__SUPERCLASS             : __IndicationRelated
__DYNASTY                : __SystemClass
__RELPATH                : __
FilterToConsumerBinding.Consumer="ActiveScriptEventConsumer.Name=\"AlsidForAD-Launcher\"",F
                           ilter="__EventFilter.Name=\"AlsidForAD-Launcher\""
__PROPERTY_COUNT         : 7
__DERIVATION             : {__IndicationRelated, __SystemClass}
__SERVER                 : DC-999
__NAMESPACE              : ROOT\subscription
__PATH                   : \\DC-999\ROOT\subscription:__
FilterToConsumerBinding.Consumer="ActiveScriptEventConsumer.Name
                           =\"AlsidForAD-Launcher\"",Filter="__EventFilter.Name=\"AlsidForAD-
Launcher\""
Consumer                 : ActiveScriptEventConsumer.Name="AlsidForAD-Launcher"
CreatorSID               : {1, 1, 0, 0...}
DeliverSynchronously     : False
DeliveryQoS              :
Filter                   : __EventFilter.Name="AlsidForAD-Launcher"
MaintainSecurityContext : False
SlowDownProviders        : False
PSComputerName           : DC-999
```

  - If there is no registered WMI consumer, the command returns nothing.
  - This is a prerequisite for the process to run on the DC for WMI.

To retrieve the WMI process (for versions = or < 3.19):

- In PowerShell, run the following command:

```
gcim win32_process | Where-Object { $_.CommandLine -match "TenableADWMIListener"}
```

- Valid result example:

```
> gcim win32_process | Where-Object { $_.CommandLine -match "TenableADWMIListener"}

ProcessId Name           HandleCount WorkingSetSize VirtualSize
--------- ----           ----------- -------------- -----------
952       powershell.exe 502         26513408       2199678185472

```

To retrieve the event logs listener (for versions = or > 3.29):

- In PowerShell, run the following command:

```
gcim win32_process | Where-Object { $_.CommandLine -match "Register-
TenableADEventsListener.exe"}
```

- Valid result example:

```
PS C:\IOAInstall> gcim win32_process | Where-Object { $_.CommandLine -match "Register-
TenableADEventsListener.exe"}

ProcessId Name                                 HandleCount WorkingSetSize VirtualSize

5748      Register-TenableADEventsListener.exe 152         4096000        4384534528
```

Tenable Identity Exposure Log Files

If you still do not see Indicators of Attack alerts after you validate the GPO and WMI Consumer, you can review Tenable Identity Exposure's internal logs.

Ceti Log

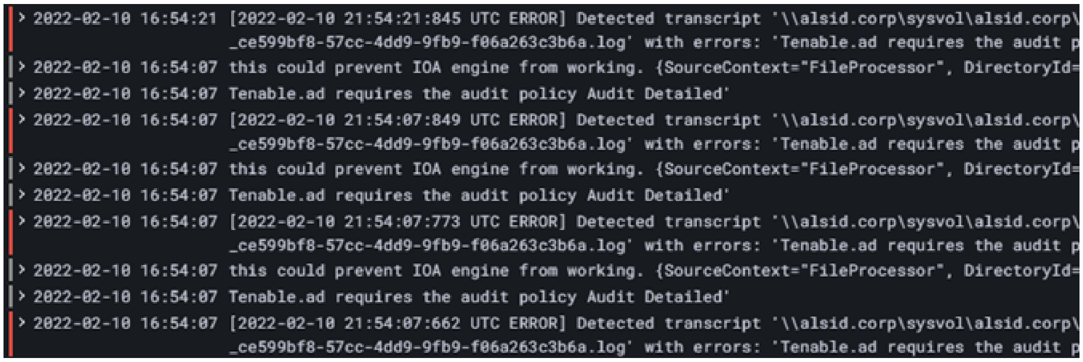
- Check for the following error message in the CETI Log:

  ```
  [2022-02-22 22:23:27:570 UTC WARNING] Some domain controllers are not generating IOA
  events: 'CORP-DC'. {SourceContext="DirectoryEventToCetiAdObjectMessageMapper",
  DirectoryId=2, Dns="corp.bank.com", Host="10.10.20.10", Source=SYSVOL, Version="3.11.5"}
  ```

- If you see this message, verify that the GPO settings and WMI consumer are running on the domain controller (DC) listed in the above error message.

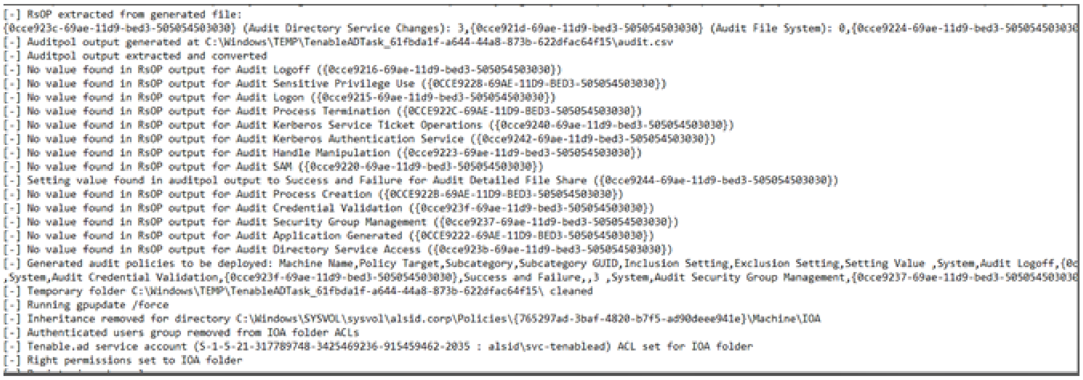
Audit settings

- If you see an error similar to the following one: "Tenable Identity Exposure requires the Audit Policy...", check your existing GPOs to ensure that you did not set the required audit policies to "No Auditing."

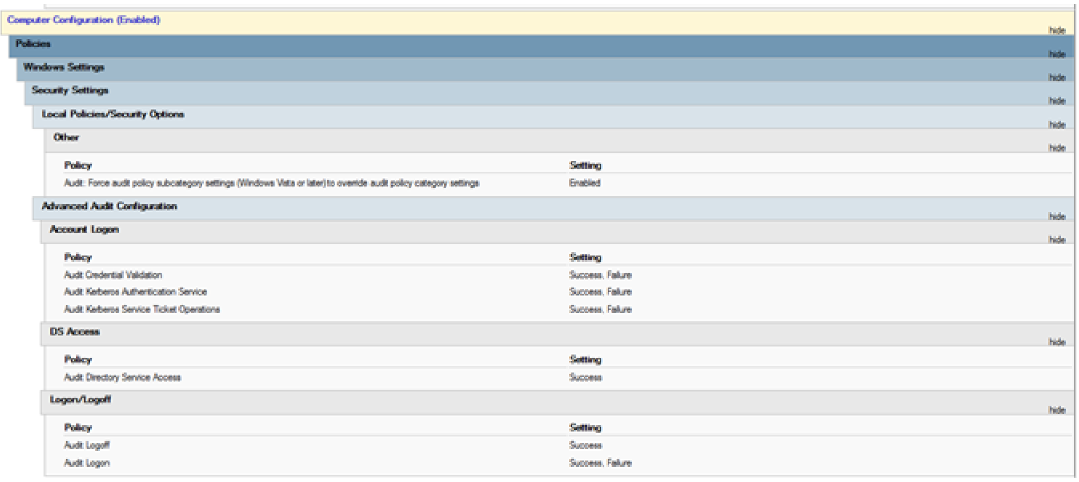
  ```
  > 2022-02-10 16:54:21 [2022-02-10 21:54:21:845 UTC ERROR] Detected transcript '\\alsid.corp\sysvol\alsid.corp\
                       _ce599bf8-57cc-4dd9-9fb9-f06a263c3b6a.log' with errors: 'Tenable.ad requires the audit p
  > 2022-02-10 16:54:07 this could prevent IOA engine from working. {SourceContext="FileProcessor", DirectoryId=
  > 2022-02-10 16:54:07 Tenable.ad requires the audit policy Audit Detailed'
  > 2022-02-10 16:54:07 [2022-02-10 21:54:07:849 UTC ERROR] Detected transcript '\\alsid.corp\sysvol\alsid.corp\
                       _ce599bf8-57cc-4dd9-9fb9-f06a263c3b6a.log' with errors: 'Tenable.ad requires the audit p
  > 2022-02-10 16:54:07 this could prevent IOA engine from working. {SourceContext="FileProcessor", DirectoryId=
  > 2022-02-10 16:54:07 Tenable.ad requires the audit policy Audit Detailed'
  > 2022-02-10 16:54:07 [2022-02-10 21:54:07:773 UTC ERROR] Detected transcript '\\alsid.corp\sysvol\alsid.corp\
                       _ce599bf8-57cc-4dd9-9fb9-f06a263c3b6a.log' with errors: 'Tenable.ad requires the audit p
  > 2022-02-10 16:54:07 this could prevent IOA engine from working. {SourceContext="FileProcessor", DirectoryId=
  > 2022-02-10 16:54:07 Tenable.ad requires the audit policy Audit Detailed'
  > 2022-02-10 16:54:07 [2022-02-10 21:54:07:662 UTC ERROR] Detected transcript '\\alsid.corp\sysvol\alsid.corp\
                       _ce599bf8-57cc-4dd9-9fb9-f06a263c3b6a.log' with errors: 'Tenable.ad requires the audit p
  ```

- If you get an error that states "RSOP...":



```
[-] RsOP extracted from generated file:
{0cce923c-69ae-11d9-bed3-505054503030} (Audit Directory Service Changes): 3,{0cce921d-69ae-11d9-bed3-505054503030} (Audit File System): 0,{0cce9224-69ae-11d9-bed3-505054503030
[-] Auditpol output generated at C:\Windows\TEMP\TenableADTask_61fbda1f-a644-44a8-873b-622dfac64f15\audit.csv
[-] Auditpol output extracted and converted
[-] No value found in RsOP output for Audit Logoff ({0cce9216-69ae-11d9-bed3-505054503030})
[-] No value found in RsOP output for Audit Sensitive Privilege Use ({0CCE9228-69AE-11D9-BED3-505054503030})
[-] No value found in RsOP output for Audit Logon ({0cce9215-69ae-11d9-bed3-505054503030})
[-] No value found in RsOP output for Audit Process Termination ({0CCE922C-69AE-11D9-BED3-505054503030})
[-] No value found in RsOP output for Audit Kerberos Service Ticket Operations ({0cce9240-69ae-11d9-bed3-505054503030})
[-] No value found in RsOP output for Audit Kerberos Authentication Service ({0cce9242-69ae-11d9-bed3-505054503030})
[-] No value found in RsOP output for Audit Handle Manipulation ({0cce9223-69ae-11d9-bed3-505054503030})
[-] No value found in RsOP output for Audit SAM ({0cce9220-69ae-11d9-bed3-505054503030})
[-] Setting value found in auditpol output to Success and Failure for Audit Detailed File Share ({0cce9244-69ae-11d9-bed3-505054503030})
[-] No value found in RsOP output for Audit Process Creation ({0CCE922B-69AE-11D9-BED3-505054503030})
[-] No value found in RsOP output for Audit Credential Validation ({0cce923f-69ae-11d9-bed3-505054503030})
[-] No value found in RsOP output for Audit Security Group Management ({0cce9237-69ae-11d9-bed3-505054503030})
[-] No value found in RsOP output for Audit Application Generated ({0CCE9222-69AE-11D9-BED3-505054503030})
[-] No value found in RsOP output for Audit Directory Service Access ({0cce923b-69ae-11d9-bed3-505054503030})
[-] Generated audit policies to be deployed: Machine Name,Policy Target,Subcategory,Subcategory GUID,Inclusion Setting,Exclusion Setting,Setting Value ,System,Audit Logoff,{0c
,System,Audit Credential Validation,{0cce923f-69ae-11d9-bed3-505054503030},Success and Failure,,3 ,System,Audit Security Group Management,{0cce9237-69ae-11d9-bed3-505054503030
[-] Temporary folder C:\Windows\TEMP\TenableADTask_61fbda1f-a644-44a8-873b-622dfac64f15\ cleaned
[-] Running gpupdate /force
[-] Inheritance removed for directory C:\Windows\SYSVOL\sysvol\alsid.corp\Policies\{765297ad-3baf-4820-b7f5-ad90deee941e}\Machine\IOA
[-] Authenticated users group removed from IOA folder ACLs
[-] Tenable.ad service account (S-1-5-21-317789748-3425469236-915459462-2035 : alsid\svc-tenablead) ACL set for IOA folder
[-] Right permissions set to IOA folder
```

- Check the audit policies and look at the transcript file in the Sysvol folder to see if you encountered any issues during the installation.



Computer Configuration (Enabled) hide

Policies hide

Windows Settings hide

Security Settings hide

Local Policies/Security Options hide

Other hide

Policy	Setting
Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings	Enabled

Advanced Audit Configuration hide

Account Logon hide

Policy	Setting
Audit Credential Validation	Success, Failure
Audit Kerberos Authentication Service	Success, Failure
Audit Kerberos Service Ticket Operations	Success, Failure

DS Access hide

Policy	Setting
Audit Directory Service Access	Success

Logon/Logoff hide

Policy	Setting
Audit Logoff	Success
Audit Logon	Success, Failure

Cygni Log

Cygni logs the attack and lists the specific `.gz` file that Tenable Identity Exposure called to generate the alert.

I-DCSync

```
2022-03-15 11:39:31
[2022-03-15 15:39:30:759 UTC INFORMATION] Anomaly 'ControlAccess' has been raised for Indicator 'I-DCSync' and Event '110052' {SourceContext="AttackEngine", CodeName="I-DCSync", ProfileId=4, AdObjectId="5:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\{08D6D98F-7455-464B-BBEC-23DE4BDF856C}\\Machine\\IOA\\dc-vm-10.0.17763-16_.gz", Event.Id=0, Version="3.16.0"}
```

I-GoldenTicket

```
2022-03-15 11:40:31
[2022-03-15 15:40:31:490 UTC INFORMATION] Anomaly 'Logon' has been raised for Indicator 'I-
GoldenTicket' and Event '110061' {SourceContext="AttackEngine", CodeName="I-GoldenTicket",
ProfileId=3, AdObjectId="5:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\{08D6D98F-7455-464B-BBEC-
23DE4BDF856C}\\Machine\\IOA\\dc-vm-10.0.17763-16_.gz", Event.Id=0, Version="3.16.0"}
```

I-ProcessInjectionLsass

```
022-03-15 12:47:09
[2022-03-15 16:47:09:811 UTC INFORMATION] Anomaly 'ProcessAccess' has been raised for Indicator 'I-
ProcessInjectionLsass' and Event '115948' {SourceContext="AttackEngine", CodeName="I-
ProcessInjectionLsass", ProfileId=1, AdObjectId="5:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\
{08D6D98F-7455-464B-BBEC-23DE4BDF856C}\\Machine\\IOA\\dc-vm-10.0.17763-16_.gz", Event.Id=0,
Version="3.16.0"}
```

I-DCShadow

```
2022-03-15 11:30:30
[2022-03-15 15:30:30:657 UTC INFORMATION] Anomaly 'ControlAccess' has been raised for Indicator 'I-
DCShadow' and Event '109948' {SourceContext="AttackEngine", CodeName="I-DCShadow", ProfileId=4,
AdObjectId="5:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\{08D6D98F-7455-464B-BBEC-
23DE4BDF856C}\\Machine\\IOA\\dc-vm-10.0.17763-16_.gz", Event.Id=0, Version="3.16.0"}
```

I-BruteForce

```
2022-03-15 08:02:11
[2022-03-15 12:02:11:231 UTC INFORMATION] Anomaly 'An account failed to log on' has been raised for
Indicator 'I-BruteForce' and Event '109082' {SourceContext="AttackEngine", CodeName="I-BruteForce",
ProfileId=6, AdObjectId="3:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\{765297AD-3BAF-4820-B7F5-
AD90DEEE941E}\\Machine\\IOA\\dc-vm-10.0.17763-8_.gz", Event.Id=0, Version="3.16.0"}
```

I-PasswordSpraying

```
2022-03-15 12:39:43
[2022-03-15 16:39:43:793 UTC INFORMATION] Anomaly 'An account failed to log on.' has been raised for
Indicator 'I-PasswordSpraying' and Event '115067' {SourceContext="AttackEngine", CodeName="I-
PasswordSpraying", ProfileId=4, AdObjectId="5:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\
{08D6D98F-7455-464B-BBEC-23DE4BDF856C}\\Machine\\IOA\\dc-vm-10.0.17763-16_.gz", Event.Id=0,
Version="3.16.0"}
```

I-PetitPotam

```
2022-03-15 12:43:02
[2022-03-15 16:43:02:737 UTC INFORMATION] Anomaly 'PetitPotamEFSError' has been raised for Indicator
'I-PetitPotam' and Event '115844' {SourceContext="AttackEngine", CodeName="I-PetitPotam",
ProfileId=4, AdObjectId="5:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\{08D6D98F-7455-464B-BBEC-
23DE4BDF856C}\\Machine\\IOA\\dc-vm-10.0.17763-16_.gz", Event.Id=0, Version="3.16.0"}
```

I-ReconAdminsEnum

```
022-03-15 12:55:31
[2022-03-15 16:55:31:638 UTC INFORMATION] Anomaly 'LocalAdmin enumeration (BloodHound/SharpHound).
Version 2016+' has been raised for Indicator 'I-ReconAdminsEnum' and Event '116085'
{SourceContext="AttackEngine", CodeName="I-ReconAdminsEnum", ProfileId=4,
AdObjectId="5:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\{08D6D98F-7455-464B-BBEC-
23DE4BDF856C}\\Machine\\IOA\\dc-vm-10.0.17763-16_.gz", Event.Id=0, Version="3.16.0"}
```

I-Kerberoasting

```
022-03-15 12:51:30
[2022-03-15 16:51:30:236 UTC INFORMATION] Anomaly 'Kerberos TGS requested on honey account' has been
raised for Indicator 'I-Kerberoasting' and Event '116013' {SourceContext="AttackEngine", CodeName="I-
Kerberoasting", ProfileId=3, AdObjectId="5:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\{08D6D98F-
7455-464B-BBEC-23DE4BDF856C}\\Machine\\IOA\\dc-vm-10.0.17763-16_.gz", Event.Id=0, Version="3.16.0"}
```

I-NtdsExtraction

```
2022-03-15 12:03:51
[2022-03-15 16:03:50:949 UTC INFORMATION] Anomaly 'Shadow copy created on 2012 and above' has been
raised for Indicator 'I-NtdsExtraction' and Event '111168' {SourceContext="AttackEngine",
CodeName="I-NtdsExtraction", ProfileId=4,
AdObjectId="5:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\{08D6D98F-7455-464B-BBEC-
23DE4BDF856C}\\Machine\\IOA\\dc-vm-10.0.17763-16_.gz", Event.Id=0, Version="3.16.0"}
```

Cephei Log

The following log entries validate that Cephei is writing attacks. The key value is the **attackTypeID** that specifies the type of attack which you can use to correlate with the Cygni entries:

I-DCSync attackTypeID:1

```
2022-03-15 11:39:52
2022-03-15T15:39:52.037023041Z stdout F [2022-03-15 15:39:52:035 UTC INFORMATION] [Equuleus] POST
```

```
http://equuleus:3004/attacks/write responded 204 in 32.16 ms : Request Body=
{"timestamp":"1647358722449","directoryId":5,"profileId":4,"attackTypeId":1,"count":1}
{SourceContext="Equuleus", Version="3.16.0"}
```

I-GoldenTicket attackTypeID:2

```
2022-03-15 11:40:52
2022-03-15T15:40:52.084931986Z stdout F [2022-03-15 15:40:52:084 UTC INFORMATION] [Equuleus] POST
http://equuleus:3004/attacks/write responded 204 in 24.6607 ms : Request Body=
{"timestamp":"1647358773608","directoryId":5,"profileId":4,"attackTypeId":2,"count":1}
{SourceContext="Equuleus", Version="3.16.0"}
```

I-ProcessInjectionLsass attackTypeID:3

```
2022-03-15 12:47:52
2022-03-15T16:47:52.29927328Z stdout F [2022-03-15 16:47:52:298 UTC INFORMATION] [Equuleus] POST
http://equuleus:3004/attacks/write responded 204 in 35.7532 ms : Request Body=
{"timestamp":"1647362812784","directoryId":5,"profileId":1,"attackTypeId":3,"count":2}
{SourceContext="Equuleus", Version="3.16.0"}
```

I-DCShadow attackTypeID:4

```
2022-03-15 11:30:52
2022-03-15T15:30:51.949399295Z stdout F [2022-03-15 15:30:51:944 UTC INFORMATION] [Equuleus] POST
http://equuleus:3004/attacks/write responded 204 in 24.2605 ms : Request Body=
{"timestamp":"1647358182800","directoryId":5,"profileId":3,"attackTypeId":4,"count":1}
{SourceContext="Equuleus", Version="3.16.0"}
```

I-BruteForce attackTypeID:5

```
2022-03-15 08:02:54
2022-03-15T12:02:54.698814039Z stdout F [2022-03-15 12:02:54:698 UTC INFORMATION] [Equuleus] POST
http://equuleus:3004/attacks/write responded 204 in 30.7623 ms : Request Body=
{"timestamp":"1647345728023","directoryId":3,"profileId":6,"attackTypeId":5,"count":1}
{SourceContext="Equuleus", Version="3.16.0"}
```

I-PasswordSpraying attackTypeID:6

```
2022-03-15 12:39:52
2022-03-15T16:39:52.187309945Z stdout F [2022-03-15 16:39:52:186 UTC INFORMATION] [Equuleus] POST
http://equuleus:3004/attacks/write responded 204 in 21.9422 ms : Request Body=
{"timestamp":"1647362356837","directoryId":5,"profileId":4,"attackTypeId":6,"count":1}
{SourceContext="Equuleus", Version="3.16.0"}
```

I-PetitPotam attackTypeID:7

```
022-03-15 12:43:52
2022-03-15T16:43:52.226125918Z stdout F [2022-03-15 16:43:52:223 UTC INFORMATION] [Equuleus] POST
http://equuleus:3004/attacks/write responded 204 in 15.8402 ms : Request Body=
{"timestamp":"1647362570534","directoryId":5,"profileId":1,"attackTypeId":7,"count":1}
{SourceContext="Equuleus", Version="3.16.0"}
```

I-ReconAdminsEnum attackTypeID:8

```
2022-03-15 12:55:52
2022-03-15T16:55:52.399889635Z stdout F [2022-03-15 16:55:52:399 UTC INFORMATION] [Equuleus] POST
http://equuleus:3004/attacks/write responded 204 in 40.6632 ms : Request Body=
{"timestamp":"1647363305295","directoryId":5,"profileId":4,"attackTypeId":8,"count":1}
{SourceContext="Equuleus", Version="3.16.0"}
```

I-Kerberoasting attackTypeID:10

```
2022-03-15 12:51:52
2022-03-15T16:51:52.352432644Z stdout F [2022-03-15 16:51:52:351 UTC INFORMATION] [Equuleus] POST
http://equuleus:3004/attacks/write responded 204 in 21.0547 ms : Request Body=
{"timestamp":"1647363026345","directoryId":5,"profileId":4,"attackTypeId":10,"count":1}
{SourceContext="Equuleus", Version="3.16.0"}
```

I-NtdsExtraction attackTypeID:11

```
022-03-15 12:03:52
2022-03-15T16:03:52.137547488Z stdout F [2022-03-15 16:03:52:137 UTC INFORMATION] [Equuleus] POST
http://equuleus:3004/attacks/write responded 204 in 13.0304 ms : Request Body=
{"timestamp":"1647360224606","directoryId":5,"profileId":4,"attackTypeId":11,"count":1}
{SourceContext="Equuleus", Version="3.16.0"}
```

Electra Log

You should see the following entry:

[2022-03-15T14:04:39.151Z] INFO: server/4016 on WIN-UQRSCEN0CI3: Message received from MQ: attack-alert (namespace=electra)

```
[2022-03-15T14:04:39.151Z]  INFO: server/4016 on WIN-UQRSCEN0CI3: Message received from MQ: attack-
alert (namespace=electra)
[2022-03-15T14:04:39.168Z]  INFO: server/4016 on WIN-UQRSCEN0CI3: Sending ws message to listeners.
alertIoA (namespace=electra)
```

Eridanis Log

You should see the following entry:

```
022-03-15T14:04:39.150Z]  INFO: server/4988 on WIN-UQRSCEN0CI3: KAPTEYN get /attack-alerts/2010 200
122 - 7ms (namespace=hapi)
[2022-03-15T14:04:39.165Z]  INFO: server/4988 on WIN-UQRSCEN0CI3: notifyAttackAndAttackAlertCreation
success { attackId: 2011 } (namespace=eridanis)
[2022-03-15T14:04:39.170Z]  INFO: server/4988 on WIN-UQRSCEN0CI3: KAPTEYN get /attack-alerts/2011 200
122 - 6ms (namespace=hapi)
```

DFS Replication Issues Mitigation

An additional parameter, `-EventLogsFileWriteFrequency X`, in the Indicator of Attack deployment script allows you to address potential issues with slow or broken Distributed File System (DFS) replication that you may experience.

This parameter is optional and Tenable recommends using it only if you are experiencing DFS replication issues or have noticed them since deploying the IoA script. Under normal circumstances, the parameter remains at its default value and you do not need to include it in the command line when running the script.

When to modify the parameter

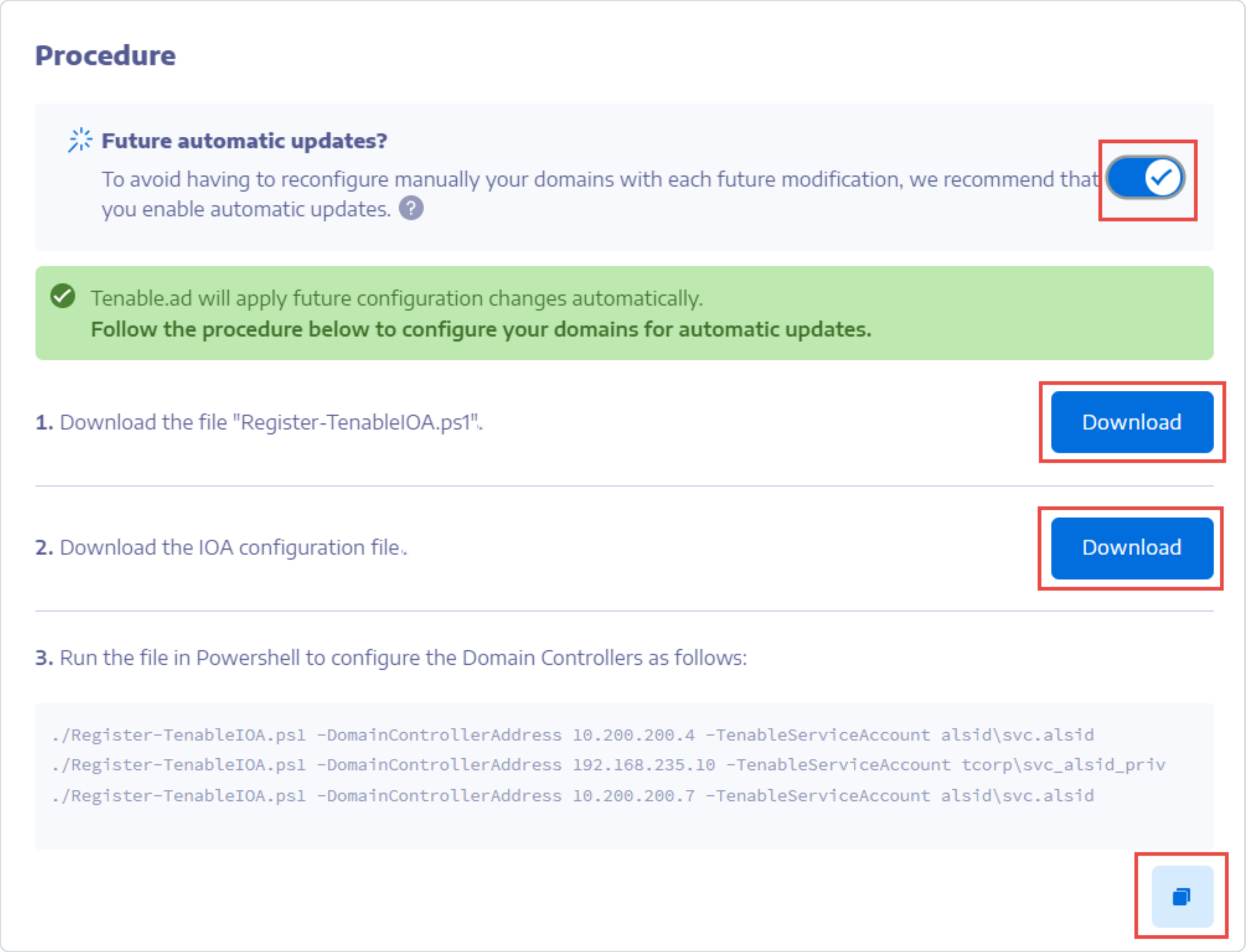
The value [`X`] of the parameter `-EventLogsFileWriteFrequency X` is the frequency at which the Tenable Identity Exposure listener generates an event logs file on non-PDCe domain controllers (DCs). The default and recommended value that the Tenable Identity Exposure listener uses is 15 seconds. However, the customized value does not apply to PDCe DCs and remains at its default 15-second interval to ensure that attack detection capabilities are fully operational. Tenable recommends using this parameter and increasing its value beyond its default 15-second value to up to 300 seconds (5 minutes) only if your infrastructure faces or is prone to DFS replication issues.

Recommendations

Be aware that increasing the event log file write frequency will generate the file less often, thereby increasing the delay in attack detection (for example, if the file generates every 30 seconds instead of the default 15 seconds on non PDCe DCs). Also, increasing the delay augments the size of the generated event logs file within set limits as defined in Technical Changes and Potential Impact. Therefore, use this parameter only as a mitigation strategy and not as a replacement for proper investigation of DFS replication issues.

To apply the parameter:

1. Configure your domains for IoAs as described in the procedure. For more information, see Install Indicators of Attack.



Procedure

Future automatic updates? ✓

To avoid having to reconfigure manually your domains with each future modification, we recommend that you enable automatic updates. ?

Tenable.ad will apply future configuration changes automatically.
Follow the procedure below to configure your domains for automatic updates.

1. Download the file "Register-TenableIOA.ps1".

2. Download the IOA configuration file.

3. Run the file in Powershell to configure the Domain Controllers as follows:

```
./Register-TenableIOA.ps1 -DomainControllerAddress 10.200.200.4 -TenableServiceAccount alsid\svc.alsid
./Register-TenableIOA.ps1 -DomainControllerAddress 192.168.235.10 -TenableServiceAccount tcorp\svc_alsid_priv
./Register-TenableIOA.ps1 -DomainControllerAddress 10.200.200.7 -TenableServiceAccount alsid\svc.alsid
```

2. Open a PowerShell terminal with administrative rights.

3. Run the script to configure your domain controllers for IoAs and append the `-EventLogsFileWriteFrequency X` parameter, where [X] is the frequency you want to set for the event logs file frequency.

Authentication

There are several ways to authenticate Tenable Identity Exposure users:

- Authentication Using a Tenable Identity Exposure Account
- Authentication Using LDAP
- Authentication Using SAML

Authentication using Tenable One

Required license: Tenable One

Note: With a Tenable One license, you manage all your authentication settings in Tenable Vulnerability Management. For more information, see Access Control in the *Tenable Vulnerability Management User Guide*.

To configure authentication using Tenable One:

1. In Tenable Identity Exposure, click **Systems** > **Configuration**.

   The configuration pane appears.

2. Under the **Authentication** section, click **Tenable One**.

3. In the **Default profile** drop-down box, select the profile for the user.

4. In the **Default roles** box, select the roles for the user.

   Tip: Authenticated users in Tenable One who have not connected previously to Tenable Identity Exposure automatically have an account when they log in to Tenable Identity Exposure. The default profile and default role apply to the user by default. **Exception**: Users with the "Administrator" role in Tenable Vulnerability Management also have the "Global Administrator" role in Tenable Identity Exposure.

5. Click **Save**.

Authentication Using a Tenable Identity Exposure Account

The simplest authentication method is through a Tenable Identity Exposure account that requires a username and a password.

This authentication method offers a default lockout policy, a security control designed to mitigate brute force attacks against authentication mechanisms. It locks out user accounts after too many failed login attempts. When an account is locked, users do not have access to Tenable Identity Exposure APIs.

To configure authentication using a Tenable Identity Exposure account:

1. In Tenable Identity Exposure, click **Systems** > **Configuration**.

   The configuration pane appears.

2. Under the **Authentication** section, click **Tenable Identity Exposure**.

3. In the **Default profile** drop-down box, select the profile for the user.

4. In the **Default roles** box, select the roles for the user.

5. Configure the lockout policy settings:

Setting	Description	Default Value
Enabled	- **Enabled** — Tenable Identity Exposure blocks the account after a set number of failed login attempts. - **Disabled** — Tenable Identity Exposure does not lock the account after failed login attempts.	Enabled
Lockout duration	The time duration that Tenable Identity Exposure locks the account from any login attempts. Tenable Identity Exposure automatically unlocks the account after this time elapses to allow the user to attempt to log in again. To configure the lockout duration: 1. Click on the slider to set a lockout duration. 2. Select **Infinite** if you do not want to unlock the account automatically after a set duration. **Note**: If all the accounts within the 'Global Administrator' group become locked, Tenable Identity Exposure unlocks the default administrative account after 10 seconds.	300 seconds
Number of attempts before lockout	The number of failed login attempts before Tenable Identity Exposure locks the account.	3
Redemption period	The time interval during which Tenable Identity Exposure counts the number of unsuccessful login attempts. After a specified number of unsuccessful login attempts, Tenable Identity Exposure locks the	900 seconds

	account. To set the redemption period: 1. Click on the slider to set a time interval. 2. Select "Infinite" if you do not want to set a time interval to count unsuccessful login attempts before Tenable Identity Exposure locks the account.	

6. Click **Save**.

To disable the lockout policy:

1. In Tenable Identity Exposure, click **Systems** > **Configuration**.

   The configuration pane appears.

2. Click the **Enabled** toggle to turn off the lockout policy.

Note: If you disable the lockout policy, locked user accounts can attempt to reconnect.

To view the list of locked accounts:

- In Tenable Identity Exposure, go to **Accounts** > **User accounts management**.

  In the list of users, Tenable Identity Exposure displays the locked accounts with a red padlock icon. Tenable Identity Exposure displays the following message to users with locked accounts: "Your account is blocked due to too many failed authentication attempts. You have to contact an administrator."

To unlock an account:

You must have permissions to edit users in order to unlock accounts.

1. In Tenable Identity Exposure, click **Accounts** > **User accounts management**.

   The user accounts management pane appears.

2. In the list of users, locate the locked account.

3. Click the pencil icon to edit the locked user account.

   The user's information pane appears.

4. Click the **Remove lockout** button.

To grant permissions to user roles to configure the lockout policy:

1. In Tenable Identity Exposure, click **Accounts** > **Roles management**.

   The **Roles management** pane appears.

2. Click the pencil icon next to a role name to edit the role.

   The **Edit a role** pane appears.

3. Click the **System configuration entities** tab.

4. Under the **Permissions Management** section, select the **Accounts Lockout Policy** checkbox.

5. Click the toggle to **Unauthorized** or **Granted**.

   A message confirms that Tenable Identity Exposure updated the user's permissions.

   > **Note**: Tenable Identity Exposure disables the lockout policy settings for users who only have read permission in this pane.

Authentication Using LDAP

Tenable Identity Exposure allows you to authenticate using Lightweight Directory Access Protocol (LDAP).

To enable LDAP authentication, you must have the following:

- A preconfigured service account with a user and password to access the Active Directory.
- A preconfigured Active Directory group.

After you set up LDAP authentication, the LDAP option appears in a tab on the login page.

To configure LDAP authentication:

1. In Tenable Identity Exposure, click **Systems** > **Configuration**.

   The configuration pane appears.

2. Under the **Authentication** section, click **LDAP**.

3. Click the **Enable LDAP authentication** toggle to enabled.

   An LDAP information form appears.

4. Provide the following information:

   - In the **Address of the LDAP server** box, type the LDAP server's IP address beginning with `ldap://` and ending with the domain name and port number.

     > **Note**: If you use an LDAPS server, type its address beginning with `ldaps://` and ending with the domain name and port number. See the procedure To add a custom trusted Certificate Authorities (CA) certificate for LDAPS: to complete the configuration for LDAPS.

   - In the **Service account use to query the LDAP server** box, type the Distinguished Name (DN), SamAccountName, or UserPrincipalName that you use to access the LDAP server.

   - In the **Service account password** box, type the password for this service account.

   - In the **LDAP search base** box, type the LDAP directory that Tenable Identity Exposure uses to search for users who attempt to connect, beginning with `DC=` or

OU=. This can be a root directory or a specific organizational unit.

    - In the **LDAP search filter** box, type the attribute that Tenable Identity Exposure uses to filter users. A standard attribute for authentication in Active Directory is `sAMAccountname={{login}}`. The value for `login` is the value that user provides during authentication.

5. For **Enable SASL bindings**, do one of the following:

    - If you use SamAccountName for the service account, click the **Enable SASL bindings** toggle to enabled.

    - If you use the Distinguished Name or UserPrincipalName for the service account, leave the **Enable SASL bindings** as disabled.

6. Under the **Default Profile and Roles** section, click **Add an LDAP group** to specify the groups allowed to authenticate.

    An LDAP group information form appears.

    - In the **LDAP group name** box, type the distinguished name of the group (example: `CN=TAD_User`,`OU=Groups`,`DC=Tenable,DC=ad`)

    - In the **Default profile** drop-down box, select the profile for the allowed group.

    - In the **Default roles** box, select the roles for the allowed group.

7. If necessary, click on the ⊕ icon to add a new allowed group.

8. Click **Save**.

To add a custom trusted Certificate Authorities (CA) certificate for LDAPS:

1. In Tenable Identity Exposure, click **Systems**.

2. Click the **Configuration** tab to display the configuration pane.

3. Under the **Application Services** section, click **Trusted Certificate Authorities**.

4. In the **Additional CA certificates** box, paste your company's PEM-encoded trusted CA certificate for Tenable Identity Exposure to use.

5. Click **Save**.

For more information about security profiles and roles, see:

- Security Profiles
- User Roles

Authentication Using SAML

You can configure SAML authentication so that Tenable Identity Exposure users can use identity provider-initiated single sign-on (SSO) when logging into Tenable Identity Exposure.

Before you begin:

- Review the Tenable SAML Configuration Quick-Reference guide for a step-by-step guide of how to configure SAML for use with Tenable Identity Exposure.
- Check that you have the following for the identity provider (IDP):
  - SAML v2 only.
  - "Assertion encryption" is enabled.
  - IDP groups that Tenable Identity Exposure uses to grant access to in the Tenable Identity Exposure web portal.
  - URL of the SAML server.
  - Trusted Certificate Authority (CA) that signed the SAML server certificate in PEM-encoded format, beginning with `-----BEGIN CERTIFICATE -----` and ending with `-----END CERTIFICATE -----`.

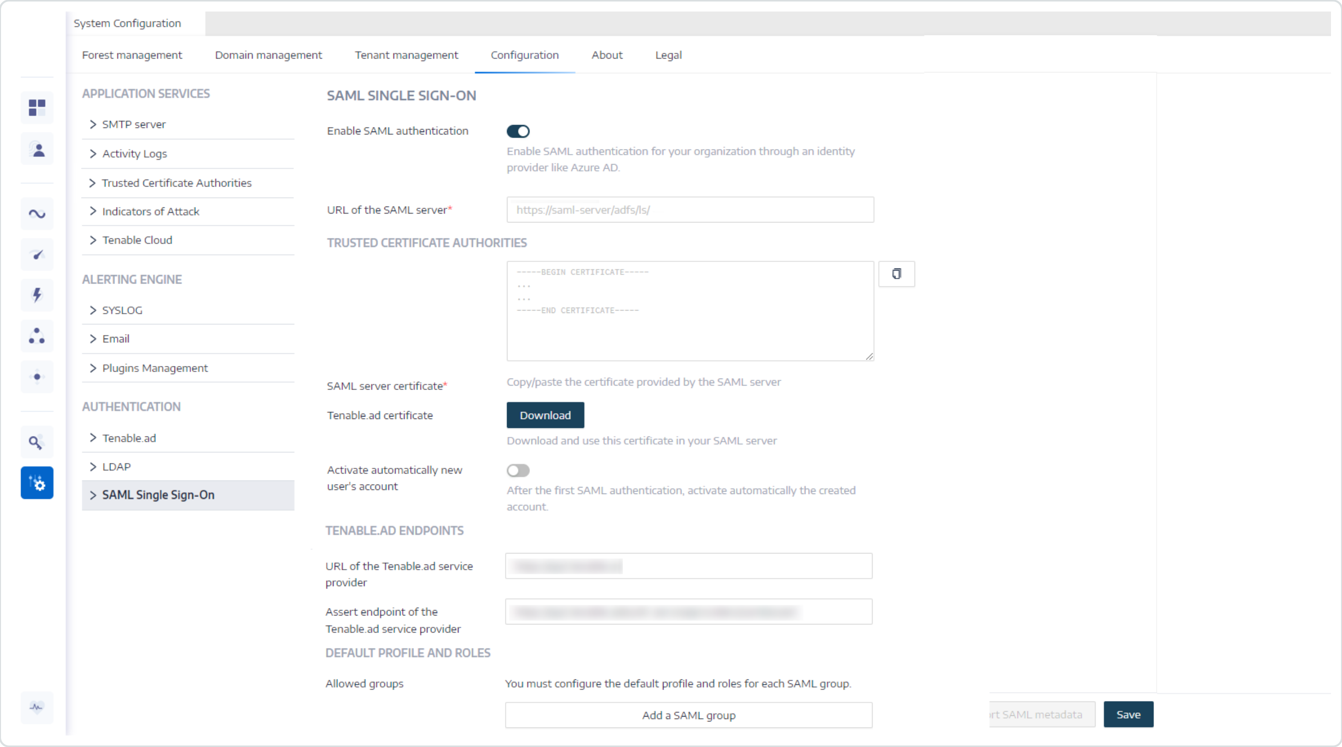
To configure SAML authentication:

1. In Tenable Identity Exposure, click **Systems** > **Configuration**.

   The configuration pane appears.

2. Under the **Authentication** section, click **SAML Single Sign-on**.
3. Click the **Enable SAML authentication** toggle.

   A SAML information form appears.



SAML SINGLE SIGN-ON

Enable SAML authentication ●

Enable SAML authentication for your organization through an identity provider like Azure AD.

URL of the SAML server* https://saml-server/adfs/ls/

TRUSTED CERTIFICATE AUTHORITIES

```
-----BEGIN CERTIFICATE-----
...
...
-----END CERTIFICATE-----
```

SAML server certificate* Copy/paste the certificate provided by the SAML server

Tenable.ad certificate Download

Download and use this certificate in your SAML server

Activate automatically new user's account ○

After the first SAML authentication, activate automatically the created account.

TENABLE.AD ENDPOINTS

URL of the Tenable.ad service provider [redacted]

Assert endpoint of the Tenable.ad service provider [redacted]

DEFAULT PROFILE AND ROLES

Allowed groups You must configure the default profile and roles for each SAML group.

4. Provide the following information:

   - In the **URL of the SAML server** box, type the full URL of the IDP's SAML server where Tenable Identity Exposure must connect.

   - In the **Trusted Certificate Authorities** box, paste the CA that signed the certificate from the SAML server.

5. In the **Tenable Identity Exposure certificate** box, click **Generate and Download**. This generates a new self-signed certificate, updates the SAML configuration in the database, and returns a new certificate for you to download.

   > **Caution**: When you click this button, it disrupts your SAML configuration because Tenable Identity Exposure expects the IDP to authenticate immediately with the most recently generated certificate while the IDP is still using a previous certificate, if it exists. If you generate a new Tenable Identity Exposure certificate, you must reconfigure your IDP to use the new certificate.

6. Click the **Activate automatically new user's account** toggle to activate new user accounts after the first SAML login.

7. Under **Tenable Identity Exposure Endpoints**, provide the following information:

    - URL of the Tenable Identity Exposure service provider

    - Assert endpoint of the Tenable Identity Exposure service provider

8. Under the **Default Profile and Roles** section, click **Add a SAML group** to specify the groups allowed to authenticate.

   A SAML group information form appears.

9. Provide the following information:

    - In the **SAML group name** box, type the name of the allowed group as it appears in the SAML server.

    - In the **Default profile** drop-down box, select the profile for the allowed group.

    - In the **Default roles** box, select the roles for the allowed group.

10. If necessary, click on the ⊕ icon to add a new allowed group.

11. Click **Save**.

    After you set up SAML authentication, the SAML option appears in a tab on the login page.

For more information about security profiles and roles, see:

- Security Profiles

- User Roles

User Accounts

The **Users Accounts Management** page provides the ability to add, edit, delete, or view the details of Tenable Identity Exposure user accounts.

Users belongs to two categories:

- Global Administrator — An administrator role that includes all permissions.
- User — A simple user role with read-only permissions over business data only.

For more information, see:

- Create a User
- Edit a User
- Deactivate a User
- Delete a User

Create a User

Required User Role: Administrator or organizational user with appropriate permissions.

Note: The following instructions apply to standalone instances of Tenable Identity Exposure. For instances linked to Tenable Vulnerability Management, you create users in Tenable Vulnerability Management which subsequently propagate to Tenable Identity Exposure.

To create a user:

1. In Tenable Identity Exposure, click **Accounts** > **User accounts management**.

   The **User accounts management** pane appears.

2. Click the **Create a user** button on the right.

   The **Create a user** pane appears.

3. Under the **Main Information** section, type the following information about the user:

   - First name
   - Surname (last name)
   - Email
   - Password: requires at least 12 characters with at least: 1 lowercase, 1 uppercase, 1 number, and 1 special character
   - Password confirmation
   - Department
   - Biography

4. Click the toggle **Allow authentication** to activate the user.

5. Under the **Roles Management** section, select a role to apply to the user.

6. Click **Create**.

   A message confirms that Tenable Identity Exposure created the user with the selected role.

See also

- Edit a User
- Deactivate a User
- Delete a User

Edit a User

Required User Role: Administrator or organizational user with appropriate permissions.

To edit a user:

1. In Tenable Identity Exposure, click **Accounts** > **User accounts management**.

   The **User accounts management** pane appears.

2. In the list of users, hover over the line where the user's name appears and click the ✎ icon at the end of the line.

   The **Edit a user** pane appears.

3. Under the **Main Information** section, modify the information about the user as needed:

   - First name
   - Surname (last name)
   - Email
   - Password: requires at least 8 characters
   - Password confirmation
   - Department
   - Biography

4. Under the **Roles Management** section, modify the user's role as needed.

5. Click **Edit**.

   A message confirms that Tenable Identity Exposure updated the user with the selected role.

See also

- Create a User
- Deactivate a User
- Delete a User

Deactivate a User

Required User Role: Administrator or organizational user with appropriate permissions.

To deactivate a user:

1. In Tenable Identity Exposure, click **Accounts** > **User accounts management**.

   The **User accounts management** pane appears.

2. In the list of users, hover over the line where the user's name appears and click the ✎ icon at the end of the line.

   The **Edit a user** pane appears.

3. Click the toggle **Allow authentication** to deactivate the user.

4. Click **Edit**.

   A message confirms that Tenable Identity Exposure updated the user.

See also

- Create a User
- Edit a User
- Delete a User

Delete a User

Required User Role: Administrator or organizational user with appropriate permissions.

To delete a user:

1. In Tenable Identity Exposure, click **Accounts** > **User accounts management**.

   The **User accounts management** pane appears.

2. In the list of users, hover over the line where the name of the user you want to delete appears and click the 🗑 icon at the end of the line.

   A message asks you to confirm the deletion.

3. Click **Delete**.

   A message confirms that Tenable Identity Exposure deleted the user.

See also

- Create a User
- Edit a User
- Deactivate a User

Security Profiles

Required User Role: Administrator or organizational user with appropriate permissions.

Profiles allow you to create and customize your own view of risks affecting your Active Directory.

Each profile shows exposure and attack scenarios configured for users with that profile. For example, an IT administrator's general view of the data analysis can be different from that of the Security team, which shows a comprehensive view of all the risks that AD infrastructures face.

Applying a security profile allows different types of users to review the data analysis from different reporting angles, as defined by the indicators for that security profile.

The Security Profiles Management pane allows you to maintain different types of users who can review security analysis from different reporting angles. Security profiles also allow you to customize the behavior of indicators of exposure and indicators of attack.

Note: Tenable Identity Exposure provides a default security profile called "Tenable". **You cannot modify or delete the Tenable profile**, but you can use it as a template to create other security profiles with adjusted settings according to your needs.

To create a new security profile:

1. In Tenable Identity Exposure, click **Accounts** > **Security profiles management**.

   The **Security profiles management** pane appears.

2. Click the **Create a profile** button on the right.

   The **Create a profile** pane appears.

3. From the Action drop-down box, you can either:

   - **Create a new profile**.

   - **Copy** an existing security profile from which you can create a new profile (for example, the "Tenable" profile.)

4. In the **Name of the new profile** box, type a name for the new profile.

   Note: Tenable Identity Exposure only accepts alphanumeric characters and underscores.

5. Click the **Create** button in the lower-right corner.

   A message indicates that Tenable Identity Exposure created the profile. The **Profile Configuration** pane appears.

To delete a security profile:

1. In Tenable Identity Exposure, click **Accounts** > **Security profiles management**.

   The **Security profiles management** pane appears.

2. In the list of security profiles, hover over the security profile you want to delete and click on the 🗑 icon at the end of the line.

   A message asks you to confirm the deletion.

3. Click **Delete**.

   A message confirms that Tenable Identity Exposure deleted the profile.

What to do next

To complete the profile creation, see Customize an Indicator for more information.

For more information, see:

- Customize an Indicator
- Refine Customization on an Indicator

Customize an Indicator

> **Required User Role**: Administrator or organizational user with appropriate permissions.

You can customize Indicators of Exposure and Indicators of Attack for a security profile.

Each security profile operates independently to ensure that one profile does not impact the results of another. You should use the "Tenable" profile solely as a reference, as you cannot customize it or use it to whitelist deviances. You must create your own custom profiles to fulfill specific requirements.

The term "Global customization" on the indicator customization pane **pertains to all domains** rather than all profiles. Consequently, any settings that you apply to the "Global customization" for one security profile do not influence the "Tenable" profile or another profile.

> **Tip**: To view the settings for the "Tenable" security profile, click on the 👁 icon at the end of the line.

To customize an indicator:

1. In Tenable Identity Exposure, click **Accounts** > **Security profiles management**.

   The **Security profiles management** pane appears.

2. In the list of security profiles, hover over the security profile that contains the indicator you want to customize. Click on the ✎ icon at the end of the line where the security profile file name appears.

   The **Profile configuration** pane appears.

3. Select the tab for **Indicators of Exposure** or **Indicators of Attack**.

4. (Optional) In the **Search an indicator** box, type an indicator name.

5. Click the name of the indicator to customize.

   The **Indicator Customization** pane appears.

6. Make the necessary customization to the indicator.

   > **Note**: Certain indicator options require the use of regular expressions (regex). Regex is a 'contain' match instead of an 'equal' match. Example: When you provide "`admin`" as the input option, you can

> whitelist a user with "`samAccountName=admin`" as well as a user with "`samAccountName=admintoto`".
> - To get an exact match, you must use Regex special characters (`"^...$"`) syntax.
> - You must also escape special characters with a backslash when using regex. Example: To declare `"domain\user"` and "`CN=Vincent C (Test)`,`DC=tenable,DC=corp`", you type `"domain\\user"` and `"CN=Vincent C. \(Test\),DC=tenable,DC=corp"`.

7. Click **Save as draft**.

   A message confirms that Tenable Identity Exposure saved the customization options.

To apply the customization:

1. You can either:

   - In the **Profile configuration** pane, click **Apply pending customization** in the lower-right corner, or
   - In the **Security profiles management** pane, click the ✓ icon at the end of the line where the name of the security profile appears.

   A message appears to warn you that applying the customization erases all its data and requires a complete analysis of the monitored Active Directory, which can take some time.

2. Click **OK**.

   A message confirms that Tenable Identity Exposure applied the customization options. In the *Security analysis* column in the **Security profiles managementt** table, **Waiting** indicates that the analysis according to your security profile is waiting to be run.

To discard the customization:

- You can either:
  - In the **Profile configuration** pane, click **Revert pending customization** in the lower-left corner, or
  - In the **Security profiles management** pane, click the ↺ icon at the end of the line where the name of the security profile appears.

  A message confirms that Tenable Identity Exposure canceled the customization options.

See also

- Refine Customization on an Indicator

Refine Customization on an Indicator

Required User Role: Administrator or organizational user with appropriate permissions.

Additional customization on an indicator for a security profile allows you to select indicator options for specific domains. By default, the global customization applies to all domains.

To refine the customization on an indicator:

1. In Tenable Identity Exposure, click **Accounts** > **Security profiles management**.

   The **Security profiles management** pane appears.

2. In the list of security profiles, hover over the security profile that contains the indicator you want to customize. Click on the ✎ icon at the end of the line where the security profile file name appears.

   The **Profile configuration** pane appears.

3. Select the tab for **Indicators of Exposure** or **Indicators of Attack**.

4. (Optional) In the **Search an indicator** box, type an indicator name.

5. Click the name of the an indicator to customize.

   The **Indicator Customization** pane appears.

6. Next to the **Global customization** tab, click the + icon.

   A **Customization No. 1** tab appears.

7. Click the **Apply on** box.

   The **Forests and Domains** pane appears.

8. (Optional) In the search box, type the forest or domain name.

9. Select the domain.

10. Click **Filter on selection**.

11. Make further customization as needed to the indicator for the selected domain.

12. Click **Save as draft**.

To discard the refined customization:

1. Click on tab for the customization.
2. Click **Remove this configuration** at the bottom of the pane.

See also

- Customize an Indicator

User Roles

Tenable Identity Exposure uses Role-Based Access Control (RBAC) to secure access to data and functions within your organization. Roles determine the type of information that a user can access from their account depending on their role.

Users with appropriate permissions can assign permissions to other users based on their role to perform the following actions:

- Read contents and menus, system, and Indicator of Exposure configurations.
- Edit contents and menus, system and Indicator of Attack configurations.
- Create accounts, security profiles, and roles.

See also

- Manage Roles
- Set Permissions for a Role
- Set Permissions on User Interface Entities (Example)

Manage Roles

To create a new role:

1. In Tenable Identity Exposure, go to **Accounts** > **Roles management**.
2. Click the **Create a role** button in the upper-right corner.

   The **Create a role** pane appears.
3. In the Name box, type the name for the role.
4. In the Description box, type some information about the role.
5. Click **Add** in the lower-right corner.

   A message appears confirms that Tenable Identity Exposure created the role. The **Edit a role** pane appears for you to set permissions for the role.

> **Note**: You cannot modify the Tenable Identity Exposure administrator role (called Global administrator). Click on the 👁 icon to display the Tenable Identity Exposure role settings.

To delete a role:

1. In Tenable Identity Exposure, go to **Accounts** > **Roles management**.
2. In the list of roles, hover over the role you want to delete and click the 🗑 icon on the right.

   A message asks you to confirm the deletion.
3. Click Delete.

   A message appears to confirm the deletion of the role.

See also

- Set Permissions for a Role

Set Permissions for a Role

Required User Role: Administrator or organizational user with appropriate permissions.

Tenable Identity Exposure uses Role-Based Access Control (RBAC) to secure access to its data. A role determines what type of information users can access depending on their functional roles in the organization. When you create a new user in Tenable Identity Exposure, you assign that user a specific role with its associated permissions.

To set permissions for a role:

1. In Tenable Identity Exposure, click **Accounts** > **Roles management**.
2. Hover over the role for which you want to set permissions and click the ✎ icon on the right.

   The **Edit a role** pane appears.
3. Under **Permissions Management**, select an entity type:
   - Data Entities
   - User Entities
   - System Configuration Entities
   - Interface Entities
4. In the list of entity names, select the entity to set permissions on.
5. Under the columns **Read**, **Edit**, or **Create**, click the toggle to Granted or Unauthorized.
6. You can either:
   - Click Apply to apply the permission and keep the **Edit a role** pane open for further modifications.
   - Click Apply and close to apply the permission and close the **Edit a role** pane.

   A message confirms that Tenable Identity Exposure updated the role.

To set permissions in bulk for a role:

1. In Tenable Identity Exposure, click **Accounts** > **Roles management**.

2. Hover over the role for which you want to set permissions and click the ✎ icon on the right.

   The **Edit a role** pane appears.

3. Under **Permissions Management**, select an entity type.

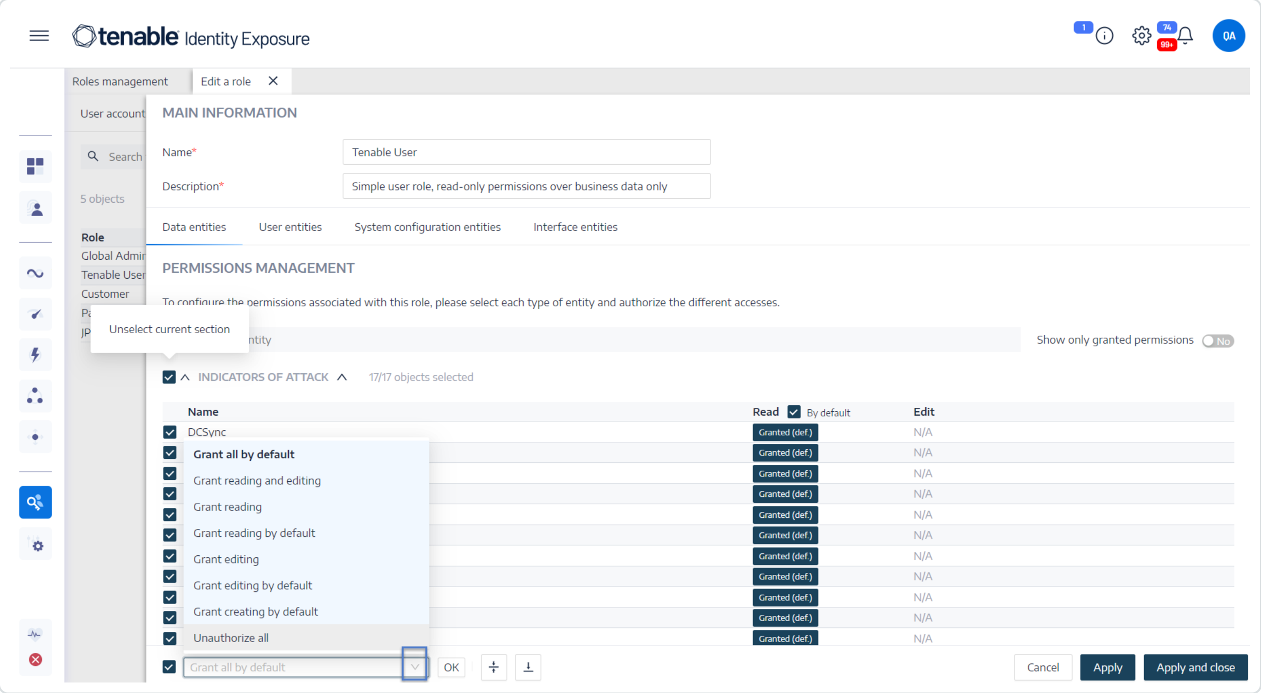
4. Select the entities or section(s) of entities (for example Indicators of Exposure) to set permissions on.

5. At the bottom of the page, click the arrow on the drop-down box to display a list of permissions.

6. Select the permission(s) for the role.

7. Click **OK**.

   A message confirms that Tenable Identity Exposure set the permissions on the entities.



MAIN INFORMATION

Name*: Tenable User

Description*: Simple user role, read-only permissions over business data only

PERMISSIONS MANAGEMENT

To configure the permissions associated with this role, please select each type of entity and authorize the different accesses.

Show only granted permissions: No

☑ INDICATORS OF ATTACK — 17/17 objects selected

	Name	Read ☑ By default	Edit
☑	DCSync	Granted (def.)	N/A
☑		Granted (def.)	N/A
☑		Granted (def.)	N/A
☑		Granted (def.)	N/A
☑		Granted (def.)	N/A
☑		Granted (def.)	N/A
☑		Granted (def.)	N/A
☑		Granted (def.)	N/A
☑		Granted (def.)	N/A
☑		Granted (def.)	N/A
☑		Granted (def.)	N/A

☑ Grant all by default

Permission Types

Permission	Description
Read	Permission to view an object or a configuration.

Edit	Permission to modify an object or a configuration. Requires the Read permission to apply modifications.
Create	Permission to create an object or a configuration. The **Create** permission requires the **Read** and **Edit** permissions to perform permitted actions on permitted resources.

Entity Types

There are four types of entities in Tenable Identity Exposure that require permissions to access which you can tailor for each user role in your organization:

Entity Type	Contains	Permissions
Data Entities		
This entity controls the permissions for setting up the monitored Active Directory and configuring the data analysis in Tenable Identity Exposure.	• Indicators of Attack • Indicators of Exposure • Forests • Domains • Profiles • Users • Alerts by email • Alerts by Syslog • Roles • Entity Relay • Reports	Read, Edit, Create
User Entities		
This entity controls a user's ability to configure information that Tenable Identity Exposure displays for data	• Preferences • Dashboards	Edit, Create

analysis and to modify personal information and preferences.	• Widgets • API key • Personal information	
System Configuration Entities		
This entity controls the access to the Tenable Identity Exposure platform and services.	• Application services (SMTP, logs, authentication Tenable Identity Exposure, Indicators of Attack, Trusted Certificate Authorities) • Scores through public API • Licenses • LDAP authentication • SAML authentication **Note**: Permissions for LDAP and SAML authentication are not available if you have a Tenable Vulnerability Management license. • Topology • Accounts Lockout Policy • Recrawl domains • Activity Logs • Tenable Cloud Service (Tenable Cloud Data Collection) • Microsoft Entra ID Support • Health Checks	Read, Edit

	- Display only user's own traces	
Interface Entities		
This entity defines the permissions to access specific parts of the Tenable Identity Exposure user interface and features.	Access paths to specific Tenable Identity Exposure features. For more information, see Set Permissions on User Interface Entities (Example)	Granted, Unauthorized

See also

- User Accounts
- User Roles

Set Permissions on User Interface Entities (Example)

Tenable Identity Exposure applies permissions along the path used to access a certain user interface feature. The following example shows how to set permissions to allow the configuration of Syslog.

To reach Syslog parameters, users require permissions along the path **System** > **Configuration** > **SYSLOG** in Tenable Identity Exposure:

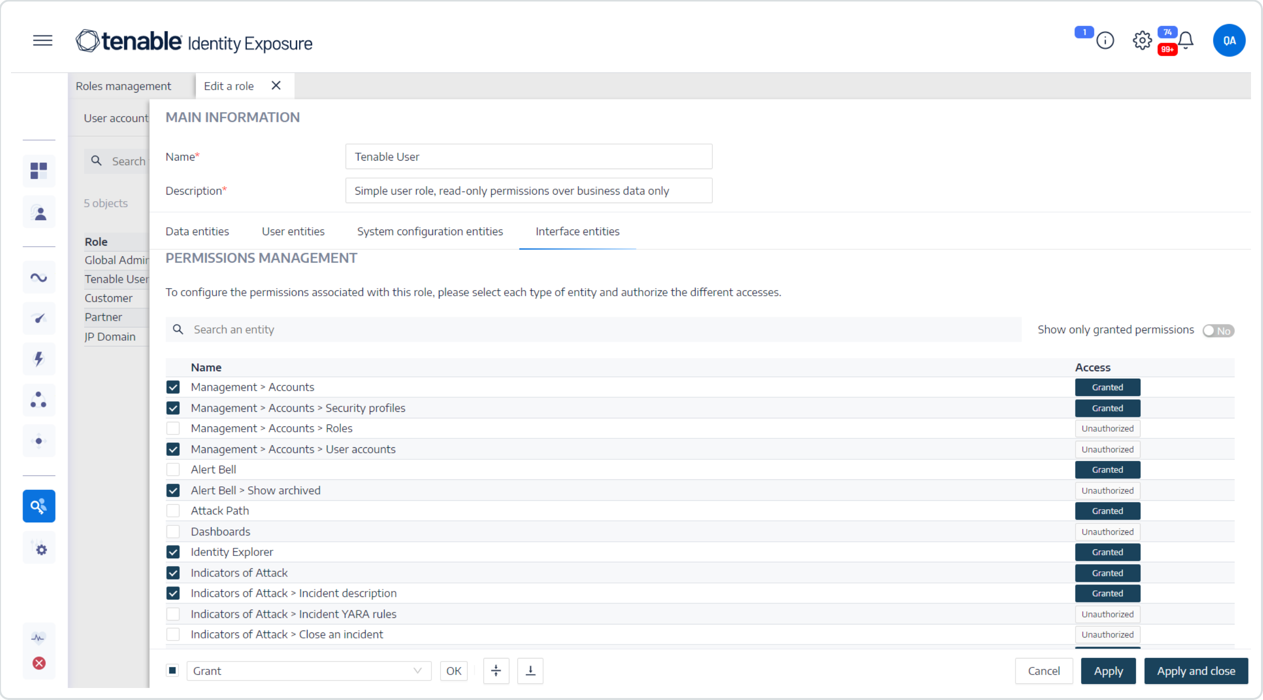
- System configuration: **Management** > **System**
- Configuration parameters: **Management** > **System** > **Configuration**
- Syslog alerts: **Management** > **System** > **Configuration** > **Alerting engine** > **SYSLOG**

To set permissions for Syslog configuration:

1. In Tenable Identity Exposure, click **Accounts** > **Roles management**.
2. Hover over the role for which you want to set permissions and click the ✎ icon on the right.

   The **Edit a role** pane appears.
3. Under **Permissions Management**, select **Interface Entities**.
4. In the list of entities, do the following:
   - Select **Management** > **System** and click the Access toggle to **Granted**.
   - Select **Management** > **System** > **Configuration** and click the Access toggle to **Granted**.
   - Select **Management** > **System Configuration** > **Alerting engine** > **SYSLOG** and click the Access toggle to **Granted**.
5. Click **Apply**.

   A message confirms that Tenable Identity Exposure updated permissions on the entities.



MAIN INFORMATION

Name*: Tenable User

Description*: Simple user role, read-only permissions over business data only

PERMISSIONS MANAGEMENT

To configure the permissions associated with this role, please select each type of entity and authorize the different accesses.

	Name	Access
☑	Management > Accounts	Granted
☑	Management > Accounts > Security profiles	Granted
☐	Management > Accounts > Roles	Unauthorized
☑	Management > Accounts > User accounts	Unauthorized
☐	Alert Bell	Granted
☑	Alert Bell > Show archived	Unauthorized
☐	Attack Path	Granted
☐	Dashboards	Unauthorized
☑	Identity Explorer	Granted
☑	Indicators of Attack	Granted
☑	Indicators of Attack > Incident description	Granted
☐	Indicators of Attack > Incident YARA rules	Unauthorized
☐	Indicators of Attack > Close an incident	Unauthorized

6. Under **Permissions Management**, select **Data Entities**.

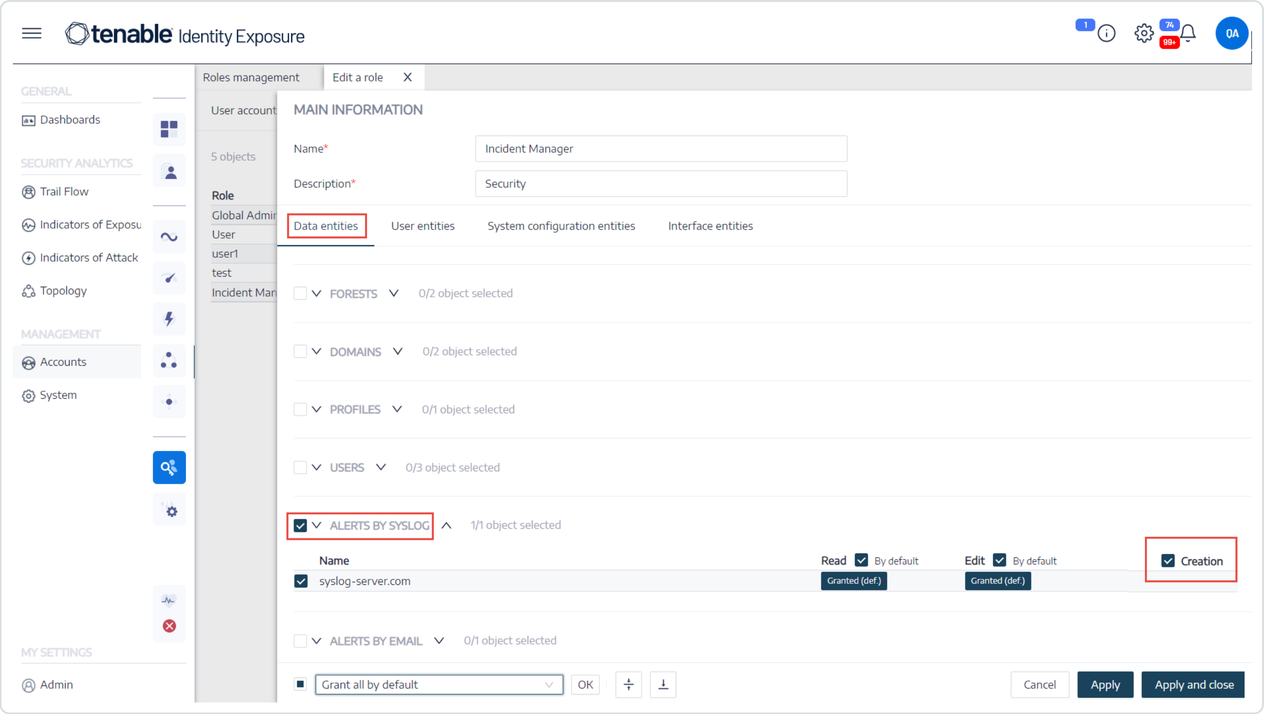
7. In the list of entity sections, select **Alerts by Syslog**.

8. Select the **Creation** permission.

   Tenable Identity Exposure implicitly grants the Read and Edit permissions.

9. Click **Apply and Close**.

   A message confirms that Tenable Identity Exposure updated permissions on the entities.



MAIN INFORMATION

Name*: Incident Manager

Description*: Security

Data entities | User entities | System configuration entities | Interface entities

- □ FORESTS 0/2 object selected
- □ DOMAINS 0/2 object selected
- □ PROFILES 0/1 object selected
- □ USERS 0/3 object selected
- ☑ ALERTS BY SYSLOG 1/1 object selected

	Name	Read ☑ By default	Edit ☑ By default	☑ Creation
☑	syslog-server.com	Granted (def.)	Granted (def.)	

- □ ALERTS BY EMAIL 0/1 object selected

Forests

An Active Directory (AD) forest is a collection of domains that share a common schema, configuration, and trust relationships. It provides a hierarchical structure for managing and organizing resources, enabling centralized administration and secure authentication across multiple domains within an organization.

Managing Forests

To add a forest:

1. In Tenable Identity Exposure, click **System**> **Forest management**.

2. Click **Add a forest** on the right.

   The Add a forest pane appears.

3. In the **Name** box, type the forest name.

4. In the **Account** section, provide the following for the service account that Tenable Identity Exposure uses:

   - **Login**: Type the name of the service account.
     Format: User Principal Name, such as “`tenablead@domain.example.com`” (recommended for compatibility with Kerberos Authentication) or NetBIOS, such as “`DomainNetBIOSName\SamAccountName`”.

   - **Password**: Type the password for the service account.

   > **Note**: If you must set the AD service account of Tenable Identity Exposure as a Protected Users group member, ensure your Tenable Identity Exposure configuration supports Kerberos Authentication, because Protected Users cannot use NTLM authentication.

5. Click **Add**.

   A message confirms the addition a new forest.

To edit a forest:

1. In Tenable Identity Exposure, click **System**> **Forest management**.

2. In the list of forests, hover over the forest you want to modify and click the ✎ icon on the right.

   The **Edit a forest** pane appears.

3. Modify as necessary.

4. Click **Edit**.

A message confirms that Tenable Identity Exposure updated the forest.

Protecting Service Accounts

Tenable recommends protecting service accounts to maintain security by correctly setting User Account Control (UAC) attributes to prevent delegation, require preauthentication, use stronger encryption, enforce password expiration and requirements, and allow authorized password changes. These measures mitigate the risk of unauthorized access and potential security breaches, ensuring the integrity of an organization's systems and data.

To modify settings using a Windows policy editor:

You can modify user account control settings using Windows' Local Security Policy editor or Group Policy Editor with the appropriate administrative privileges.

- In the editor, navigate to **Local Policies** -> **Security Options** to locate and configure the following settings: (This may vary depending on your Windows version.)
    - "*Network access: Do not allow storage of passwords and credentials for network authentication*": set it to **Enabled**.
    - "*Accounts: Do not require Kerberos preauthentication*": and set it to **Disabled**.
    - "*Network security: Configure encryption types allowed for Kerberos*": ensure that the option "*Use Kerberos DES encryption types for this account*" is **not** selected.
    - "*Accounts: Maximum password age*": set the password expiration period (for example, 30, 60, or 90 days so that `PasswordNeverExpires = FALSE`).
    - "*Accounts: Limit local account use of blank passwords to console logon only*": set it to **Disabled**.
    - "*Interactive logon: Number of previous logons to cache (in case domain controller is not available)*": set the desired value, such as "10" to allow users to change their passwords.

To modify settings using Powershell:

- On a machine hosting AD, open PowerShell with the appropriate administrative privileges and run the following command:

```
Set-ADAccountControl -Identity <AD_ACCOUNT> -AccountNotDelegated $true -UseDESKeyOnly
```

```
$false -DoesNotRequirePreAuth $false -PasswordNeverExpires $false -PasswordNotRequired
$false -CannotChangePassword $false
```

Where `<AD_ACCOUNT>` is the name of the Active Directory account you want to modify.

Domains

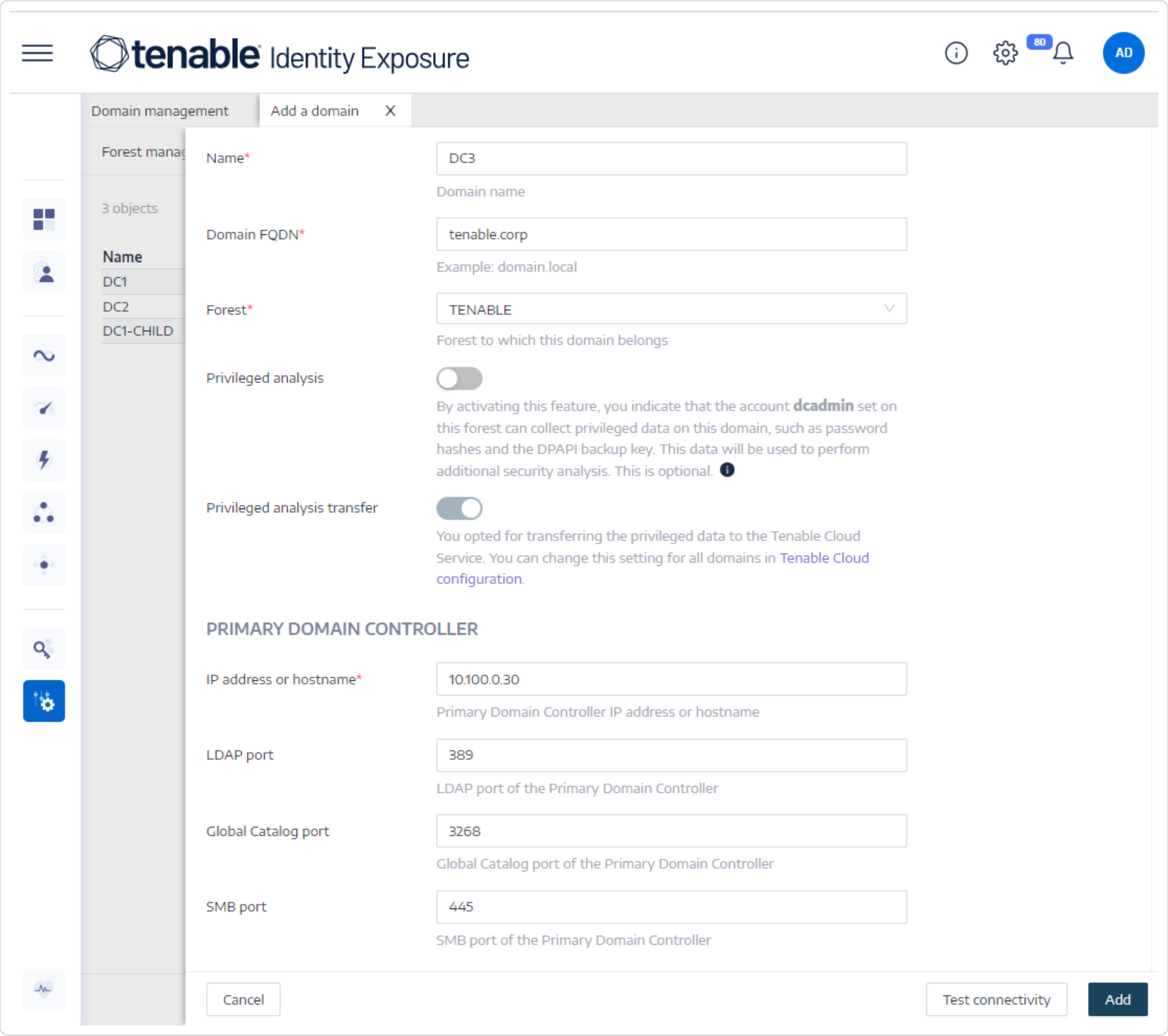
Tenable Identity Exposure monitors domains which group objects that share common settings in a logical manner for centralized management.

To add a domain:

1. In Tenable Identity Exposure, click **System**.
2. Click the **Domain management** tab.

   The **Domain Management** pane appears.
3. Click **Add a domain** in the upper-right corner.

   The **Add a domain** pane appears.



Name* DC3
Domain name

Domain FQDN* tenable.corp
Example: domain.local

Forest* TENABLE
Forest to which this domain belongs

Privileged analysis
By activating this feature, you indicate that the account **dcadmin** set on this forest can collect privileged data on this domain, such as password hashes and the DPAPI backup key. This data will be used to perform additional security analysis. This is optional.

Privileged analysis transfer
You opted for transferring the privileged data to the Tenable Cloud Service. You can change this setting for all domains in Tenable Cloud configuration.

PRIMARY DOMAIN CONTROLLER

IP address or hostname* 10.100.0.30
Primary Domain Controller IP address or hostname

LDAP port 389
LDAP port of the Primary Domain Controller

Global Catalog port 3268
Global Catalog port of the Primary Domain Controller

SMB port 445
SMB port of the Primary Domain Controller

4. In the **Main Information** section, give the following information:

   - In the **Name** box, type the name of the domain.

   - In the **Domain FQDN** box, type the Fully Qualified Domain Name (FQDN) for the domain.

   - In the **Forest** drop-down box, select the forest to which the domain belongs.

5. **Privileged analysis** (optional): If you enable the toggle, you allow the "dcadmin" account on this forest to collect privileged data on this domain to perform advanced security analysis.

6. **Privileged analysis transfer**: For more information about this option, see Tenable Cloud Data Collection

7. In the **Primary Domain Controller** section, give the following information:

   - In the **IP address or hostname** box, type the primary domain controller's hostname (required for compatibility with Kerberos Authentication, but incompatible with SaaS-VPN deployment modes) or IP address.

     > Tenable Identity Exposure does not support load balancers.

   - In the **LDAP port** box, type the primary domain controller's LDAP port.

     > **Note**: If you use port TCP/636 (LDAPS) to connect to your domain, Tenable Identity Exposure must have access to your Active Directory's Certificate Authority (CA) certificate to validate your AD certificate in order to perform the connection. In Secure Relay environments, you can install the CA certificate on the Relay machine. In VPN environments, this configuration is not possible.

   - In the **Global Catalog port** box, type the primary domain controller's global catalog port.

   - In the **SMB port** box, type the primary domain controller's SMB port.

8. Click **Add**.

   A message appears to confirm that Tenable Identity Exposure added the domain.

To edit a domain:

1. In Tenable Identity Exposure, click **Systems**.

2. Click the **Domain management** tab.

   The **Domain Management** pane appears.

3. Hover over the name of the domain you want to edit to display the ✎ icon on the right.

4. Click the ✎ icon.

   The **Edit a domain** pane appears.

5. Edit the information for the domain.

6. Click **Edit**.

   A message appears to confirm that Tenable Identity Exposure updated the domain.

To delete a domain:

1. In Tenable Identity Exposure, click **Systems**.
2. Click the **Domain management** tab.

   The **Domain Management** pane appears.

3. Hover over the name of the domain you want to delete to display the 🗑 icon.
4. Click the 🗑 icon.

   A message appears to ask you to confirm the deletion.

5. Click **Delete**.

   A message appears to confirm that Tenable Identity Exposure deleted the domain.

See also

- Force Data Refresh on a Domain
- Honey Accounts
- Kerberos Authentication

Force Data Refresh on a Domain

To force data refresh on a domain:

1. In Tenable Identity Exposure, click **System**.
2. Click the **Domain management** tab.

   The **Domain Management** pane appears.
3. Hover over the name of the domain on which you want to force data refresh to display the ⟳ icon on the right.
4. Click the ⟳ icon.

   A message appears with information about the data refresh action.
5. Click **Confirm**.

See also

- Honey Accounts

Honey Accounts

Required User Role: Administrator on the local machine

A Honey Account is a decoy account whose unique purpose is to detect an attacker trying to compromise the network through the Active Directory.

It is a prerequisite for Tenable Identity Exposure's Indicator of Attack to detect Kerberoasting exploitation attempts which seek to gain access to service accounts by requesting and extracting service tickets and then cracking the service account's credentials offline. The Kerberoasting Indicator of Attack sends out alerts when the Honey Account receives login attempts or ticket requests.

You associate one Honey Account per domain. Honey Accounts are not related to security profiles.

To add a Honey Account:

1. In Tenable Identity Exposure, click **Systems** > **Domain management**.

   The **Domain Management** pane appears.

2. Hover over the domain for which you want to add a Honey Account.

3. Under **Honey Account configuration status**, click **+**.

   The **Add a Honey Account** pane appears.

4. In the **Name** box, type a Distinguished Name (DN) for the user account to use as the Honey Account.

   Tip: You can type any string and Tenable Identity Exposure searches for and displays matching user account names in the drop-down box if that user account already exists in the Active Directory.

5. In the **Deployment** section, Tenable Identity Exposure generates a script with the appropriate settings for you to run to deploy the Honey Account. Click ⧉ to copy this script.

6. Click **Add**.

   A message appears to confirm that Tenable Identity Exposure added the Honey Account. In the Domain Management pane, the selected domain's **Honey Account configuration status** appears orange (●) to indicate that you must run the Honey Account deployment script to activate it.

> **Note**: If the **Honey Account configuration status** appears red (●), it indicates that Tenable Identity Exposure did not find this user account in the Active Directory. You must create this user account and proceed to the next step.

7. In a Windows PowerShell on a machine with the Active Directory module, run the Honey Account deployment script that you copied.

   In the **Domain Management** pane, the selected domain's **Honey Account configuration status** appears with an green status (●) to indicate that it is active.

   > **Note**: Tenable Identity Exposure may take some time to process and activate the Honey Account.

To edit a Honey Account:

1. In Tenable Identity Exposure, click **Systems** > **Domain management**.

   The **Domain Management** pane appears.

2. Hover over the domain for which you want to add a Honey Account.

3. Under **Honey Account configuration status**, click the 🐝 icon at the right.

   The **Edit a Honey Account** pane appears.

4. In the **Name** box, modify the user account as necessary.

5. In the **Deployment** section, click ⧉ to copy the Honey Account Deployment script.

6. Click **Edit**.

   A message appears to confirm that Tenable Identity Exposure updated the Honey Account. In the Domain Management pane, the selected domain's **Honey Account configuration status** appears orange (●) to indicate that you must run the Honey Account deployment script to activate it.

   > **Note**: If the **Honey Account configuration status** appears red (●), it indicates that Tenable Identity Exposure did not find this user account in the Active Directory. You must create this user account and proceed to the next step.

7. In a Windows PowerShell on a machine with the Active Directory module, run the Honey Account deployment script that you copied.

   In the **Domain Management** pane, the selected domain's **Honey Account configuration status** appears with an green status (●) to indicate that it is configured.

   > **Note**: Tenable Identity Exposure may take some time to process and activate the Honey Account.

To delete a Honey Account:

1. In Tenable Identity Exposure, click **Systems** > **Domain management**.

   The **Domain Management** pane appears.

2. Hover over the domain for which you want to add a Honey Account.

3. Under **Honey Account configuration status**, click the ✎ icon at the right.

   The **Edit a Honey Account** pane appears.

4. Click **Delete**.

   A message appears to confirm that Tenable Identity Exposure deleted the Honey Account.

See also

- Force Data Refresh on a Domain

Kerberos Authentication

Tenable Identity Exposure authenticates to the configured Domain Controller(s) using the credentials you provided. These DCs accept either NTLM or Kerberos authentication. NTLM is a legacy protocol with documented security issues, and Microsoft and all cybersecurity standards now discourage its use. Kerberos, on the other hand, is a more robust protocol that you should consider. Windows always attempts Kerberos first and resorts only to NTLM if Kerberos is not available.

Tenable Identity Exposure is compatible with both NTLM and Kerberos with a few exceptions. Tenable Identity Exposure prioritizes Kerberos as the preferred protocol when it fulfills all the required conditions. This section describes the requirements and shows you how to configure Tenable Identity Exposure to ensure the use of Kerberos.

The use of NTLM instead of Kerberos is also the reason why SYSVOL hardening interferes with Tenable Identity Exposure. For more information, see SYSVOL Hardening Interference with Tenable Identity Exposure.

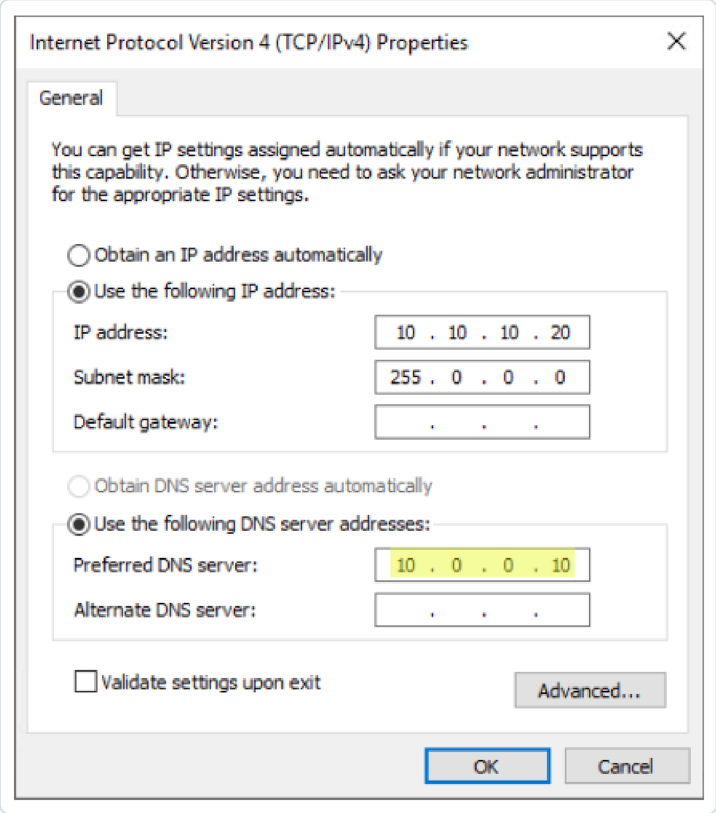
Compatibility with Tenable Identity Exposure Deployment Modes

Deployment Mode	Kerberos Support
On-premises	Yes
SaaS-TLS (legacy)	Yes
SaaS with Secure Relay	Yes
SaaS with VPN	No — You must switch your installation to the Secure Relay deployment mode.

Technical requirements

- **The AD service account configured in Tenable Identity Exposure must have a UserPrincipalName (UPN)**. See Service Account and Domain Configuration for instructions.

- **DNS configuration and DNS server must allow resolving all necessary DNS entries** — You must configure the Directory Listener or Relay machine to use DNS servers that know the domain controllers. If the Directory Listener or Relay machine is domain-joined, which Tenable Identity Exposure does not recommend, you should already meet this requirement. The easiest way is to use the domain controller itself as the preferred DNS server because it usually also runs DNS. For example:



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

IP address: 10 . 10 . 10 . 20
Subnet mask: 255 . 0 . 0 . 0
Default gateway: . . .

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server: 10 . 0 . 0 . 10
Alternate DNS server: . . .

□ Validate settings upon exit

> **Note**: If the Directory Listener or Relay machine is connected to several domains, and potentially in several forests, ensure that the configured DNS servers can resolve all required DNS entries for all domains. Otherwise you need to set up several Directory Listener or Relay machines.

- **Reachability of the Kerberos "server" (KDC)** — This requires network connectivity from the Directory Listener or Relay to domain controllers over port TCP/88. If the Directory Listener or Relay is domain-joined, which Tenable does not recommend, you should already meet this requirement. Each configured Tenable Identity Exposure forest requires Kerberos network connectivity with at least one domain controller in its respective domain containing the service account, as well as at least one domain controller in each connected domain.

For more information about requirements, see Network Flow Matrix and TLS Network Matrix.

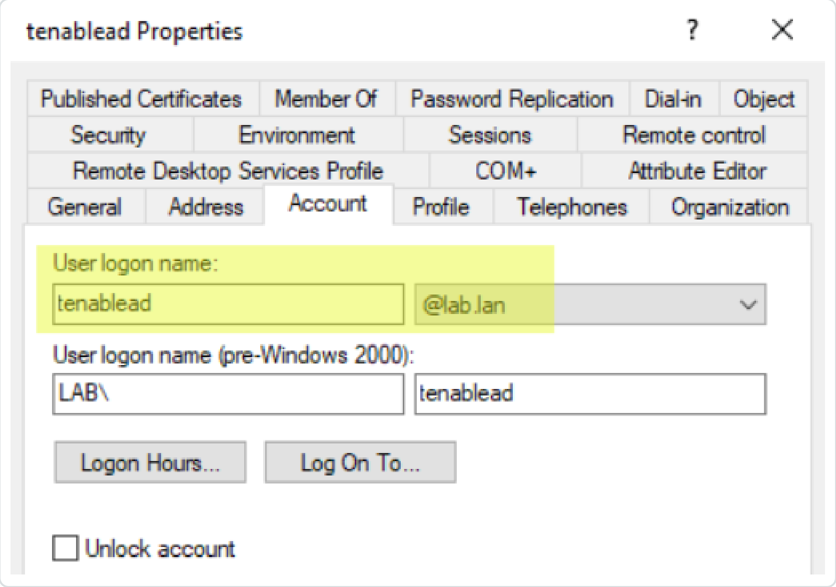
Note: The Directory Listener or Relay machine does not need to be domain-joined to use Kerberos.

Service Account and Domain Configuration

To configure the AD service account and AD domain in Tenable Identity Exposure to use Kerberos:

1. Use the User PrincipalName (UPN) format for the login. In this example, the UPN attribute is "`tenablead@lab.lan`".

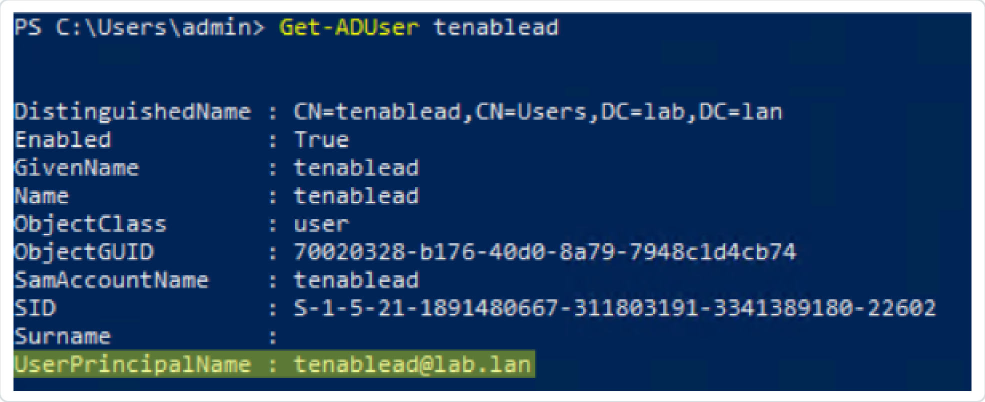
   a. Locate the UPN attribute in the domain of the forest that contains the service account as follows:



User logon name:
tenablead @lab.lan

User logon name (pre-Windows 2000):
LAB\ tenablead

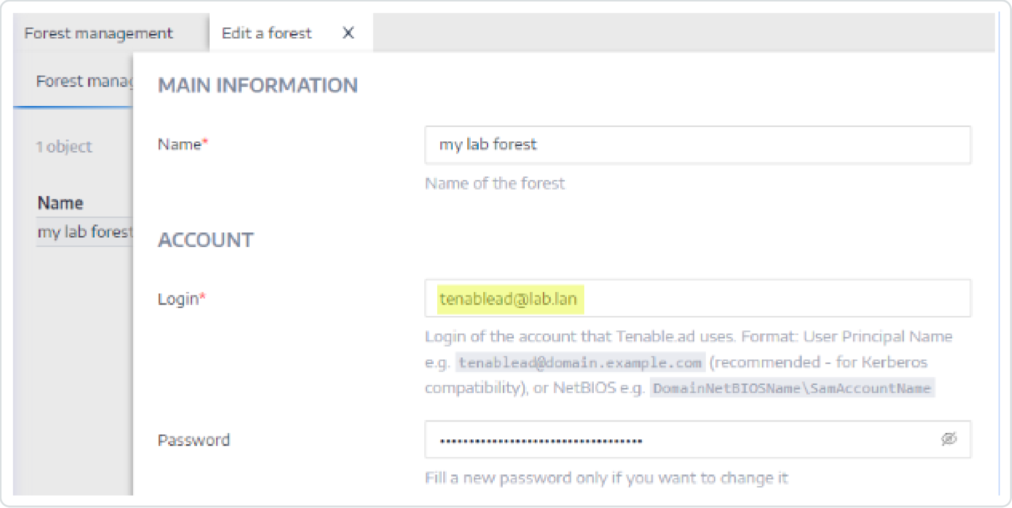
□ Unlock account



```
PS C:\Users\admin> Get-ADUser tenablead


DistinguishedName : CN=tenablead,CN=Users,DC=lab,DC=lan
Enabled           : True
GivenName         : tenablead
Name              : tenablead
ObjectClass       : user
ObjectGUID        : 70020328-b176-40d0-8a79-7948c1d4cb74
SamAccountName    : tenablead
SID               : S-1-5-21-1891480667-311803191-3341389180-22602
Surname           :
UserPrincipalName : tenablead@lab.lan
```

> **Note**: The UPN looks like an email address, and it is even often - but not always – the same as the user’s email.

b. In Tenable Identity Exposure, in the forest configuration section , set this UPN instead of the short “`username`” format or the NetBIOS “`domain\username`” format, as follows:



MAIN INFORMATION

Name* my lab forest

Name of the forest

ACCOUNT

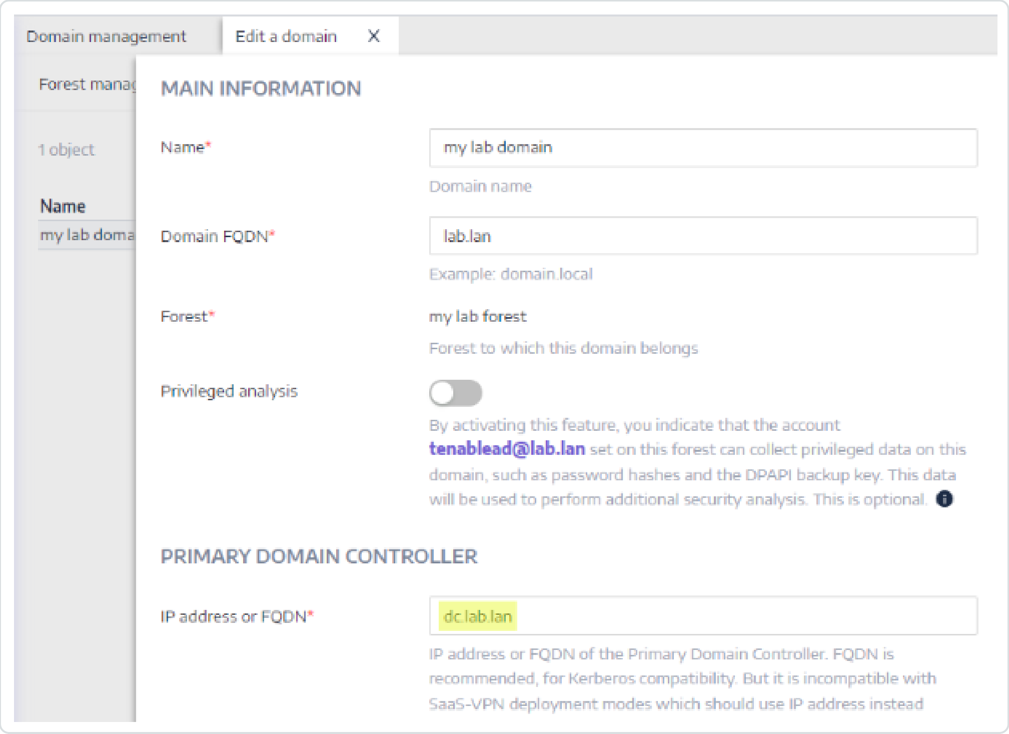
Login* tenablead@lab.lan

Login of the account that Tenable.ad uses. Format: User Principal Name e.g. `tenablead@domain.example.com` (recommended - for Kerberos compatibility), or NetBIOS e.g. `DomainNetBIOSName\SamAccountName`

Password ••••••••••••••••••••••••••••••••••••••

Fill a new password only if you want to change it

2. Use the Fully Qualified Domain Name (FQDN) In the domain configuration in Tenable Identity Exposure, set the FQDN for the Primary Domain Controller (PDC) instead of its IP.



MAIN INFORMATION

Name* my lab domain

Domain name

Domain FQDN* lab.lan

Example: domain.local

Forest* my lab forest

Forest to which this domain belongs

Privileged analysis ○

By activating this feature, you indicate that the account **tenablead@lab.lan** set on this forest can collect privileged data on this domain, such as password hashes and the DPAPI backup key. This data will be used to perform additional security analysis. This is optional.

PRIMARY DOMAIN CONTROLLER

IP address or FQDN* dc.lab.lan

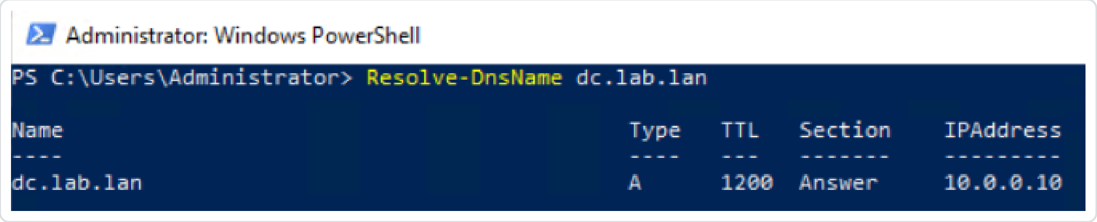
IP address or FQDN of the Primary Domain Controller. FQDN is recommended, for Kerberos compatibility. But it is incompatible with SaaS-VPN deployment modes which should use IP address instead

Troubleshooting

Kerberos requires several configuration steps to work properly. Otherwise, Windows, and by extension Tenable Identity Exposure, silently fall back to NTLM authentication.

DNS

Ensure that the DNS server(s) used on the Directory Listener or Relay machine can resolve the provided PDC FQDN, such as:



Administrator: Windows PowerShell

```
PS C:\Users\Administrator> Resolve-DnsName dc.lab.lan

Name                                           Type   TTL   Section    IPAddress
----                                           ----   ---   -------    ---------
dc.lab.lan                                     A      1200  Answer     10.0.0.10
```

Kerberos

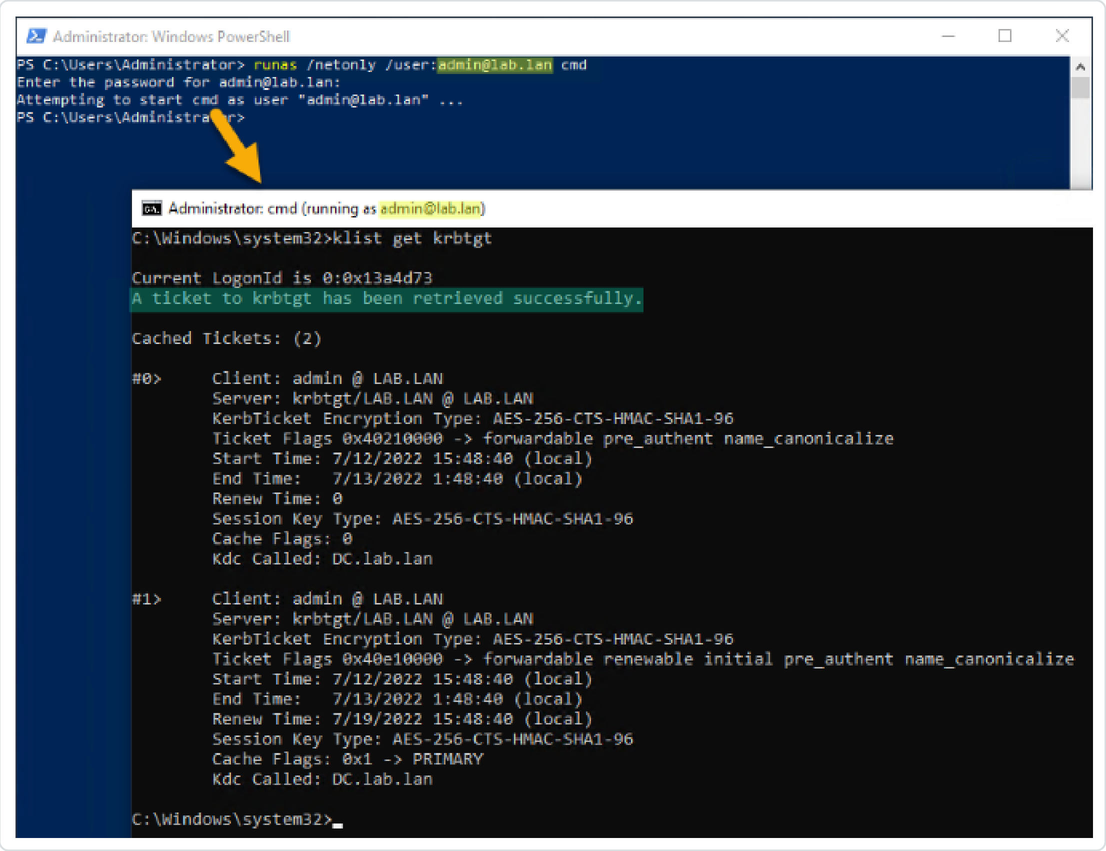
To verify that Kerberos works with the commands you run on the Directory Listener or Relay machine:

1. Verify that the AD service account configured in Tenable Identity Exposure can obtain a TGT:

    a. In a command line or PowerShell, run "`runas /netonly /user:<UPN> cmd`" and type the password. Be extra cautious when typing or pasting the password because there is no verification due to the "`/netonly`" flag.

    b. At the second command prompt, run "`klist get krbtgt`" to request a TGT ticket.

    The following example shows a successful result:


Administrator: Windows PowerShell
Administrator: cmd (running as admin@lab.lan)

```
PS C:\Users\Administrator> runas /netonly /user:admin@lab.lan cmd
Enter the password for admin@lab.lan:
Attempting to start cmd as user "admin@lab.lan" ...
PS C:\Users\Administrator>
```

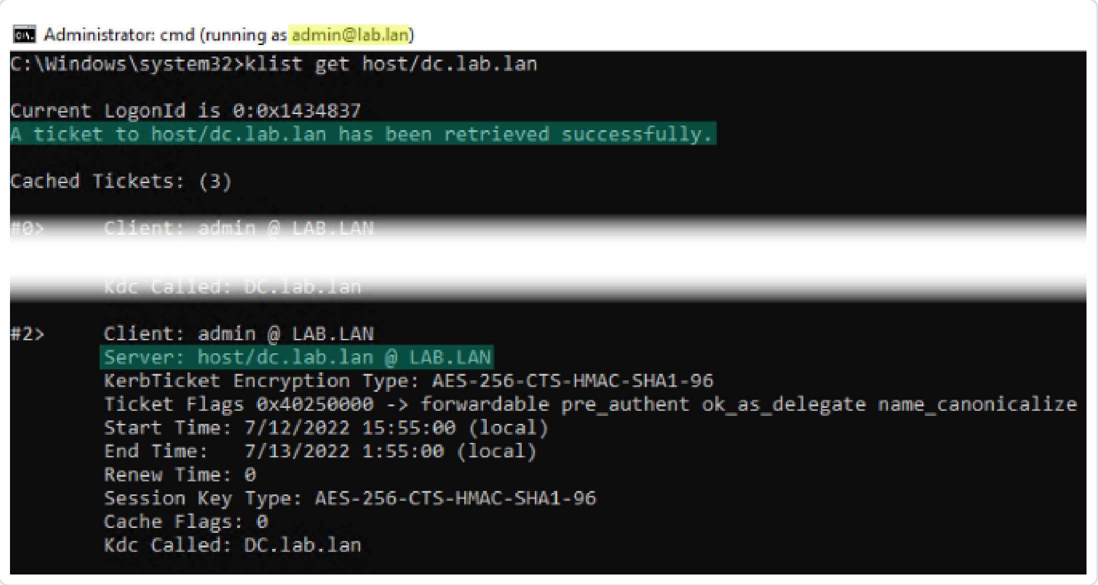
```
C:\Windows\system32>klist get krbtgt

Current LogonId is 0:0x13a4d73
A ticket to krbtgt has been retrieved successfully.

Cached Tickets: (2)

#0>     Client: admin @ LAB.LAN
        Server: krbtgt/LAB.LAN @ LAB.LAN
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40210000 -> forwardable pre_authent name_canonicalize
        Start Time: 7/12/2022 15:48:40 (local)
        End Time:   7/13/2022 1:48:40 (local)
        Renew Time: 0
        Session Key Type: AES-256-CTS-HMAC-SHA1-96
        Cache Flags: 0
        Kdc Called: DC.lab.lan

#1>     Client: admin @ LAB.LAN
        Server: krbtgt/LAB.LAN @ LAB.LAN
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40e10000 -> forwardable renewable initial pre_authent name_canonicalize
        Start Time: 7/12/2022 15:48:40 (local)
        End Time:   7/13/2022 1:48:40 (local)
        Renew Time: 7/19/2022 15:48:40 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96
        Cache Flags: 0x1 -> PRIMARY
        Kdc Called: DC.lab.lan

C:\Windows\system32>_
```

The following are potential error codes:

- `0xc0000064`: "User logon with misspelled or bad user account" -> Check the login (i.e. the part before the '@' in the UPN).
- `0xc000006a`: "User logon with misspelled or bad password" -> Check the password.
- `0xc000005e`: "There are currently no logon servers available to service the logon request." -> Check that DNS resolution works and that the server can contact the returned KDC(s), etc.
- Other error codes: See the Microsoft documentation relating to 4625 events.

2. Verify that the domain controller configured in Tenable Identity Exposure can obtain a service ticket. In the same second command prompt, run `"klist get host/<DC_FQDN>"` (replace "<DC_FQDN>").

The following example shows a successful result:



Administrator: cmd (running as admin@lab.lan)

```
C:\Windows\system32>klist get host/dc.lab.lan

Current LogonId is 0:0x1434837
A ticket to host/dc.lab.lan has been retrieved successfully.

Cached Tickets: (3)

#0>     Client: admin @ LAB.LAN

        Kdc Called: DC.lab.lan

#2>     Client: admin @ LAB.LAN
        Server: host/dc.lab.lan @ LAB.LAN
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40250000 -> forwardable pre_authent ok_as_delegate name_canonicalize
        Start Time: 7/12/2022 15:55:00 (local)
        End Time:   7/13/2022 1:55:00 (local)
        Renew Time: 0
        Session Key Type: AES-256-CTS-HMAC-SHA1-96
        Cache Flags: 0
        Kdc Called: DC.lab.lan
```

Alerts

License required: Depending on the type of alert you want to send, you may require licenses for Indicators of Attack or Indicators of Exposure.

Tenable Identity Exposure's alerting system helps you identify security regressions and/or attacks on your monitored Active Directory. It pushes analytics data about vulnerabilities and attacks in real-time through email or Syslog notification.

- SMTP Server Configuration
- Email Alerts
- Syslog Alerts
- Syslog and Email Alert Details

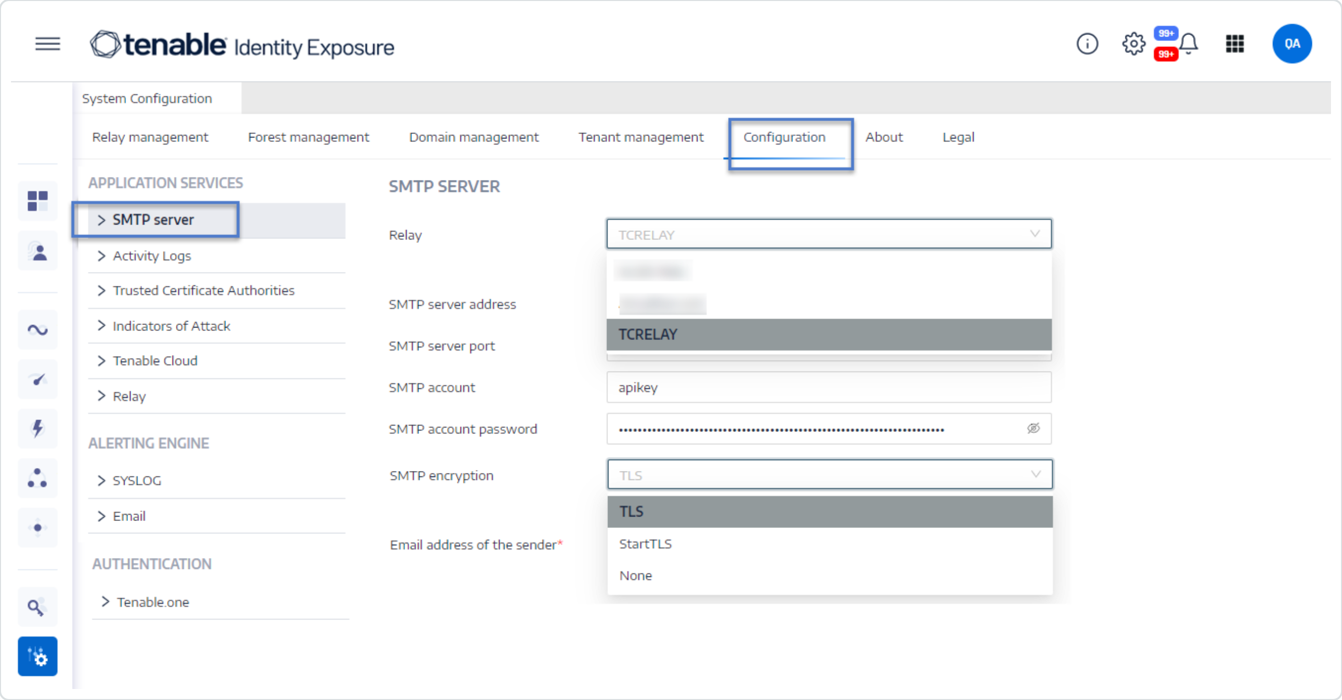
SMTP Server Configuration

Tenable Identity Exposure requires Simple Mail Transfer Protocol (SMTP) configuration to send out alert notifications.

To configure the SMTP server:

1. In Tenable Identity Exposure, click **System** > **Configuration**.
2. Under **Application Services**, select **SMTP Server**.

   The **SMTP Server** pane opens.



Relay: TCRELAY

SMTP server address

SMTP server port

SMTP account: apikey

SMTP account password: ••

SMTP encryption: TLS

Email address of the sender*

3. **If your network uses Secure Relay:** In the **Relay** box, click the arrow to select a Relay to communicate with your SMTP Server from the drop-down list.
4. Provide the following information:
   - SMTP Server address
   - SMTP Server port
   - SMTP account
   - SMTP account password

5. In the SMTP Encryption box, click the arrow to select an encryption method from the drop-down list.

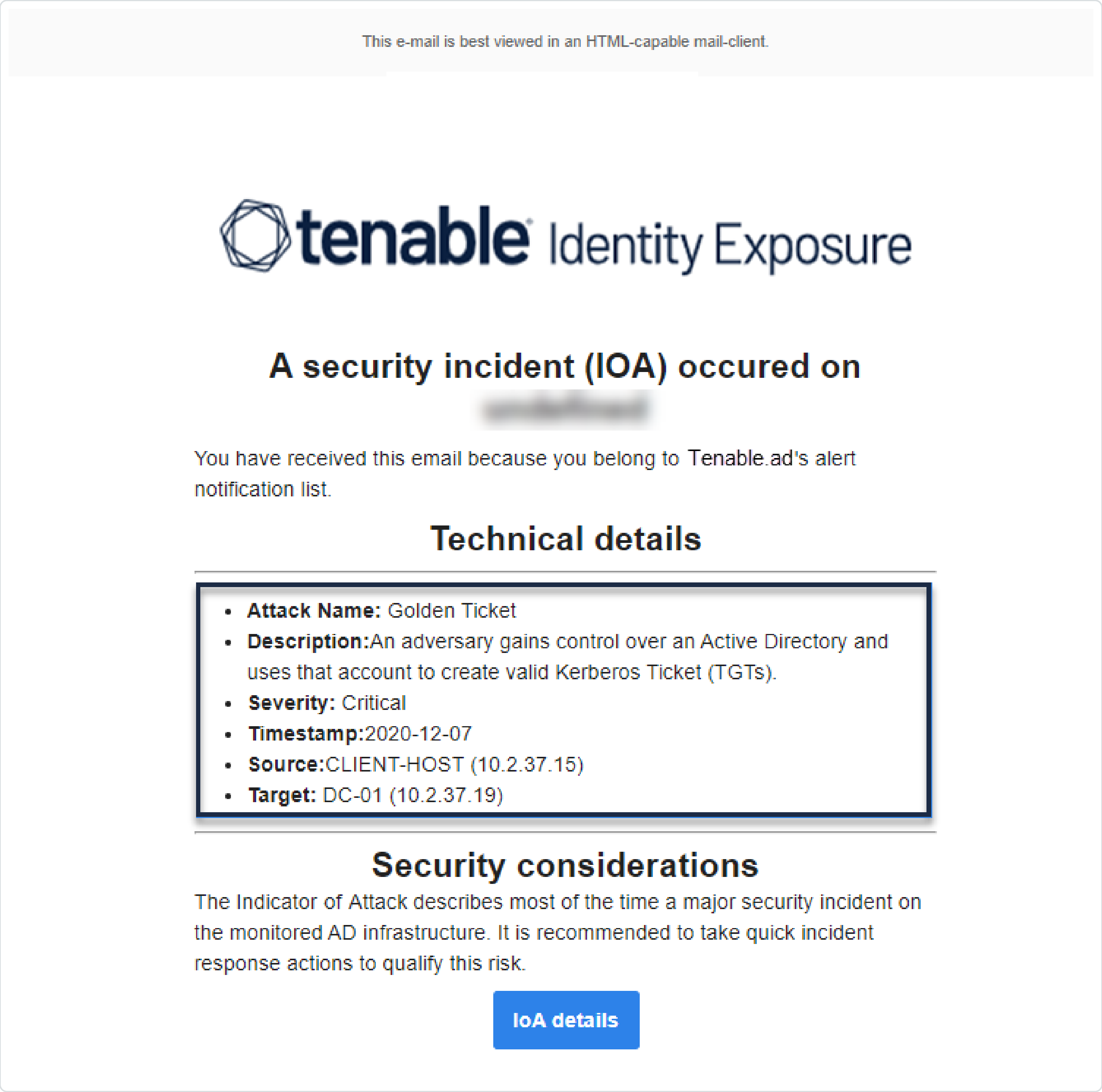
6. In the **Email address of the sender** box, provide an email address for Tenable Identity Exposure to use when sending emails.

7. Click **Save**.

   A message confirms that Tenable Identity Exposure updated the SMTP parameters.

Email Alerts

Tenable Identity Exposure sends out email alerts to notify you automatically if events reach a certain severity threshold and require remediation actions. The following is an example of an email alert:



This e-mail is best viewed in an HTML-capable mail-client.

A security incident (IOA) occured on [redacted]

You have received this email because you belong to Tenable.ad's alert notification list.

Technical details

- **Attack Name:** Golden Ticket
- **Description:**An adversary gains control over an Active Directory and uses that account to create valid Kerberos Ticket (TGTs).
- **Severity:** Critical
- **Timestamp:**2020-12-07
- **Source:**CLIENT-HOST (10.2.37.15)
- **Target:** DC-01 (10.2.37.19)

Security considerations

The Indicator of Attack describes most of the time a major security incident on the monitored AD infrastructure. It is recommended to take quick incident response actions to qualify this risk.

To add an email alert:

1. In Tenable Identity Exposure, click **System** > **Configuration** > **Email**.
2. Click the **Add an email alert** button on the right.

   The **Add an email alert** pane appears.
3. Under the **Main Information** section, provide the following:
   - In the **Email address** box, type the recipient's email address to receive notifications.
   - In the **Description** box, type a description for the recipient address.
4. In the **Trigger the alert** drop-down list, select one of the following:
   - **On each deviance**: Tenable Identity Exposure sends out a notification on each deviant IoE detection.
   - **On each attack**: Tenable Identity Exposure sends out a notification on each deviant IoA detection.
   - **On each health check status changes**: Tenable Identity Exposure sends out a notification whenever a health check status changes.
5. In the **Profiles** box, click to select the profile(s) to use for this email alert (if applicable).
6. **Send alerts when deviances are detected during the initial analysis phase**: do one of the following (if applicable):
   - Select the checkbox: Tenable Identity Exposure sends out a large volume of email notifications when a system reboot triggers alerts.
   - Unselect the checkbox: Tenable Identity Exposure does not send out email notifications when a system reboot triggers alerts.
7. **Severity threshold**: click the arrow of the drop-down box to select the threshold at which Tenable Identity Exposure sends alerts (if applicable).
8. Depending on the alert trigger you selected previously:
   - **Indicators of Exposure**: If you set alerts to trigger **on each deviance**, click the arrow next to each severity level to expand the list of Indicators of Exposure and select the ones for which to send alerts.

   - **Indicators of Attack**: If you set alerts to trigger **on each attack**, click the arrow next to each severity level to expand the list of Indicators of Attack and select the ones for which to send alerts.

   - **Health check status changes**: Click **Health Checks** to select the health check type to trigger an alert, and click **Filter on selection**.

9. Click the **Domains** box to select the domains for which Tenable Identity Exposure sends out alerts.

   The Forests and Domains pane appears.

   a. Select the forest or domain.

   b. Click **Filter on selection**.

10. Click **Test the configuration**.

    A message confirms that Tenable Identity Exposure sent an email alert to the server.

11. Click **Add**.

    A message confirms that Tenable Identity Exposure created the email alert.

To edit an email alert:

1. In Tenable Identity Exposure, click **System** > **Configuration** > **Email**.

2. In the list of email alerts, hover over the one you want to modify and click the ✎ icon at the end of the line.

   The **Edit an email alert** pane appears.

3. Make the necessary modifications as described in the procedure To add an email alert:

4. Click **Edit**.

   A message confirms that Tenable Identity Exposure updated the alert.

To delete an email alert:

1. In Tenable Identity Exposure, click **System** > **Configuration** > **Email**.

2. In the list of email alerts, hover over the one you want to delete and click the 🗑 icon at the end of the line.

   A message asks you to confirm the deletion.

3. Click **Delete**.

   A message confirms that Tenable Identity Exposure deleted the alert.

See also

- SMTP Server Configuration
- Syslog and Email Alert Details

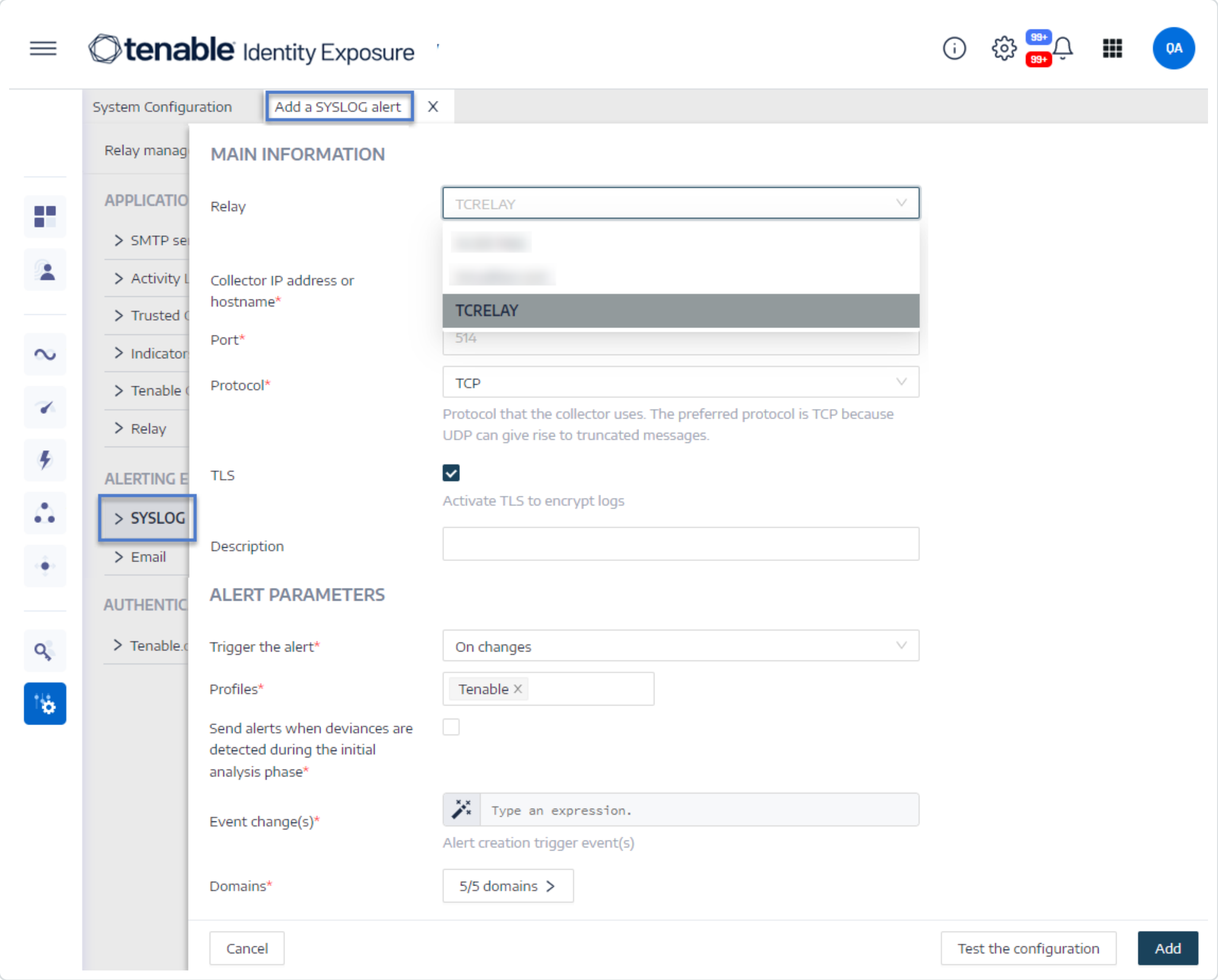
Syslog Alerts

Some organizations use SIEM (Security Information and Event Management) to gather logs on potential threats and security incidents. Tenable Identity Exposure can push security information related to Active Directory to the SIEM Syslog servers to improve their alerting mechanisms.

To add a new Syslog alert:

1. In Tenable Identity Exposure, click **System** > **Configuration** > **Syslog**.
2. Click the **Add a Syslog alert** button on the right.

   The **Add a Syslog alert** pane appears.



MAIN INFORMATION

Relay: TCRELAY

[redacted]

[redacted]

TCRELAY

Collector IP address or hostname*

Port*: 514

Protocol*: TCP

Protocol that the collector uses. The preferred protocol is TCP because UDP can give rise to truncated messages.

TLS: ☑

Activate TLS to encrypt logs

Description:

ALERT PARAMETERS

Trigger the alert*: On changes

Profiles*: Tenable ×

Send alerts when deviances are detected during the initial analysis phase*: ☐

Event change(s)*: Type an expression.

Alert creation trigger event(s)

Domains*: 5/5 domains >

3. Under the **Main Information** section, provide the following:

- **If your network uses Secure Relay:** In the **Relay** box, click the arrow to select a Relay to communicate with your SIEM from the drop-down list.
- In the **Collector IP address or hostname** box, type the server IP or hostname that receives notifications.
- In the **Port** box, type the port number for the collector.
- In the **Protocol** box, click the arrow to select either UDP or TCP.
  - If you choose TCP, select the **TLS** option checkbox if you want to enable the TLS security protocol to encrypt the logs.
- In the **Description** box, type a brief description for the collector.

4. In the **Trigger the alert** drop-down list, select one:
   - **On changes**: Tenable Identity Exposure sends out a notification whenever an event that you specified occurs.
   - **On each deviance**: Tenable Identity Exposure sends out a notification on each deviant IoE detection.
   - **On each attack**: Tenable Identity Exposure sends out a notification on each deviant IoA detection.
   - **On each health check status changes**: Tenable Identity Exposure sends out a notification whenever a health check status changes.
5. In the **Profiles** box, click to select the profile to use for this Syslog alert (if applicable).
6. **Send alerts when deviances are detected during the initial analysis phase**: do one of the following (if applicable):
   - Select the checkbox: Tenable Identity Exposure sends out a large volume of email notifications when a system reboot triggers alerts.
   - Unselect the checkbox: Tenable Identity Exposure does not send out email notifications when a system reboot triggers alerts.
7. **Severity threshold**: click the arrow of the drop-down box to select the threshold at which Tenable Identity Exposure sends alerts (if applicable).
8. Depending on the alert trigger you selected previously:

- **Event changes**: If you set alerts to trigger **on changes**, type an expression to trigger the event notification.

  You can either click on the ✨ icon to use the search wizard or type a query expression in the search box and click **Validate**. For more information, see [Customize Trail Flow Queries](#).

- **Indicators of Exposure**: If you set alerts to trigger **on each deviance**, click the arrow next to each severity level to expand the list of Indicators of Exposure and select the ones for which to send alerts.

- **Indicators of Attack**: If you set alerts to trigger **on each attack**, click the arrow next to each severity level to expand the list of Indicators of Attack and select the ones for which to send alerts.

- **Health check status changes**: Click **Health Checks** to select the health check type to trigger an alert, and click **Filter on selection**.

9. Click the **Domains** box to select the domains for which Tenable Identity Exposure sends out alerts.

   The **Forests and Domains** pane appears.

   a. Select the forest or domain.

   b. Click **Filter on selection**.

10. Click **Test the configuration**.

    A message confirms that Tenable Identity Exposure sent a Syslog alert to the server.

11. Click **Add**.

    A message confirms that Tenable Identity Exposure created the Syslog alert.

To edit a Syslog alert:

1. In Tenable Identity Exposure, click **System** > **Configuration** > **Syslog**.

2. In the list of Syslog alerts, hover over the one you want to modify and click the ✎ icon at the end of the line.

   The **Edit a Syslog alert** pane appears.

3. Make the necessary modifications as described in the procedure To add a new Syslog alert:

4. Click **Edit**.

   A message confirms that Tenable Identity Exposure updated the alert.

To delete a Syslog alert:

1. In Tenable Identity Exposure, click **System** > **Configuration** > **Syslog**.

2. In the list of Syslog alerts, hover over the one you want to delete and click the 🗑 icon at the end of the line.

   A message asks you to confirm the deletion.

3. Click **Delete**.

   A message confirms that Tenable Identity Exposure deleted the alert.

See also

- Syslog and Email Alert Details

Syslog and Email Alert Details

When you enable Syslog or email alerts, Tenable Identity Exposure sends out notifications when it detects a deviance, an attack, or a change.

Alert Header

Syslog alert headers (RFC-3164) use the Common Event Format (CEF), a common format in solutions that integrate Security Information and Event Management (SIEM).

Example of an alert for an Indicator of Exposure (IoE)

IoE Alert Header

```
<116>Jan  9 09:24:42 qradar.alsid.app AlsidForAD[4]: "0" "1" "Alsid Forest" "emea.corp" "C-PASSWORD-
DONT-EXPIRE" "medium" "CN=Gustavo Fring,OU=Los_Pollos_Hermanos,OU=Emea,DC=emea,DC=corp" "28" "1" "R-
DONT-EXPIRE-SET" "2434" "TrusteeCn"="Gustavo Fring"
```

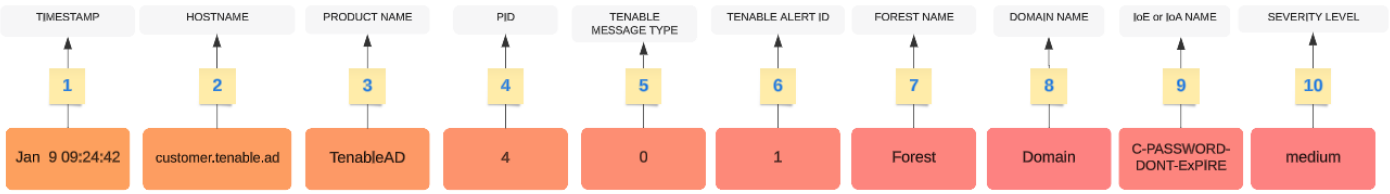
Example of an alert for an Indicator of Attack (IoA)

IoA Alert Header

```
<116>Jan  9 09:24:42 qradar.alsid.app AlsidForAD[4]: "2" "1337" "Alsid Forest" "emea.corp" "DC Sync"
"medium" "yoda.alsid.corp" "10.0.0.1" "antoinex1x.alsid.corp" "10.1.0.1" "user"="Gustavo Fring" "dc_
name"="MyDC"
```

Alert Information

Generic Elements

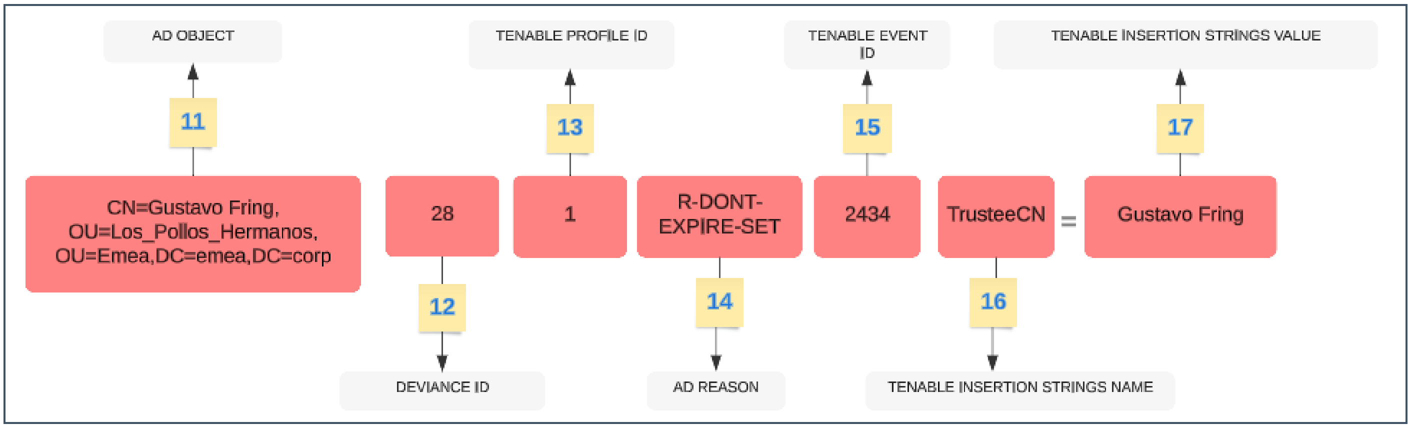


The header structure includes the following parts, as described in the table.

Part	Description
1	**Time Stamp**— The date of the detection. Example: "Jun 7 05:37:03"

2	**Hostname** — The hostname of your application. Example: "customer.tenable.ad"
3	**Product Name** — The name of the product that triggered the deviance. Example: "TenableAD", "AnotherTenableADProduct"
4	**PID** — The product (Tenable Identity Exposure) ID. Example: [4]
5	**Tenable Msg Type** — The identifier of event sources. Example: "0" (= On each deviance), "1" (= On changes), "2" (= On each attack)
6	**Tenable Alert ID** — The unique ID of the alert. Example: "0", "132"
7	**Forest Name** — The forest name of the related event. Example: "Corp Forest"
8	**Domain Name** — The domain name related to the event. Example: "tenable.corp", "zwx.com"
9	**Tenable Codename** — The code name of the Indicator of Exposure (IoE) or Indicator of Attack (IoA). Examples: "C-PASSWORD-DONT-EXPIRE", "DC Sync".
10	**Tenable Severity Level** — The severity level of the related deviance. Example: "critical", "high", "medium"

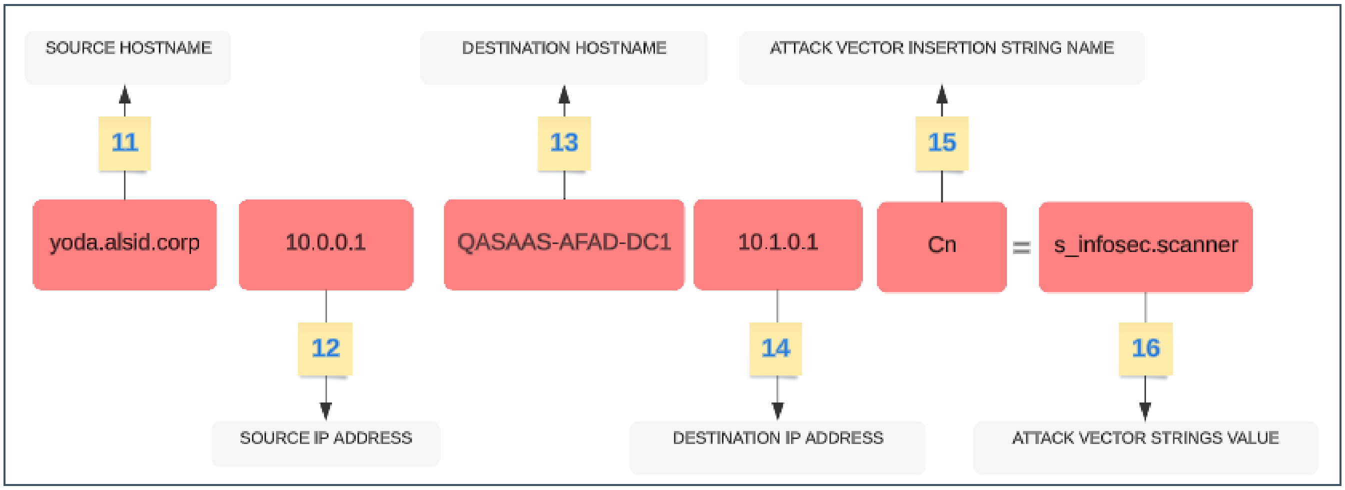
IoE Specific Elements


AD OBJECT
TENABLE PROFILE ID
TENABLE EVENT ID
TENABLE INSERTION STRINGS VALUE
11
13
15
17
CN=Gustavo Fring, OU=Los_Pollos_Hermanos, OU=Emea,DC=emea,DC=corp
28
1
R-DONT-EXPIRE-SET
2434
TrusteeCN
=
Gustavo Fring
12
14
16
DEVIANCE ID
AD REASON
TENABLE INSERTION STRINGS NAME

Part	Description
11	**AD Object** — The Distinguished Name of the deviant object. Example: "CN=s_infosec.scanner,OU=ADManagers,DC=domain,DC=local"
12	**Tenable Deviance ID** — The ID of the deviance. Example: "24980", "132", "28"

13	**Tenable Profile ID** — The ID of the profile on which Tenable Identity Exposure triggered the deviance. Example: "1" (Tenable), "2" (sec_team)
14	**AD Reason Codename** — The code name of the deviance reason. Example: "R-DONT-EXPIRE-SET", "R-UNCONST-DELEG"
15	**Tenable Event ID** — The ID of the event that the deviance triggered. Example: "40667", "28"
16	**Tenable Insertion Strings Name** — The attribute name that the deviant object triggered. Example: "Cn", "useraccountcontrol", "member", "pwdlastset"
17	**Tenable Insertion Strings Value** — The value of the attribute that the deviant object triggered. Example: "s_infosec.scanner", "CN=Backup Operators,CN=Builtin,DC=domain,DC=local"

IoA Specific Elements



Part	Description
11	**Source hostname** — The hostname of the attacking host. Value can also be "Unknown".
12	**Source IP Address** — The IP address of the attacking host. Values can be IPv4 or IPv6.
13	**Destination Hostname** — The hostname of the attacked host.
14	**Destination IP Address** — The IP address of the attacked host. Values can be IPv4

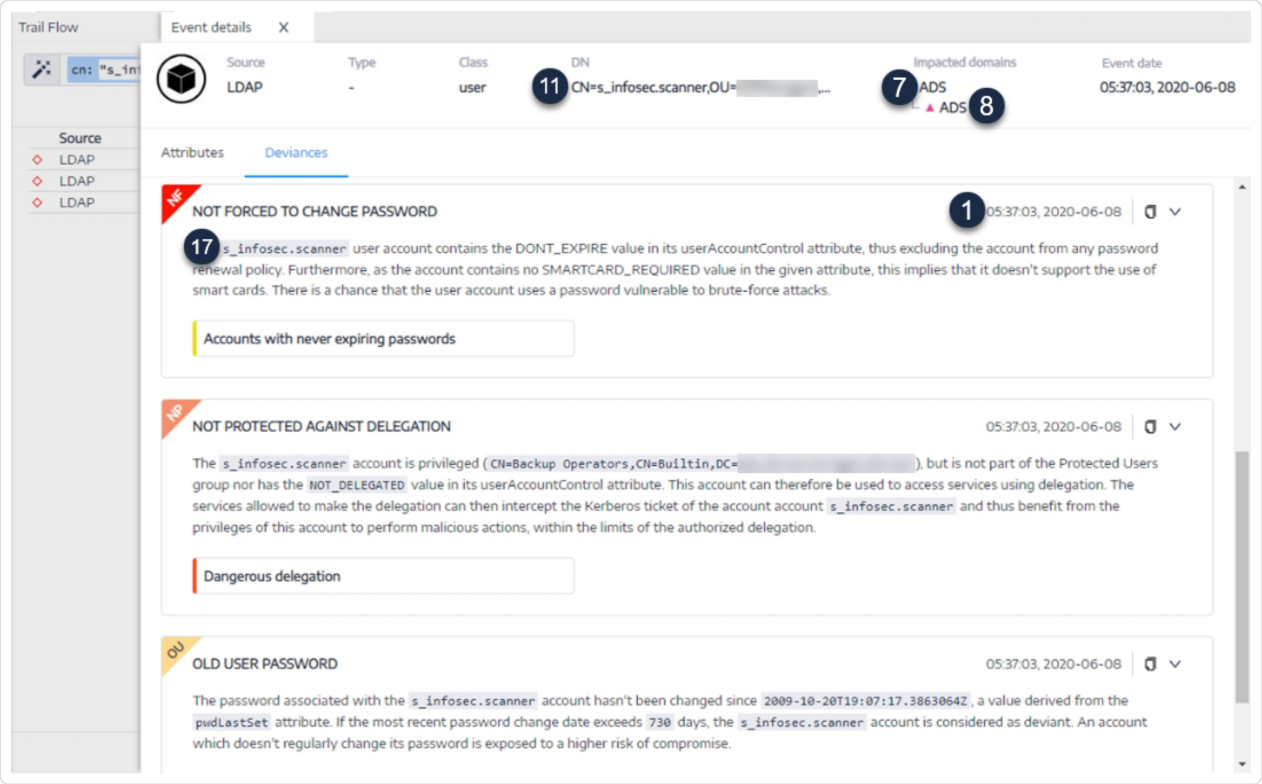
	or IPv6.
15	**Attack Vector Insertion Strings Name** – The attribute name that the deviant object triggered.
16	**Attack Vector Insertion Strings Value** – The value of the attribute that the deviant object triggered.

Examples

Trail Flow Event Details

The following example shows details of an event in the Trail Flow containing the following:

- The time stamp (1)
- The deviant object name (11)
- The forest (7) and domain (8) names
- The value of the attribute that the deviant object triggered (17)



Source	Type	Class	DN	Impacted domains	Event date
LDAP	-	user	CN=s_infosec.scanner,OU=[redacted],...	ADS ADS	05:37:03, 2020-06-08

NOT FORCED TO CHANGE PASSWORD 05:37:03, 2020-06-08

s_infosec.scanner 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.

Accounts with never expiring passwords

NOT PROTECTED AGAINST DELEGATION 05:37:03, 2020-06-08

The s_infosec.scanner account is privileged (CN=Backup Operators,CN=Builtin,DC=[redacted]), but is not part of the Protected Users group nor has the NOT_DELEGATED value in its userAccountControl attribute. This account can therefore be used to access services using delegation. The services allowed to make the delegation can then intercept the Kerberos ticket of the account account s_infosec.scanner and thus benefit from the privileges of this account to perform malicious actions, within the limits of the authorized delegation.

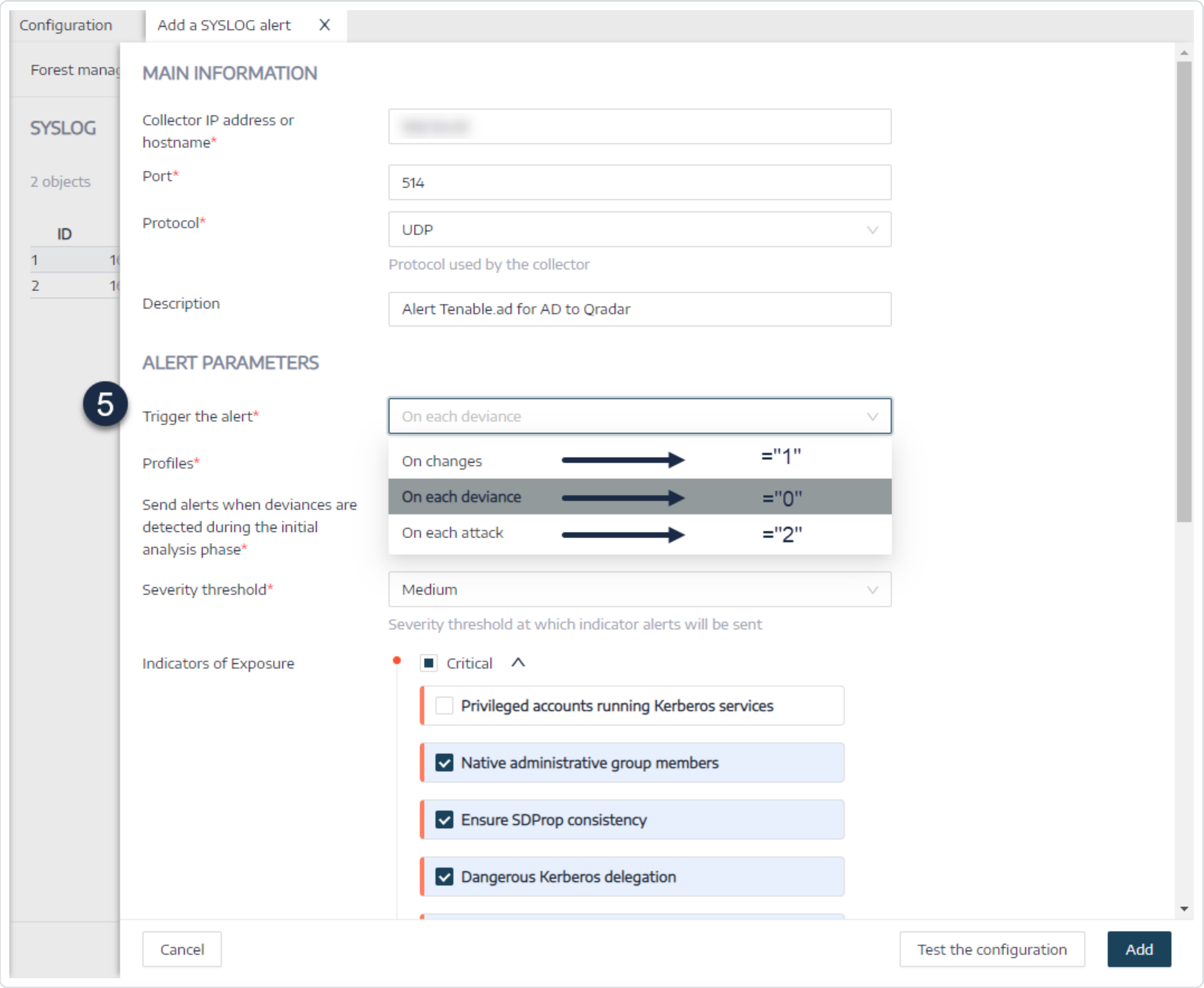
Dangerous delegation

OLD USER PASSWORD 05:37:03, 2020-06-08

The password associated with the s_infosec.scanner account hasn't been changed since 2009-10-20T19:07:17.3863064Z, a value derived from the pwdLastSet attribute. If the most recent password change date exceeds 730 days, the s_infosec.scanner account is considered as deviant. An account which doesn't regularly change its password is exposed to a higher risk of compromise.

Event Source

This example shows the source for the event (5). You set this parameter in the Syslog configuration page. For more information, see Syslog Alerts.



MAIN INFORMATION

Collector IP address or hostname*: [redacted]

Port*: 514

Protocol*: UDP

Protocol used by the collector

Description: Alert Tenable.ad for AD to Qradar

ALERT PARAMETERS

5 Trigger the alert*: On each deviance

- On changes → ="1"
- On each deviance → ="0"
- On each attack → ="2"

Profiles*

Send alerts when deviances are detected during the initial analysis phase*

Severity threshold*: Medium

Severity threshold at which indicator alerts will be sent

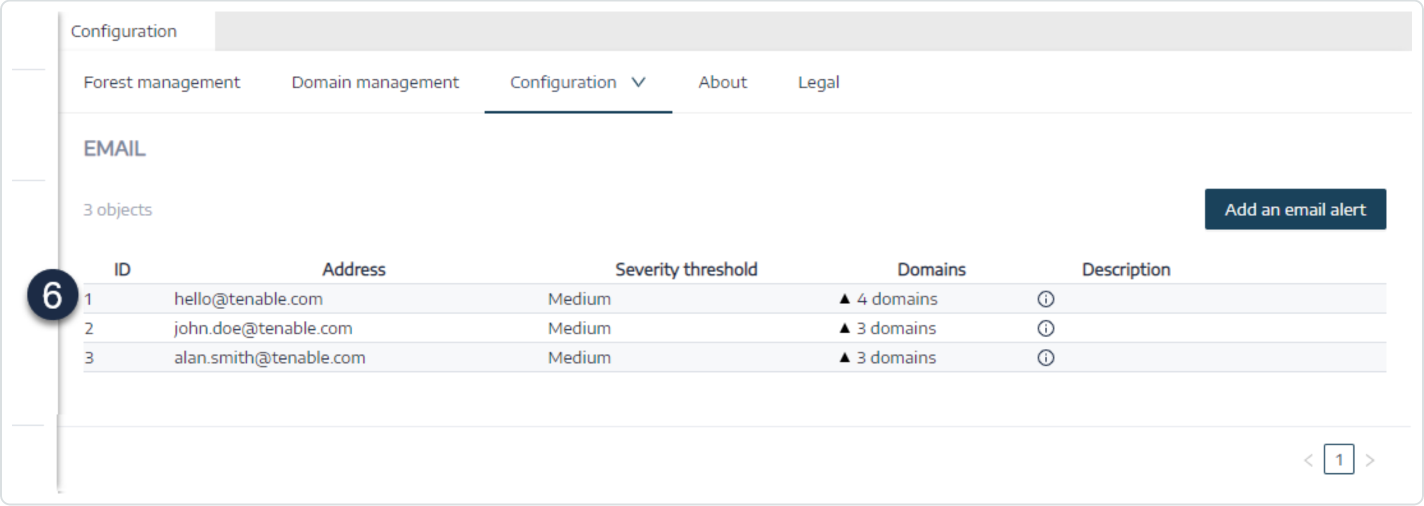
Indicators of Exposure

■ Critical ^

- □ Privileged accounts running Kerberos services
- ☑ Native administrative group members
- ☑ Ensure SDProp consistency
- ☑ Dangerous Kerberos delegation

Alert ID

This example shows the unique ID of the alert (6), which you can see in the list of configured email addresses in Tenable Identity Exposure's **System** > **Configuration** > **Email**.



EMAIL

3 objects

ID	Address	Severity threshold	Domains	Description
1	hello@tenable.com	Medium	▲ 4 domains	ⓘ
2	john.doe@tenable.com	Medium	▲ 3 domains	ⓘ
3	alan.smith@tenable.com	Medium	▲ 3 domains	ⓘ

Health Checks

The **health check** feature in Tenable Identity Exposure provides you with real-time visibility into the configuration of your domains and service accounts in one consolidated view, from which you can drill down to investigate any configuration anomalies leading to connectivity or other issues in your infrastructure. It verifies that everything is properly set up to ensure the smooth operation of Tenable Identity Exposure and gives you the ability to take quick and precise actions to remedy issues, as well as the confidence that your configuration settings are optimal to enable Tenable Identity Exposure to function efficiently.

Health checks are visible by default for administrative roles and by permission for certain user roles. You can also create Syslog or email alerts on each change in health check status.

Heath Checks and DC Sync Attack Detection

Health checks provide valuable information about the status and usability of Tenable Identity Exposure services. It verifies the service account's capability to collect sensitive information like password hashes and DPAPI backup keys used for Privileged Analysis. In the health check report, Tenable attempts to collect sensitive data to determine if the service account has the Privileged Analysis feature properly configured, without actually collecting anything if this feature is not in use. To prevent detection of a DCSync attack during this process, Tenable automatically whitelists the provided service account for the DCSync Indicator of Attack.

Domain Status

Tenable Identity Exposure performs the following checks for each domain:

- Authentication to the AD domain — LDAP settings and status, credentials, and SMB access
- Domain reachability — Working connection to the dynamic RPC port, a reachable SMB server, a reachable domain controller IP address or FQDN, a working connection to the RPC port, a reachable LDAP server, and a reachable global catalog LDAP server.
- Permissions — Ability to access AD domain data and collect privileged data.
- Domain Linked to Relay — The domain is correctly associated to a relay service.

Platform Status

Tenable Identity Exposure performs the following checks on your platform configuration:

- Running Relay service — Whether or not the Relay configuration is correct with troubleshooting tips.
- Relay version consistency — Whether or not the Relay version is consistent with the Tenable Identity Exposure version.
- Running AD data collector service — Whether or not the data collector service, broker, and collector bridge are operational to relay data to other services.

To access health checks:

1. At the bottom-left corner of the Tenable Identity Exposure page, hover over the ♥ icon to see the global status of your infrastructure.
2. Click on the icon to open the **Health Check** page. Under the **Domain Status** or the **Platform Status** tab, you see either one of the following:
   - A message that all health checks passed
   - A list of warnings or issues with specific statuses:

✓	The check succeeded and shows a normal result.
✗	The check failed and identifies an issue.
⚠	The check failed but the issue does not prevent Tenable Identity Exposure from working correctly. For example, the check for data collection will result in failure due to a misconfiguration of the Active Directory on the client end if the service account cannot collect privileged data. However, it is not a serious issue because you haven't activated the Privileged Analysis feature on this domain in Tenable Identity Exposure, hence the warning. But if you activate Privileged Analysis, the check will immediately fail.
?	The check shows an unknown result because a dependent check failed. For example, the check for network reachability cannot proceed if the check for authentication failed.

To see all health checks:

- Above the list of health checks on the right, click the toggle **Show successful checks** to enabled to list all the checks that Tenable Identity Exposure performed with the following information:
    - Health check name
    - Status (pass, fail, fail but non-blocking, or unknown)
    - Impacted domain and its associated forest (for domain status checks only)
    - Time of the last check performed
    - How long the check has remained in this status

To refresh the health check page:

- Although it performs health checks on a regular basis, Tenable Identity Exposure does not update the page with the results in real time. Click on ↻ to refresh the list of results.

To filter results by health check type or by domain:

1. Above the list of health checks on the right, click on **n/n health checks** or **n/n domains** (for domain status only).

   The **Health Checks** or **Forests and Domains** pane opens.

2. Select the health check types or forests/domains (if applicable) and click on **Filter on selection**.

To drill down for more information on each health check:

1. In the list of health checks, click on a health check name or the blue arrow (→) at the end of the line.

   The Details pane opens and shows a description of the check and a list of relevant details.

Health Check Name	Type	Description of Check	Reasons

Domain Reachability	Domain	Ability to establish a connection with the AD domain	• `IP-UNREACHABLE R-LDAP-GLOBAL-CATALOG-UNREACHABLE` • `LDAP-SERVER-UNREACHABLE` • `SMB-SERVER-UNREACHABLE` • `DYNAMIC-RPC-CONNECTION-NOT-WORKING` • `RPC-CONNECTION-NOT-WORKING`
Authentication to the AD Domain	Domain	Ability to authenticate to the AD domain	• `INCORRECT-CREDENTIALS` • `LDAP-SERVER-BUSY` • `LDAP-SERVER-UNAVAILABLE` • `LDAP-SERVER-ACCESS-DENIED` • `SMB-SERVER-ACCESS-DENIED`
Permissions to Collect the AD Domain Data	Domain	Ability to collect the AD domain data	• `MISSING-PERMISSIONS-PRIVILEGED-DATA`
Permissions to	Domain	Ability to can access	• `MISSING-`

Access the AD Containers		the AD containers	`PERMISSIONS-DELETED-OBJECTS-ACCESS` • `MISSING-PERMISSIONS-PASSWORD-SETTINGS-ACCESS`
Domain Linked to Relay	Domain	The domain is linked to a Relay	• `LINKED-TO-RELAY-DOWN`
Relay Service Up	Platform	The Relay is working as expected	• `RELAY-DOWN`
Relay Service Version	Platform	The Relay version is aligned with the product	• `VERSION-MISMATCH`
AD Data Collector Up	Platform	The AD data collector is working as expected	• `DATA-COLLECTOR-SERVICE-DOWN` • `DATA-COLLECTOR-BRIDGE-DOWN` • `BROKER-DOWN`

2. Click the arrow at the end of the detail line to expand it and show more information about the result.

To hide the health check status icon:

By default, Tenable Identity Exposure shows the health check status icon at the bottom-left corner of the screen.

1. In Tenable Identity Exposure, go to **System** in the left navigation bar and select the **Configuration** tab.

Alternatively, you can click on ⋯ at the top-right corner of the Health Check page and select **Configuration**.

2. Under **Application Services**, select **Health Check**.

3. Click the toggle **Show the Global Health Check Status** to disabled.

   Tenable Identity Exposure hides the health check icon at the bottom-left corner of the screen.

To assign health check permissions to user roles:

1. In Tenable Identity Exposure, go to **Accounts** in the left navigation bar and select the **Roles Management** tab.

2. In the list of roles, select the user role and click on ✎ at the end of the line.

   The **Edit a role** pane opens.

3. Select the **System configuration entities** tab.

4. Select the **Health Check** entity and click the permission toggle from **Unauthorized** to **Granted**.

5. Click **Apply and close**.

For more information about permissions, see Set Permissions for a Role.

To set up alerts for health check status changes:

1. In Tenable Identity Exposure, go to **System** in the left navigation bar and select the **Configuration** tab.

   Alternatively, you can click on ⋯ at the top-right corner of the Health Check page and select **Alerts**.

2. Under **Alerting Engine**, select **Syslog** or **Email**.

3. Click **Add a Syslog alert** or **Add an email alert**.

   A new pane opens. For the complete procedure, see Alerts.

4. Under **Alert Parameters**, in the **Trigger the Alert** box, select **On health check status change** from the drop-down menu.

5. Click the arrow in the **Health Checks** box to select the health check type to trigger an alert, and click **Filter on selection**.

6. Click **Add**.

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.

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.

To create a report:

1. In the **Reporting Center** pane, click **Create a report**.

   The **Report configuration** pane opens.
2. Under **Report Type**, complete the following information:

   a. In **Report Type**, select either **Deviances** or **Attacks**.

   b. In **Indicators**, click **n/n indicators** to select either **Indicators of Exposure** (for deviances) or **Indicators of Attack** (for attacks) and click **Filter on selection**.

   c. In **Domains**, click **n/n domains** to select the forests or domains for the report and click **Filter on selection**.

   d. In **Profiles**, click the arrow to select a profile from the drop-down menu.

3. In **Report Name**, type a name for the report.

4. Under **Generation Parameters**, select the following settings:

   a. **Data timeframe** — The report encompasses the period preceding the current one such as previous day, week, month, or quarter.

   b. **Recurrence** — Tenable Identity Exposure generates a new report for each timeframe that you define: click the arrow to select the corresponding values from the drop-down menu.

   c. **Time zone** — The time zone associated to the report.

5. Under **Recipients**, click **Add emails** and type the email address for the recipient. You can add as many recipients as necessary.

   For information on how to set up emails for report recipients, see SMTP Server Configuration

6. Click **Create report**.

To allow users to download a report:

- At the top of the **Reporting Center** pane, under **Reports access key**, click ⧉ to copy it. This access key is required to download the report from the link in the email sent to the recipient. It is unique for all users and reports.

- If necessary, click ↻ to generate a new access key.

  > **Caution**: Generating a new access key renders the previous one unusable. Only the new access key can grant access to the existing reports.

To edit the report configuration:

1. In the list of reports, select a report and click ✎ at the end of the line to open the **Report configuration** pane.

2. Modify as necessary.

3. Click **Save**.

To delete a report:

1. In the list of reports, select a report and click 🗑 at the end of the line to delete it.

   A message asks you to confirm the deletion.

2. Click **Delete**.

   The most recently generated report associated to this report configuration is no longer available for download.

To grant permissions to roles:

- In **Permissions Management**, under **Data Entities** > **Reports**, administrators can grant permissions to user roles to create, read, or edit all or specific report configurations.

  For more information, see Set Permissions for a Role.

See also

- Widgets

Microsoft Entra ID Support

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. Configure Microsoft Entra ID settings
4. Activate Microsoft Entra ID support
5. Enable tenant scans

Prerequisites

You must have a **Tenable Vulnerability Management account** to use the Microsoft Entra ID support feature. This account allows you to configure Tenable scans for your Microsoft Entra ID and collect the results of these scans.

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.

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".

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.

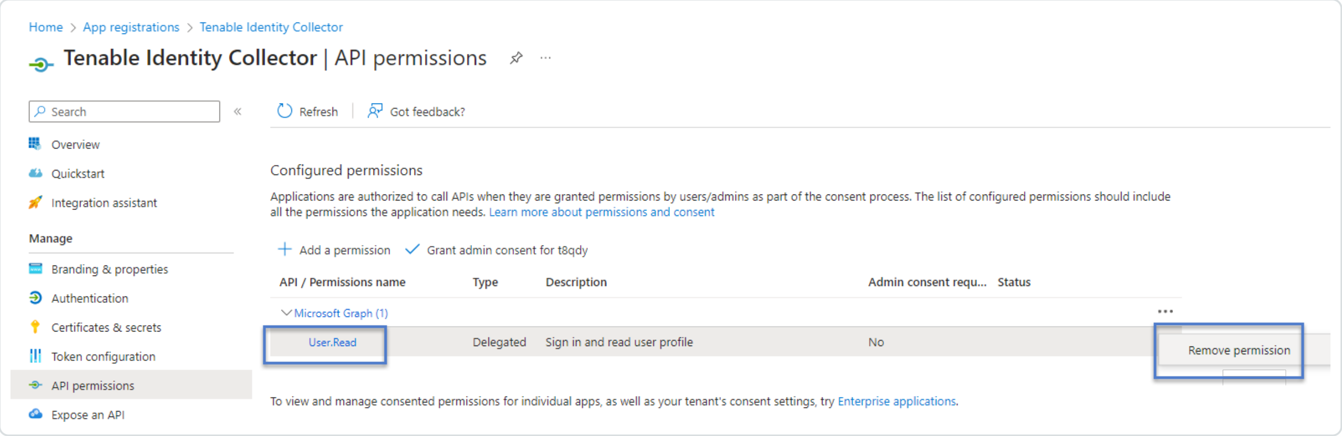
3. **Assign permissions to the application:**

   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:



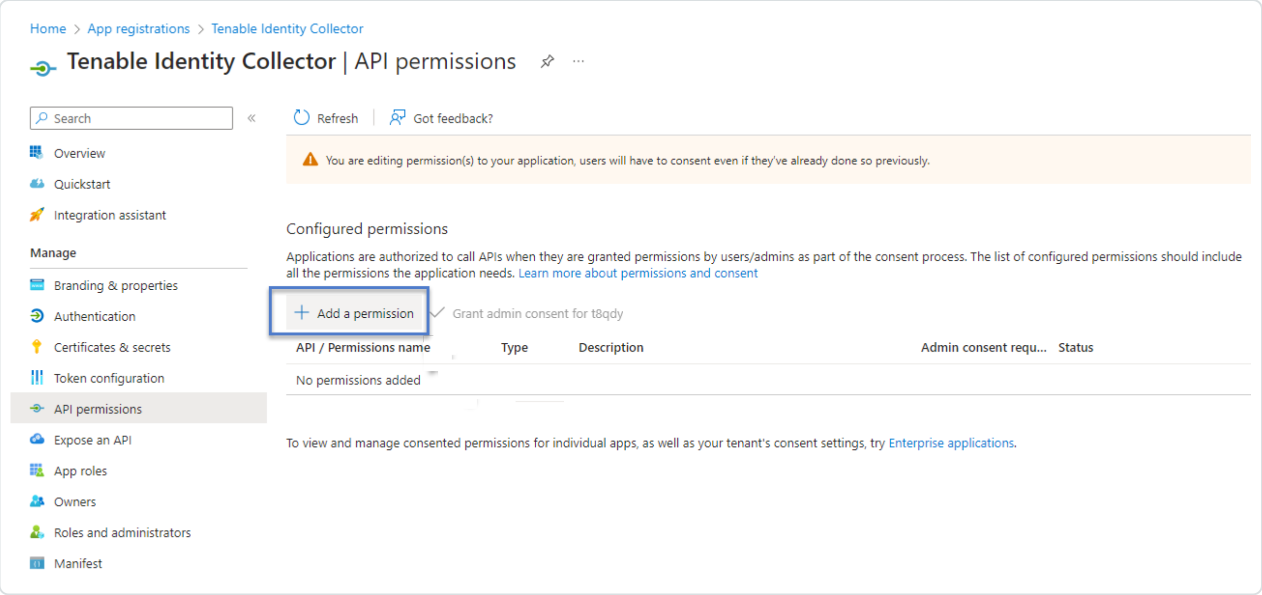
Configured permissions

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**:



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

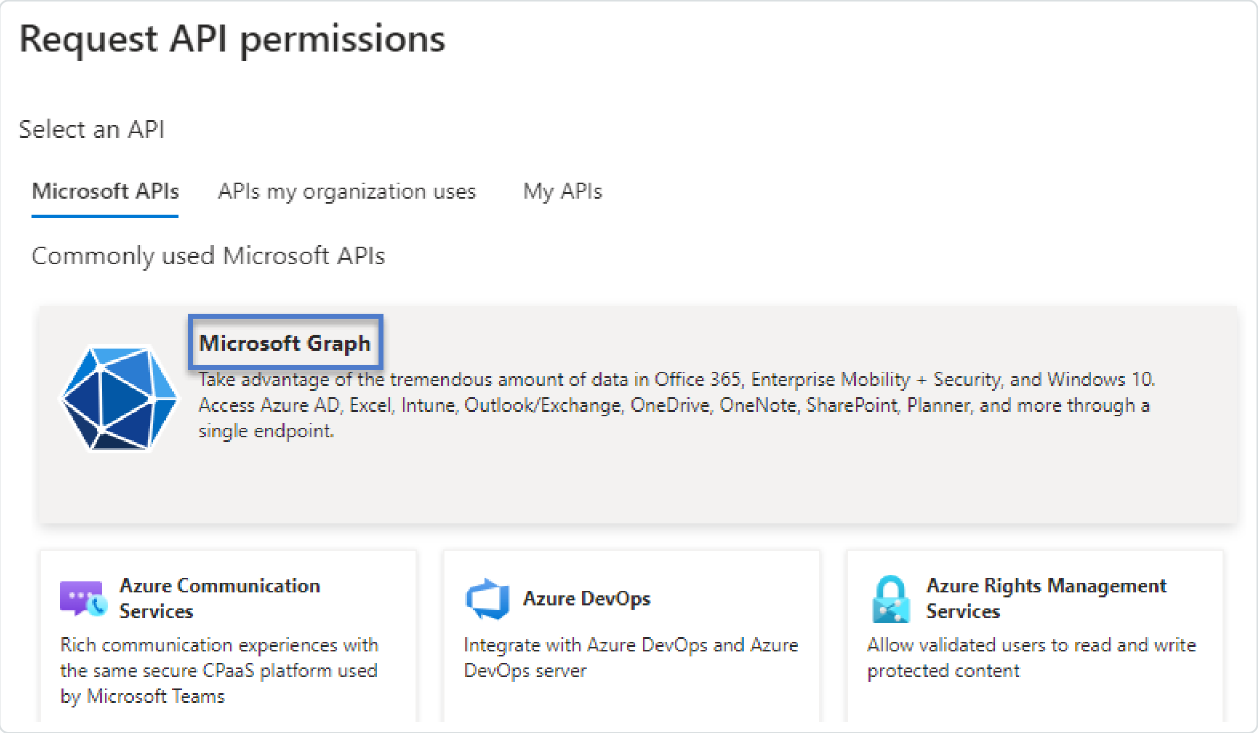
Configured permissions

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

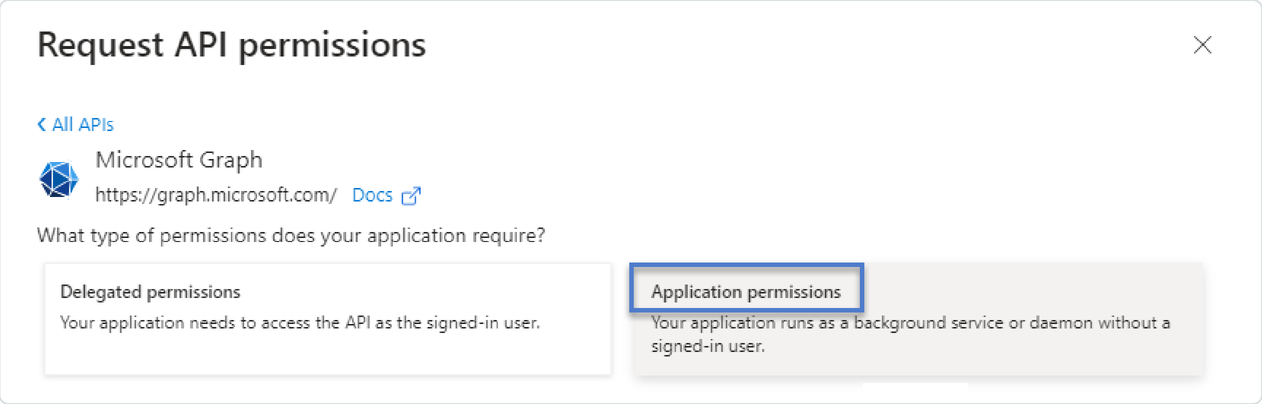
Microsoft Graph
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

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

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.

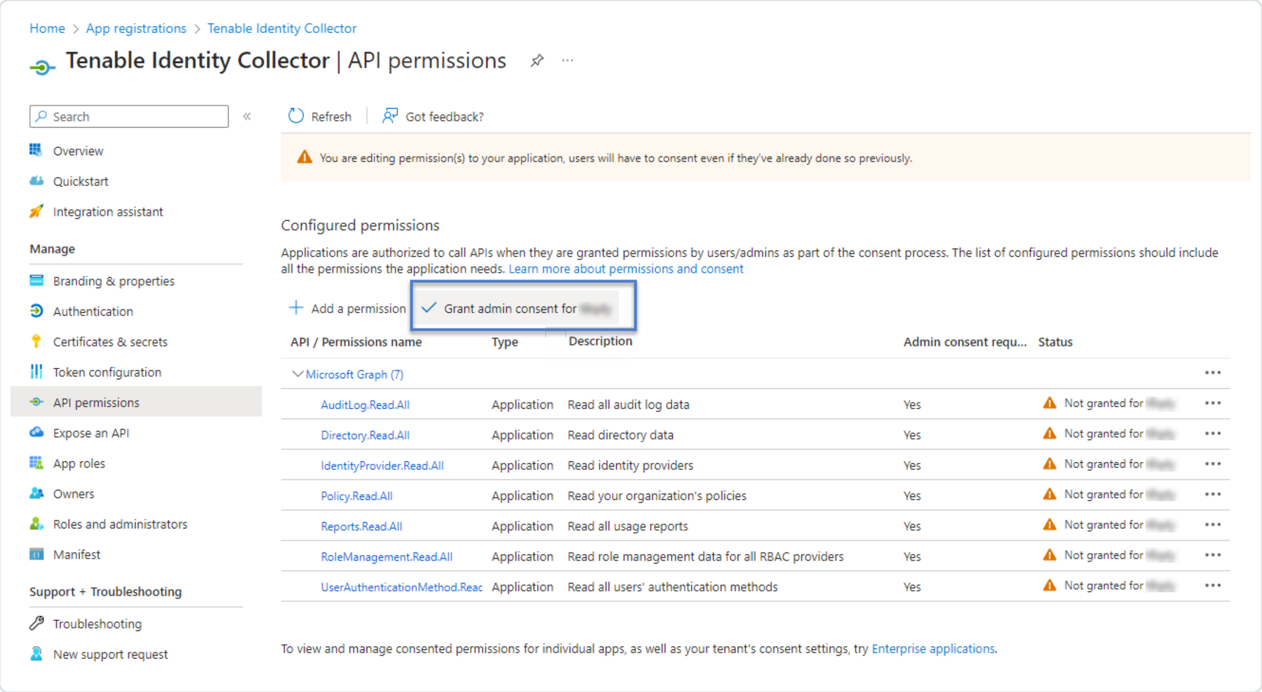
h. Use the list or the search bar to find and select all the following permissions:

- `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:



Home > App registrations > Tenable Identity Collector

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.

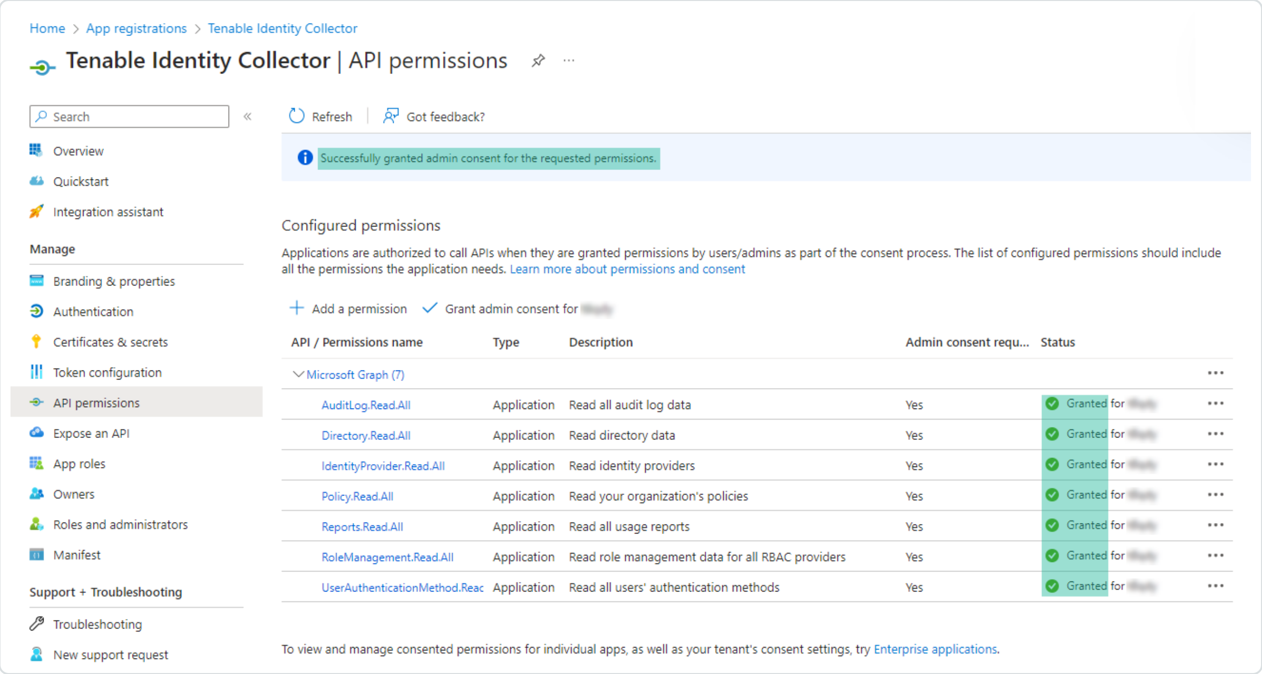
Configured permissions

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

+ Add a permission ✓ Grant admin consent for [redacted]

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.



Home > App registrations > Tenable Identity Collector

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

+ Add a permission ✓ Grant admin consent for [redacted]

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 activate Microsoft Entra ID support:

> **Note**: To activate this feature successfully, the Tenable Cloud user who created the access and secret keys must have administrative privileges in the Tenable Cloud container referenced by the Tenable Identity Exposure license. For more information, see Tenable Identity Exposure Licensing.

1. In Tenable Identity Exposure, click on the Systems icon ⚙ in the left navigation menu.

2. Click on the **Configuration** tab.

   The **Configuration** page opens.

3. Under Application Services, click on **Tenable Cloud**.

4. In **Activate Microsoft Entra ID** Support, click the toggle to enabled.

5. If you have not previously logged in to the Tenable Cloud, click the link to go to the login page:

   a. Click **Forgot your password?** to request a password reset.

   b. Type the email address associated with your Tenable Identity Exposure license and click **Request Password Reset**.

      Tenable sends an email to that address with a link to reset your password.

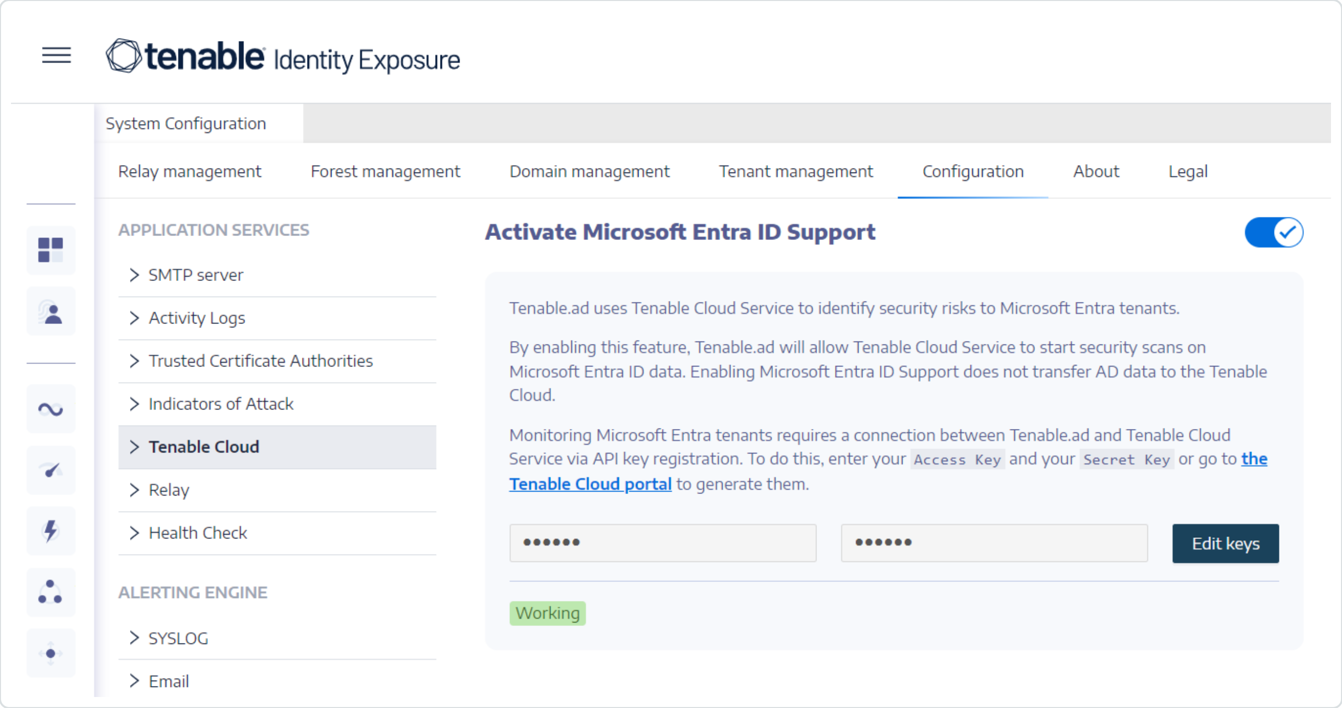
      > **Note**: If your email address is not the same as the one associated with the Tenable Identity Exposure license, contact your Customer Support for assistance.

6. Log in to Tenable Vulnerability Management.

7. To generate API keys in Tenable Vulnerability Management, go to Tenable Vulnerability Management > **Settings** > **My Account** > **API Keys**.

8. Enter your Tenable Vulnerability Management "Admin" user `AccessKey` and `SecretKey` to set up a connection between Tenable Identity Exposure and the Tenable Cloud Service.

9. Click **Edit keys** to submit the API keys.



Activate Microsoft Entra ID Support

Tenable.ad uses Tenable Cloud Service to identify security risks to Microsoft Entra tenants.

By enabling this feature, Tenable.ad will allow Tenable Cloud Service to start security scans on Microsoft Entra ID data. Enabling Microsoft Entra ID Support does not transfer AD data to the Tenable Cloud.

Monitoring Microsoft Entra tenants requires a connection between Tenable.ad and Tenable Cloud Service via API key registration. To do this, enter your `Access Key` and your `Secret Key` or go to **the Tenable Cloud portal** to generate them.

Tenable Identity Exposure shows a message to confirm that it updated the API keys.

Enable tenant scans

To add a new Microsoft Entra ID tenant:

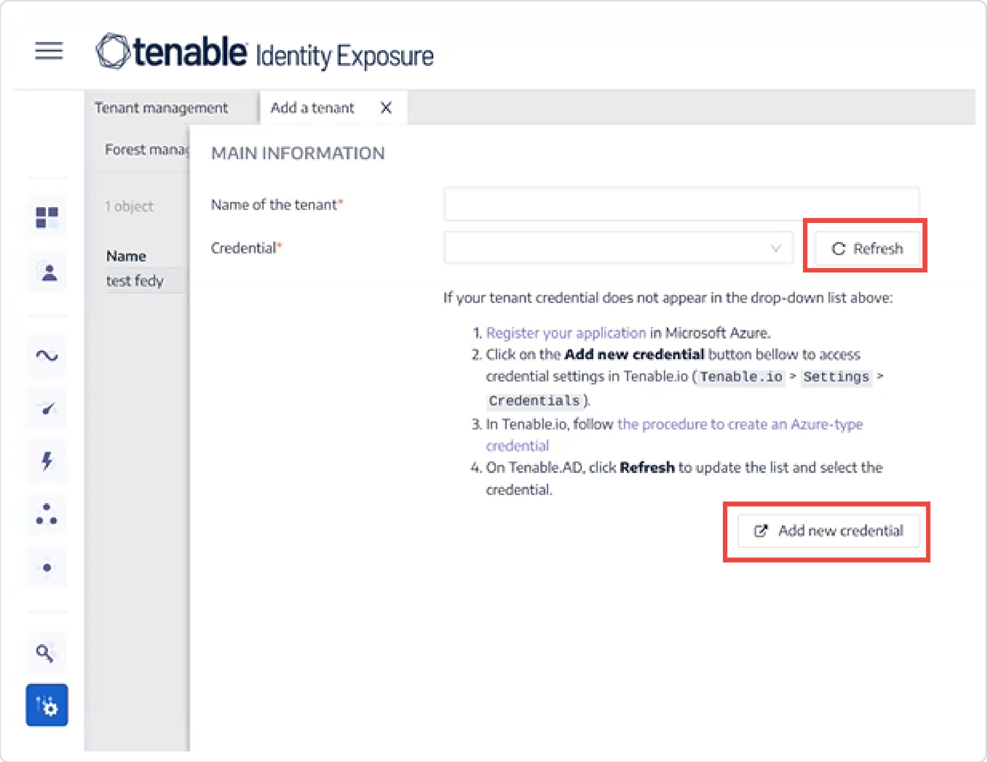
Adding a tenant links Tenable Identity Exposure with the Microsoft Entra ID tenant to perform scans on that tenant.

1. In the Configuration page, click on the **Tenant Management** 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.

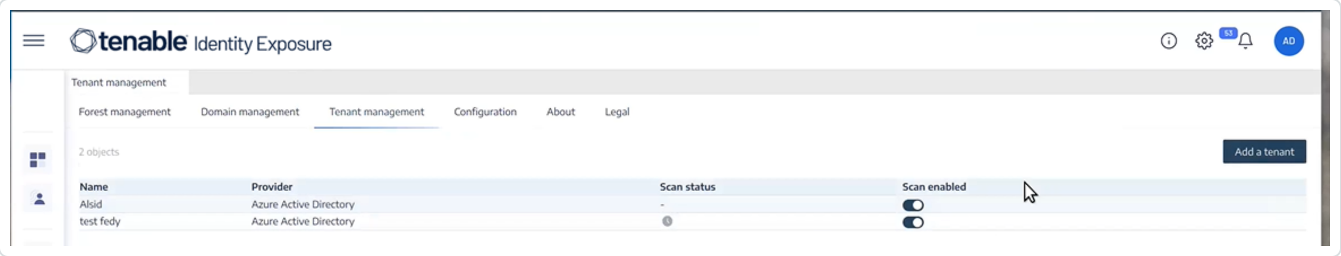
8. Click **Add**.

   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.

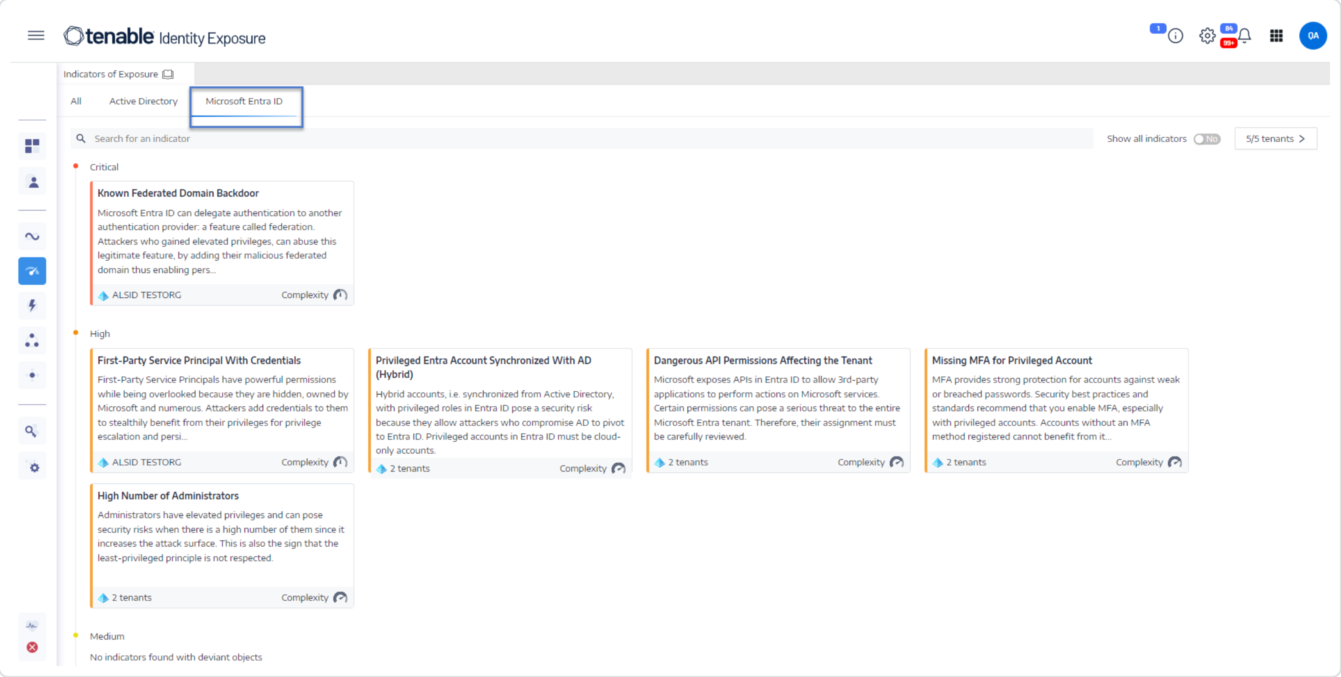
- Select a tenant on the list and click the toggle to **Scan enabled**.



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**.



Critical

Known Federated Domain Backdoor
Microsoft Entra ID can delegate authentication to another authentication provider: a feature called federation. Attackers who gained elevated privileges, can abuse this legitimate feature, by adding their malicious federated domain thus enabling pers...
ALSID TESTORG — Complexity

High

First-Party Service Principal With Credentials
First-Party Service Principals have powerful permissions while being overlooked because they are hidden, owned by Microsoft and numerous. Attackers add credentials to them to stealthily benefit from their privileges for privilege escalation and persi...
ALSID TESTORG — Complexity

Privileged Entra Account Synchronized With AD (Hybrid)
Hybrid accounts, i.e. synchronized from Active Directory, with privileged roles in Entra ID pose a security risk because they allow attackers who compromise AD to pivot to Entra ID. Privileged accounts in Entra ID must be cloud-only accounts.
2 tenants — Complexity

Dangerous API Permissions Affecting the Tenant
Microsoft exposes APIs in Entra ID to allow 3rd-party applications to perform actions on Microsoft services. Certain permissions can pose a serious threat to the entire Microsoft Entra tenant. Therefore, their assignment must be carefully reviewed.
2 tenants — Complexity

Missing MFA for Privileged Account
MFA provides strong protection for accounts against weak or breached passwords. Security best practices and standards recommend that you enable MFA, especially with privileged accounts. Accounts without an MFA method registered cannot benefit from it...
2 tenants — Complexity

High Number of Administrators
Administrators have elevated privileges and can pose security risks when there is a high number of them since it increases the attack surface. This is also the sign that the least-privileged principle is not respected.
2 tenants — Complexity

Medium

No indicators found with deviant objects

Tenable Cloud Data Collection

Tenable Cloud — the data collection feature in Tenable Identity Exposure — transfers your information to its private cloud to provide security analysis and services. For more information about data collection, see Tenable's Trust and Assurance statement.

To use Tenable Cloud:

1. In Tenable Identity Exposure, click **System** on the side navigation bar, click **System**.

   The **System Configuration** pane opens.

2. Select the **Configuration** tab.

3. Under the **Application Services** section, click **Tenable Cloud**.

   The **Tenable Cloud** pane opens.

4. Click the Use Tenable Cloud service toggle to **enabled**.

   A message confirms that Tenable Identity Exposure updated the information transfer configuration.

Privileged Analysis

Privileged Analysis is an optional feature in Tenable Identity Exposure that requires more privileges — contrary to its other features — to fetch otherwise protected data and provide more security analysis.

Data Fetching

> Note: The Privileged Analysis feature requires elevated privileges. See Access for Privileged Analysis.

When enabled, Privileged Analysis fetches the following additional data:

- **Password hashes** — Tenable Identity Exposure fetches LM and NT hashes for password analysis. Tenable Identity Exposure fetches LM hashes only to warn about their presence as they use an old and weak algorithm but does not store them. The hashes collection scope includes:
  - All enabled user accounts
  - All enabled domain controller computer accounts

Data Protection

The Active Directory (AD) itself does not directly store user passwords — only their hashes using the LM or NT hashing algorithms which do not allow recovery of the original password. Tenable Identity Exposure does not store LM hashes.

Except for clients hosting their Relay in a SAAS-VPN platform, passwords never leave the client's infrastructure, as only the Relay handles them. The Relay does not store passwords but retrieves the user's password every time it's needed for analysis, keeping it in its cache only temporarily, typically for just a few milliseconds. However, Tenable Identity Exposure retains a minimal number of bits of password hash data, securely stored in the Relay's RAM, solely for performing a K-anonymity analysis to check for users with identical passwords.

> **Note**: For SaaS-VPN platform clients, the behavior is the same, but it is Tenable that hosts your Relay.

Activity Logs

The activity logs in Tenable Identity Exposure allow you to view the traces of all activities that occurred on the Tenable Identity Exposure platform related to specific IP addresses, users, or actions.

To configure the activity logs:

1. Under **Management** in the Tenable Identity Exposure side navigation pane, click **System**.

   The **System Configuration** pane opens.

2. Under the **Application Services** section, click **Activity Logs**.

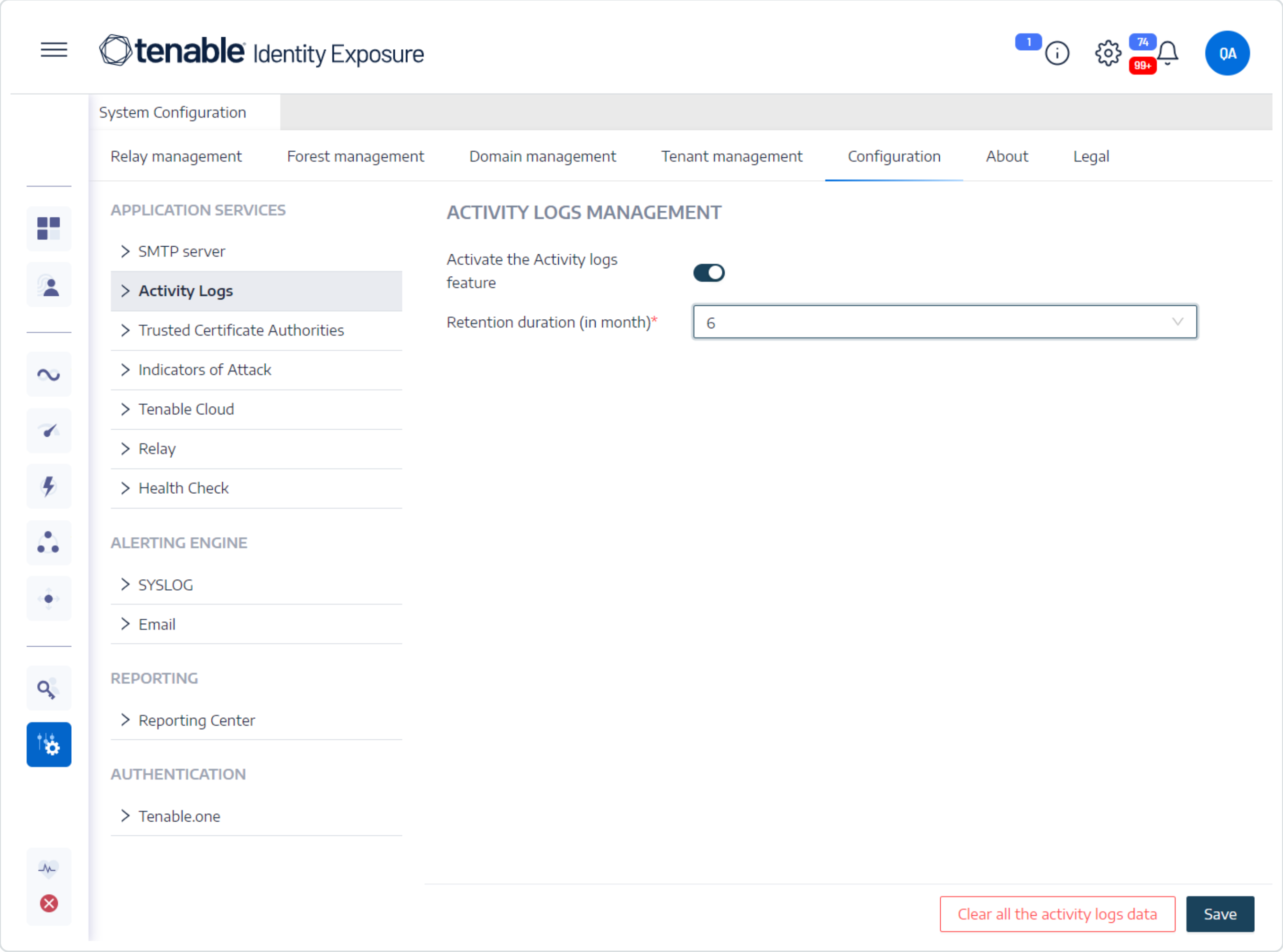
   The **Activity Logs Management** pane opens.

3. To activate the activity logs feature, click the toggle to **enabled**.

4. In the Retention duration (in months) box, click **>** to select the number of months to log activities.

5. Click **Save**.

A message confirms that Tenable Identity Exposure updated the settings.



ACTIVITY LOGS MANAGEMENT

Activate the Activity logs feature

Retention duration (in month)* 6

To clear the activity logs data:

1. Under **Management** in the Tenable Identity Exposure side navigation pane, click **System**.

   The **System Configuration** pane opens.

2. Under the **Application Services** section, click **Activity Logs**.

   The **Activity Logs Management** pane opens.

3. Under **Clear all the activity logs data**, click **Clear**.

   A message asks you to confirm.

4. Click **Confirm**.

   A message confirms that Tenable Identity Exposure updated the settings.

To set permissions for a user's own activity logs:

1. Under **Management** in the Tenable Identity Exposure side navigation pane, click **Accounts**.

   The **User Accounts Management** pane opens.

2. Select the **Roles Management** tab.

3. In the list of roles, hover over the user role requiring this permission and click the ✎ icon at the end of the line.

   The **Edit a role** pane opens.

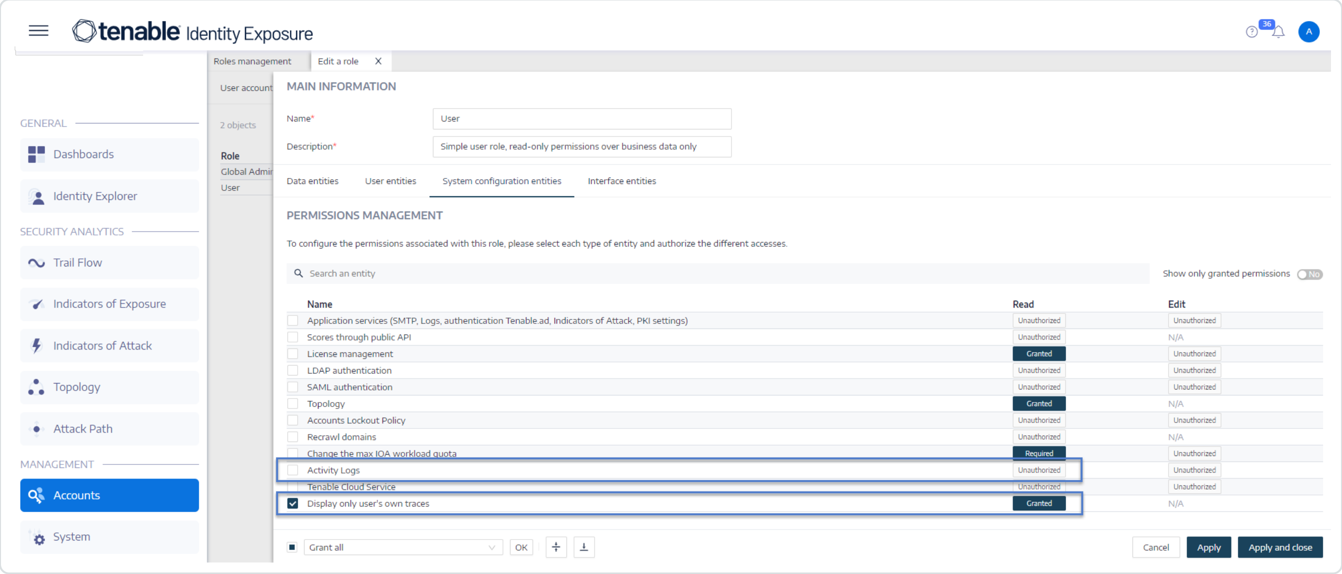
4. Under the **Main Information** section, select the **System Configuration Entities** tab.

5. Under the **Permissions Management** section, do the following:

   - Deselect the permission for **Activity Logs** to *Unauthorized*.
   - Select the permission for **Display only user's own traces** to *Granted*.

6. Click **Apply and Close**.

   A message confirms that Tenable Identity Exposure updated the user role.



MAIN INFORMATION

Name*: User

Description*: Simple user role, read-only permissions over business data only

PERMISSIONS MANAGEMENT

To configure the permissions associated with this role, please select each type of entity and authorize the different accesses.

	Name	Read	Edit
□	Application services (SMTP, Logs, authentication Tenable.ad, Indicators of Attack, PKI settings)	Unauthorized	Unauthorized
□	Scores through public API	Unauthorized	N/A
□	License management	Granted	Unauthorized
□	LDAP authentication	Unauthorized	Unauthorized
□	SAML authentication	Unauthorized	Unauthorized
□	Topology	Granted	N/A
□	Accounts Lockout Policy	Unauthorized	Unauthorized
□	Recrawl domains	Unauthorized	N/A
□	Change the max IOA workload quota	Required	Unauthorized
□	Activity Logs	Unauthorized	Unauthorized
□	Tenable Cloud Service	Unauthorized	Unauthorized
☑	Display only user's own traces	Granted	N/A

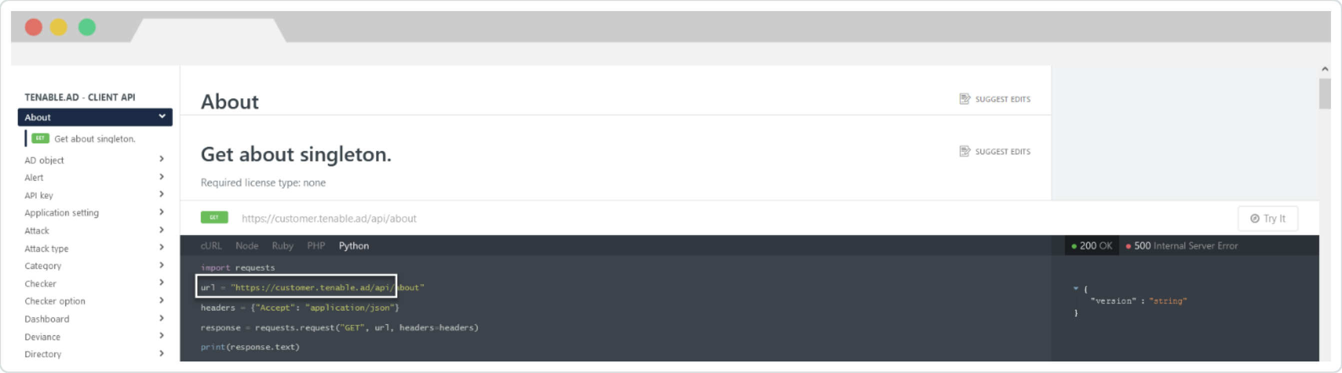
Tenable Identity Exposure Public API

Tenable Identity Exposure's API allows you to communicate with its database services.

The OpenAPI file containing Tenable Identity Exposure's API structure and resources is available here.

To access the API for your Tenable Identity Exposure instance:

- In your browser, open this URL:



About

Get about singleton.

Required license type: none

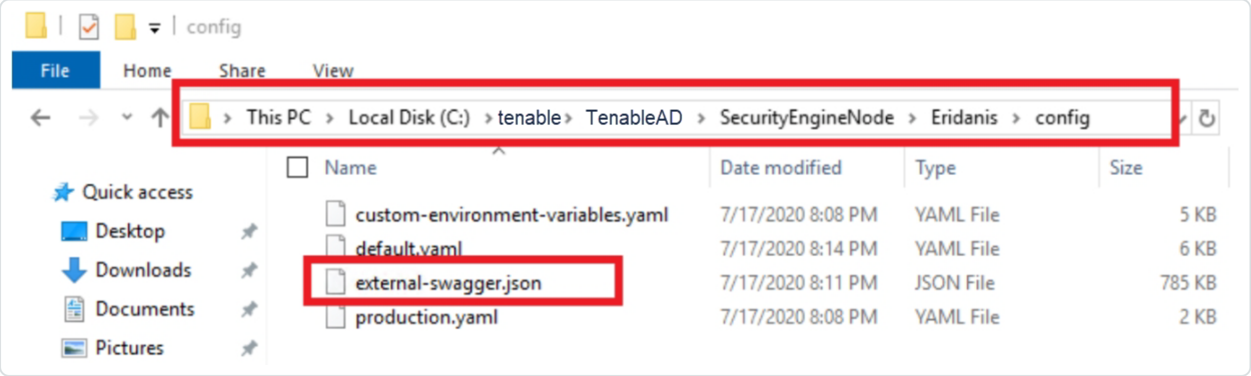
GET https://customer.tenable.ad/api/about

```
import requests
url = "https://customer.tenable.ad/api/about"
headers = {"Accept": "application/json"}
response = requests.request("GET", url, headers=headers)
print(response.text)
```

```
{
  "version" : "string"
}
```

To download the OpenAPI file:

- For on-premise installations, follow this path to the Security Engine Node:



This PC > Local Disk (C:) > tenable > TenableAD > SecurityEngineNode > Eridanis > config

Name	Date modified	Type	Size
custom-environment-variables.yaml	7/17/2020 8:08 PM	YAML File	5 KB
default.yaml	7/17/2020 8:14 PM	YAML File	6 KB
external-swagger.json	7/17/2020 8:11 PM	JSON File	785 KB
production.yaml	7/17/2020 8:08 PM	YAML File	2 KB

- For SaaS installations, go to the Tenable Identity Exposure API Explorer.

To retrieve an API key:

1. In Tenable Identity Exposure, click on your user profile icon and select **Preferences**.

   The Preferences pane opens.

2. From the menu, select **API key**.

   Tenable Identity Exposure shows your current API key.

3. To copy the API key to the clipboard, click the ⧉ icon.

To refresh an API key:

Access tokens expire if you click on **Refresh API key** or if you lose the right to generate an API key or access token. The expiration is not related to time or to the number of API requests. Generating or refreshing an API key is specific to the current user and does not interfere with other account API keys. When you obtain an API key, you also receive a refresh token. You can use this refresh token to retrieve a new API key.

> **Caution**: When you refresh your API key, Tenable Identity Exposure deactivates the current API key. You also receive a refresh token.

1. Click on **Refresh API key**.

   A message asks you for confirmation.

2. Click **Confirm**.

Data Management

Tenable Identity Exposure keeps data for six months. This data management period is not configurable.

Deployment Regions

Tenable Identity Exposure SaaS currently deploys in the following Azure regions:

Country	Azure Region
Americas	
Brazil — Sao Paulo	Brazil South
Canada — Quebec City	Canada East
Canada — Toronto	Canada Central
United States — California	West US
United States — Iowa	Central US
United States — Virginia	East US 2
Europe, Middle East, Africa	
France — Paris	France Central
Ireland	North Europe
Netherlands	West Europe
South Africa — Johannesburg	South Africa North
Switzerland — Zurich	Switzerland North
United Arab Emirates — Dubai	UAE North
United Kingdom — London	UK South
Asia Pacific	
Australia — New South Wales	Australia East
Australia — Victoria	Australia Southeast
Hong Kong	East Asia
India — Pune	Central India

Japan — Osaka	Japan West
Singapore	Southeast Asia

Tenable Identity Exposure Licensing

This topic breaks down the licensing process for Tenable Identity Exposure as a standalone product. It also explains how assets are counted and describes what happens during license overages or expirations. To learn how to use Tenable Identity Exposure, see the Tenable Identity Exposure User Guide.

Licensing Tenable Identity Exposure

Tenable Identity Exposure has two versions: a cloud version and an on-premises version. Tenable also offers subscription pricing in some cases.

To use Tenable Identity Exposure, you purchase licenses based on your organizational needs and environmental details. Tenable Identity Exposure then assigns those licenses to your *assets*: enabled users in your directory services.

When your environment expands, so does your asset count, so you purchase more licenses to account for the change. Tenable licenses use progressive pricing, so the more you purchase, the lower the per-unit price. For prices, contact your Tenable representative.

> **Tip**: To view your current license count and available assets, in the Tenable top navigation bar, click ⚙ and then click **License Information**. To learn more, see License Information Page.

> **Note**: Tenable offers simplified pricing to managed security service providers (MSSPs). To learn more, contact your Tenable representative.

How Assets are Counted

Each Tenable Identity Exposure license you purchase entitles you to scan one unique identity or digital representation of a user. Tenable does not double count identities. For example, enabled user accounts for the same identity in both Microsoft Active Directory and Microsoft Entra ID count as one Tenable license.

Tenable Identity Exposure Components

Both versions of Tenable Identity Exposure come with the following components:

- Trail Flow view
- Topology view
- Indicators of exposure
- Indicators of attacks
- Attack paths
- Identity Explorer
- Microsoft Entra ID support

Reclaiming Licenses

When you purchase licenses, your total license count remains static for the length of your contract unless you purchase more licenses. However, Tenable Identity Exposure reclaims licenses in real time when you delete enabled users from your environment's directory service.

Exceeding the License Limit

To allow for usage spikes due to hardware refreshes, sudden environment growth, or unanticipated threats, Tenable licenses are elastic. However, when you scan more assets than you have licensed, Tenable clearly communicates the overage and then reduces functionality in three stages.

Scenario	Result
You have more enabled identities than are licensed for three consecutive days	A message appears in Tenable Identity Exposure.
You have more enabled identities than are licensed for 15+ days	A message and a warning about reduced functionality appears in Tenable Identity Exposure.
You have more enabled identities than are licensed for 45+ days	A message appears in Tenable Identity Exposure; export features are disabled.

Expired Licenses

The Tenable Identity Exposure licenses you purchase are valid for the length of your contract. 30 days before your license expires, a warning appears in the user interface. During this renewal period, work with your Tenable representative to add or remove products or change your license count.

After your license expires, you can no longer sign in to the Tenable platform.

Manage Your License

Tenable Identity Exposure requires a license file from Tenable or through Authorized Enterprise Partners. The license user count covers all enabled users and service accounts.

You must upload the license file to configure and use Tenable Identity Exposure.

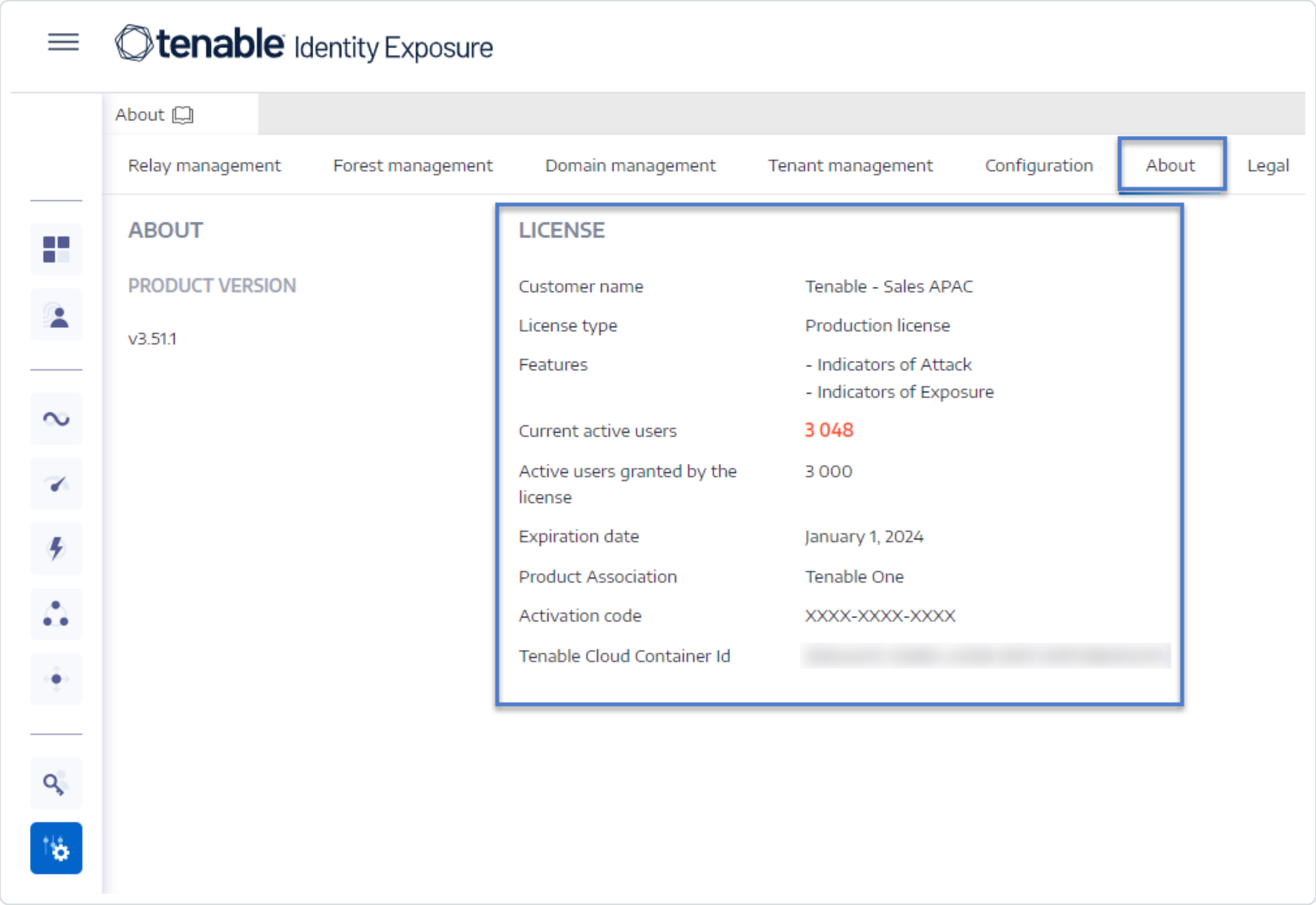
The Tenable Identity Exposure licenses can include:

- Indicators of Attack
- Indicators of Exposure
- Both of the above

To view your license:

- In Tenable Identity Exposure, click on the **Systems**⚙ > **About** tab.

  The license appears.



ABOUT

PRODUCT VERSION

v3.51.1

LICENSE

Customer name	Tenable - Sales APAC
License type	Production license
Features	- Indicators of Attack - Indicators of Exposure
Current active users	3 048
Active users granted by the license	3 000
Expiration date	January 1, 2024
Product Association	Tenable One
Activation code	XXXX-XXXX-XXXX
Tenable Cloud Container Id	[redacted]

License Consumption

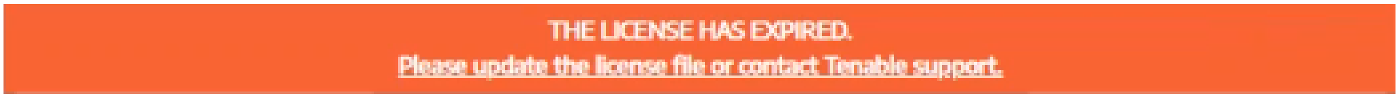
For on-premise installations, Tenable Identity Exposure tracks the license consumption if there is an internet connection available.

License Validity

The Tenable Identity Exposure license remains valid as long as you meet the following criteria:

- The number of users does not exceed the number granted on the license.
- The date of expiration is not past.

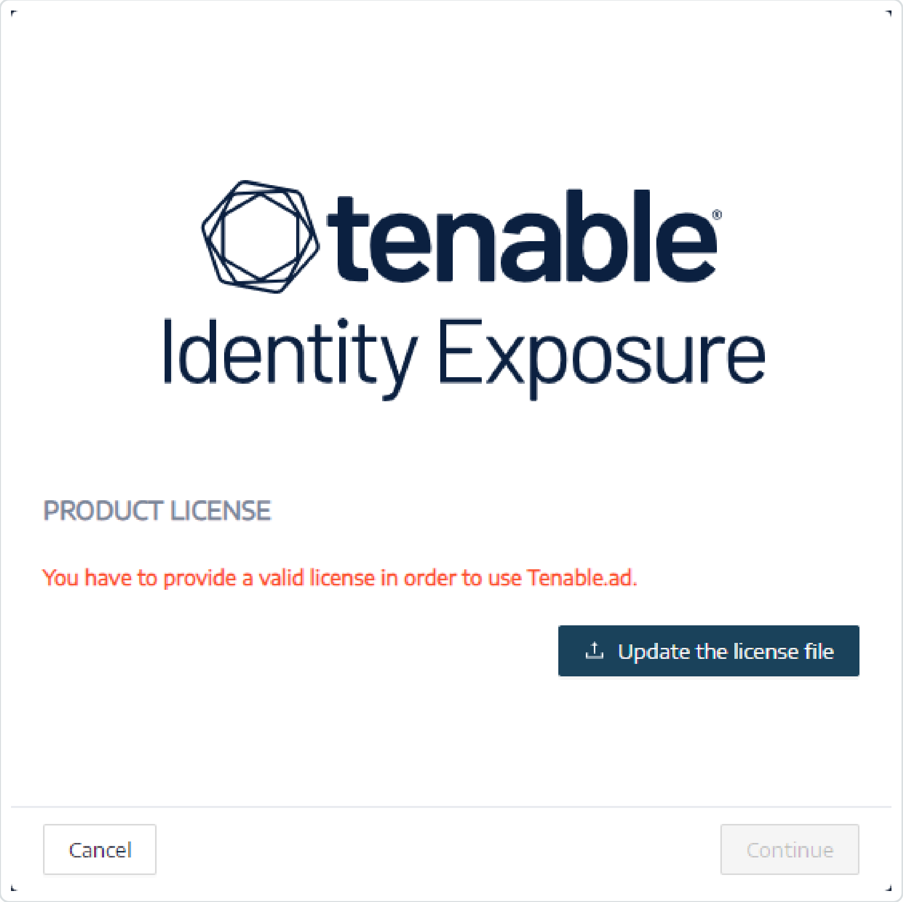
If you do not meet either of the above criteria, Tenable Identity Exposure displays a warning to prompt you to update your license:



THE LICENSE HAS EXPIRED.
Please update the license file or contact Tenable support.

To upload a license file:

1. From the login window, click **Update the license file**.

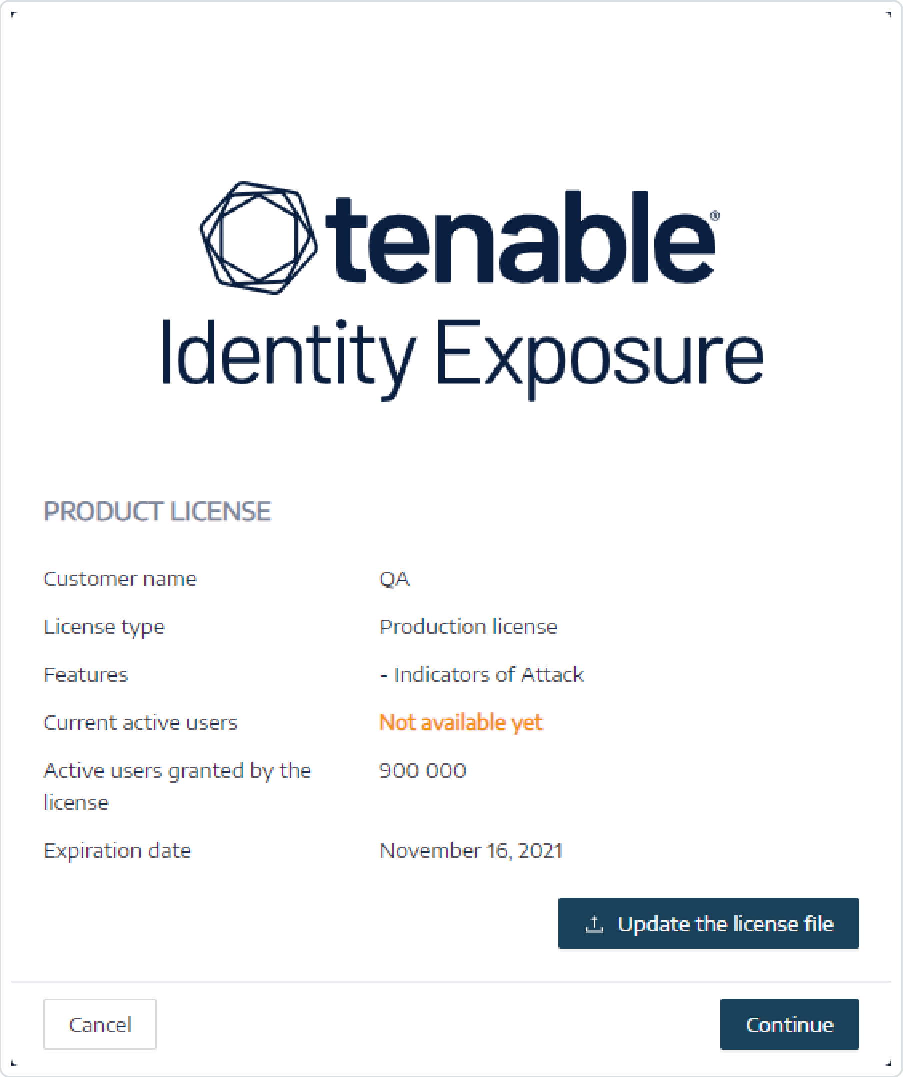


PRODUCT LICENSE

You have to provide a valid license in order to use Tenable.ad.

2. Browse to the location of your license file and click **Open**.

   The following example shows a successfully applied license file:



PRODUCT LICENSE

Customer name	QA
License type	Production license
Features	- Indicators of Attack
Current active users	Not available yet
Active users granted by the license	900 000
Expiration date	November 16, 2021

3. Click **Continue** to open Tenable Identity Exposure.

To update a license file:

1. In Tenable Identity Exposure, click **System** and **About**.
2. Click **Update the license file**.
3. Browse to the location of your license file and click **Open**.

   Tenable Identity Exposure updates your license file. In the case of an invalid license file, contact customer support.

Troubleshooting Tenable Identity Exposure

The following topics assist you with issues that may arise when using Tenable Identity Exposure (formerly known as Tenable.ad):

- Tenable Identity Exposure Diagnostics Tool
- SYSVOL Hardening Interference with Tenable Identity Exposure

Tenable Identity Exposure Diagnostics Tool

Tenable Identity Exposure provides a diagnostics tool that allows you to retrieve log information related to your Tenable Identity Exposure installation so that customer support can analyze and assist you with any issue.

You download this diagnostics tool from the Tenable downloads portal.

> **Note**: This diagnostics tool only works for **on-premises installations** of Tenable Identity Exposure.

The diagnostics tool can do the following:

- Identify whether the current machine (where you launched the executable file) hosts the Storage Manager (SM), Security Engine Node (SEN), or the Directory Listener (DL).
- Scan the environment to find other Tenable Identity Exposure installations available on your network.
- Detect a list of log sources related to your Tenable Identity Exposure installations to test and retrieve information about them accordingly.
- Retrieve MSI logs on failed Tenable Identity Exposure installation attempts.

Some tips for best results

- Run the diagnostics tool on the SEN.
- Run the diagnostics tool with an elevated user to activate most or all log sources.
- To detect the SM or other installation, check that you have the following conditions:
  - The configuration allows remote command to run on the remote computer (Invoke-Command cmdlet).
  - The configuration allows remote access to disks.
  - WMI is enabled and allowed for the current user account.

To run the diagnostics tool:

1. Download the file `TenableAdDiagnosticTool.OnPrem.Console.exe` from the Tenable downloads portal.

2. Run the executable file as an administrator on a Tenable Identity Exposure machine, preferably the one hosting the SEN.

3. At the prompt, type one of the following options:

   - `E` — All logs (default option)

   - `Msi` — Logs related to Tenable Identity Exposure installations

   - `Tenable` — Logs related to Tenable Identity Exposure

4. Press Enter.

   The diagnostics tool scans your installation. When the scan completes, the resulting output is a zipped file located in your current directory.

5. Send this zipped file to Tenable Identity Exposure customer support. Be sure not to alter the file contents in any way.

To run the diagnostics tool using the command line:

1. In the command line, run the executable file `TenableAdDiagnosticTool.OnPrem.Console.exe` as an administrator on the Tenable Identity Exposure machine, preferably the one hosting the SEN.

   The diagnostics tool scans your installation. When the scan completes, the resulting output is a zip file located in your current directory.

2. Send this zipped file to Tenable Identity Exposure customer support. Be sure not to alter the file contents in any way.

Other options

The diagnostics tool also offers the following options using the command line:

- `-- help` — A brief description of the diagnostics tool's usage.

- `-- commands` — A list of Powershell / WMI queries to test the machine capabilities and scan other installations.

SYSVOL Hardening Interference with Tenable Identity Exposure

SYSVOL is a shared folder located on each Domain Controller (DC) in an Active Directory domain. It stores the folders and files for Group Policies (GPOs). The content of SYSVOL replicates across all DCs, and is accessed via Universal Naming Convention (UNC) paths such as `\\<example.com>\SYSVOL` or `\\<DC_IP_or_FQDN>\SYSVOL`.

SYSVOL hardening refers to the use of the UNC Hardened Paths parameter, also known as “UNC hardened access”, “hardened UNC paths”, “UNC path hardening”, or “hardened paths”, etc. This feature came about to respond to the MS15-011 (KB 3000483) vulnerability in Group Policy. Many cybersecurity standards such as CIS Benchmarks mandate the enforcement of this feature.

When you apply this hardening parameter on Server Message Block (SMB) clients, it actually increases the security of the domain-joined machines to ensure that the GPO content they retrieve from SYSVOL is free from tampering by an attacker on the network. But in certain situations, this parameter can also interfere with Tenable Identity Exposure’s operation.

Follow the guidance in this troubleshooting section if you notice that hardened UNC paths are disrupting the connectivity between Tenable Identity Exposure and the SYSVOL share.

Affected environments

The following Tenable Identity Exposure deployment options may experience this issue:

- On-premises
- SaaS with Secure Relay

This deployment option is not affected:

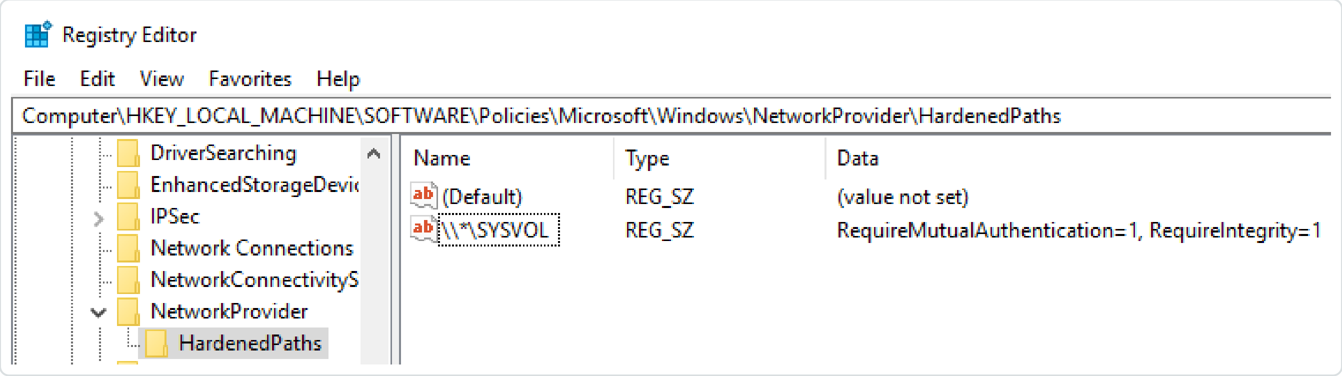
- SaaS with VPN

SYSVOL hardening is a client-side parameter, which means that it operates on the machines that connect to the SYSVOL share and not on the Domain Controllers.

Windows enables this parameter by default, and it can interfere with Tenable Identity Exposure.

Some organizations also want to ensure the activation of this parameter and enforce it by using the related GPO setting or by setting the corresponding registry key directly.

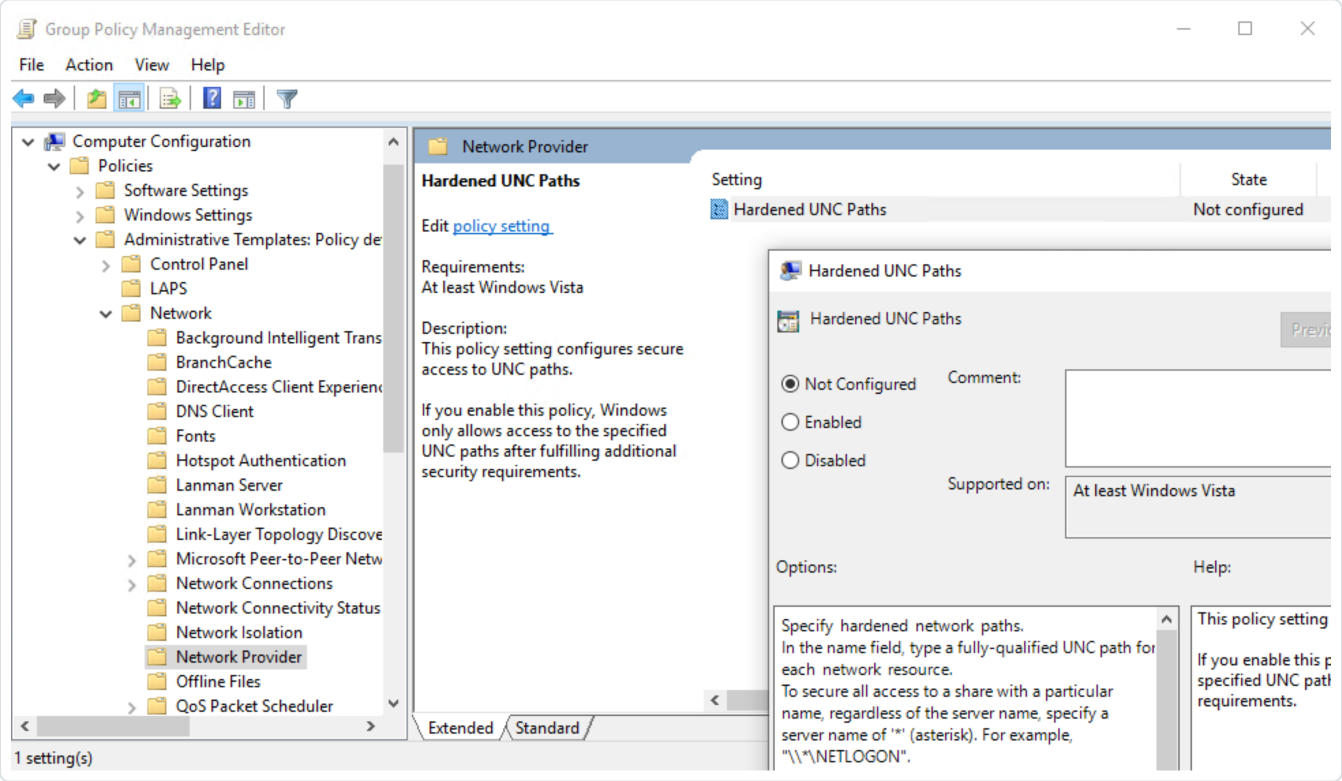
- You can find the registry keys related to UNC hardened paths under "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetworkProvider\HardenedPaths":



Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetworkProvider\HardenedPaths

Name	Type	Data
(Default)	REG_SZ	(value not set)
*\SYSVOL	REG_SZ	RequireMutualAuthentication=1, RequireIntegrity=1

- You can find the corresponding GPO setting under "Computer Configuration/Administrative Templates/Network/Network Provider/Hardened UNC paths":



Network Provider

Hardened UNC Paths

Edit policy setting

Requirements:
At least Windows Vista

Description:
This policy setting configures secure access to UNC paths.

If you enable this policy, Windows only allows access to the specified UNC paths after fulfilling additional security requirements.

Setting	State
Hardened UNC Paths	Not configured

Hardened UNC Paths

Hardened UNC Paths

● Not Configured
○ Enabled
○ Disabled

Comment:

Supported on: At least Windows Vista

Options:

Specify hardened network paths.
In the name field, type a fully-qualified UNC path for each network resource.
To secure all access to a share with a particular name, regardless of the server name, specify a server name of '*' (asterisk). For example, "\*\NETLOGON".

Help:

This policy setting

If you enable this p
specified UNC path
requirements.

1 setting(s)

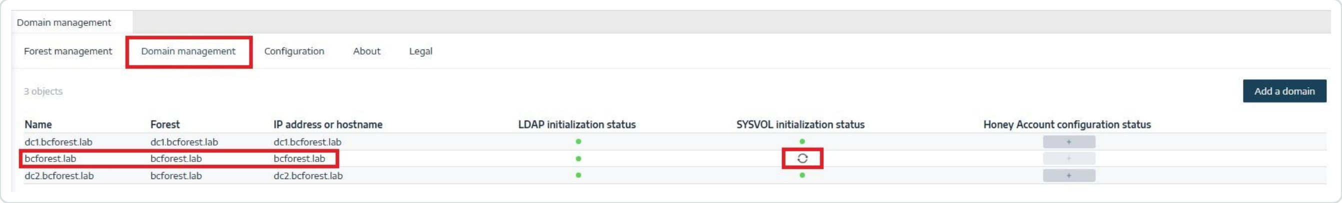
SYSVOL hardening enforcement occurs when a UNC path referring to SYSVOL – for example "\\*\SYSVOL" – has the parameters "RequireMutualAuthentication" and "RequireIntegrity" set to the value "1".

Signs of SYSVOL Hardening Issues

When you suspect that SYSVOL hardening interferes with Tenable Identity Exposure, check for the following:

1. In Tenable Identity Exposure, go to **System** > **Domain Management** to view the LDAP and SYSVOL initialization status for each domain.

   A domain with normal connectivity shows a green indicator, while a domain with connectivity issues can show a crawling indicator that continues endlessly.

   Domain management

   Forest management | Domain management | Configuration | About | Legal

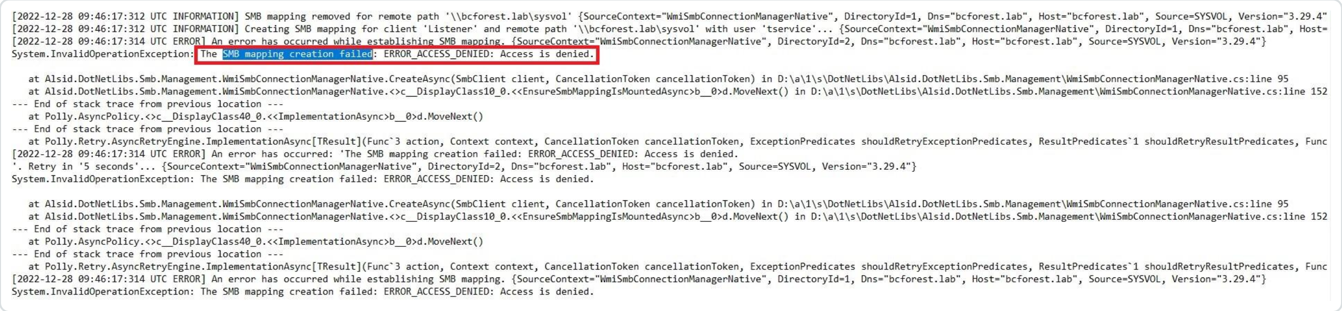
   3 objects

   Add a domain

Name	Forest	IP address or hostname	LDAP initialization status	SYSVOL initialization status	Honey Account configuration status
dc1.bcforest.lab	dc1.bcforest.lab	dc1.bcforest.lab	●	●	+
bcforest.lab	bcforest.lab	bcforest.lab	●	⟳	+
dc2.bcforest.lab	bcforest.lab	dc2.bcforest.lab	●	●	+

2. On the Directory Listener or Relay machine, open the logs folder: `<Installation Folder>\DirectoryListener\logs`.

3. Open the Ceti log file and search for the string "SMB mapping creation failed" or “Access is denied”. Error logs containing this phrase indicate that UNC hardening is likely in place on the Directory Listener or Relay machine.

```
[2022-12-28 09:46:17:312 UTC INFORMATION] SMB mapping removed for remote path '\\bcforest.lab\sysvol' {SourceContext="WmiSmbConnectionManagerNative", DirectoryId=1, Dns="bcforest.lab", Host="bcforest.lab", Source=SYSVOL, Version="3.29.4"
[2022-12-28 09:46:17:312 UTC INFORMATION] Creating SMB mapping for client 'Listener' and remote path '\\bcforest.lab\sysvol' with user 'tservice'... {SourceContext="WmiSmbConnectionManagerNative", DirectoryId=1, Dns="bcforest.lab", Host=
[2022-12-28 09:46:17:314 UTC ERROR] An error has occurred while establishing SMB mapping. {SourceContext="WmiSmbConnectionManagerNative", DirectoryId=2, Dns="bcforest.lab", Host="bcforest.lab", Source=SYSVOL, Version="3.29.4"}
System.InvalidOperationException: The SMB mapping creation failed: ERROR_ACCESS_DENIED: Access is denied.

   at Alsid.DotNetLibs.Smb.Management.WmiSmbConnectionManagerNative.CreateAsync(SmbClient client, CancellationToken cancellationToken) in D:\a\1\s\DotNetLibs\Alsid.DotNetLibs.Smb.Management\WmiSmbConnectionManagerNative.cs:line 95
   at Alsid.DotNetLibs.Smb.Management.WmiSmbConnectionManagerNative.<>c__DisplayClass10_0.<<EnsureSmbMappingIsMountedAsync>b__0>d.MoveNext() in D:\a\1\s\DotNetLibs\Alsid.DotNetLibs.Smb.Management\WmiSmbConnectionManagerNative.cs:line 152
--- End of stack trace from previous location ---
   at Polly.AsyncPolicy.<>c__DisplayClass40_0.<<ImplementationAsync>b__0>d.MoveNext()
--- End of stack trace from previous location ---
   at Polly.Retry.AsyncRetryEngine.ImplementationAsync[TResult](Func`3 action, Context context, CancellationToken cancellationToken, ExceptionPredicates shouldRetryExceptionPredicates, ResultPredicates`1 shouldRetryResultPredicates, Func
[2022-12-28 09:46:17:314 UTC ERROR] An error has occurred: 'The SMB mapping creation failed: ERROR_ACCESS_DENIED: Access is denied.
'. Retry in '5 seconds'... {SourceContext="WmiSmbConnectionManagerNative", DirectoryId=2, Dns="bcforest.lab", Host="bcforest.lab", Source=SYSVOL, Version="3.29.4"}
System.InvalidOperationException: The SMB mapping creation failed: ERROR_ACCESS_DENIED: Access is denied.

   at Alsid.DotNetLibs.Smb.Management.WmiSmbConnectionManagerNative.CreateAsync(SmbClient client, CancellationToken cancellationToken) in D:\a\1\s\DotNetLibs\Alsid.DotNetLibs.Smb.Management\WmiSmbConnectionManagerNative.cs:line 95
   at Alsid.DotNetLibs.Smb.Management.WmiSmbConnectionManagerNative.<>c__DisplayClass10_0.<<EnsureSmbMappingIsMountedAsync>b__0>d.MoveNext() in D:\a\1\s\DotNetLibs\Alsid.DotNetLibs.Smb.Management\WmiSmbConnectionManagerNative.cs:line 152
--- End of stack trace from previous location ---
   at Polly.AsyncPolicy.<>c__DisplayClass40_0.<<ImplementationAsync>b__0>d.MoveNext()
--- End of stack trace from previous location ---
   at Polly.Retry.AsyncRetryEngine.ImplementationAsync[TResult](Func`3 action, Context context, CancellationToken cancellationToken, ExceptionPredicates shouldRetryExceptionPredicates, ResultPredicates`1 shouldRetryResultPredicates, Func
[2022-12-28 09:46:17:314 UTC ERROR] An error has occurred while establishing SMB mapping. {SourceContext="WmiSmbConnectionManagerNative", DirectoryId=1, Dns="bcforest.lab", Host="bcforest.lab", Source=SYSVOL, Version="3.29.4"}
System.InvalidOperationException: The SMB mapping creation failed: ERROR_ACCESS_DENIED: Access is denied.
```

Remediation Options

There are two possible remediation options: Switching to Kerberos authentication or Disabling SYSVOL hardening.

Switching to Kerberos authentication

This is the preferred option since it avoids disabling the hardening feature.

It is only when connecting to the monitored Domain Controller(s) using NTLM authentication that SYSVOL hardening interferes with Tenable Identity Exposure. This is because NTLM is not compatible with the “`RequireMutualAuthentication=1`” parameter. Tenable Identity Exposure also supports Kerberos. It is not necessary to disable SYSVOL hardening if you configure and use Kerberos properly. For more information, see Kerberos Authentication

Disabling SYSVOL hardening

If you cannot switch to Kerberos authentication, you also have the option of disabling SYSVOL hardening.

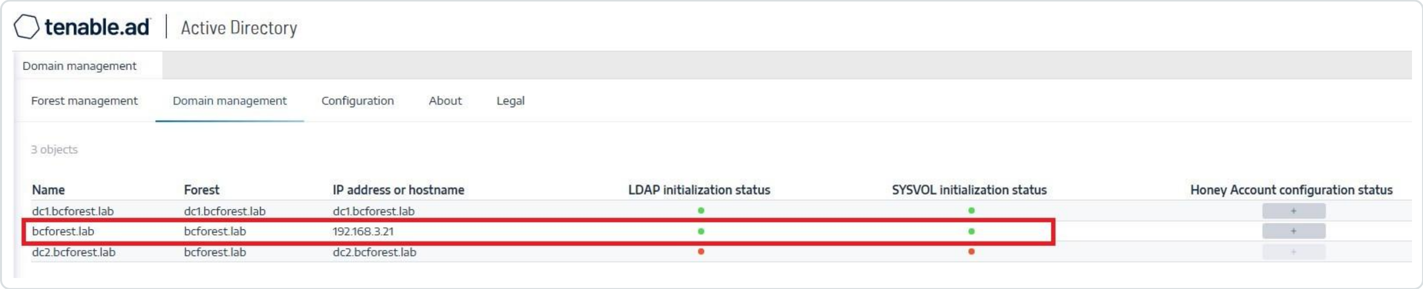
Windows enables SYSVOL hardening by default, so it is not sufficient to remove the registry key or the GPO setting. You must explicitly disable it and apply this change only on the machine hosting the Directory Listener (on-premises) or the Relay (SaaS with Secure Relay). This does not affect other machines, and you never need to disable SYSVOL hardening on the Domain Controllers themselves.

The Tenable Identity Exposure installers used on the machine hosting the Directory Listener (on-premises) or Relay (SaaS with Secure Relay) already disable SYSVOL hardening locally. However, a GPO or a script in your environment may remove or overwrite the registry key.

There are two possible cases:

- If the Directory Listener or Relay machine **is not domain-joined** — You cannot use a GPO to configure the machine. You must disable SYSVOL hardening in the registry (see Registry — GUI or Registry — PowerShell).
- If the Directory Listener or Relay machine **is domain-joined** (which Tenable Identity Exposure does not recommend) — You can either apply the setting directly either in the registry (see Registry — GUI or Registry — PowerShell) or using a GPO. Using any of these methods, you must ensure that a GPO or a script does not overwrite the registry key. You can do this in either way:
  - Carefully review all the GPOs that apply on this machine.
  - Apply the change and wait a bit, or force the GPOs application with “`gpupdate /force`”, and check that the registry key kept its value.

After you restart the Directory Listener or Relay machine, the crawling indicator on the modified domain should change to a green indicator:



tenable.ad | Active Directory

Domain management

Forest management | Domain management | Configuration | About | Legal

3 objects

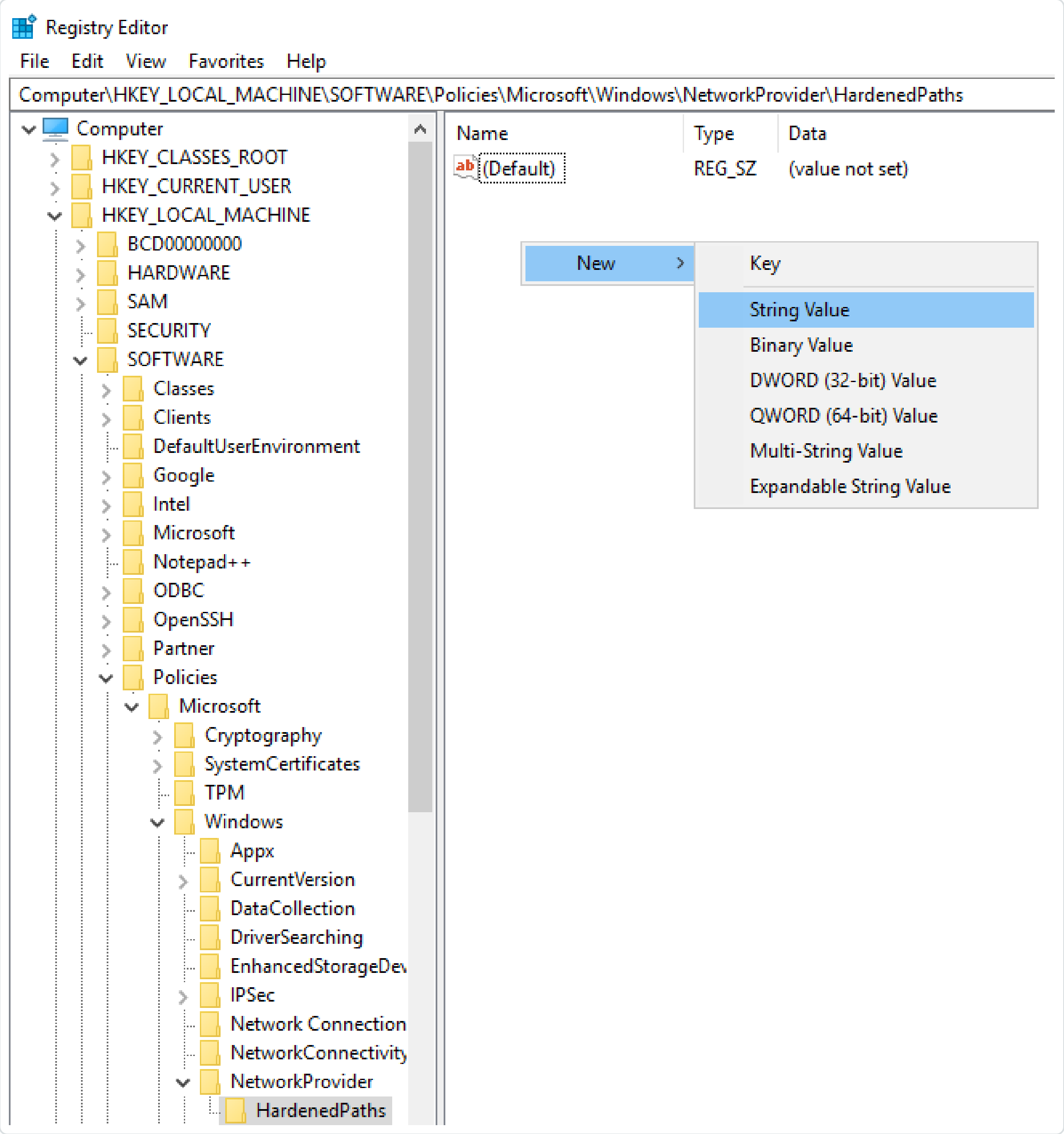
Name	Forest	IP address or hostname	LDAP initialization status	SYSVOL initialization status	Honey Account configuration status
dc1.bcforest.lab	dc1.bcforest.lab	dc1.bcforest.lab	🟢	🟢	+
bcforest.lab	bcforest.lab	192.168.3.21	🟢	🟢	+
dc2.bcforest.lab	bcforest.lab	dc2.bcforest.lab	🔴	🔴	+

Registry — GUI

To disable SYSVOL hardening in the Registry using the GUI:

1. Connect to the Directory Listener or Relay machine with administrative rights.
2. Open the Registry Editor and navigate to: `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetworkProvider\HardenedPaths`.
3. Create a key named "`\\*\SYSVOL`" if it doesn't already exist, as follows:

a. Right-click in the right pane and choose **New** > **String Value**.



Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetworkProvider\HardenedPaths

Name	Type	Data
(Default)	REG_SZ	(value not set)

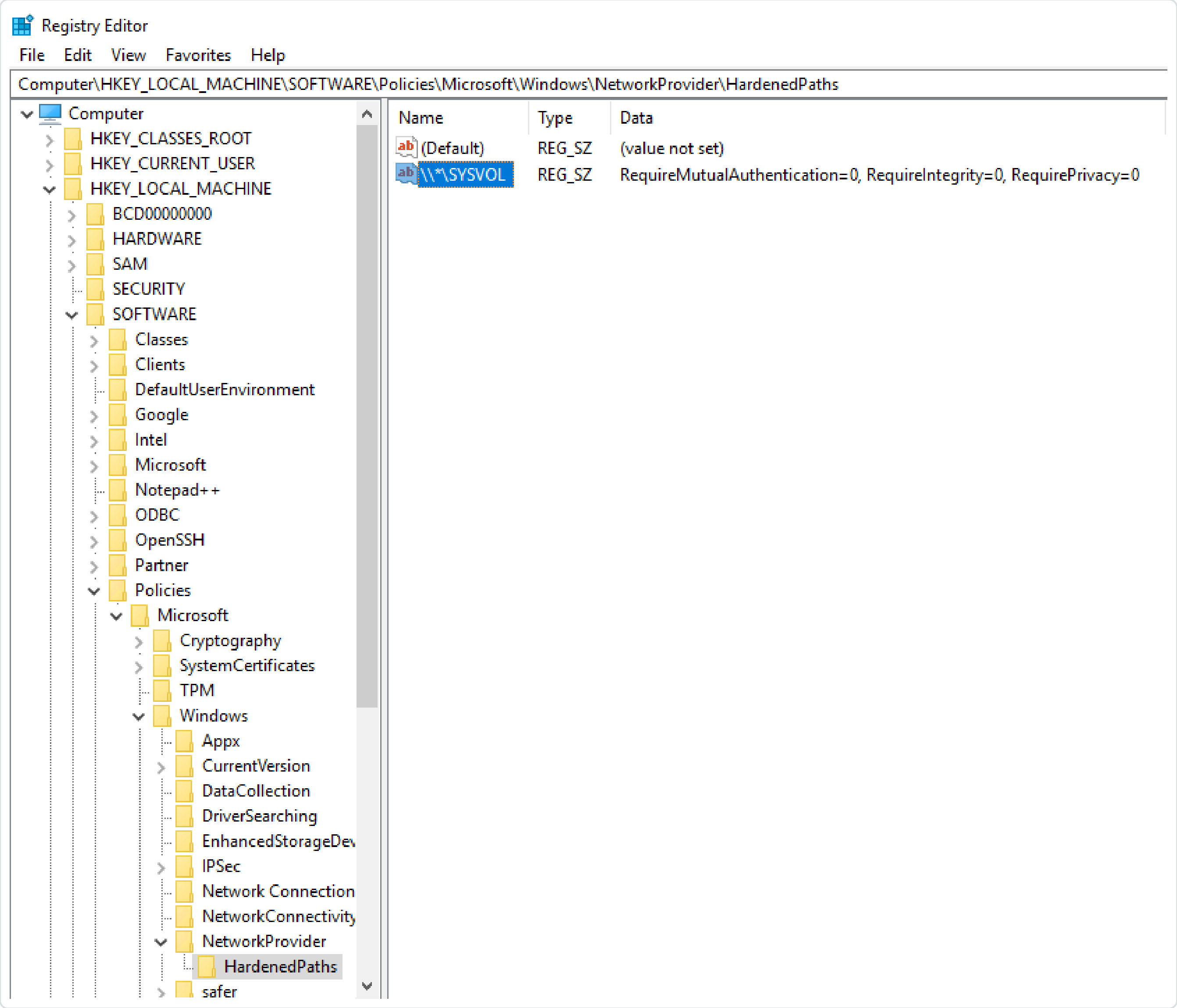
b. In the Name field, enter `\\*\SYSVOL`.

4. Double-click the "`\\*\SYSVOL`" key (newly created or previously existing) to open the **Edit String** window.

5. In the **Value** data field, enter the following value: `RequireMutualAuthentication=0`, `RequireIntegrity=0`, `RequirePrivacy=0`

6. Click **Save**.

   The result should appear as follows:



Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetworkProvider\HardenedPaths

Name	Type	Data
(Default)	REG_SZ	(value not set)
*\SYSVOL	REG_SZ	RequireMutualAuthentication=0, RequireIntegrity=0, RequirePrivacy=0

7. Restart the machine.

Registry — PowerShell

To disable SYSVOL hardening in the registry using PowerShell:

1. Collect the current values of the UNC hardened paths registry keys for reference using this PowerShell command:

   ```
   Get-Item -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\NetworkProvider\HardenedPaths"
   ```

2. Set the recommended value:

   ```
   New-ItemProperty -Path
   "HKLM:\SOFTWARE\Policies\Microsoft\Windows\NetworkProvider\HardenedPaths" -Name "\\*\SYSVOL" -
   Value "RequireMutualAuthentication=0, RequireIntegrity=0, RequirePrivacy=0"
   ```

3. Restart the machine.

GPO

> **Prerequisite**: You must connect as an Active Directory user with the rights to create GPOs on the domain and to link them to the Organizational Unit that contains the Tenable Identity Exposure Directory Listener or Relay machine.

To disable SYSVOL hardening using a GPO:

1. Open the Group Policy Management console.

2. Create a new GPO.

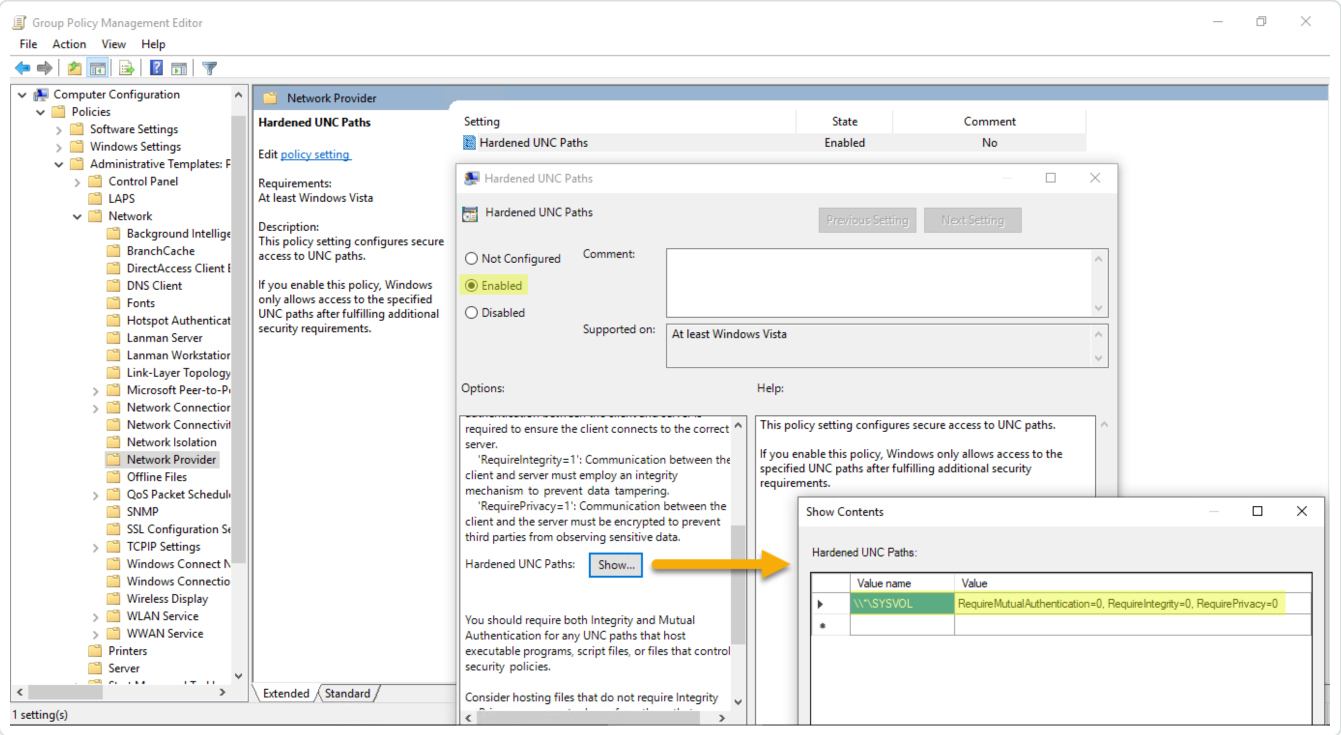
3. Edit the GPO and browse to the following location: `Computer Configuration/Administrative Templates/Network/Network Provider/Hardened UNC paths`.

4. Enable this setting and create a new Hardened UNC Path with:

   - Value name = `\\*\SYSVOL`

   - Value = `RequireMutualAuthentication=0`, `RequireIntegrity=0`, `RequirePrivacy=0`

   The result should appear as follows:



Hardened UNC Paths

Edit policy setting

Requirements:
At least Windows Vista

Description:
This policy setting configures secure access to UNC paths.

If you enable this policy, Windows only allows access to the specified UNC paths after fulfilling additional security requirements.

Setting	State	Comment
Hardened UNC Paths	Enabled	No

Hardened UNC Paths

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows Vista

Options:

required to ensure the client connects to the correct server.
'RequireIntegrity=1': Communication between the client and server must employ an integrity mechanism to prevent data tampering.
'RequirePrivacy=1': Communication between the client and the server must be encrypted to prevent third parties from observing sensitive data.

Hardened UNC Paths: Show...

You should require both Integrity and Mutual Authentication for any UNC paths that host executable programs, script files, or files that control security policies.

Consider hosting files that do not require Integrity

Help:

This policy setting configures secure access to UNC paths.

If you enable this policy, Windows only allows access to the specified UNC paths after fulfilling additional security requirements.

Hardened UNC Paths:

	Value name	Value
▶	*\SYSVOL	RequireMutualAuthentication=0, RequireIntegrity=0, RequirePrivacy=0
*		

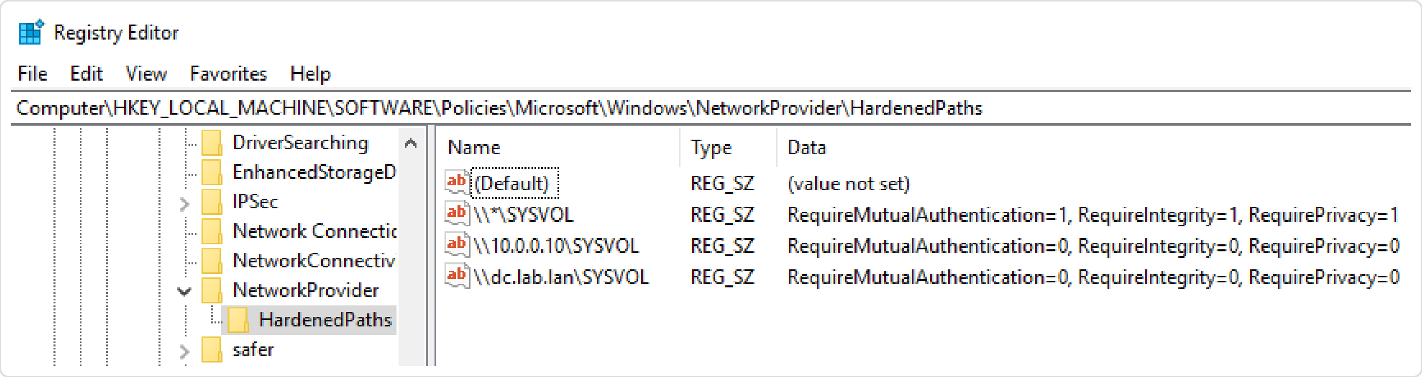
5. Click **OK** to confirm.

6. Link this GPO to the Organizational Unit that contains theTenable Identity Exposure Directory Listener or Relay machine. You can also use the security group filters GPO feature to ensure that this GPO applies only to this machine.

Specific UNC path exceptions

The previous procedures disable SYSVOL hardening using a wildcard UNC path: "`\\*\SYSVOL`". You can also disable it only for a specific IP address or FQDN. This means that you can keep the UNC hardened paths settings enabled (with value "`1`") for "`\\*\SYSVOL`", and have an exception corresponding to each IP address or FQDN of a Domain Controller configured in Tenable Identity Exposure.

The following image shows an example of SYSVOL hardening enabled for all servers ("`*`"), except for "`10.0.0.10`" and "`dc.lab.lan`", which are domain controllers that we configured in Tenable Identity Exposure:



Registry Editor

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetworkProvider\HardenedPaths

Name	Type	Data
(Default)	REG_SZ	(value not set)
\*\SYSVOL	REG_SZ	RequireMutualAuthentication=1, RequireIntegrity=1, RequirePrivacy=1
\\10.0.0.10\SYSVOL	REG_SZ	RequireMutualAuthentication=0, RequireIntegrity=0, RequirePrivacy=0
\\dc.lab.lan\SYSVOL	REG_SZ	RequireMutualAuthentication=0, RequireIntegrity=0, RequirePrivacy=0

You can add these additional settings using the registry or GPO methods described above.

Note: You must specify the exact value configured in Tenable Identity Exposure (for example, you cannot specify an IP address if the Tenable Identity Exposure configuration uses an FQDN.). Also, remember to update these keys each time you change an IP address or FQDN in the Tenable Identity Exposure domain management page.

Risks When Disabling SYSVOL Hardening

SYSVOL hardening is a security feature and disabling it can raise valid concerns.

- Non-domain-joined machines — There is no risk in disabling SYSVOL hardening. Since these machines do not apply GPOs, they do not get content from the SYSVOL share to execute it.
- Domain-joined machines (Directory Listener or Relay machine) which Tenable Identity Exposure does not recommend — If there is a potential risk of having an attacker in a "Man-in-the-Middle" situation between the Directory Listener or Relay machine and the Domain Controllers, it is unsafe to disable SYSVOL hardening. In this case, Tenable Identity Exposure recommends that you switch to Kerberos authentication instead.

The scope of this deactivation is only on the Directory Listener or Relay machine and not other domain computers, and never the Domain Controllers.