Tenable Identity Exposure 3.59 On-Premises User Guide

Last Revised: August 27, 2025

Copyright © 2025 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Table of Contents

Welcome to Tenable Identity Exposure 3.59 On-Premises User Guide **11**

About this Guide 11

Get Started with Tenable Identity Exposure 3.59 On-Premises **12**

Check Prerequisites 13

Install 14

Configure 14

Use 14

Expand Tenable Identity Exposure into Tenable One 14

On-Premises Architectures 17

Pre-deployment Requirements 22

See also 30

Resource Sizing 30

Storage Manager Disk Requirements 36

Hardware Requirements 39

Network Requirements 39

Network Flow Matrix 41

Secure Relay Requirements 48

Web Portal Requirements 55

Integration with an Active Directory Domain 56

Install Tenable Identity Exposure 57

Installation Procedures 59

TLS Installation Types 82

Split Security Engine Node (SEN) Services 86

Upgrade Tenable Identity Exposure 95
Upgrade Procedures 97
Restart Services 121
Restart Sequence 121
Secure Relay for Tenable Identity Exposure 3.59 123
Secure Relay Architectures for On-Premises Platforms 132
Standard 3 Servers with DL and SR on the Same Server 133
Standard 3 Servers with DL and SR on a Separate Server 133
Multiple DLs to a Single DL Running SR 134
Multiple DLs to a New DL Communicating with SR(s) 134
Configure the Relay 135
Secure Relay - FAQs 137
Logs for Troubleshooting 138
Troubleshoot Secure Relay Installation 140
Start Using Tenable Identity Exposure 149
Essential Basics in Tenable Identity Exposure 171
Tenable Identity Exposure User Portal 171
Trusted Certificates 174
Log in to Tenable Identity Exposure 176
Access the Workspace 181
Workspace Menu 182
Workspace Page 182
User Preferences 185
Notifications 188

Dashboards 190
Widgets 193
Identity Explorer 197
Trail Flow 198
Trail Flow Table 202
Search the Trail Flow Using the Wizard 204
Search the Trail Flow Manually 206
Customize Trail Flow Queries 207
Bookmark Queries 210
Query History 213
Display Deviant Events 214
Event Details 216
Attribute Changes 219
Trail Flow Use Cases 222
Indicators of Exposure 226
Deviance Resolution and Detection Date 229
Indicator of Exposure Details 229
Deviant Objects 232
Search Deviant Objects 234
Ignore a Deviant Object or a Reason (Deviance) 238
Incriminating Attributes 242
RSoP-Based Indicators of Exposure 244
Remediate Deviances from Indicators of Exposure 245
AdminCount Attribute Set on Standard Users 245

Dangerous Kerberos Delegation 248
Ensure SDProp Consistency 254
Indicators of Attack 258
Indicator of Attack Details 261
Indicators of Attack Incidents 262
Topology 268
Trust Relationships 270
Dangerous Trusts 272
Attack Path 274
Attack Relations 279
Add Key Credential 280
Add Member 281
Allowed To Act 283
Allowed To Delegate 285
Belongs To GPO 288
DCSync 290
Grant Allowed To Act 292
Has SID History 294
Implicit Takeover 296
Inherit GPO 298
Linked GPO 299
Member Of 301
Owns 302
Reset Password 304

RODC Manage ... 306
Write DACL ... 308
Write Owner ... 309
Identifying Tier 0 Assets ... 311
Accounts with Attack Paths ... 313
Attack Path Node Types ... 315
Activity Logs ... 317
SAML Authentication and Impersonation Entries ... 319
Privileged Entity Definitions ... 320
Active Directory ... 320
Entra ID ... 321
Tenable Identity Exposure Configuration and Administration ... 322
Active Directory Configuration ... 322
Access to AD Objects or Containers ... 322
Access for Privileged Analysis ... 324
Indicators of Attack Deployment ... 330
Install Indicators of Attack ... 333
Indicators of Attack Installation Script ... 344
Technical Changes and Potential Impact ... 355
Attack Scenarios (< v. 3.36) ... 357
Install Microsoft Sysmon ... 361
Uninstall Indicators of Attack ... 366
Manual Removal of Outdated GPO Folders from SYSVOL ... 367
Deactivated Indicators of Attack ... 368

First Row Icon Status 369
Other Row Icon Status 369
Troubleshoot Indicators of Attack 371
Antivirus Detection 371
Advanced Audit Policy Configuration Precedence 373
Event Logs Listener Validation 375
Tenable Identity Exposure Log Files 376
DFS Replication Issues Mitigation 383
Windows Event Log Retention 384
On-Premises Environments 385
“Unknowns” in the Indicators of Attack Alerts 386
Operational Indicators of Attack 389
Indicator of Attack Detection Delays 390
Authentication 391
Authentication using Tenable One 391
Authentication Using a Tenable Identity Exposure Account 391
Authentication Using LDAP 395
Authentication Using SAML 401
User Accounts 404
Security Profiles 407
Customize an Indicator 410
Refine Customization on an Indicator 412
User Roles 413
Manage Roles 413

Set Permissions for a Role 414
Set Permissions on User Interface Entities (Example) 419
Forests 421
Managing Forests 421
Protecting Service Accounts 422
Domains 423
Force Data Refresh on a Domain 427
Honey Accounts 427
Kerberos Authentication 430
Alerts 437
SMTP Server Configuration 437
Differences in Deployment Architecture 438
SMTP Server Configuration for Secure Relay Environments 438
SMTP Server Configuration for VPN Environments 439
Email Alerts 440
Syslog Alerts 444
Syslog and Email Alert Details 448
Syslog Message Framing 451
Health Checks 455
List of Health Checks 460
Reporting Center 464
Configuring Microsoft Entra ID as an Identity Provider 465
Refresh Entra ID Credentials 474
To refresh your credentials and restore synchronization: 475

Tenable Cloud Data Collection ... 478
Privileged Analysis ... 479
Activity Logs ... 480
Tenable Identity Exposure Public API ... 483
Data Management ... 485
Deployment Regions ... 485
Tenable Identity Exposure Licensing ... 486
Manage Your License ... 489
Prevention of Container UUID Mismatches ... 490
Long-Term Support (LTS) vs. Interim Versions: Key Differences and Benefits ... 493
What is LTS? ... 493
What are Interim Versions? ... 494
Key Differences Between LTS and Interim Versions: ... 494
Why Choose LTS? ... 494
Why Choose Interim Versions? ... 494
Troubleshooting Tenable Identity Exposure ... 494
Tenable Identity Exposure Diagnostics Tool ... 495
SYSVOL Hardening Interference with Tenable Identity Exposure ... 497
System Utility (handle.exe) ... 507
Manage Tenable Identity Exposure ... 508
Connect to an Event Log Collector ... 509
Scale Tenable Identity Exposure Services ... 510
Change IP Addresses or FQDNs for Tenable Identity Exposure Nodes ... 513
HTTPS for Tenable Identity Exposure Web Application ... 515

View the IIS Certificate 516
Change the IIS Certificate 518
Upgrade and Maintenance 520
Uninstall Tenable Identity Exposure 521

Welcome to Tenable Identity Exposure 3.59 On-Premises User Guide

Last updated: August 27, 2025

Tenable Identity Exposure 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.

To begin, see Start Using Tenable Identity Exposure.

For a successful deployment of your platform, follow the Get Started with Tenable Identity Exposure 3.59 On-Premises.

About this Guide

This on-premises guide for Tenable Identity Exposure**On-Premises version 3.59.x** gives the following information:

- The technical requirements to deploy and operate Tenable Identity Exposure as an on-premises platform.
- The environment specifications from a network and application perspective.
- The tasks to perform before enabling security monitoring.
- The configuration and use of Tenable Identity Exposure

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

Note: Tenable Identity Exposure is available 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, French, German, Japanese, Korean, Simplified Chinese, Spanish, and Traditional Chinese. The *Tenable Identity Exposure* user interface is available

in English, French, German, Japanese, Korean, Simplified Chinese, Spanish, 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 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:

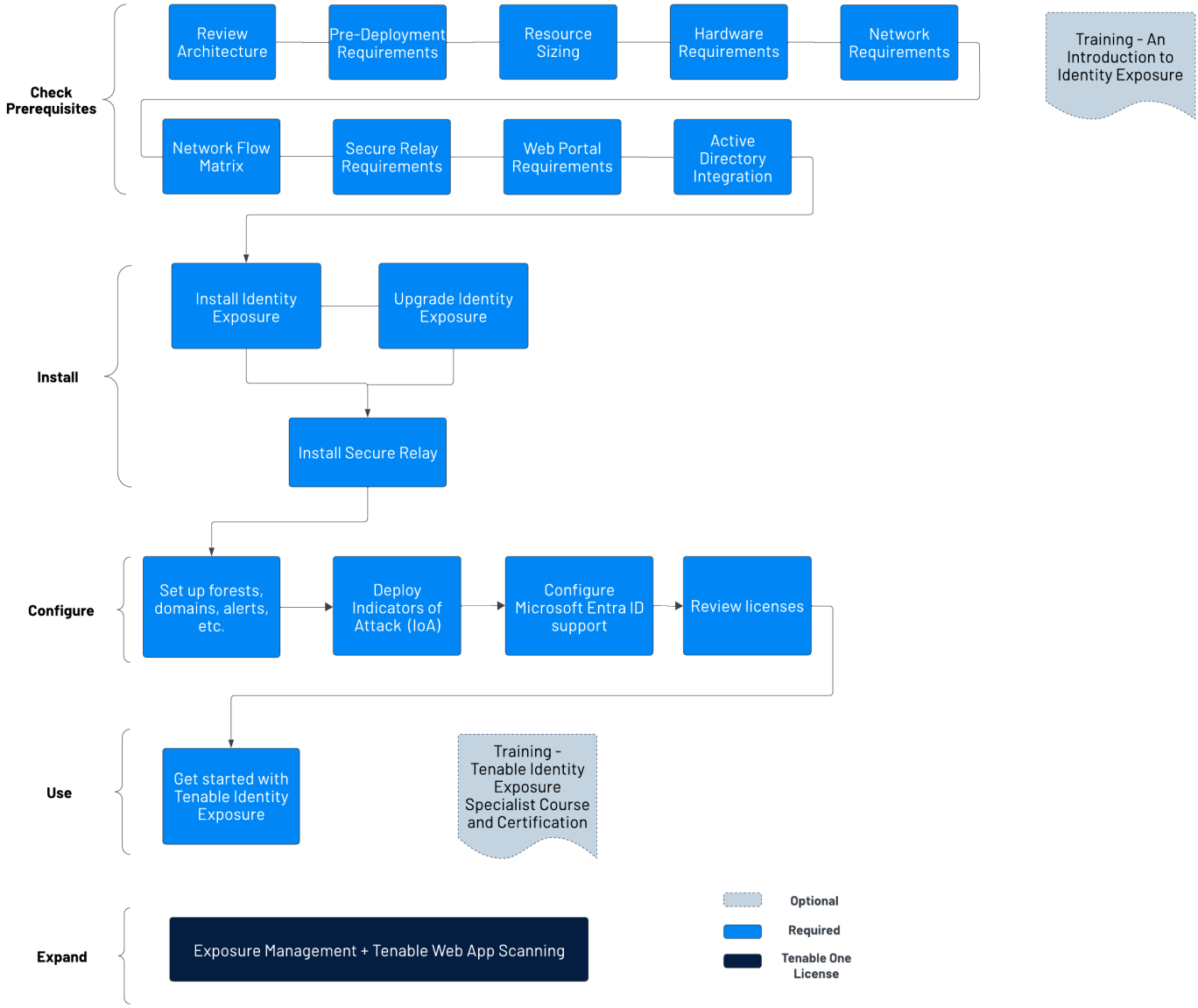
- Gain comprehensive visibility across the modern attack surface
- Anticipate threats and prioritize efforts to prevent attacks
- Communicate cyber risk to make better decisions

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.

Get Started with Tenable Identity Exposure 3.59 On-Premises

Use the following workflow to perform your deployment of Tenable Identity Exposure 3.59.



Check Prerequisites

1. **Review** the Release Notes.
2. **Select** your On-Premises Architectures – Tenable Identity Exposure offers two deployment options depending on your specific needs.
3. **Check** Pre-deployment Requirements – For optimal performance, Tenable Identity Exposure requires careful resource planning. This entails analyzing your Active Directory environment, specifically the total number of objects, to determine the necessary memory and processing power.

Caution: Starting with Tenable Identity Exposure version **3.59.5**, ensure that your **TLS certificates use OpenSSL 3.0.x**.

Install

1. **Select your deployment**:
   - Install Tenable Identity Exposure.
   - Upgrade Tenable Identity Exposure.

     Tip: If you are upgrading from **v. 3.42** to **3.59**, be sure you review the sections Secure Relay Requirements and Secure Relay Architectures for On-Premises Platforms.
2. **Install** the Secure Relay for Tenable Identity Exposure 3.59.

Configure

1. **Post-deployment** – Restart Services, Logs for Troubleshooting, Post-deployment Tasks.
2. **Review** Tenable Identity Exposure Licensing.

Use

- Start Using Tenable Identity Exposure

Expand Tenable Identity Exposure into Tenable One

Note: This requires a Tenable One license. For more information about trying Tenable One, see Tenable One.

Integrate Tenable Identity Exposure with Tenable One and leverage the following features:

- Access the **Exposure View** page, where you can gain critical business context by getting business-aligned cyber exposure score for critical business services, processes and functions, and track delivery against SLAs. Track overall identity risk to understand the risk contribution of web applications to your overall cyber exposure score.

- View and manage cyber exposure cards.
- View CES and CES trend data for the Global and **Active Directory** exposure cards.
- View Remediation Service Level Agreement (SLA) data.
- View Tag Performance data.

- Access the **Exposure Signals** page, where you can generate exposure signals that use queries to search for asset *violations*. Simply put, if an asset is impacted by a weakness related to the query, then the asset is considered a *violation*. Using this, you can gain visibility into your most critical risk scenarios.
  - Find top active threats in your environment with up-to-date feeds from Tenable Research.
  - View, generate, and interact with the data from queries and their impacted asset violations.
  - Create custom exposure signals to view business-specific risks and weaknesses
- Access the **Inventory** page, where you can enhance asset intelligence by accessing deeper asset insights, including related attack paths, tags, exposure cards, users, relationships, and more. Improve risk scoring by gaining a more complete view of asset exposure, with an asset exposure score that assesses total asset risk and asset criticality.
  - View and interact with the data on the **Assets** tab:
    - Review your AD assets to understand the strategic nature of the interface. This should help set your expectations on what features to use within Tenable Exposure Management, and when.
    - Familiarize yourself with the Global Asset Search and its objects and properties. Bookmark custom queries for later use.
    - Find devices, user accounts, software, cloud assets, SaaS applications, networks, and their weaknesses.
    - Drill down into the **Asset Details** page to view asset properties and all associated context views.

- View and interact with the data on the **Weaknesses** tab:
  - View key context on vulnerability and misconfiguration weaknesses to make the most impactful remediation decisions.
- View and interact with the data on the **Software** tab:
  - Gain full visibility of the software deployed across your business and better understand the associated risks.
  - Identify what software may be out of date, and which pieces of software may soon be End of Life (EoL).
- View and interact with the data on the **Findings** tab:
  - View instances of weaknesses (vulnerabilities or misconfigurations) appearing on an asset, identified uniquely by plugin ID, port, and protocol.
  - Review insights into those findings, including descriptions, assets affected, criticality, and more to identify potential security risks, visibility on under-utilized resources, and support compliance efforts.

- Access the **Attack Path** page, where you can optimize risk prioritization by exposing risky attack paths that traverse the attack surface, including web apps, IT, OT, IoT, identities, ASM, and prevent material impact. Streamline mitigation by identifying choke points to disrupt attack paths with mitigation guidance, and gain deep expertise with AI insights **(Not supported in FedRAMP environments)**.
  - View the **Dashboard** tab for a high-level view of your vulnerable assets such as the number of attack paths leading to these critical assets, the number of open attack techniques and their severity, a matrix to view paths with different source node exposure score and ACR target value combinations, and a list of trending attack paths.
    - Review the **Top Attack Path Matrix** and click the **Top Attack Paths** tile to view more information about paths leading to your “Crown Jewels”, or assets with an ACR of 7 or above.

    You can adjust these if needed to ensure you’re viewing the most critical attack path data.

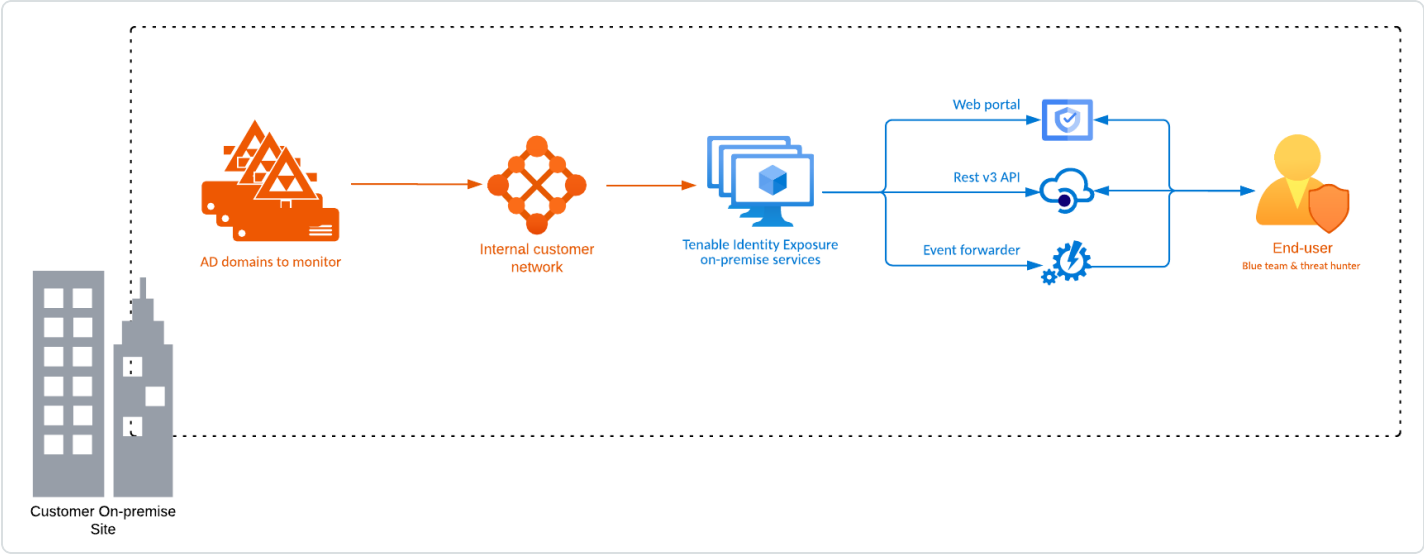
- On the **Top Attack Techniques** tab, view all attack techniques that exist in one or more attack paths that lead to one or more critical assets by pairing your data with advanced graph analytics and the MITRE ATT&CK® Framework to create attack techniques, which allow you to understand and act on the unknowns that enable and amplify threat impact on your assets and information.
- On the **Top Attack Paths** tab, generate attack path queries to view your assets as part of potential attack paths:
  - Generate an Attack Path with a Built-in Query
  - Generate an Attack Path Query with the Attack Path Query Builder
  - Generate an Asset Query with the Asset Query Builder

  Then, you can view and interact with the Attack Path Query and Asset Query data via the query result list and the interactive graph.
- Interact with the **MITRE ATT&CK Heatmap** tab.

- View and interact with the data in the **Tags** page:
  - Create and manage tags to highlight or combine different asset classes.
  - View the **Tag Details** page to gain further insight into the tags associated with your assets.

On-Premises Architectures

The Tenable Identity Exposure platform relies on several Windows services hosted on virtual machines (VMs). Your environment must support the following infrastructure:



The Tenable Identity Exposure platform consists of the following components:

- The **Storage Manager**: Providing hot and cold storage support, the Storage Managers oversee serving data to the Directory Listeners and the Security Engine Nodes. This component is the only one that must remain persistent to save information. Internally, they use Microsoft MS SQL Server to store internal data and configuration.
- The **Security Engine Nodes**: Hosting analysis-related services, the security engine nodes support the Tenable Identity Exposure security engine, internal communication bus, and end-user applications (such as the Web portal, the REST API, or the alert notifier). This component builds on different isolated Windows services.
- The **Directory Listener**: Working closely with the monitored domain controllers, the Directory Listeners receive real-time Active Directory flows and apply several treatments to decode, isolate, and correlate security changes.
- The **Secure Relay**: 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. 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. See Secure Relay Architectures for On-Premises Platforms.

For the number and sizing of these components, see Resource Sizing.

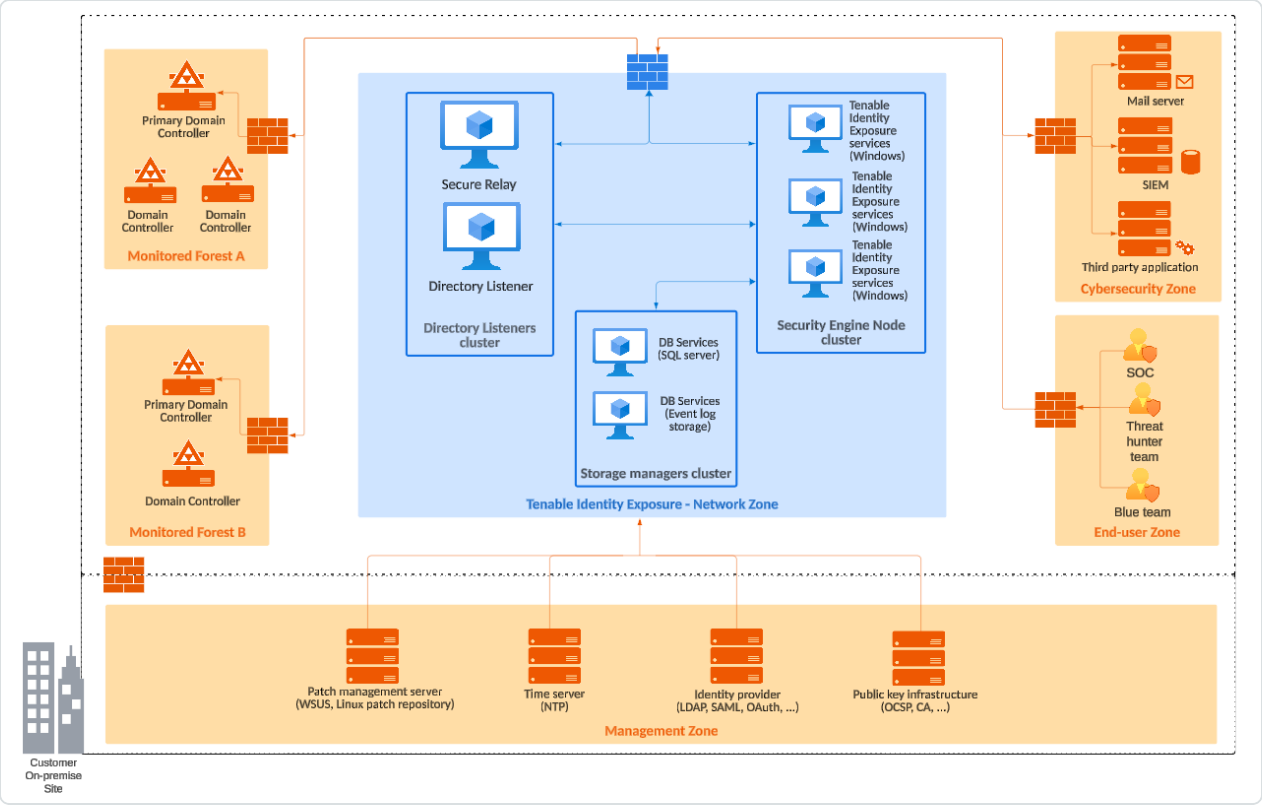
Architectures

Tenable Identity Exposure's on-premises solution uses a software package hosted in a dedicated Windows Server environment that you provide and manage, based on the following architectures:

Centralized Architecture

The centralized architecture hosts all Tenable Identity Exposure components in the same network zone.

- The main components (Secure Relay, Directory Listeners, Security Engine Nodes, and Storage Managers) work side by side and can communicate with each other without any network filtering.
- To ensure proper network security, Tenable recommends that you secure this architecture with a firewall at the entrance to the zone. The following illustration shows the ingoing and outgoing network flows as described in the Network Flow Matrix.



Advantages – This architecture offers the best balance between manageability and security:

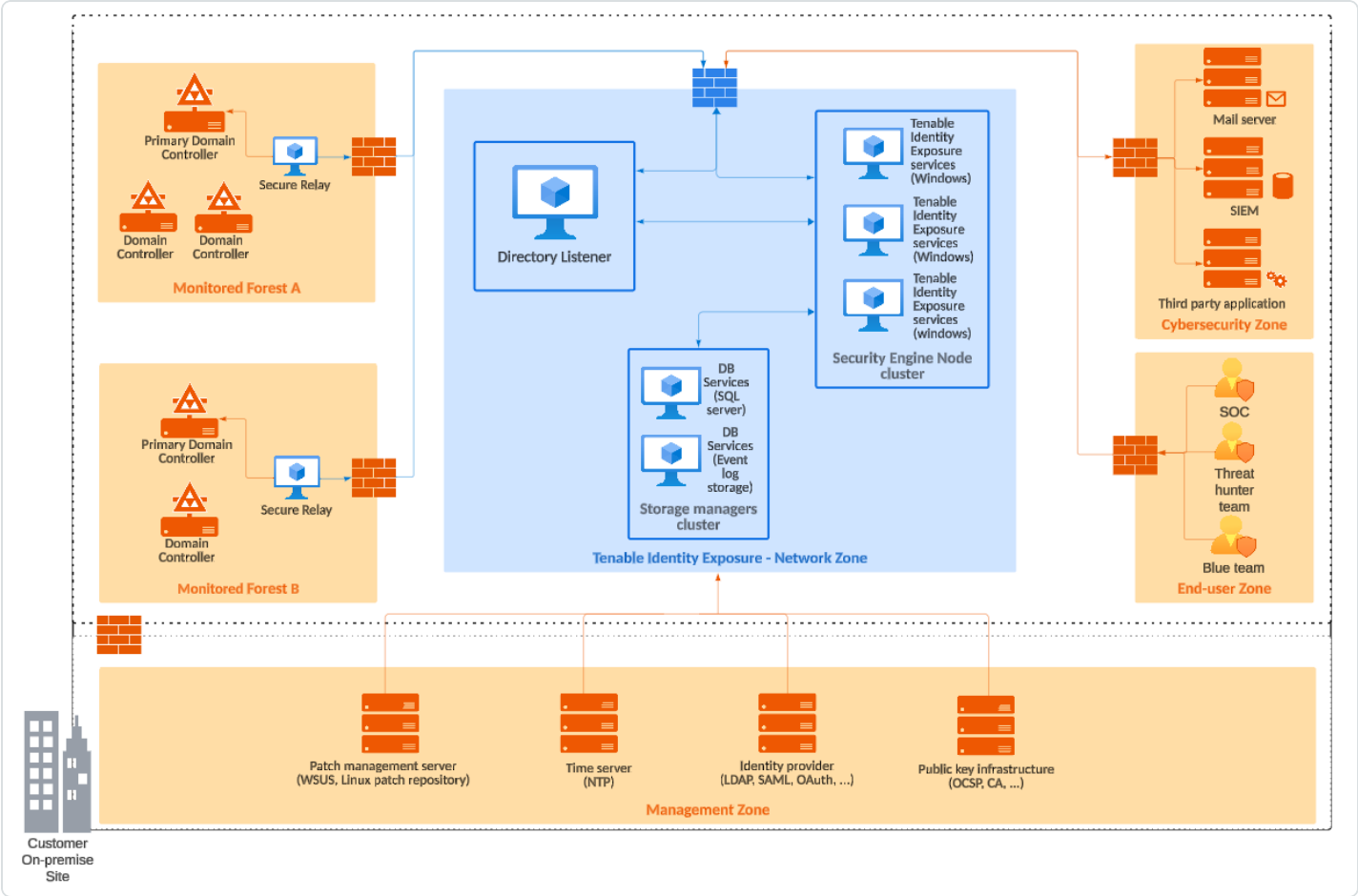
- Each Tenable Identity Exposure service is at the same logical place behind a unique firewall.
- Each service flow (Active Directory, end-users, alerts, etc.) goes through the same network equipment.
- This architecture links new Active Directory domains easily because it does not need service or extra configuration on the targeted domains.

Disadvantages – The centralized architecture can consume bandwidth because it must transfer each Active Directory flow from the monitored domain controllers to the Tenable Identity Exposure network zone.

> **Tip**: Tenable recommends using the centralized architecture because it offers better flexibility and easier deployment.

Distributed Architecture

The distributed architecture places Directory Listeners in the same network zone as the domain controllers, and hosts the Security Engine Node and the Storage Manager in another network zone, as shown in the following illustration:



Advantages

- Bandwidth reduction: Active Directory flows can be significant when monitoring large directories. By filtering relevant security changes and compressing the objects, the Directory Listeners reduce the bandwidth that the platform uses.
- Better network filtering:
  - An Active Directory infrastructure requires the use of numerous TCP and UDP ports which can be targets during a cyberattack. Following the principle of least privilege, Tenable recommends that you expose only these network ports when it is strictly necessary.
  - By placing Directory Listeners in the same network zone as the domain controllers, Tenable Identity Exposure does not need to expose Active Directory ports to another network zone.

- Isolated infrastructure: Specific contexts sometimes require a complete isolation of the Active Directory infrastructure from the rest of the information system. Using the distributed architecture, Tenable Identity Exposure's platform only requires one inbound and one outbound network flow, which preserves the security of the isolated infrastructure.
- Network security: Tenable Identity Exposure's Directory Listeners use a specific host-based firewall. Tenable also recommends that you use a specific firewall at the entrance of the zone hosting the Security Engine Nodes and Storage Managers. For more information on inbound and outbound network flows, see Network Flow Matrix.

Disadvantages – Tenable only recommends this architecture for highly sensitive environments that require high-level network isolation.

- The distributed architecture is more complex to deploy and to maintain because it requires multiple network configurations in different network locations.
- This architecture is also less flexible since it requires the deployment of new Directory Listeners each time the customer wants to add a new domain to monitor.

Pre-deployment Requirements

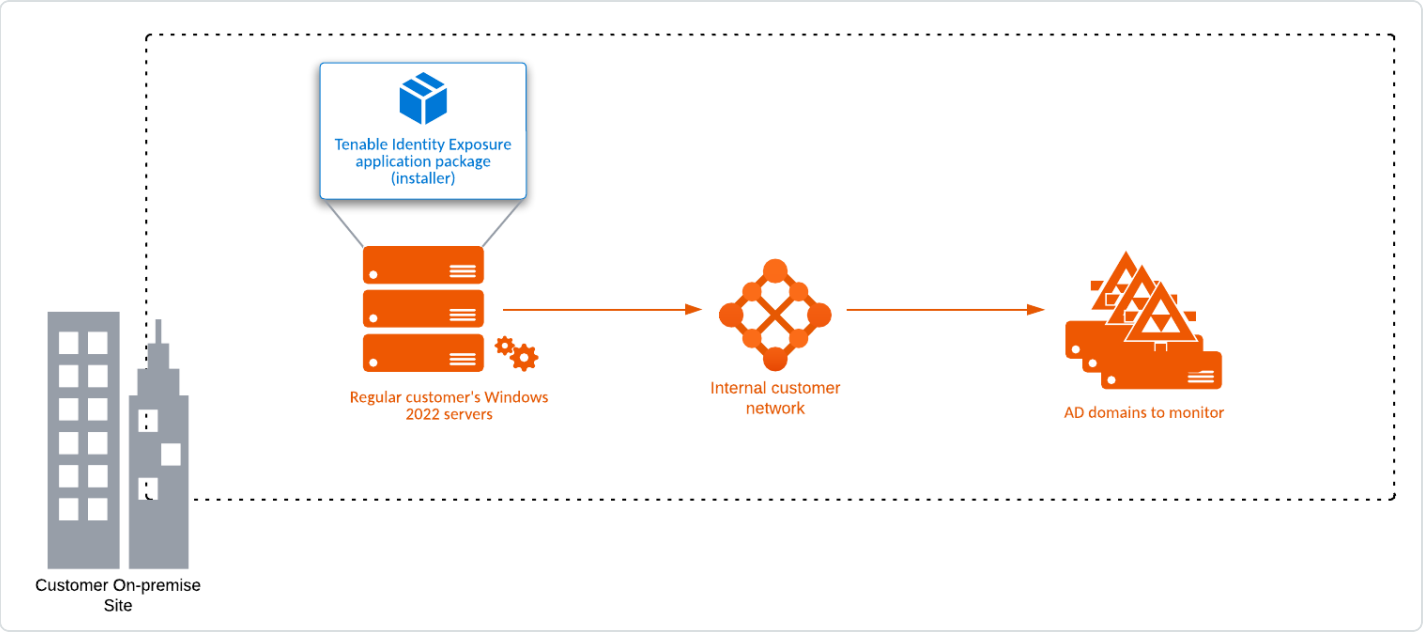
Before you begin, check that you meet the following prerequisites to ensure a smooth installation process.

Installation Overview

You install Tenable Identity Exposure as an application package hosted in a dedicated Windows environment that must fulfill specific hosting specifications.Tenable Identity Exposure requires access to the operating system's master image on the system where you install it.

Tenable preconfigures the application package with only Tenable services and your specific requirements. This deployment option offers maximum flexibility and integrates seamlessly into your specific environment.

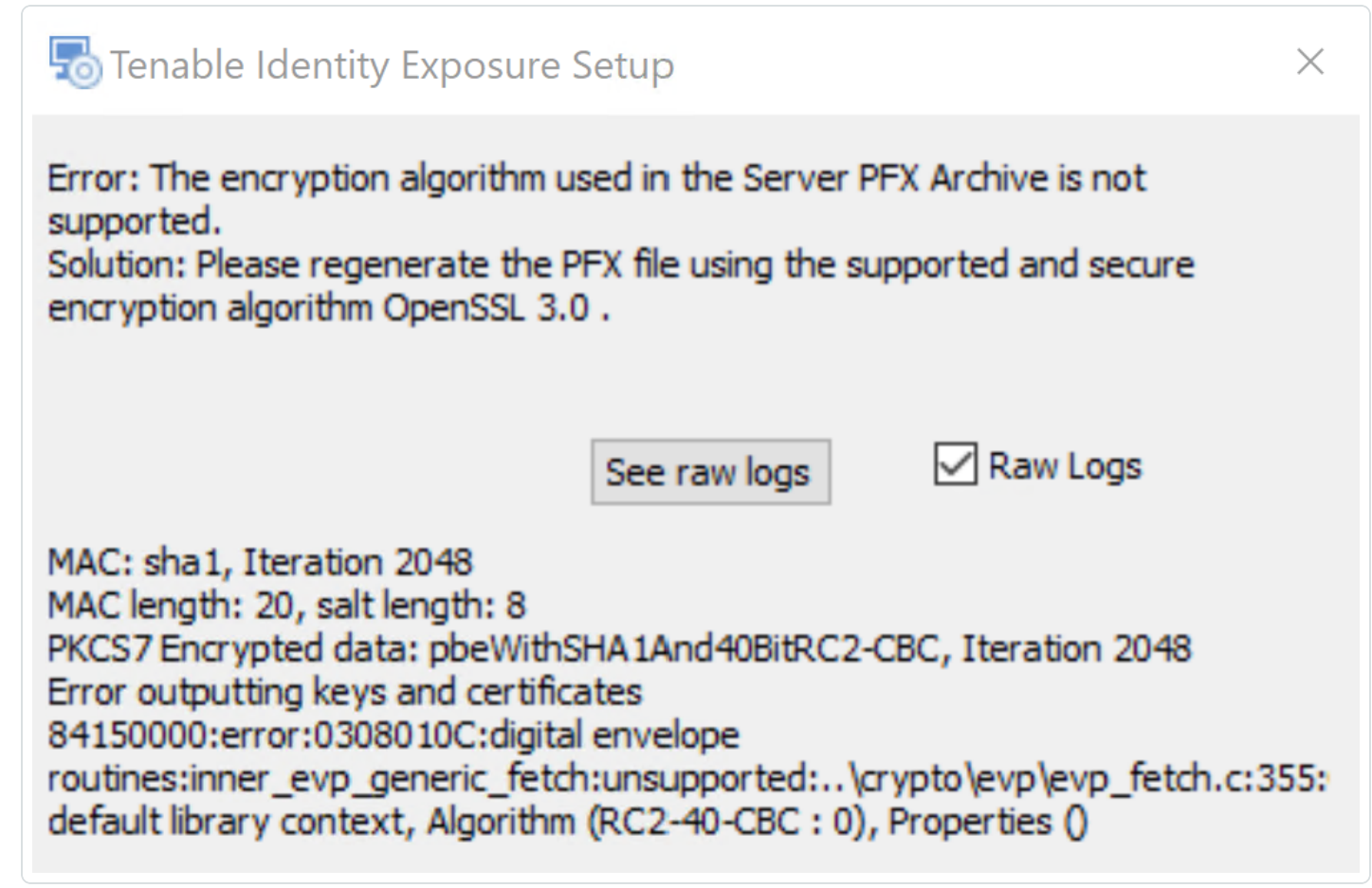
Tenable Identity Exposure runs on a micro-services architecture embedded into Windows services. These services have a dedicated purpose (storage, security analysis, application, etc.) and all are mandatory. Consequently, you can only install Tenable Identity Exposure on operating systems supporting the micro-services model.

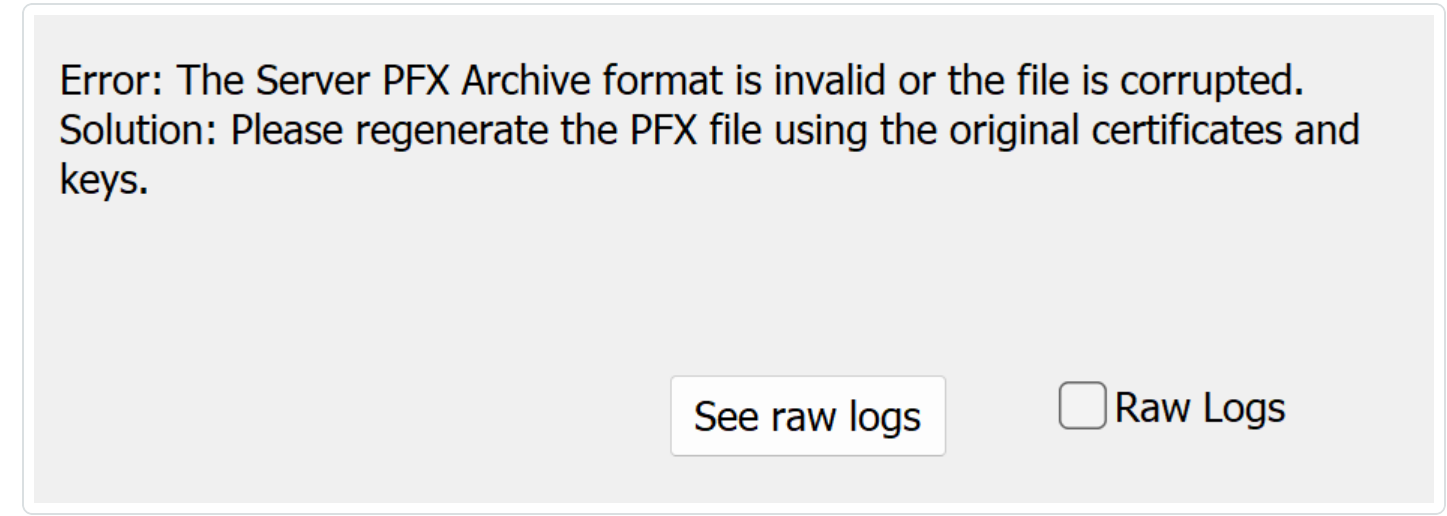


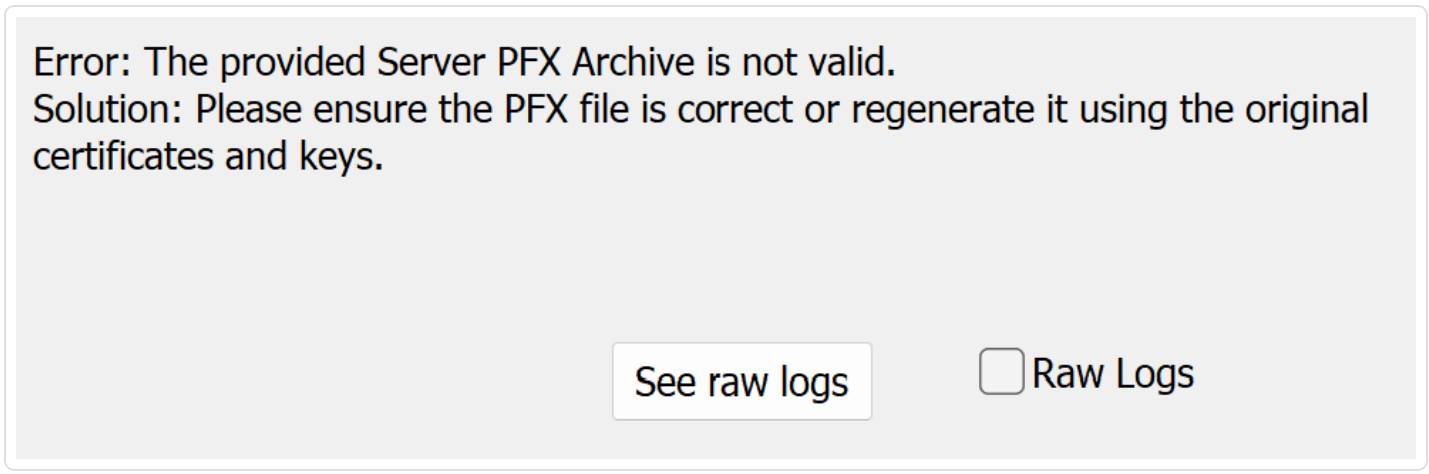
TLS Certificates

OpenSSL 3.0 Support – Starting with version **3.59.5**, Tenable Identity Exposure uses **OpenSSL 3.0.x**. As a result, X.509 certificates signed with SHA1 no longer work at security level 1 or higher. TLS defaults to security level 1, which makes SHA1-signed certificates untrusted for authenticating servers or clients.

You must upgrade your certificates in response to this change. If you continue the installation without updating your certificates to use OpenSSL 3.0, the Tenable Identity Exposure installer returns the following error messages with recommended fixes:


Tenable Identity Exposure Setup
Error: The encryption algorithm used in the Server PFX Archive is not supported.
Solution: Please regenerate the PFX file using the supported and secure encryption algorithm OpenSSL 3.0 .
See raw logs
Raw Logs
MAC: sha1, Iteration 2048
MAC length: 20, salt length: 8
PKCS7 Encrypted data: pbeWithSHA1And40BitRC2-CBC, Iteration 2048
Error outputting keys and certificates
84150000:error:0308010C:digital envelope routines:inner_evp_generic_fetch:unsupported:..\crypto\evp\evp_fetch.c:355:default library context, Algorithm (RC2-40-CBC : 0), Properties ()


Error: The Server PFX Archive format is invalid or the file is corrupted.
Solution: Please regenerate the PFX file using the original certificates and keys.
See raw logs
Raw Logs



Account Privileges

Perform the installation as the local account member of the local or built-in administrators group or as an administrator on the server where you install Tenable Identity Exposure.

Caution: Log in to the machine as this **local administrator account outside the domain**. **Do not log in as a local administrator within the domain**.

The account requires the following permissions:

- `SeBackupPrivilege`
- `SeDebugPrivilege`
- `SeSecurityPrivilege`

Antivirus (AV) and Endpoint Detection and Response (EDR)

Before installing, disable any AV and/or EDR solution on the host. Failing to do so triggers a roll-back during installation. You can safely enable AV/EDR once the installation is complete, but be aware that it may impact product performance due to high disk I/O operations. See also "Unsupported Configurations" below.

Pending Reboots

Perform any required reboots prior to installation. When you launch the installer on a server, it checks the following:

- There is no pending reboot.
- The server was restarted properly less than 11 minutes ago.
- The MSI checks the following registry keys:
    - `HKLM: \ Software \ Microsoft \ Windows \ CurrentVersion \ Component Based Servicing \ RebootPending`
    - `HKLM: \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ WindowsUpdate \ Auto Update \ RebootRequired`
    - `HKLM: \ SYSTEM \ CurrentControlSet \ Control \ Session Manager -> PendingFileRenameOperations`

Service Accounts

The use of service accounts must be allowed on the operating system.

Note: This service account must be able to read all object attributes.

Indicators of Attack

The Windows event log must have a minimum retention time of 5 minutes to ensure the application can accurately retrieve all events.

Unsupported Configurations

The following table details unsupported configurations:

Configuration	Description
Active anti-virus or Endpoint Detection and Response (EDR) solution	The Tenable Identity Exposure platform requires intensive disk I/O. • Using anti-virus and EDR can drastically decrease platform performances. • You must have an exception to allow Tenable Identity Exposure services and data folder.

Firewalls	Do the following to allow Tenable Identity Exposure services to communicate with each other to have reliable security monitoring: • Disable local firewall rules preventing outgoing traffic. • Grant local firewall rules to allow incoming traffic on Tenable Identity Exposure services.
Erlang	• Do not customize the `HOMEDRIVE` environment variable. • The `PATHEXT` environment variable must contain the `.exe` and `.bat` file extensions.

Third-Party Applications

Deploying Tenable Identity Exposure's platform in a non-certified environment can create unexpected side effects.

In particular, the deployment of third-party applications (such as a specific agent or daemon) in the master image can cause stability or performance issues.

Tenable strongly recommends that you reduce the number of third-party applications to a minimum.

Access Rights

Tenable Identity Exposure's platform requires local administrative rights to operate and ensure a proper service management.

- You must provide the Tenable technical lead with the credentials (username and password) associated with the administrative account of the host machine.
- When deploying to a production environment, consider a password renewal process that you validate jointly with the Tenable technical lead.

Product Updates

As part of its upgrade program, Tenable frequently publishes updates to its systems to provide new detection capabilities and new product features.

- In this deployment, Tenable only provides updates for Tenable Identity Exposure components. You must ensure a proper management of your operating systems, including the frequent deployment of security patches. For more information about Tenable Identity Exposure releases, see the Tenable Identity Exposure Release Notes.
- Tenable Identity Exposure's micro-services architecture supports the immediate application of operating system patches.

Other Requirements

- Tenable Identity Exposure works with Windows Servers listed in Hardware Requirements with the latest available update.
- Tenable Identity Exposure installation program requires **Local Administrator rights on Windows Server 2016 or later**. If the account used for the installation is the default account, ensure that this account can run programs without restrictions.
- Tenable Identity Exposure services require Local Administrator rights to run local services on the machine.
- Tenable Identity Exposure requires a dedicated data partition. Do not run Tenable Identity Exposure on the OS partition to prevent system freeze if the partition is full.
- Tenable Identity Exposure SQL instance requires the virtual accounts usage feature.
- When installing or upgrading Microsoft SQL Server after implementing tighter security measures, the installation process fails due to insufficient user rights. Check that you have the necessary permissions for a successful installation. For more information, see the Microsoft documentation.
- Tenable Identity Exposure must run as a black box. Dedicate each machine to Tenable Identity Exposure and do not share it with another product.
- Tenable Identity Exposure can create any folder starting with the ‘Alsid’ or ‘Tenable’ prefix on the data partition. Therefore, do not create folders starting with "Alsid" nor "‘Tenable" on the data partition.
- Erlang: Do not modify the `HOMEDRIVE` environment variable. The `PATHEXT` environment variable must contain the `.exe` and `.bat` file extensions.

- 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.

Pre-installation Checklist

This table resumes the prerequisites in a handy checklist before installation.

Information or Resource to Reserve	Status
The required agreements (NDA, Evaluation Software License), if applicable.	
The number of active AD users in the targeted domains to monitor.	
The computing and memory resources are based on Tenable Identity Exposure's sizing matrix. See Resource Sizing.	
The private IP of each virtual machine used to deploy Tenable's platform.	
The type and IP address of the update management infrastructure, the time server, PKI server, and identity provider.	
Open required network flows for each service that Tenable Identity Exposure requires. See Network Flow Matrix.	
The private IP addresses of each Primary Domain Controller emulator.	
Creation of a regular user account on each Active Directory forest to monitor.	
On the specific Active Directory containers, grant access right to the Tenable service account.	
Grant access for Privileged Analysis if you want to enable this feature.	
The AD domain user account login: • Format: User Principal Name, for example "tenablead@domain.example.com" (recommended for Kerberos compatibility) or NetBIOS, for example "DomainNetBIOSName\SamAccountName".	
A TLS certificate issued for Tenable Identity Exposure's Web Portal issued from	

the customer's PKI • Otherwise, inform Tenable of the use of self-signed certificate.	
The list of Tenable Identity Exposure user accounts to create: • Required information: first and last name, email address, and desired login.	
The list of optional configurations to activate (email notification, Syslog event forwarding, etc.)	
An identified and available project coordinator to work with Tenable.	
Technical staff to respond to potential technical issues such as network filtering issue and unreachable PDCe.	

See also

- Resource Sizing
- Hardware Requirements
- Network Requirements
- Web Portal Requirements
- Integration with an Active Directory Domain

Resource Sizing

To ensure correct behavior, the Tenable Identity Exposure components – **Storage Manager**, **Security Engine Nodes**, **Secure Relay**, and **Directory Listener** – require a certain amount of memory and computing power.

- These required resources scale depending on the size of the Active Directory (AD) infrastructure that you monitor.
- Tenable Identity Exposure uses the number of active users as a metric to compute the sizing requirements. This includes the regular user accounts and the service accounts that applications use.

To compute the AD volume:

- Run the following PowerShell command line on each Active Directory domain to monitor:

```
Import-Module ActiveDirectory
(Get-ADUser -Server "dc.domain.com" -Filter 'enabled -eq $true').Count
```

where:

- `-Server` specifies the Active Directory Domain Services (ADDS) instance to connect to.
- `dc.domain.com` is the fully qualified domain name (FQDN) of the domain controller to use for counting.

Sizing Requirements

After you compute the number of active users to monitor, see the following sections for the appropriate sizing requirements:

- The **Secure Relay** is a mode of transfer for your Active Directory data from your network to Tenable Identity Exposure.

Required sizing for the system hosting the Secure Relay:

Customer Size	Tenable Identity Exposure Services	Instance Required	vCPU (per instance)	Memory (per instance)	Available Disk Space (per instance)	Disk Topology
Any size	• `tenable_Relay` • `tenable_envoy`	1	2 vCPU	8 GB of RAM	30 GB	Partition for logs separate from the system partition

- The **Directory Listeners** receive real-time Active Directory flows.

Required sizing for the system hosting the Directory Listener components:

Directory Listener				
Active AD users	Instance required	vCPU (per instance)	Memory (per instance)	Disk space (per instance)
1 - 25,000	1 virtual machine	2 cores on 2 sockets	16 GB of RAM	30 GB (Silver)
25,001 - 50,000	1 virtual machine	4 cores on 2 sockets	16 GB of RAM	30 GB (Silver)
50,001 - 75,000	1 virtual machine	4 cores on 2 sockets	32 GB of RAM	30 GB (Silver)
75,001 - 100,000	1 virtual machine	4 cores on 2 sockets	32 GB of RAM	30 GB (Silver)
100,001 - 150,000	1 virtual machine	8 cores on 2 sockets	64 GB of RAM	30 GB (Silver)
150,001 - 300,000	1 virtual machine	8 cores on 2 sockets	64 GB of RAM	30 GB (Silver)
300,001 - 500,001+	1 virtual machine	8 cores on 2 sockets	64 GB of RAM	30 GB (Silver)

- The **Security Engine Nodes** support Tenable Identity Exposure's security engine, storage services, and end users.

Note: If you spread the SEN services over several machines, see Split Security Engine Node (SEN) Services for detailed resource sizing.

Required sizing for the system hosting the Security Engine Node components:

Security Engine Node				
Active AD users	Instance required	vCPU (per instance)	Memory (per instance)	Disk space (per instance)
1 - 25,000	1 virtual machine	8 cores on 2 sockets	16 GB of RAM	200 GB (Gold)
25,001 - 50,000	1 virtual machine	8 cores on 2 sockets	32 GB of RAM	300 GB (Gold)
50,001 - 75,000	1 virtual machine	10 cores on 3 sockets	32 GB of RAM	300 GB (Gold)
75,001 - 100,000	1 virtual machine	12 cores on 4 sockets	64 GB of RAM	400 GB (Gold)
100,001 - 150,000	1 virtual machine	16 cores on 4 sockets	96 GB of RAM	400 GB (Gold)
Split Security Engine Node				
150,001 - 300,000	5 virtual machines	VM1: 8 cores on 2 sockets	VM1: 16 GB of RAM	VM1: 1 TB
		VM2: 8 cores on 4 sockets	VM2: 16 GB of RAM	VM2: 300 GB
		VM3: 16 cores on 4 sockets	VM3: 32 GB of RAM	VM3: 100 GB
		VM4: 16 cores on 4 sockets	VM4: 16 GB of RAM	VM4: 100 GB
		VM5: 16 cores on 4 sockets	VM5: 48 GB of RAM	VM5: 100 GB
300,001 - 500,001+	5 virtual machines	VM1: 8 cores on 2 sockets	VM1: 16 GB of RAM	VM1: 1 TB

		VM2: 8 cores on 4 sockets	VM2: 16 GB of RAM	VM2: 300 GB
		VM3: 12 cores on 4 sockets	VM3: 32 GB of RAM	VM3: 100 GB
		VM4: 16 cores on 4 sockets	VM4: 32 GB of RAM	VM4: 100 GB
		VM5: 16 cores on 4 sockets	VM5: 64 GB of RAM	VM5: 100 GB

- The **Storage Manager** provides hot and cold storage support for the Directory Listeners and the security nodes services.

Required sizing for the system hosting the Storage Manager components:

Storage Manager				
Active AD users	Instance Required	vCPU (per instance)	Memory (per instance)	Disk Space (per instance)
1 - 25,000	1 virtual machine	8 cores on 2 sockets	16 GB of RAM	600 GB
25,001 - 50,000	1 virtual machine	8 cores on 2 sockets	16 GB of RAM	800 GB
50,001 - 75,000	1 virtual machine	12 cores on 4 sockets	32 GB of RAM	1.2 TB
75,001 - 100,000	1 virtual machine	12 cores on 4 sockets	32 GB of RAM	2 TB
100,001 - 150,000	1 virtual machine	12 cores on 4 sockets	64 GB of RAM	4 TB
150,001 - 300,000	1 virtual machine	16 cores on 4 sockets	64 GB of RAM	6 TB
300,001 -	1 virtual	16 cores on 4	128 GB of RAM	8 TB

500,001+	machine	sockets		

For information about disk performance, see Storage Manager Disk Requirements.

Storage Policy Management

Gold, silver, and bronze storage are different tiers or levels of storage services based on performance, reliability, and cost. Definitions may vary among providers.

- Gold is the highest tier with the best performance and reliability, suitable for critical workloads.
- Silver is a mid-tier option with balanced performance and cost.
- Bronze is the lower tier with lower performance and reliability, often chosen for less critical workloads.

Sizing Example

An Information System made of three Active Directory domains has the following sizing.

Domain	Number of Active AD users
Domain A	45,000
Domain B	15,000
Domain C	150
Total:	**60,150**

Following the sizing matrix, this Tenable Identity Exposure deployment requires the following resources.

Tenable Identity Exposure services	Instance Required	vCPU (per instance)	Memory (per instance)	Disk Space (per instance)
Directory Listeners	1	4 cores, at least 2.6 GHz	32 GB of RAM	30 GB
Security Engine Nodes	1	10 cores, at least 2.6 GHz	32 GB of RAM	300 GB

Storage Managers	1	12 cores, at least 2.6 GHz	32 GB of RAM	• 1.2 TB with 10,000 IOPs • For upgrade: At least 20 GB available

Storage Manager Disk Requirements

As part of its security analysis, Tenable Identity Exposure stores the differences for each Active Directory (AD) change either from the AD database or the SYSVOL network share.

The **Storage Manager** component oversees the storage of these events using the following:

- An event log storage for attacks related events
- A Microsoft SQL Server instance for all other events

Tenable provides both minimum and recommended hardware requirements depending on your Active Directory activity:

- A minimum sizing configuration to start and run the platform in most infrastructures.
- A recommended sizing configuration to cover the needs of most event-intensive AD infrastructures.

Tenable Identity Exposure also requires the implementation of a specific disk layout to store the different database files and to ensure that I/O performances are compatible with its activity.

Due to the amount of Active Directory data it processes, Tenable Identity Exposure is a disk-intensive application. To avoid any bottleneck introduced by the storage (disk or SAN), Tenable Identity Exposure offers a minimal and recommended configuration.

- As with sizing, the minimal disk performances generally cover the needs of most infrastructures.
- The recommended infrastructure offers better experience for large or active AD infrastructures.

Supported and Recommended Disk Layout

Some specific environments require splitting the database files across different disks:

- One data file disk
- One temporary DB disk
- One log file disk
- (Optional) 1 backup disk

Minimum and Recommended Disk Sizing

The following tables describe the minimal and recommended disk sizing to store six months of Active Directory events in Tenable Identity Exposure.

Storage managers - Disk Sizing Matrix							
Active AD users	Disk Space (per instance)	Data File Disk Space		Log File Disk Space		TempDb Disk Space	
		Minimum	Recommended	Minimum	Recommended	Minimum	Recommended
1 - 25,000	600 GB	340 GB	375 GB	100 GB	200 GB	10 GB	25 GB
25,001 - 50,000	800 GB	400 GB	500 GB	125 GB	250 GB	25 GB	50 GB
50,001 - 75,000	1.2 TB	600 GB	775 GB	150 GB	350 GB	50 GB	75 GB
75,001 - 100,000	2 TB	725 GB	1.3 TB	200 GB	600 GB	75 GB	100 GB
100,001 -	4 TB	1.6 TB	3 TB	300 GB	800 GB	100 GB	200 GB

150,000							
150,001 - 300,000	6 TB	2.45 TB	4.7 TB	400 GB	1 TB	150 GB	300 GB
300,001 - 500,001+	8 TB	3.3 TB	6.4 TB	500 GB	1.2 TB	200 GB	400 GB

Minimum and Recommended Disk Performance

The limiting factor of the database is usually the underlying disk performances. The better disk throughput/IOPS, the better overall performances of Tenable Identity Exposure are. A low latency is also necessary (<5 ms).

Storage managers - Disk Performance Matrix				
Active AD users	Minimal Disk Performance		Recommended Disk Performance	
	Throughput (MB/sec)	IOPs (read/write)	Throughput (MB/sec)	IOPs (read/write)
1 - 25,000	150	2,500	300	5,000
25,001 - 50,000	200	5,000	400	10,000
50,001 - 75,000	200	5,000	400	10,000
75,001 - 100,000	200	5,000	400	10,000
100,001 -	250	7,500	500	15,000

150,000				
150,001 – 300,000	250	7,500	500	15,000
300,001 – 500,001+	500	16,000	1,000	32,000

Hardware Requirements

Tenable Identity Exposure requires the following hardware:

- Supported Microsoft Windows Operating Systems
    - Windows Server 2016
    - Windows Server 2019
    - Windows Server 2022
    - Windows Server 2025
- The requirements described in the sizing sections are for the well-being of Tenable Identity Exposure's platform; they do not include the operating system requirements of an application package-based deployment.
- CPU speed must be at least 2.6 GHz.
- Tenable Identity Exposure's platform supports the x86-64 processor architecture (at least Sandy Bridge or Piledriver) with Intel Turbo Boost Technology 2.0.
- One required network interface: you can add other network interfaces for administration, monitoring, or any other reason.

Network Requirements

Tenable Identity Exposure requires access to your Active Directory infrastructures to initiate security monitoring. You must allow network flows between the different Tenable Identity Exposure services as described in Network Flow Matrix.

Bandwidth

As a monitoring platform, Tenable Identity Exposure receives Active Directory events continuously. Depending on the scale of the infrastructure, this process can generate a significant volume of data.

You must allocate an appropriate bandwidth to guarantee data transmission to Tenable Identity Exposure for analysis in a reasonable amount of time.

The following table defines the required bandwidth based on the size of the monitored AD.

Active AD Users	Average Number of Objects Received (per minute)	Minimum Bandwidth	Recommended Bandwidth
1 - 5,000	10	1 Mbps	2 Mbps
5,001 - 75,000	150	5 Mbps	10 Mbps
75,001 - 400,000	700	15 Mbps	30 Mbps

Microsoft APIs

To subscribe to the replication flows and begin monitoring them, Tenable Identity Exposure must contact standard directory APIs from Microsoft. Tenable Identity Exposure only requires communication with the Primary Domain Controller emulator (PDCe) with a regular user account. You must also deploy a new group policy object (GPO) to activate the attack detection engine.

Communication with AD

For an on-premises installation, Tenable Identity Exposure is a software package that you deploy on your Windows Server environment. Tenable Identity Exposure must communicate with the monitored Active Directory.

Internet Access

Tenable provides a continuous integration process to allow regular releases of new detection capabilities and features. Tenable recommends that you plan an Internet access to upgrade Tenable Identity Exposure regularly.

Network Protocols

Specific network protocols (such as Syslog, SMTP or HTTP) allow Tenable Identity Exposure to offer native alerting features, the ability to design specific analysis flows bound to a Security Information and Event Management (SIEM) platform, and a REST API that can integrate into a cybersecurity ecosystem.

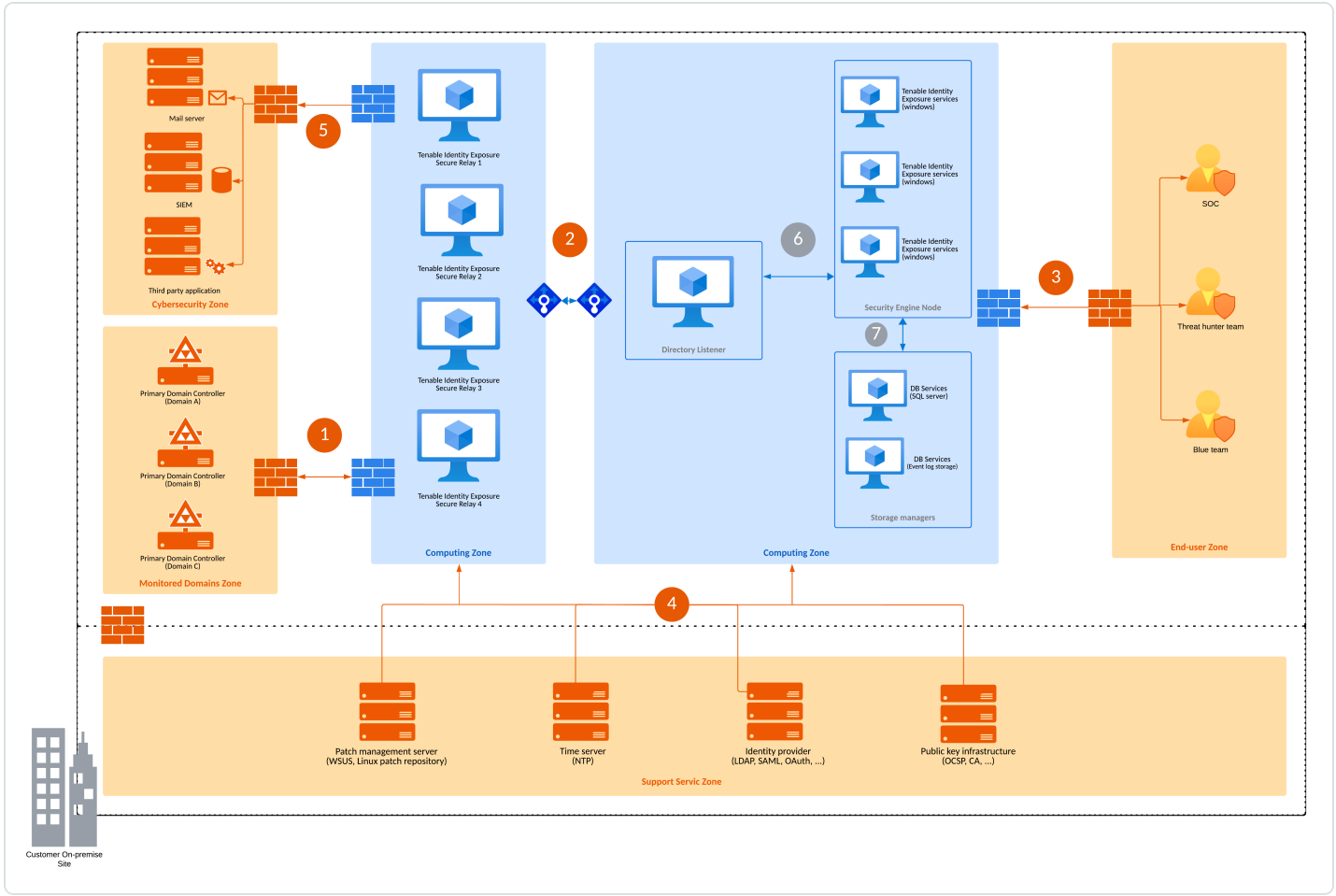
Network Flow Matrix

To do security monitoring, Tenable Identity Exposure must communicate with the Primary Domain Controller emulator (PDCe) of each domain. You must open network ports and transport protocols on each PDCe to ensure efficient monitoring.

In addition to these network flows, you must consider other network flows, such as:

- Access to the end-user services.
- The network flows between Tenable Identity Exposure services.
- The network flows from the support services that Tenable Identity Exposure uses, such as the update management infrastructure and the network time protocol.

The following network matrix diagram gives more details about the different services involved.



Required Protocols

Based on this diagram, the following table describes each required protocol and port that Tenable Identity Exposure uses.

Network Flows	From	To	Tenable Identity Exposure's Usage	Type of Traffic	Protocol and Port
1.	Tenable Identity Exposure 's Secure Relay(s)	Domain controllers	Directory, Replication, User and Computer Authentication,	LDAP/LDAPS	TCP/389 and TCP/636 ICMP/echo-request

			Group Policy, Trusts		ICMP/echo-response
			Replication, User and Computer Authentication, Group Policy, Trusts	SMB, CIFS, SMB2, DFSN, LSARPC, NbtSS, NetLogonR, SamR, SrvSvc	TCP/445
			User and Computer Authentication, Forest Level Trusts	Kerberos	TCP/88, TCP/464 and UDP/464
			User and Computer Authentication, Name Resolution, Trusts	DNS	UDP/53 and TCP/53
			Replication, User and Computer Authentication, Group Policy, Trusts	RPC, DCOM, EPM, DRSUAPI, NetLogonR, SamR, FRS	TCP Dynamic (49152-65535) **Note**: Starting with Windows Vista and Windows Server 2008, the

					default dynamic port range is 49152-65535. This is a change from earlier versions that used ports 1025-5000.
			Directory, Replication, User and Computer Authentication, Group Policy, Trusts	Global Catalog	TCP/3268 and TCP/3269
			Replication	RPC Endpoint Mapper	TCP/135
2.	Tenable Identity Exposure ’s Secure Relay(s)	Tenable Identity Exposure’s Directory Listener	Tenable Identity Exposure’s internal API flows	HTTPS	TCP/443
			Automatic updates	HTTP	TCP/5049
3.	End users	Tenable	Tenable Identity	HTTPS	TCP/443

		Identity Exposure's Security engine nodes	Exposure's end-user services (Web portal, REST API, etc.)		
4.	Tenable Identity Exposure	Support services	Time synchronization	NTP	UDP/123
			Update infrastructure (for example WSUS or SCCM)	HTTP/HTTPS	TCP/80 or TCP/443
			PKI infrastructure	HTTP/HTTPS	TCP/80 or TCP/443
			Identity provider SAML server	HTTPS	TCP/443
			Identity provider LDAP	LDAP/LDAPS	TCP/389 and TCP/636
			Identity provider OAuth	HTTPS	TCP/443

Additional Flows

In addition to the Active Directory protocols, certain Tenable Identity Exposure configurations require additional flows. You must open these protocols and ports between Tenable Identity

Exposure and the targeted service.

Network flows	From	To	Tenable Identity Exposure's Usage (optional)	Type of Traffic	Protocol and Port
5.	Tenable Identity Exposure's Secure Relay(s)	Cybersecurity services	Email notifications	SMTP	TCP/25, TCP/587, TCP/465, TCP/2525, TCP/25025 (depending on the SMTP server's configuration)
			Syslog notifications	Syslog	TCP/601, TCP/6515, UDP/514 (depending on the event log server's configuration)
		Domain controllers	Privileged Analysis	RPC dynamic ports	TCP/49152-65535, UDP/49152-65535

Internal Ports

If you split the Security Engine Nodes and the Storage Managers into two different subnets, Tenable Identity Exposure requires access to the following ports.

Note: Tenable does not recommend separating the Security Engine Nodes and the Storage Manager services on different networks to avoid performance issues.

Network flows	From	To	Tenable Identity Exposure's Usage	Type of Traffic	Protocol and Port
6.	Tenable Identity Exposure 's Directory Listener	Tenable Identity Exposure 's Security Engine Nodes	Tenable Identity Exposure's communication bus	Advanced Message Queuing Protocol	TCP/5671 and TCP/5672
			Tenable Identity Exposure's internal API flows	HTTP/HTTPS	TCP/80 or TCP/443
7.	Tenable Identity Exposure 's Security Engine Nodes	Tenable Identity Exposure 's Storage Managers	MS SQL Server database access	MS SQL queries	TCP/1433
			`EventLogStorage` database access	`EventLogStorage` queries	TCP/4244

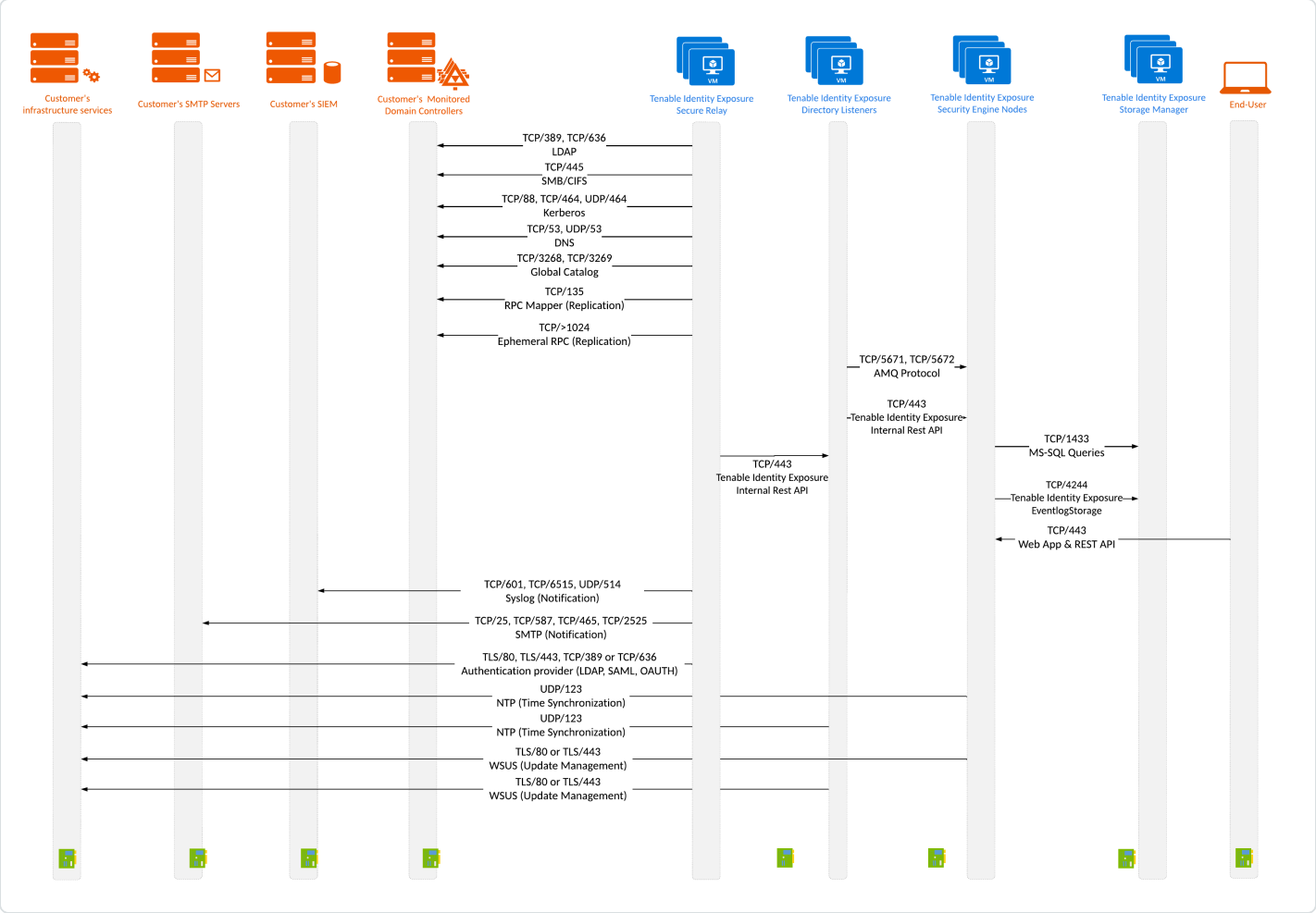
Support Services

Support services are often highly vendor or configuration-specific. For example, the WSUS service listens by default on port TCP/8530 for its 6.2 version and higher, but on TCP/80 for other versions. You can reconfigure this port to any another port.

Network Address Translation (NAT) support

Tenable Identity Exposure initiates all network connections, except those from end users. You can use network address translation (NAT) to connect to Tenable Identity Exposure through network interconnection.

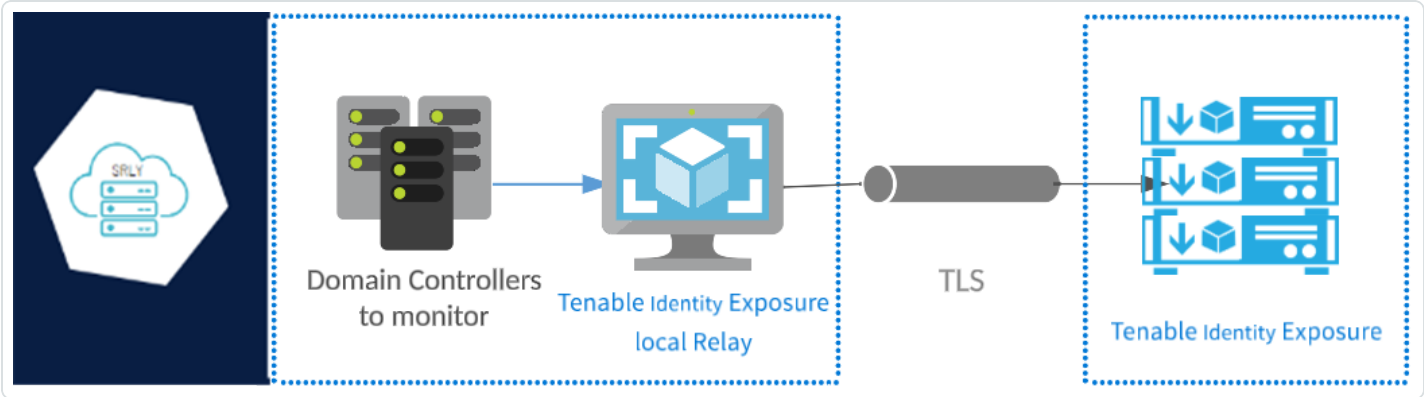
On-Premises platform using Secure Relay



Secure Relay Requirements

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.



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:

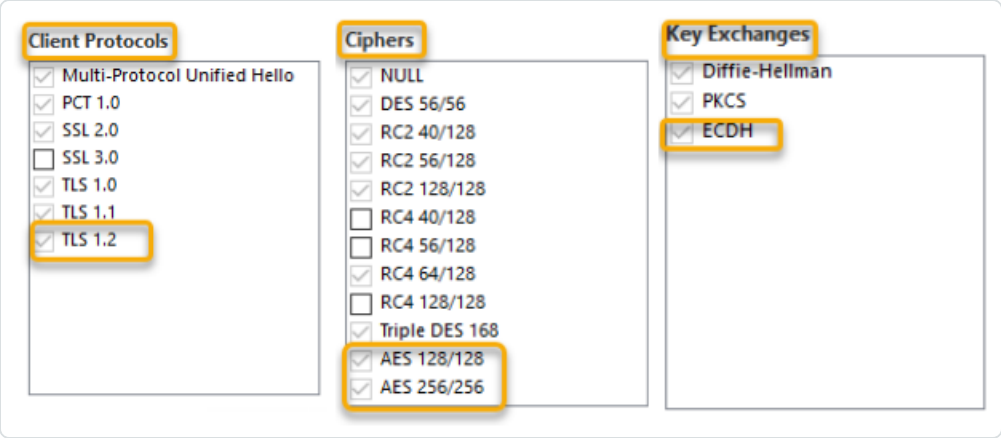
   ```
   Get-TlsEccCurve
   ```

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**

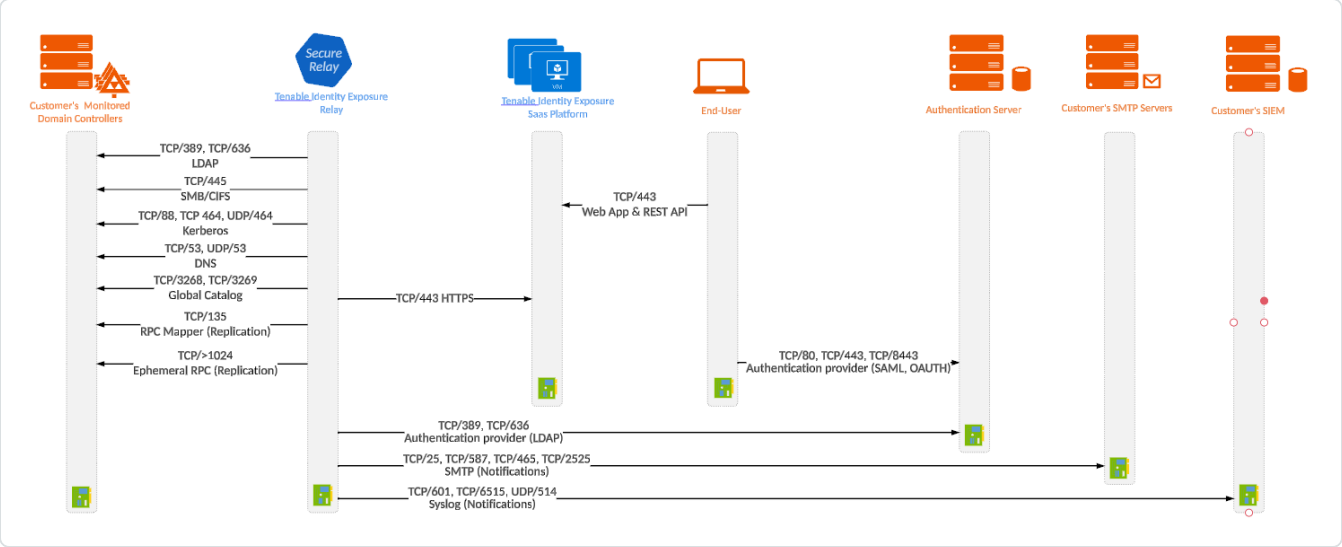


2. After you modify the cryptographic settings, restart the machine.

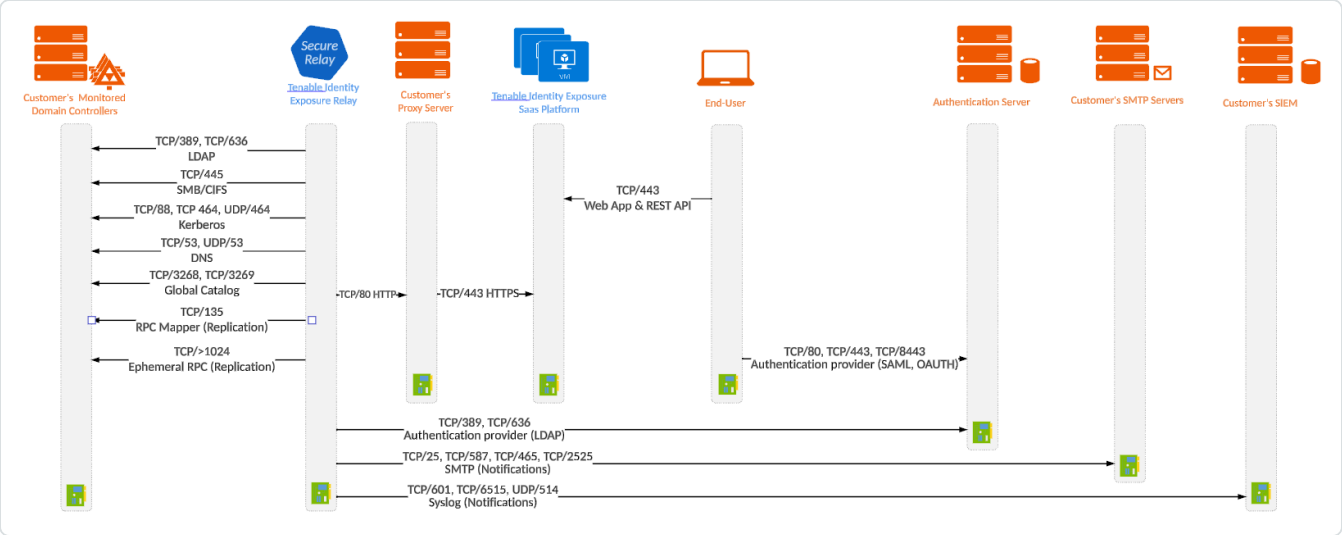
> **Note**: Modifying Windows cryptographic settings affects all applications running on the machine and using the Windows TLS library, known as "Schannel." Therefore, ensure that any adjustment you make does not cause unintended side effects. Verify that the chosen configurations align with the organization's overall hardening objectives or compliance mandates.

Required Ports

- 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:



> **Note**: The network flows works in the same way for both on-premises and SaaS platforms.

Virtual machine prerequisites

The requirements for the virtual machine (VM) hosting the Secure Relay are the following:

Customer Size	Tenable Identity	Instance Required	Memory (per	vCPU (per	Disk Topology	Available Disk

	Exposure Services		instance)	instance)		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

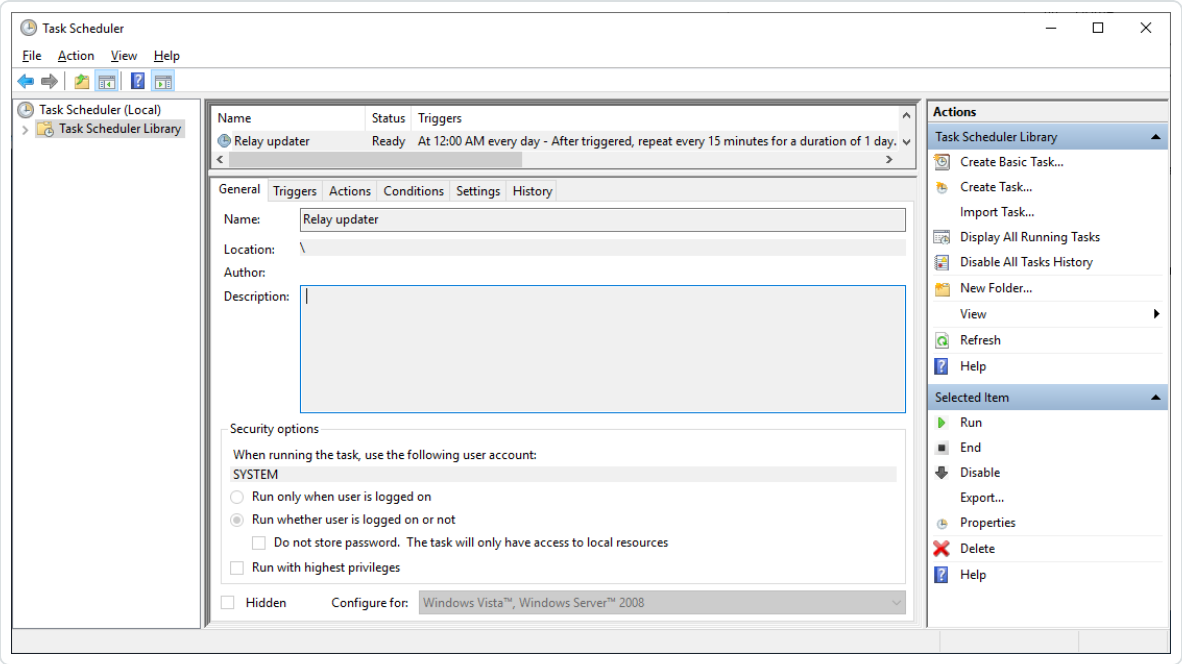
Note: If you install the Secure Relay and the Directory Listener on the same virtual machine, you must combine their sizing requirements. See Resource Sizing.

Tip: For the initial installation, it is preferable for the VM to remain non-domain joined to avoid inheriting existing GPO policies that may interfere with the installation process. After completing the installation, you can then join the VM to the domain.

The VM must also have:

- HTTP/HTTPS traffic – Remove, disable, bypass, or allowlist any client that can steer HTTP/HTTPS traffic toward the Secure Relay machine. This action blocks the Secure Relay installation and stops or slows traffic entering the Tenable platform.
- 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:



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).

> 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

Web Portal Requirements

Tenable Identity Exposure does not require any specific configuration or plugin from client browsers.

Supported Internet Browsers

You must use the most recent version of your supported web browser.

Supported Web Browsers including minimum version	
Microsoft	Edge version 38.14393 or Internet Explorer 11
Google	Chrome version 56.0.2924

Mozilla	Firefox version 52.7.3
Apple	Safari version 11.0

TLS Server Certificate

Tenable Identity Exposure uses SSL/TLS encryption mechanism to access its application.

Tenable strongly recommends using a valid certificate which you provide during installation.

Supported TLS configuration and version

- TLS 1.1 to TLS 1.3
- Self-signed certificate from Tenable
- Certificate issued from your private PKI
- Alternative TLS certificate

Recommended TLS configuration and version

- TLS 1.2
- Certificate issued from your private PKI

TLS certificate update

If you need to change your TLS certificates outside of an upgrade, you can update the CRT and key files under `Tenable\Tenable.ad\Certificates` and restart the services.

See also

- HTTPS for Tenable Identity Exposure Web Application

Integration with an Active Directory Domain

Tenable Identity Exposure runs on Microsoft Server operating systems that connect to an Active Directory (AD) domain. The following are guidelines on whether or not to connect these servers to an AD domain.

- Because Tenable Identity Exposure offers sensitive security information, **Tenable does not recommend joining its servers to any AD domain**. In fact, working on an isolated environment allows for a clear separation between the monitored perimeter and the monitoring entity (i.e., Tenable Identity Exposure). In this configuration, an attacker with initial access or limited privileges on the monitored domain cannot directly access Tenable Identity Exposure and its security analysis results.
- If you have a trustful infrastructure, you can choose to run Tenable Identity Exposure on domain-joined servers. This approach improves server management as it is part of the regular process that you use for each domain-joined server. In particular, Tenable Identity Exposure servers apply the same hardening policies as any other corporate server. Tenable recommends this architecture only on secure AD environments, and you must take into consideration the following risks in the case of an AD compromise:
    - An attacker with server-administration privileges can gather more information about ways to compromise the system using data analysis from Tenable Identity Exposure.
    - The security policy on domain-joined servers can forbid the administrative access granted to Tenable Support or its certified partners.
    - An attack can corrupt Tenable Identity Exposure's security monitoring by hiding a security incident.

Note: AWS Directory Service may be partially compatible with Tenable Identity Exposure; however, some features may not function as expected. This includes limited monitoring, unavailable Indicators of Attack, and certain permissions that cannot be applied. While it may work in some cases, full functionality is not currently supported or tested by Tenable.

Install Tenable Identity Exposure

Required User Role: Administrator on the local machine

Tenable Identity Exposure's installation program installs the following components on different servers:

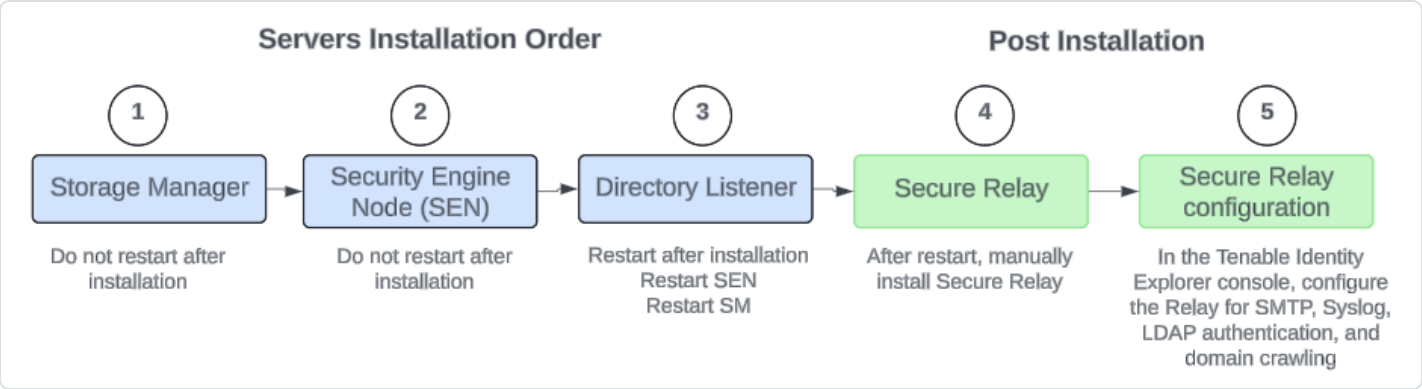
- A **Storage Manager** (SM) to host all data based on MSSQL.
- A **Directory Listener** (DL) to target audited domains.
- A **Security Engine Node** (SEN) to perform security analysis and serve the user interface.

  For more information about how to install the SEN on several machines, see Split Security Engine Node (SEN) Services.
- A **Secure Relay** (a separate installer) to allow you to configure domains from which it forwards the data to the Data Listener component, which collects AD objects.

All machines and installed binaries support the application of any security update for the underlying OS, either through Windows Server Update Services (WSUS) or System Center Configuration Manager (SCCM).

Installation Order

To install **Tenable Identity Exposure** 3.59, proceed in the following order:



Before you start

- **Download the executable programs** for Tenable Identity Exposure and Secure Relay from Tenable's Downloads site.
- **Review the** Pre-deployment Requirements.

  Caution: From Tenable Identity Exposure version **3.59.5** onwards, ensure that your **TLS certificates use OpenSSL 3.0.x**.
- **Review** On-Premises Architectures and **select the** TLS Installation Types for your platform.

- **Reserve the following resources** and have their information on hand before you install Tenable Identity Exposure:
    - Network – Private IP addresses.
    - Access – DNS name used to access Tenable Identity Exposure's web portal.
    - Security – TLS certificate and its associated private key to secure access to the web portal.

      For more information, see Network Requirements.
- **Run the installer as a local user or a domain user** who is a member of the **Local Administrators** group.
- **Have account permissions**: The account you use to deploy Tenable Identity Exposure must have these specific permissions: `SeBackupPrivilege`, `SeDebugPrivilege`, and `SeSecurityPrivilege`.
- **Restart your server** before launching the Tenable Identity Exposure installer for each component.

Installation Procedures

The following procedures install the Tenable Identity Exposure components in **TLS with autogenerated and self-signed certificates (Default)**. For more information, see TLS Installation Types.

To install the Storage Manager:

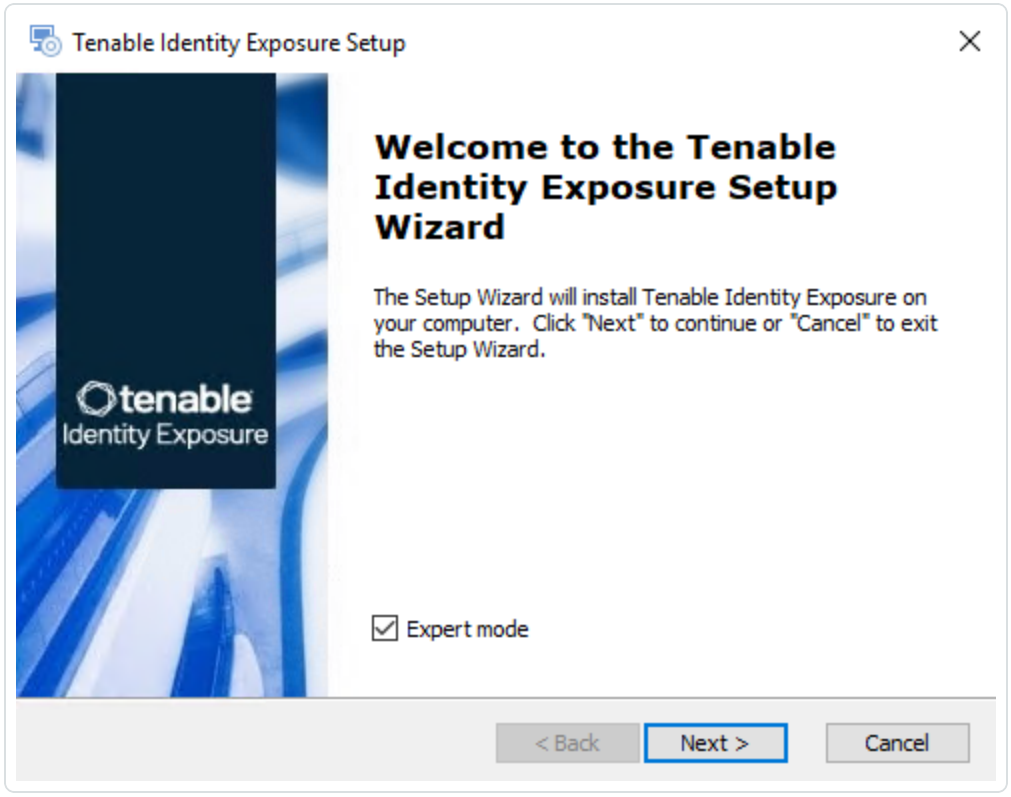
1. On the local machine, run the **Tenable Identity Exposure 3.59** On-Premises installer.

   A welcome screen appears.

2. In the setup language box, click the arrow to select the language for the installation, and click **Next**.

   The **Setup Wizard** appears.

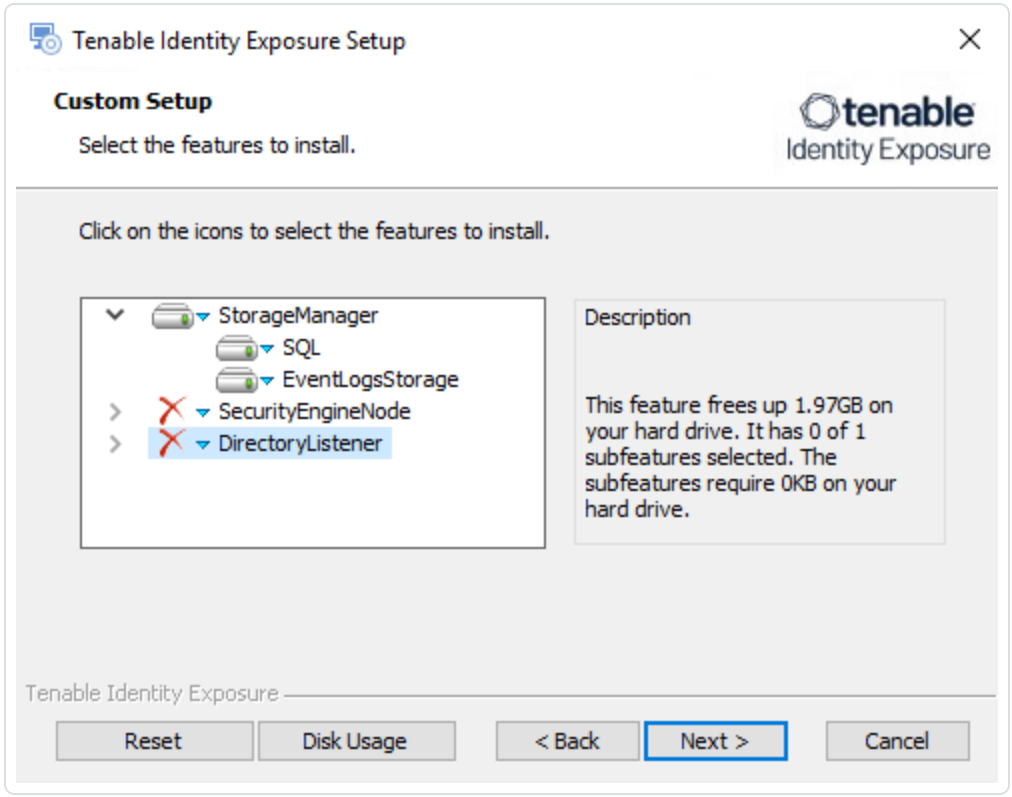
3. Select the **Expert Mode** checkbox.



4. Click **Next**.

   The **Custom Setup** window appears.

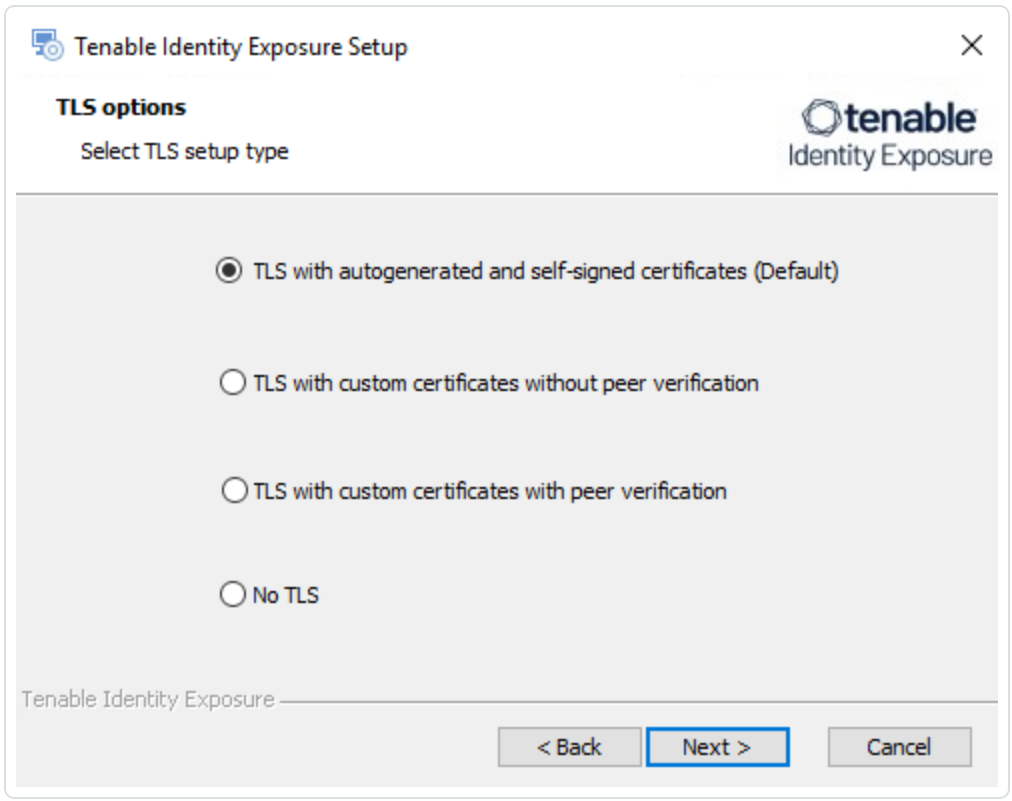
5. Deselect the *Security Engine Nodes* and *Directory Listener* components.



6. Click **Next**.

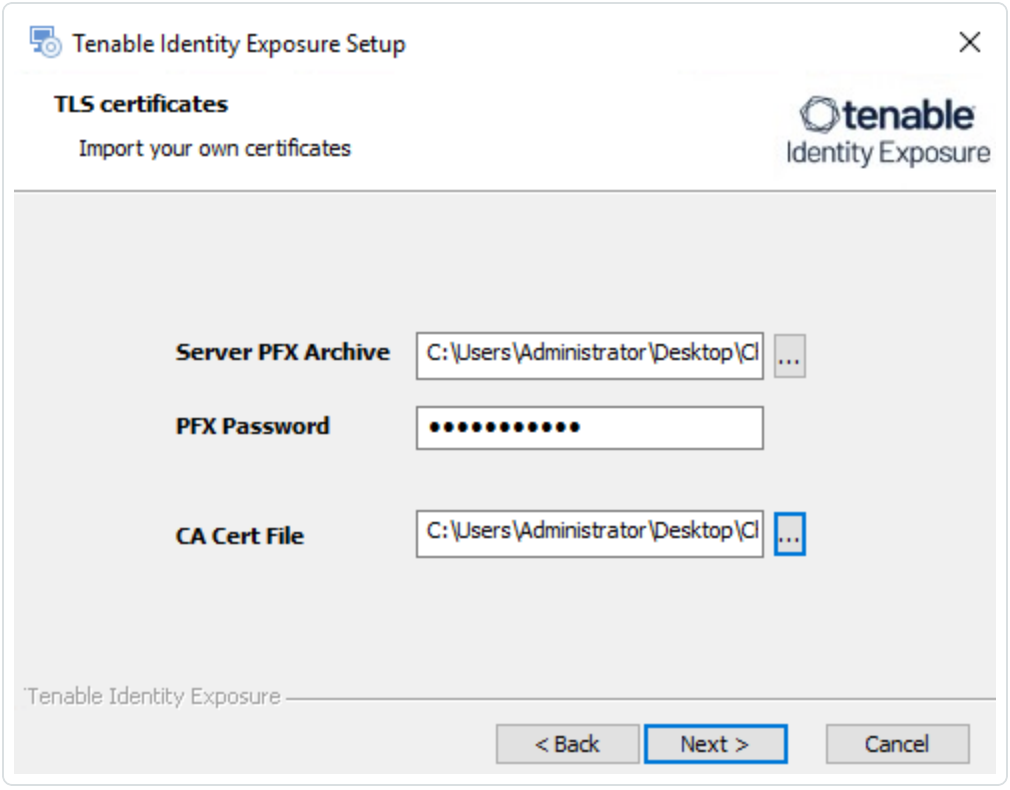
   The **TLS Options** window appears.

7. Select the **TLS with autogenerated and self-signed certificates (Default)** option.



Optional: If you select **TLS with custom certificates without peer verification** or **TLS with custom certificates with peer verification**, the next **TLS certificates** screen asks you to provide the following information:

- In the **Server PFX Archive** box, click **...** to browse to your PFX archive.
- In the **PFX Password** box, type the password for the PFX file.
- In the **CA Cert File** box, click **...** to browse to your CA certificate file.



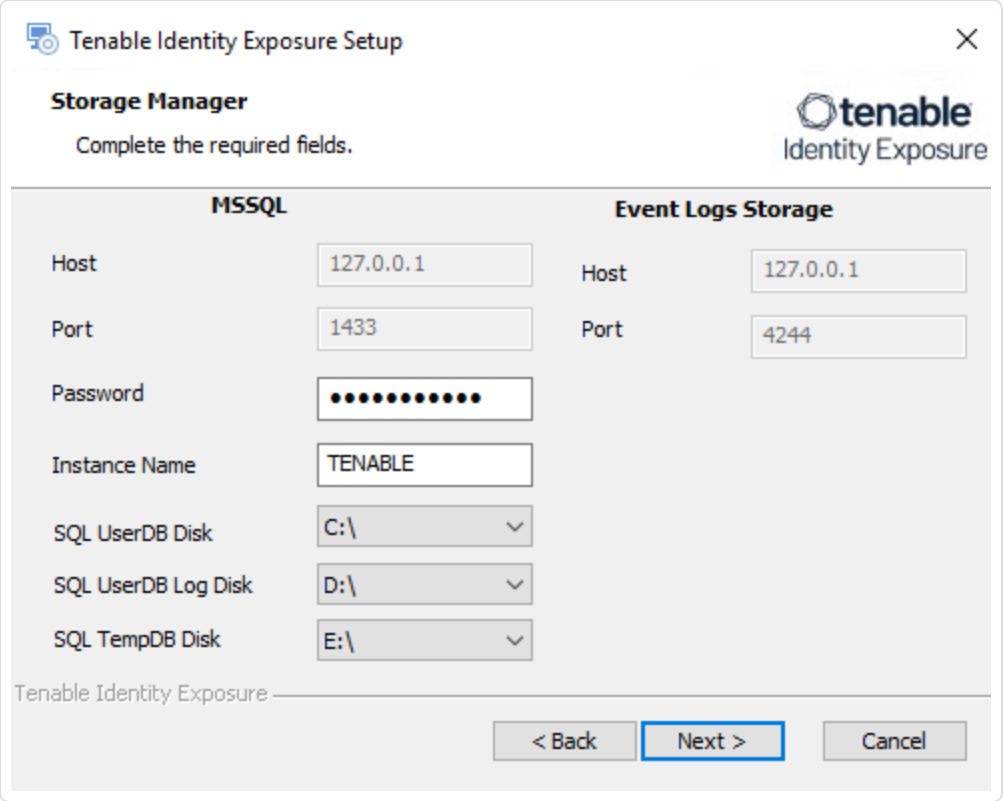
8. Click **Next**.

   The **Storage Manager** window appears.

9. In the **Password** box, type a password for the MSSQL database.

   Note: The installer requires an SA password with the syntax described in Strong Passwords for the

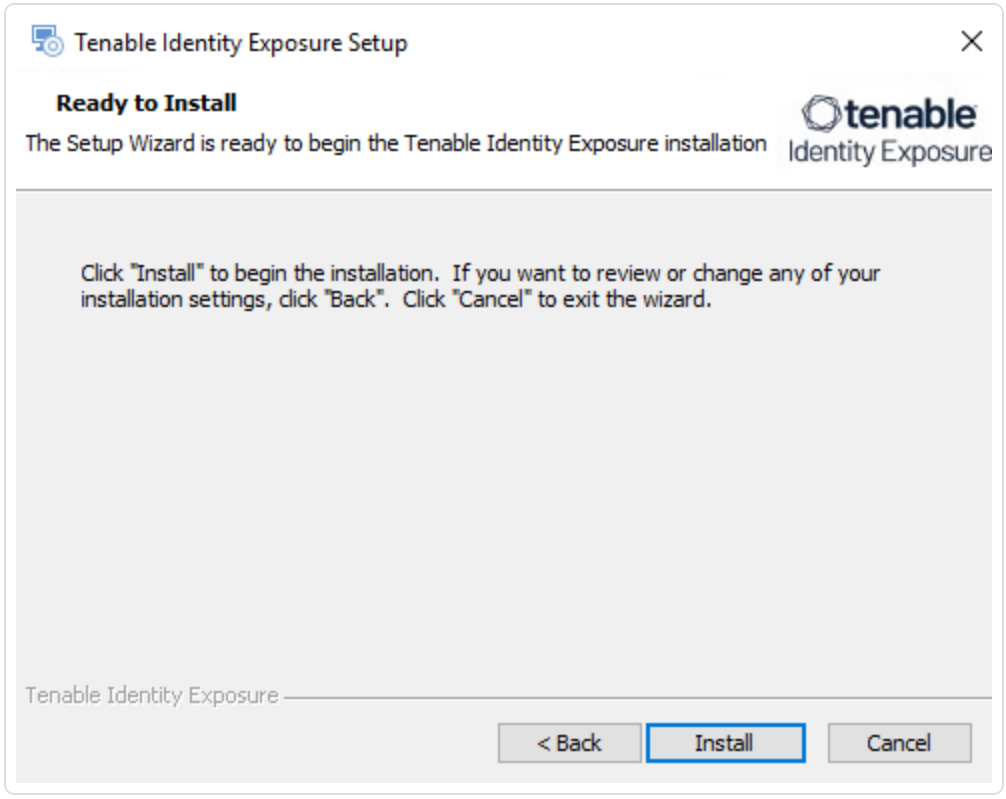
SQL Server.



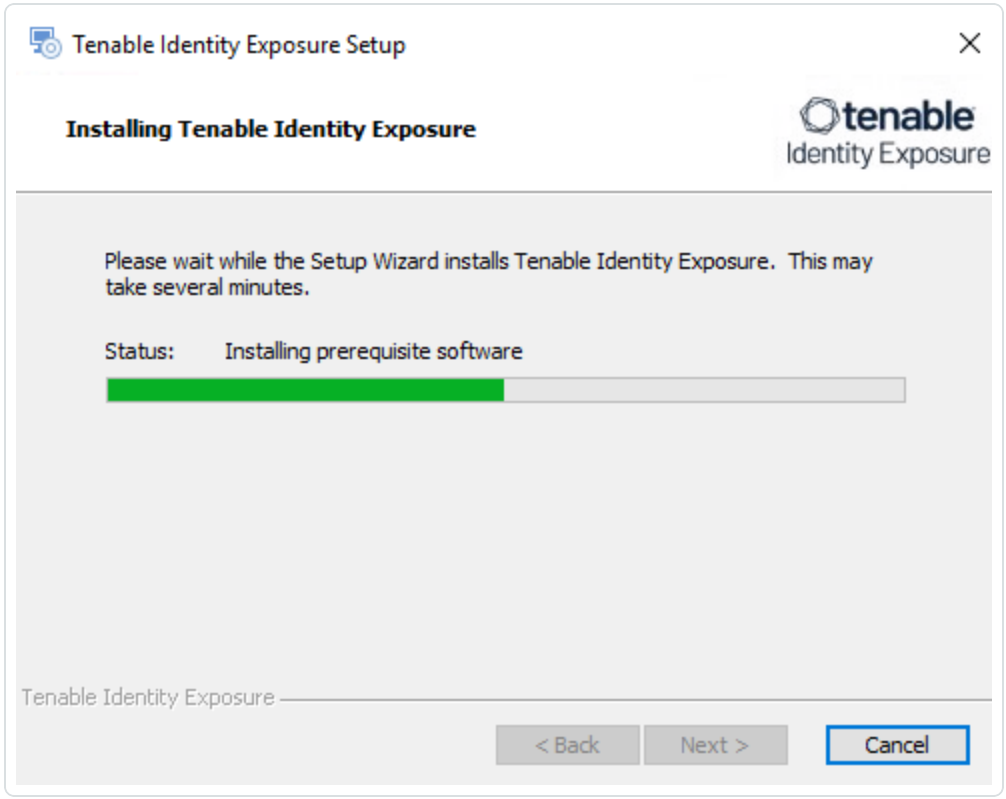
Note: Tenable strongly recommends that you keep the default TENABLE instance name.

10. Click **Next**.

    The **Ready to Install** window appears.



11. Click **Install** to begin the installation.



After the installation completes, the **Completing the Tenable Identity Exposure Setup Wizard** window appears.

12. Click **Finish**.

    A dialog box asks you to restart your machine.

13. Click **No**.

    Caution: **Do not** restart the machine now.

14. Install the Security Engine Node.

To install the Security Engine Node:

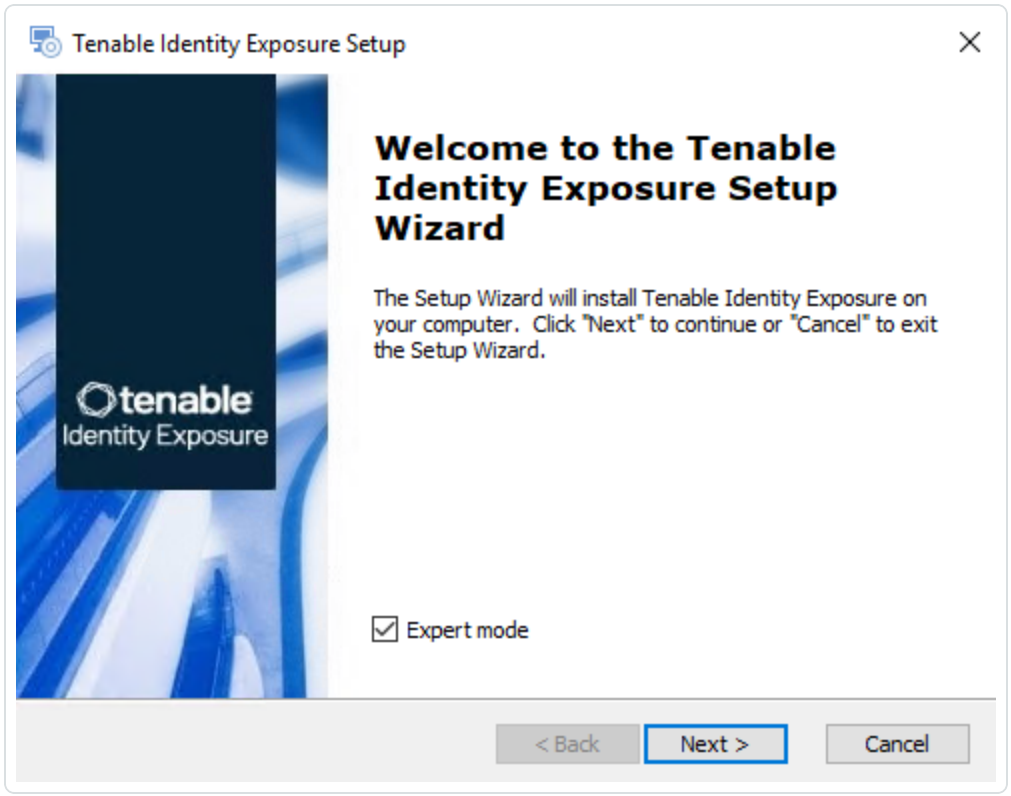
1. On the local machine, run the **Tenable Identity Exposure 3.59** On-Premises installer.

   A welcome screen appears.

2. In the setup language box, click the arrow to select the language for the installation, and click **Next**.

   The **Setup Wizard** appears.

3. Select the **Expert Mode** checkbox.

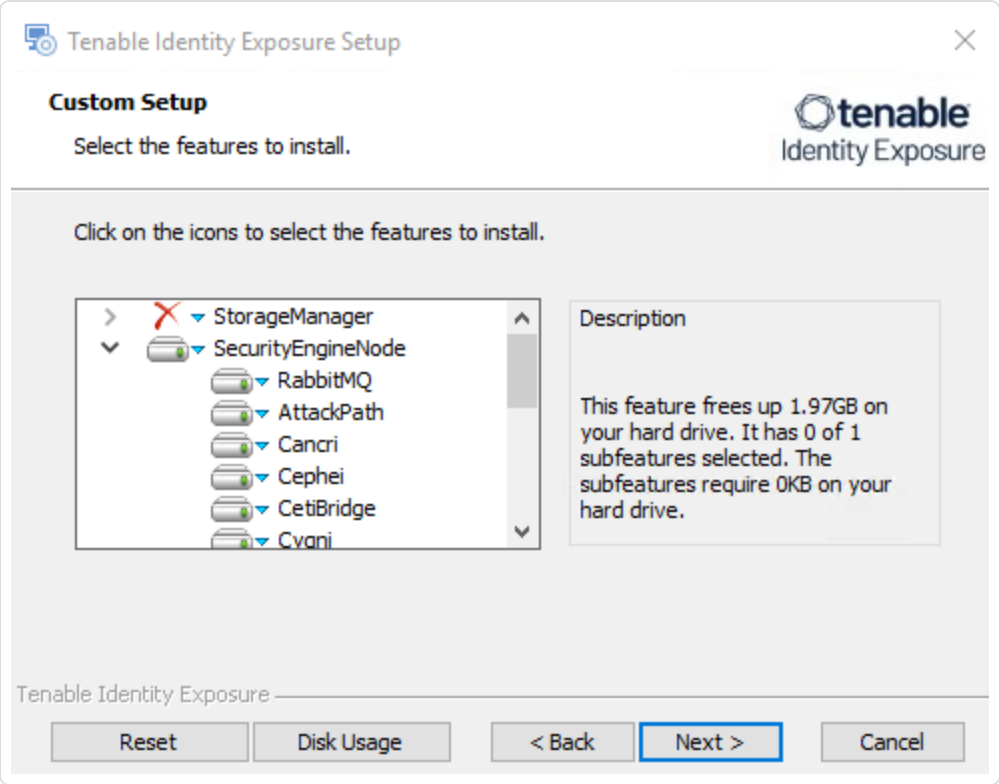


4. Click **Next**.

   The **Custom Setup** window appears.

5. Deselect the *Storage Manager* and *Directory Listener* components.

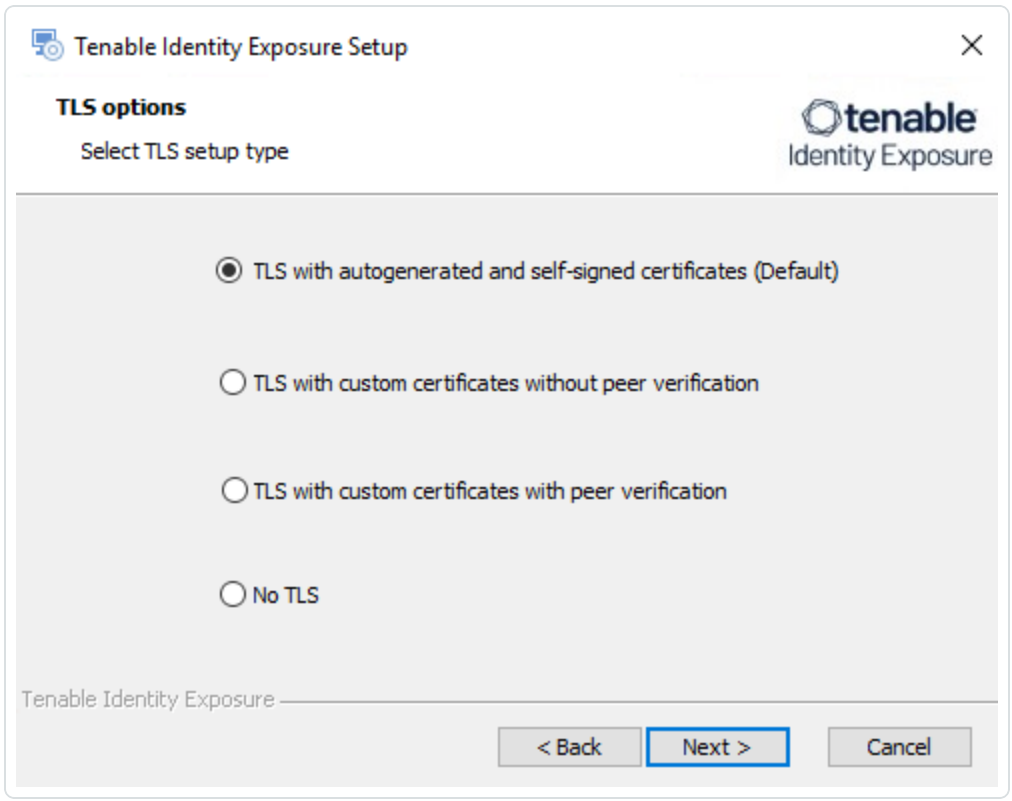
> **Note**: To install SEN services over several machines, see Split Security Engine Node (SEN) Services.



6. Click **Next**.

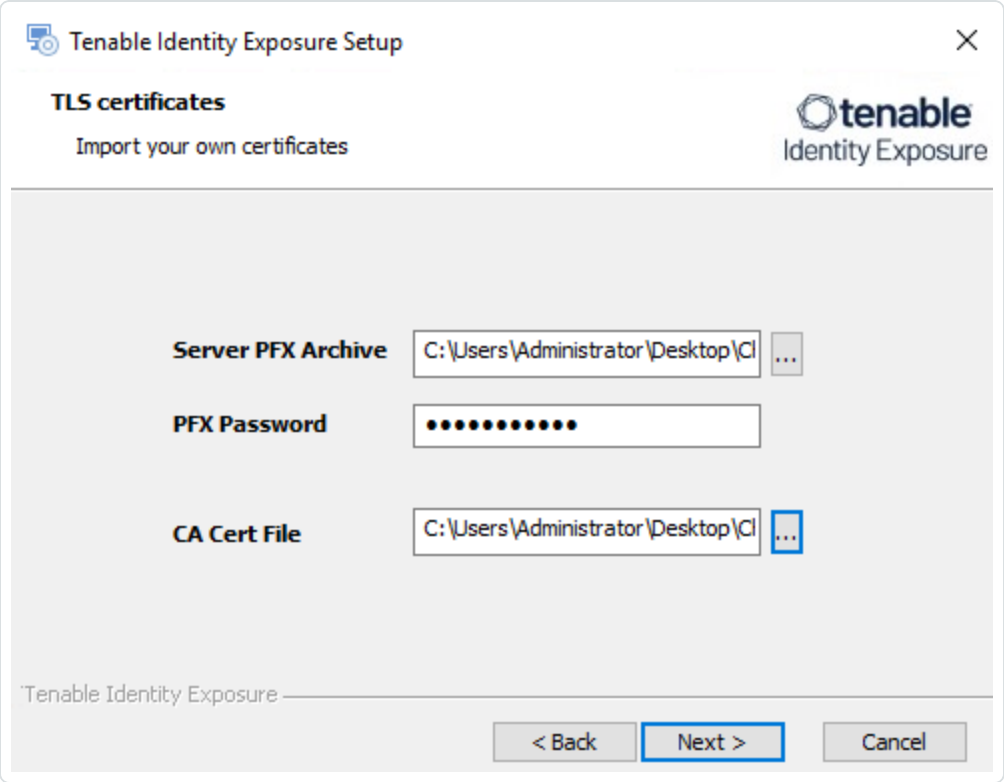
   The **TLS Options** window appears.

7. Select the **TLS with autogenerated and self-signed certificates (Default)** option.



Optional: If you select **TLS with custom certificates without peer verification** or **TLS with custom certificates with peer verification**, the next **TLS certificates** screen asks you to provide the following information:

- In the **Server PFX Archive** box, click **...** to browse to your PFX archive.
- In the **PFX Password** box, type the password for the PFX file.
- In the **CA Cert File** box, click **...** to browse to your CA certificate file.



8. Click **Next**.

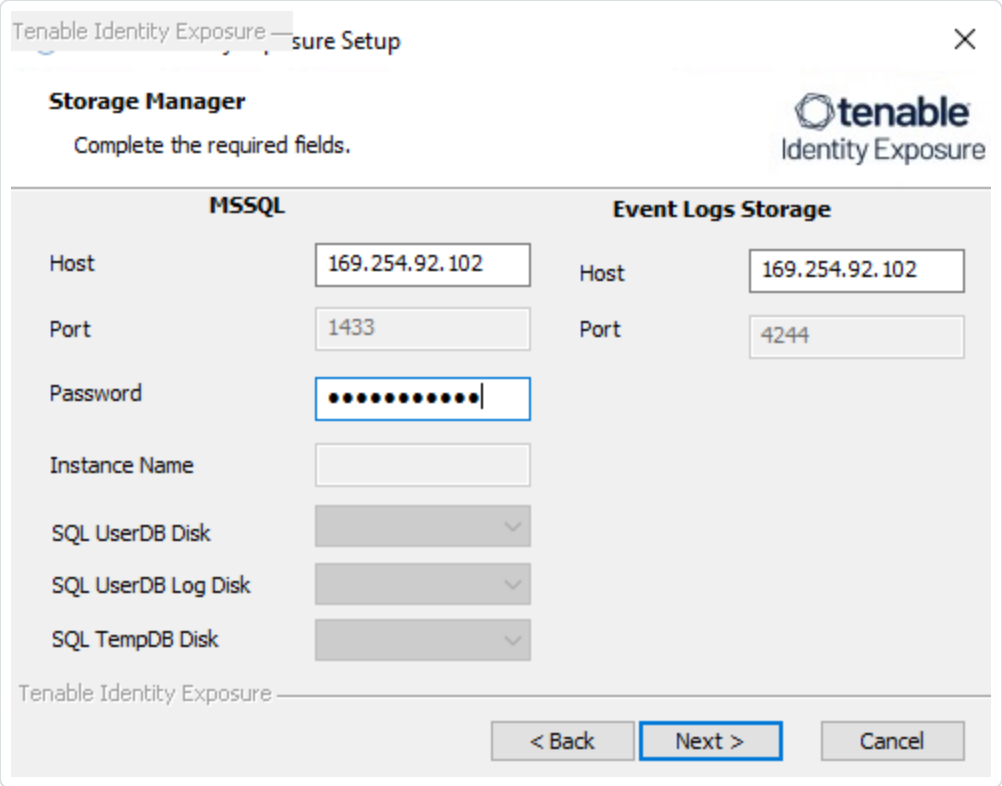
   The **Storage Manager** window appears.

9. Provide the following information:

   - In the **MSSQL** and **Event Logs Storage** boxes, type the FQDN or IP address of the Storage Manager.
   - In the **Password** box, type the service account password for the MSSQL database defined in the Storage Manager installation.

     Note: The installer requires an SA password with the syntax described in Strong Passwords for

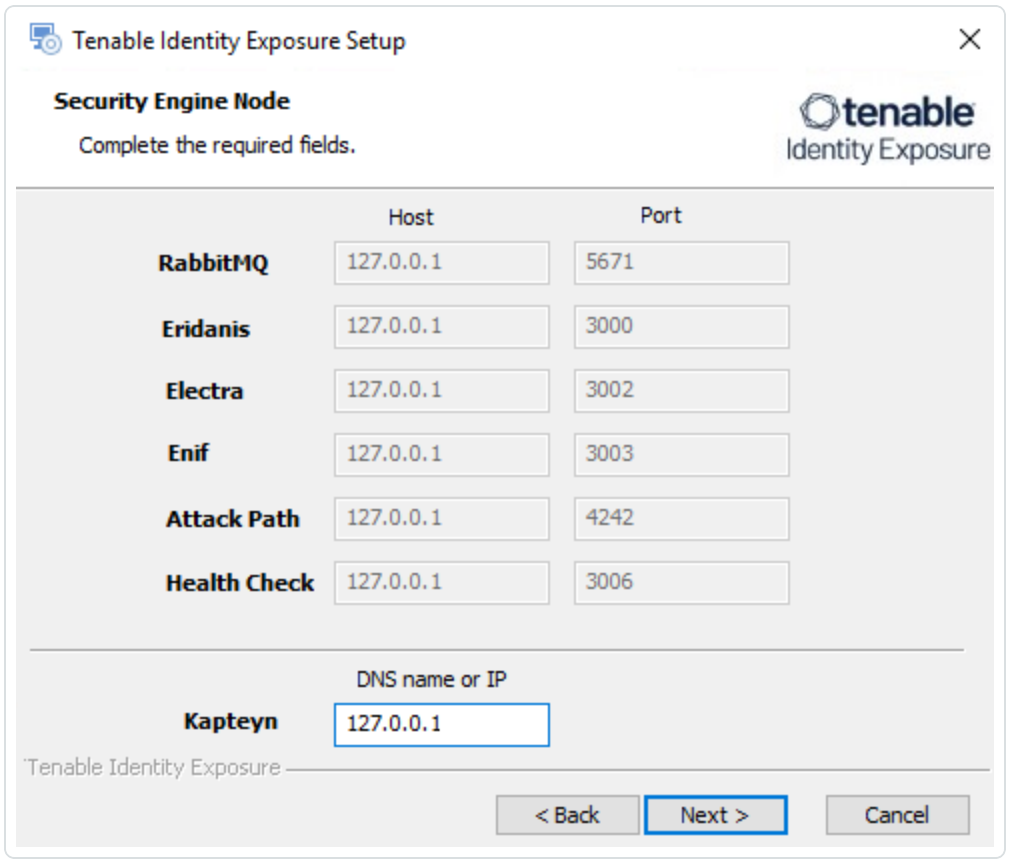
the SQL Server.



10. Click **Next**.

    The **Security Engine Node** window appears.

11. In the **Host** box, type the DNS name (preferred) or IP address of the web server that end users enter to access Tenable Identity Exposure.



Note: By default, the installation process creates a self-signed certificate with the DNS name or the IP address that you entered. For more information, see Change the IIS Certificate.

12. Click **Next**.

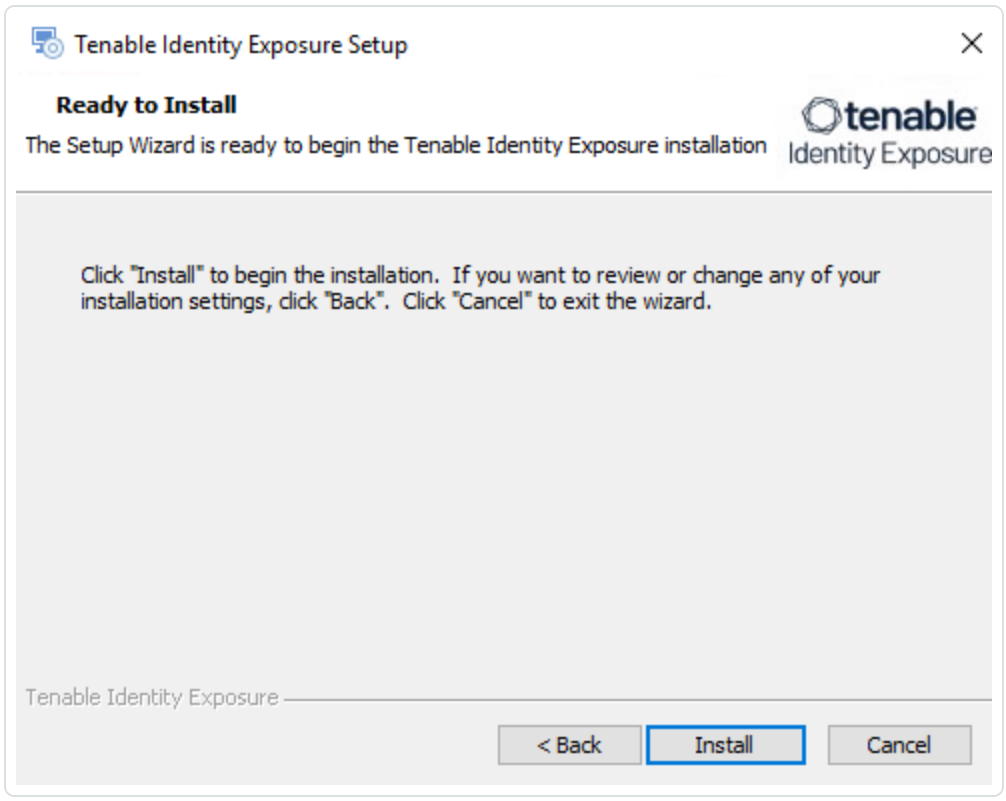
    The **Directory Listener** window appears.

13. In the **Ceti** box, type the IP address or configured FQDN for the Directory Listener machine.

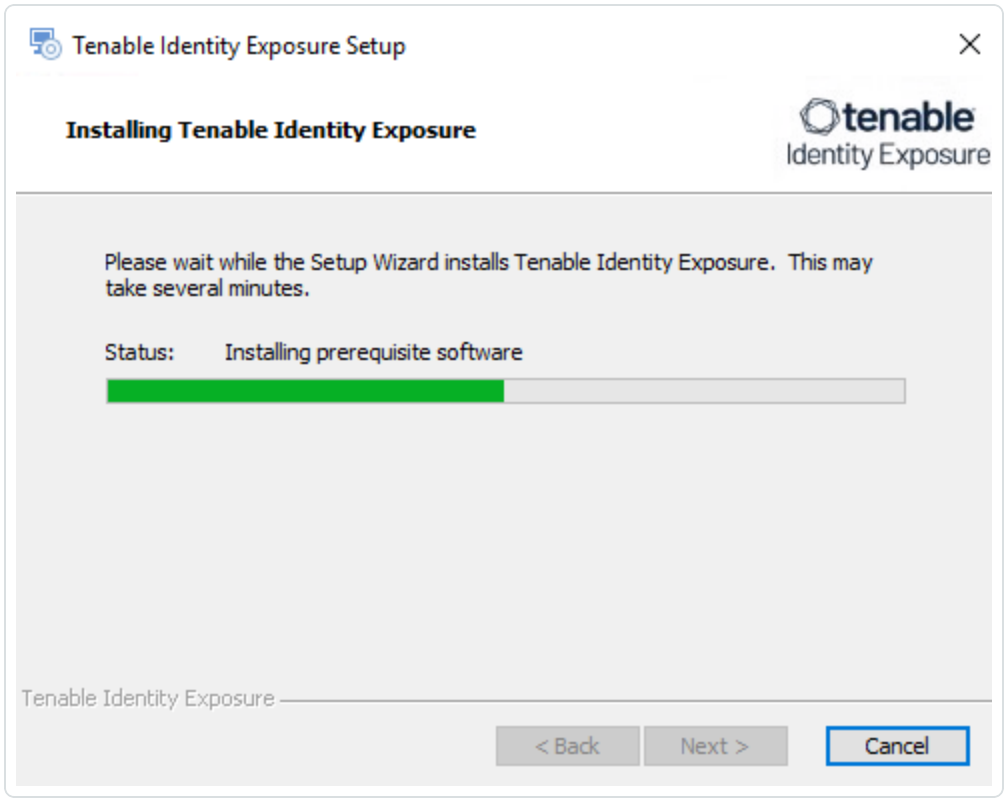
    Tip: If you plan to install the Secure Relay on the same machine as the Directory Listener, you must keep the default IP address "127.0.0.1" for Ceti on the SEN. If you install the Secure Relay on another machine, type the IP address of the Directory Listener for Ceti on the SEN.

14. Click **Next**.

    The **Ready to Install** window appears.

15. 

16. Click **Install** to begin the installation.



After the installation completes, the **Completing the Tenable Identity Exposure Setup Wizard** window appears.

17. Click **Finish**.

    A dialog box asks you to restart your machine.

18. Click **No**.

    > **Caution**: **Do not** restart the machine now.

19. Install the Directory Listener.

To install the Directory Listener:

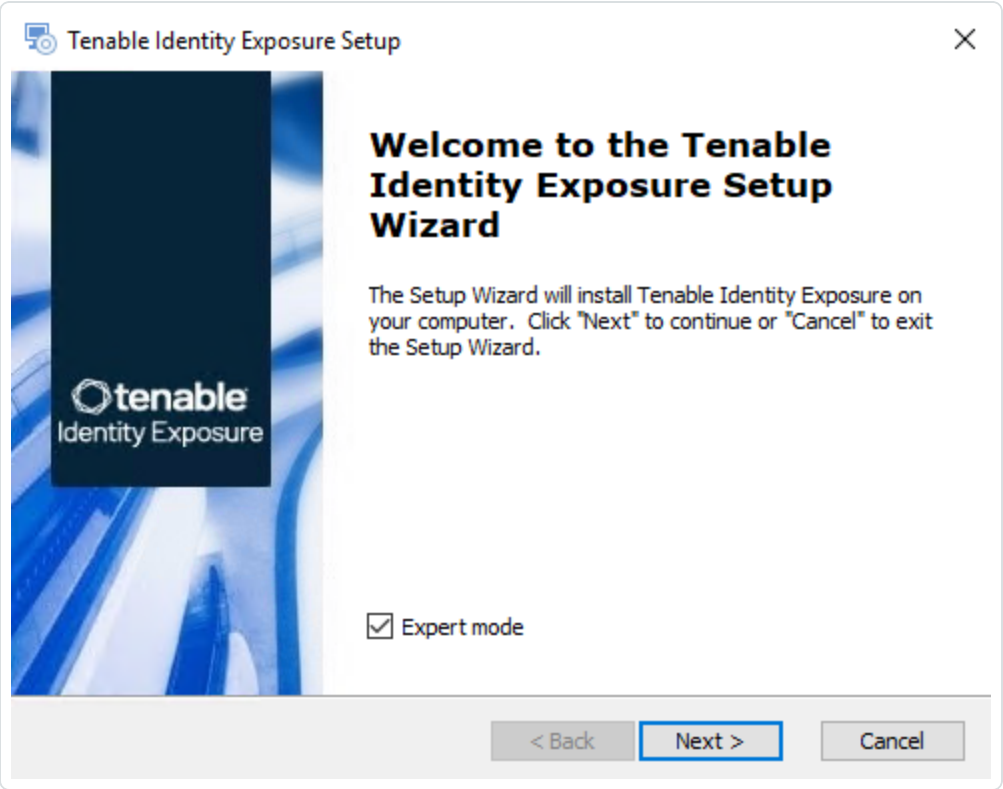
1. On the local machine, run the **Tenable Identity Exposure 3.59** On-Premises installer.

   A welcome screen appears.

2. In the setup language box, click the arrow to select the language for the installation, and click **Next**.

   The **Setup Wizard** appears.

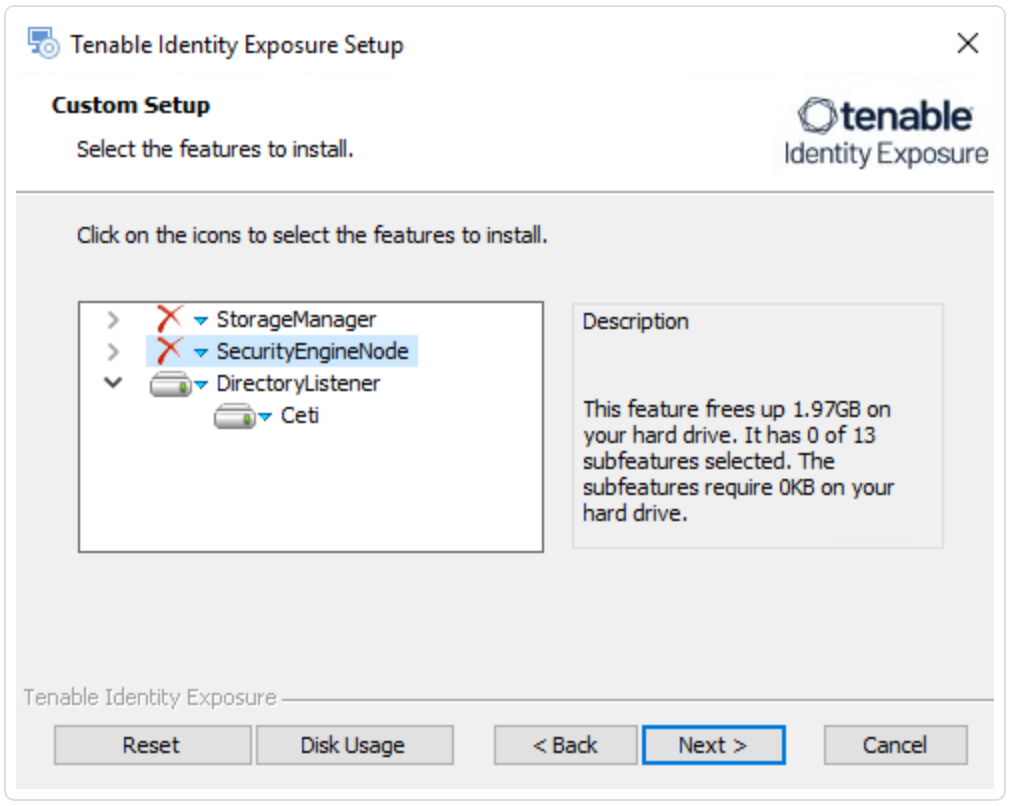
3. Select the **Expert Mode** checkbox.



4. Click **Next**.

   The **Custom Setup** window appears.

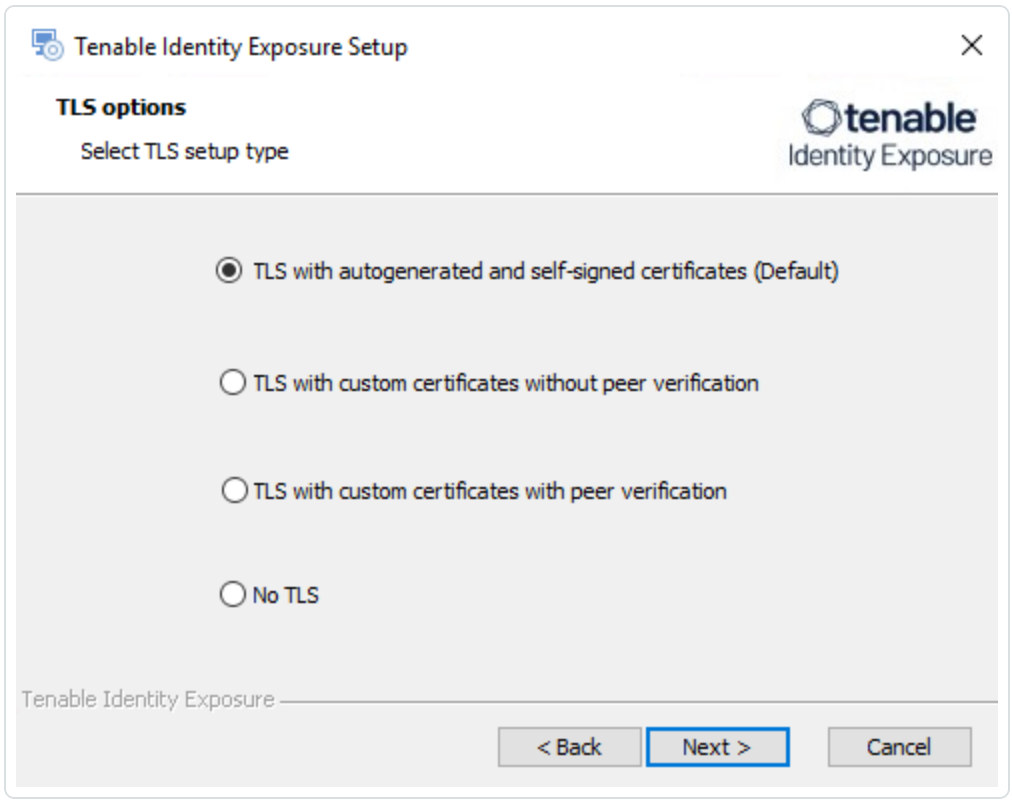
5. Deselect the *Storage Manager* and the *Security Engine Nodes* components.



6. Click **Next**.

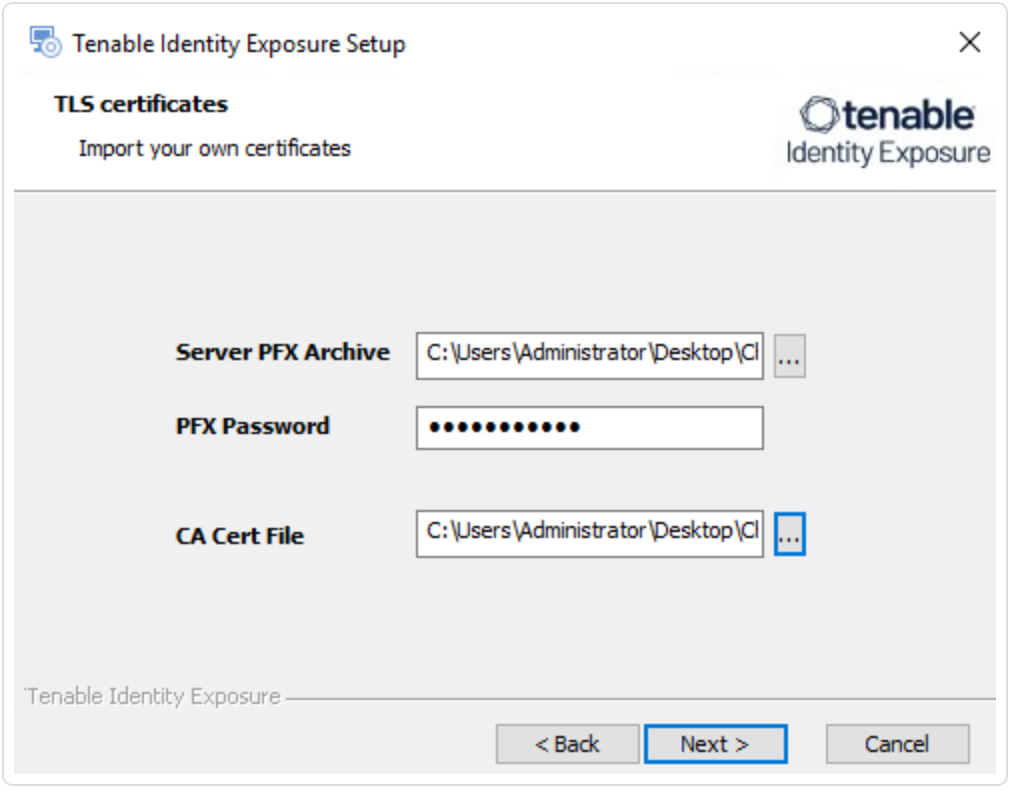
   The **TLS Options** window appears.

7. Select the **TLS with autogenerated and self-signed certificates (Default)** option.



Optional: If you select **TLS with custom certificates without peer verification** or **TLS with custom certificates with peer verification**, the next **TLS certificates** screen asks you to provide the following information:

- In the **Server PFX Archive** box, click **...** to browse to your PFX archive.
- In the **PFX Password** box, type the password for the PFX file.
- In the **CA Cert File** box, click **...** to browse to your CA certificate file.

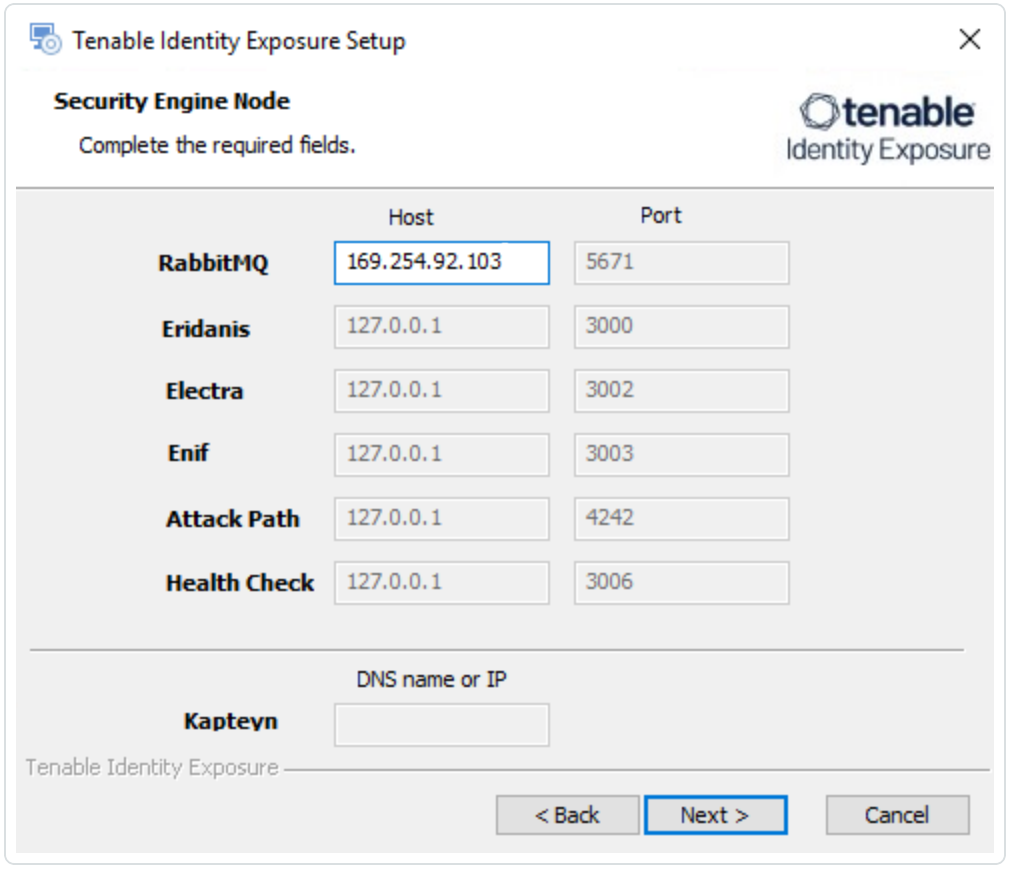


8. Click **Next**.

   The **Security Engine Node** window appears.

9. In the **Host** box for RabbitMQ, type the address of the Security Engine Node hosting

RabbitMQ.

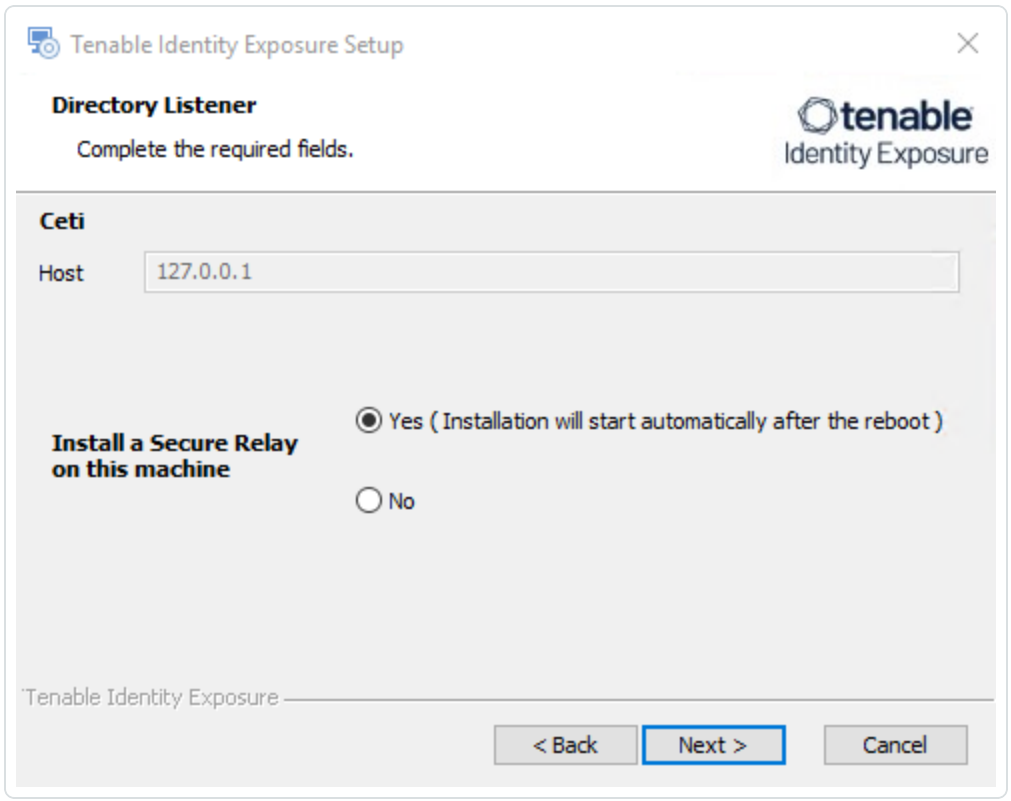


10. Click **Next**.

    The **Directory Listener** window appears.

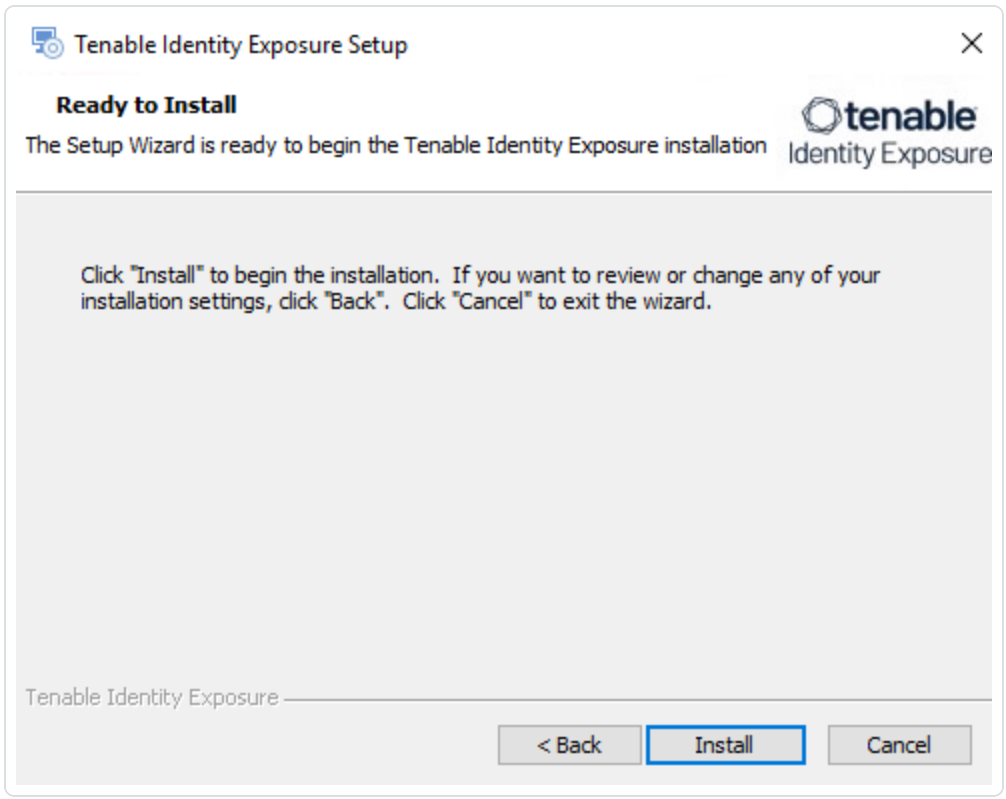
11. You have two options whether to install the Secure Relay on this Directory Listener:

    - **Yes** – After this installation completes and the Directory Listener reboots, the Secure Relay installer launches.
    - **No** – You select to install the Secure Relay at a later time **or on a separate server** (see Secure Relay Architectures for On-Premises Platforms.) A message shows you the location of the Secure Relay installer. **A Secure Relay is mandatory** whether you install it on the Directory Listener machine or on a separate machine.

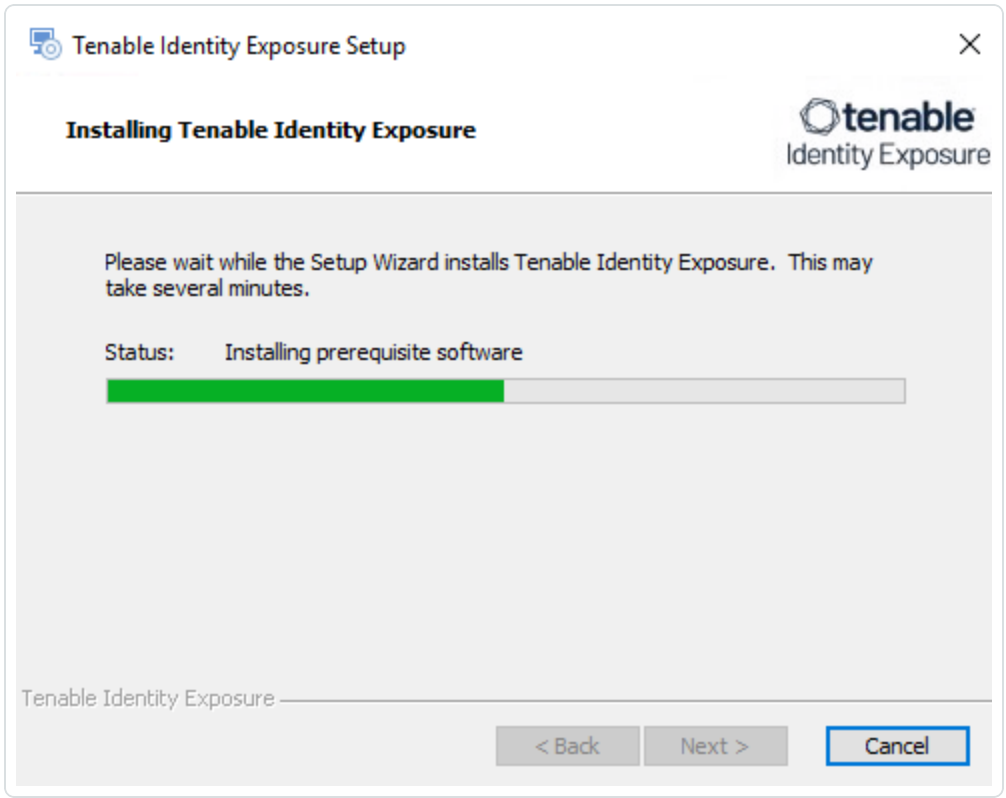


12. Click **Next**.

    The **Ready to Install** window appears.



13. Click **Install** to begin the installation.



After the installation completes, the **Completing the Tenable Identity Exposure Setup Wizard** window appears.

14. Click **Finish**.

    A dialog box asks you to restart your machine.

15. Click **Yes**.

    The machine restarts.

16. Restart the SEN machine.
17. Restart the Storage Manager machine.
18. Install the Secure Relay for Tenable Identity Exposure 3.59 using a separate installer.

To log in to Tenable Identity Exposure:

1. Log in to Tenable Identity Exposure
2. Type in your initial credentials with the username `hello@tenable.ad` and the password `verySecure1`.

To install the Secure Relay:

1. Review Secure Relay Requirements.
2. Select Secure Relay Architectures for On-Premises Platforms.
3. Install the Secure Relay for Tenable Identity Exposure 3.59.

TLS Installation Types

Tenable Identity Exposure requires Transport Layer Security (TLS) to encrypt internal communications between Tenable Identity Exposure components (micro-services) .

Tenable Identity Exposure enables TLS on protocols by using HTTPS instead of HTTP, AMQPS (AMQP+TLS) instead of AMQP (Advanced Message Queuing Protocol), and TLS encryption for MS-SQL.

> **Note**: This is not the same as the activation of HTTPS on the Tenable Identity Exposure web portal using an Internet Information Services (IIS) certificate.

Note: The TLS installations offered here concern TLS encryption between Tenable Identity Exposure components and are not related to SaaS-TLS deployments.

TLS Installation Types

Tenable Identity Exposure offers four types of TLS setups during the installation, from the least to the most hardened:

Installation Option	Recommended For	Encryption Between Internal Communications and Tenable Identity Exposure Components	Peer Verification	CA Certificate Requirement for Secure Relay
No TLS	A trusted network of machines. An easy installation with little configuration. This option falls back to the "Default TLS" option.	**Not encrypted**. Every component communicates in plain text, except for the Secure Relay that interacts with the Directory Listener.	**Disabled** Tenable Identity Exposure does not check server certificates. This setup is not resistant to active MITM	Install the public part of the Certificate Authority (CA) generated during the installation located at `C:\Tenable\Tenable.ad\DirectoryListener\envoy_server\certs` on each machine where you install the Relay.

Default TLS (no "Expert mode") **Default TLS** ("Expert mode")	An organization without its own internal public key infrastructure (PKI) that requires protection against passive eavesdropping.	**Encrypted** using an internal PKI for Tenable Identity Exposure with its own certificates and private keys, which the installation automatically generates and stores on the disk of the first machine.	attacks.	

Note: The default TLS installations – one that uses the "Expert" mode and one that does not – are essentially the same.

Custom TLS Without Peer Verification	An organization with its own internal PKI that requires protection against passive eavesdropping.	**Encrypted**, using certificates from your internal PKI. Certificates must contain the IP address of the correspondi	**Disabled** Tenable Identity Exposure does not check server certificates. This	Supply the CA that signed the provided server certificate on each machine where you intend to install the Relay. Tenable does not provide the specific path, as it is assumed that you have access to the CA.

		ng machine in the Subject Alternative Name (SAN) extension and a signature from the provided Certificate Authority (CA).	setup is not resistant to active MITM attacks.	
Custom TLS With Peer Verification	An organization with its own internal public key infrastructure (PKI) that requires protection against both passive eavesdropping and man-in-the-middle (MITM)	**Encrypted**, using certificates from your internal PKI. Certificates must contain the IP address of the corresponding machine in the Subject Alternative Name (SAN) extension and have a	**Enabled** Tenable Identity Exposure checks server certificates. This setup is resistant to active MITM attacks.	

	attacks.	signature from the provided Certificate Authority (CA).		

Update the TLS certificate

It is possible to update the TLS certificate either during an upgrade of Tenable Identity Exposure or if you need to renew an expired certificate, as follows:

1. Update the certificate (CRT) and KEY files in the default folder `Tenable\Tenable.ad\Certificates`.

   > **Note**: If your new certificate is in Personal Information Exchange (PFX) format, you can use the installed `openssl.exe` command line to extract the CRT and KEY.

2. Restart Services.

Split Security Engine Node (SEN) Services

The standard architecture for the Tenable Identity Exposure on-premises platform uses three virtual machines (VMs) by default for the Storage Manager, Security Engine Node, and Directory Listener.

However, if the environment that you monitor has **more than 150K users**, you can split the Security Engine Node (SEN) over five different machines to improve performance.

The installation process installs the following Tenable Identity Exposure components:

VM #	vCPU (per instance)	Memory (per instance)	Disk Space (per instance)	Recommended Service	Service Description
1	8 cores – at least 2.6 GHz	16 GB of RAM	1 TB	RabbitMQ	A message broker between services.

2	8 cores – at least 2.6 GHz	16 GB of RAM	100 GB	Attack Path	Computes attack path relations and maintaining them over time.
3	12 cores – at least 2.6 GHz	32 GB of RAM	300 GB	Cephei	Computes values for different analytics used for the Tenable Identity Exposure dashboards.
				CetiBridge	Communication plugins and service in charge of communicating with the Active Directory.
				Electra	Manages web sockets to update information without reloading the user interface.
				Enif	Authenticates web users.
				Eridanis	Connects to the SQL Server;

					ensures the exactness of Tenable Identity Exposure's information.
				Eltanin	Sends data to the Tenable Cloud, if enabled in Tenable Identity Exposure.
				Health Check	Alerts configuration anomalies leading to connectivity or other issues in the infrastructure.
				Kapteyn	Runs in the end user's browser to show the user interface.
4	16 cores – at least 2.6 GHz	16 GB of RAM	100 GB	Cancri	Decodes raw information; fetches delta between events; computes event type.
				EventLogsDecoder	Decodes information related to IOA

					events.
5	16 cores – at least 2.6 GHz	32 GB of RAM	100 GB	Cygni	Computes deviances and attacks.

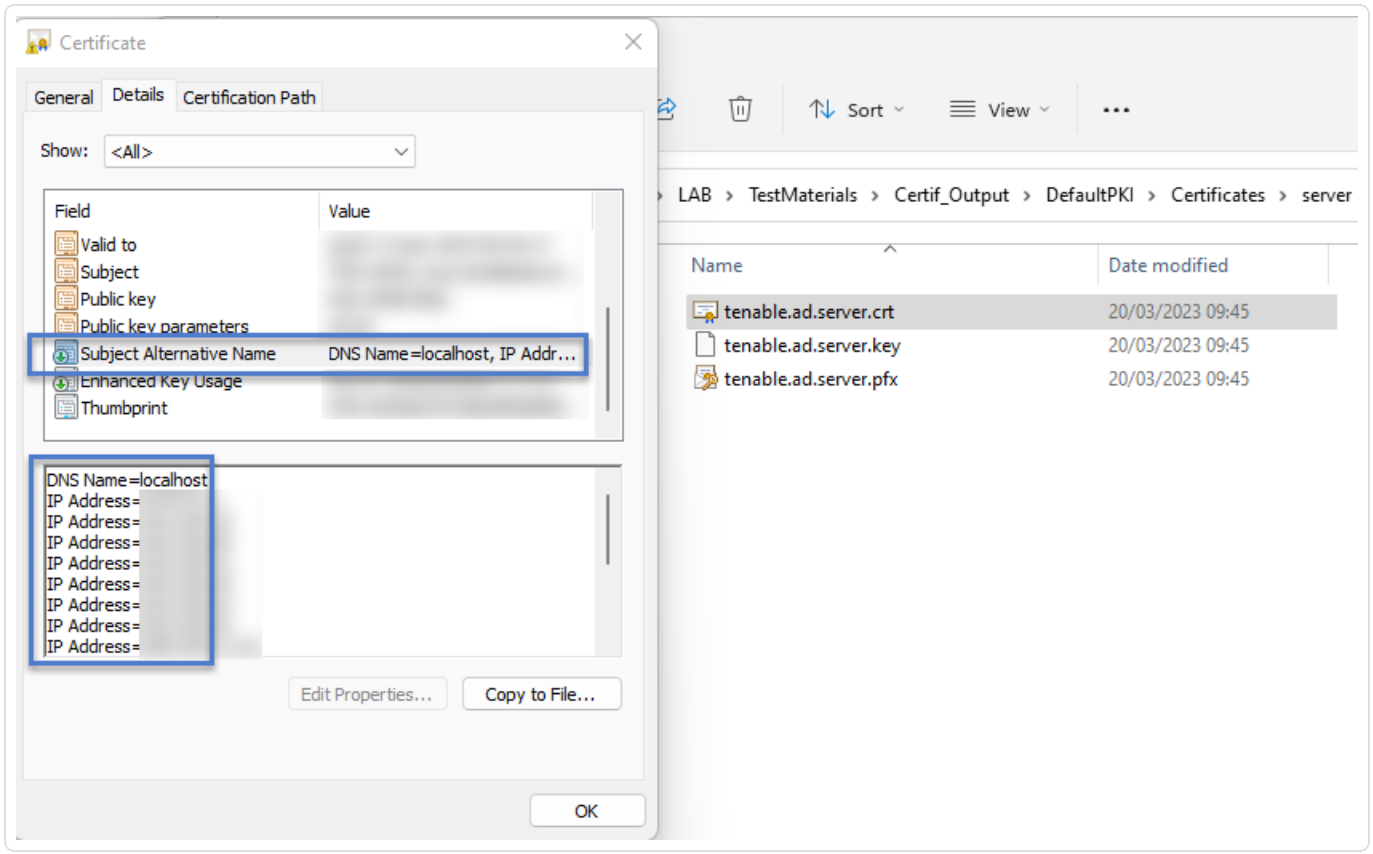
For more information, see Resource Sizing for requirements.

SEN Installation on Several Machines

To install the Security Engine Node on several machines, you select the services to install on each specific virtual machine.

Public Key Infrastructure (PKI) Certificate

To use peer verification, your PKI certificate must include the IP addresses or DNS of all the machines used to install Tenable Identity Exposure.



Example

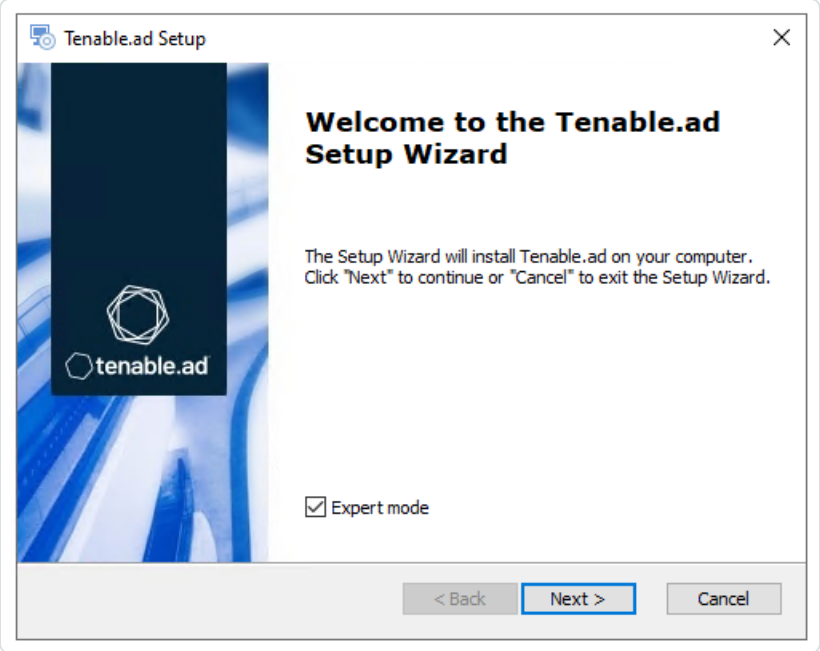
The following example shows an installation of RabbitMQ and Attack Path on one virtual machine.

To install the RabbitMQ and Attack Path services on a VM:

Note: This procedure installs Tenable Identity Exposure with TLS using the "Expert mode."

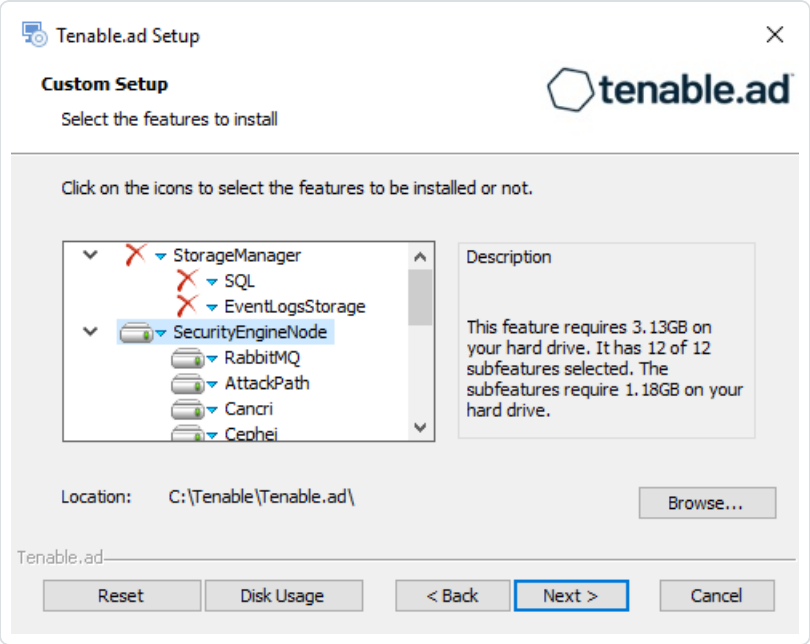
1. On the local machine, run the installation file `Tenable.ad_v3.19.x.exe`.

   The **Setup Wizard** appears.



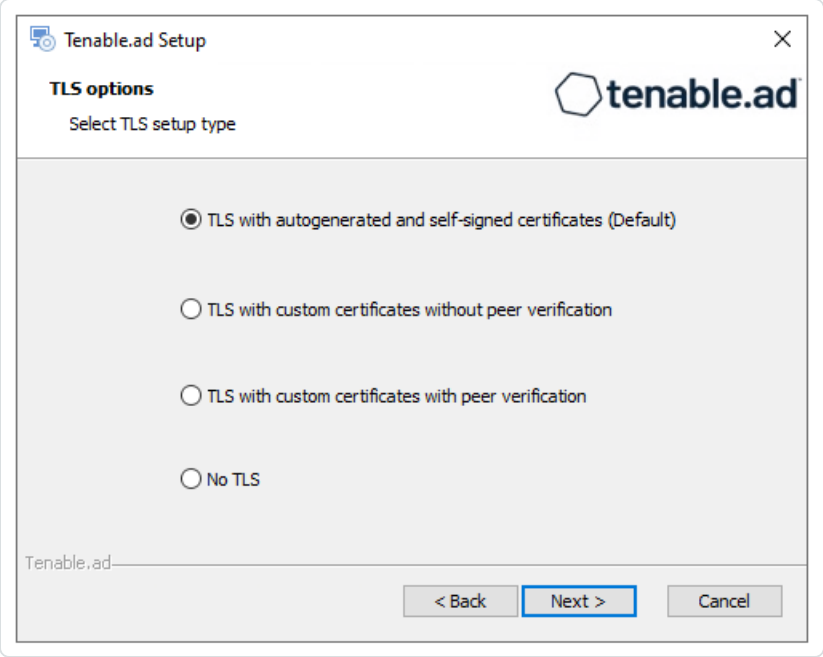
2. Select the **Expert Mode** check box.
3. Click **Next**.

   The **Custom Setup** window appears.
4. Deselect the *Storage Manager* and *Directory Listener* components.
5. Deselect all SEN services except for *RabbitMQ* and *AttackPath*.



6. (Optional) Click **Browse** to change the installation folder location. Change only the drive letter.
7. Click **Next**.

   The **TLS Options** window appears.
8. Select the **TLS with autogenerated and self-signed certificates (Default)** option.

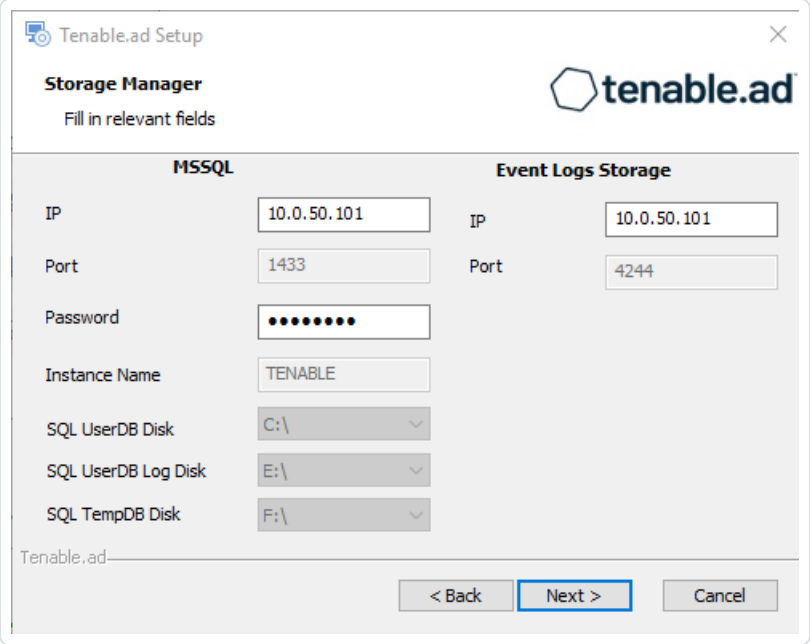


9. Click **Next**.

   The **Storage Manager** window appears.

10. Provide the following information:

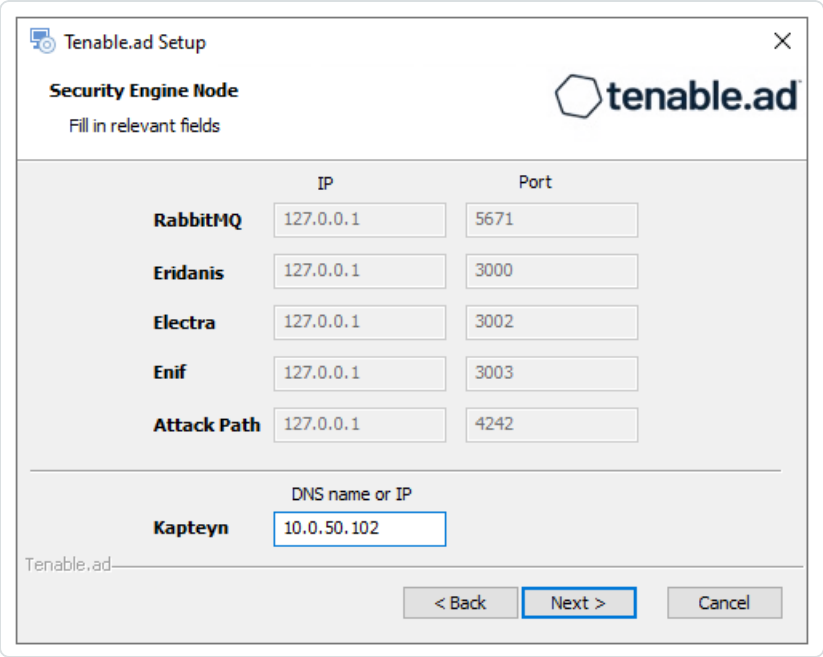
    - In the **MSSQL** box, type the IP address of the Storage Manager.
    - In the **Password** box, type the service account password for the MSSQL database defined in the Storage Manager installation.



11. Click **Next**.

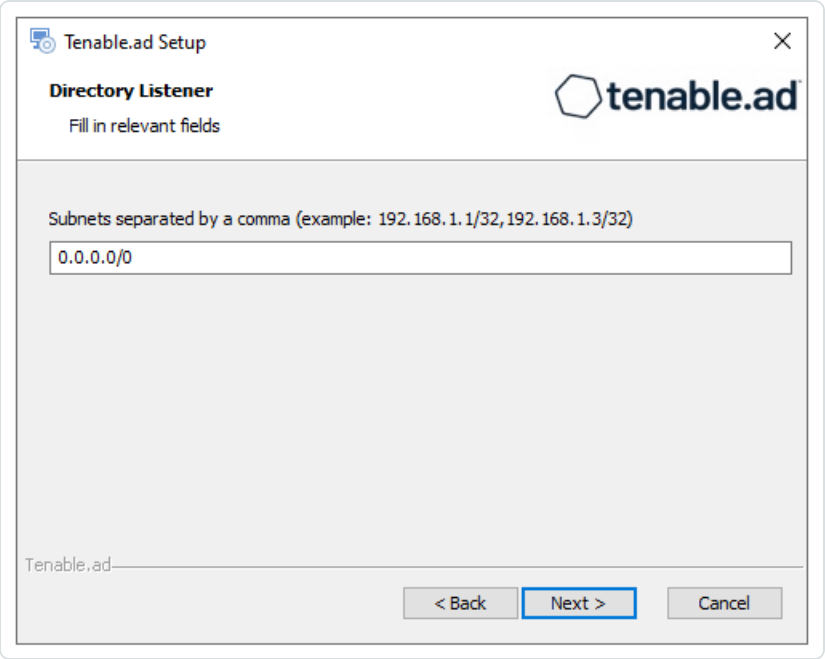
    The **Security Engine Node** window appears.

12. In the **DNS name or IP** box, type the DNS name (preferred) or IP address of the web server that end users enter to access Tenable Identity Exposure.



Note: By default, the installation process creates a self-signed certificate with the DNS name or the IP address that you entered. For more information, see Change the IIS Certificate.

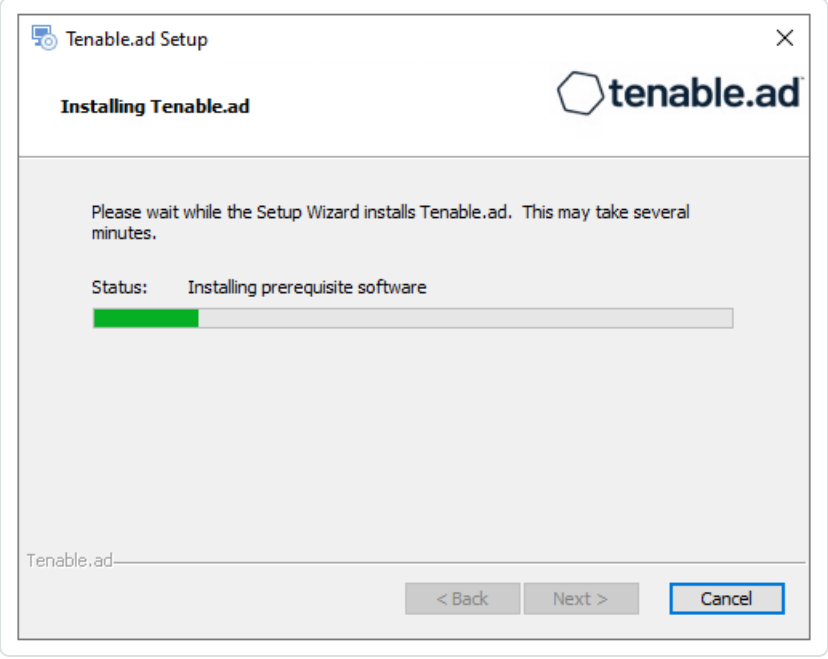
13. Click **Next**.
14. The **Directory Listener** window appears.
15. In the **Subnets** box, type the subnet address for the Directory Listener. For multiple subnets, use a comma to separate the addresses.



16. Click **Next**.

    The **Ready to Install** window appears.

17. Click **Install** to begin the installation.



After the installation completes, the **Completing the Tenable.ad Setup Wizard** window appears.

18. Click **Finish**.

    A dialog box asks you to restart your machine.

19. Click **No**.

    Caution: Do not restart the machine until **after** you install the Directory Listener.

20. Repeat this procedure to install the remaining SEN services.

See also

- Resource Sizing for Security Engine Node
- TLS Installation Types
- Install Tenable.ad
- Upgrade Tenable Identity Exposure

Upgrade Tenable Identity Exposure

Required User Role: Administrator on the local machine

Before you start

- **Download the executable programs** for Tenable Identity Exposure and Secure Relay from Tenable's Downloads site.
- **Review** Pre-deployment Requirements for TLS Certificates, Account Privileges, Antivirus (AV) and Endpoint Detection and Response (EDR), among other upgrade requirements.

The upgrade to Tenable Identity Exposure version **3.59** from previous versions requires adapting your previous architecture to include the Secure Relay component. **Before you upgrade, review carefully and understand the changes** explained in the following sections:

- Differences between Secure Relay Architectures for On-Premises Platforms pre-upgrade (3.42) and post-upgrade 3.59
- Manual installation of Secure Relay for Tenable Identity Exposure 3.59 using a separate

installer **after you upgrade the Storage Manager, Security Engine Node, and Directory Listener**.

Caution: From Tenable Identity Exposure version **3.59.5** onwards, ensure that your **TLS certificates use OpenSSL 3.0.x**. See Pre-deployment Requirements for more information.

Upgrade Path

To upgrade to the latest version of Tenable Identity Exposure, you must follow one of these installation paths:

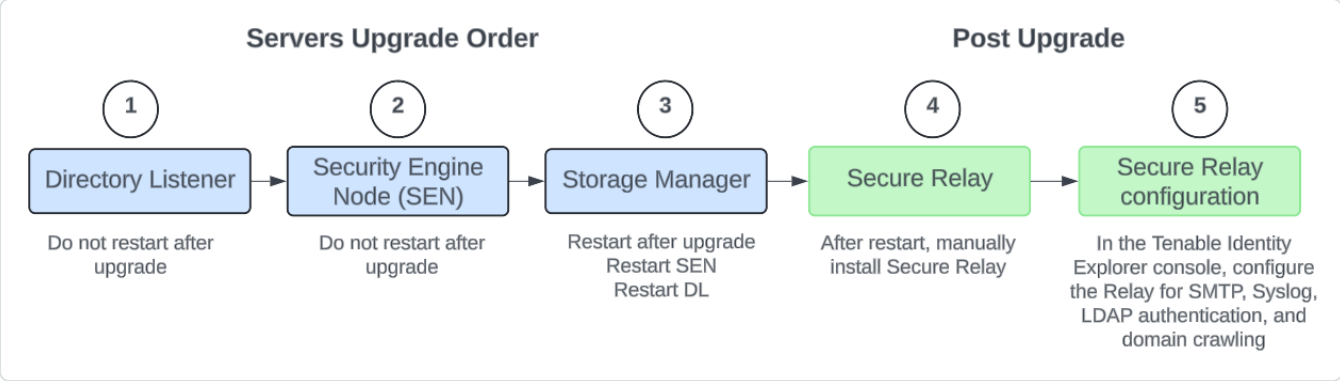
- 2.7 -> 3.1 -> 3.11 -> 3.19 -> 3.29 -> 3.42 -> 3.59.
- 3.x -> 3.59 -> 3.59.

Tip: If you are upgrading from **v. 3.59**, the Secure Relay installation and configuration are automatic.

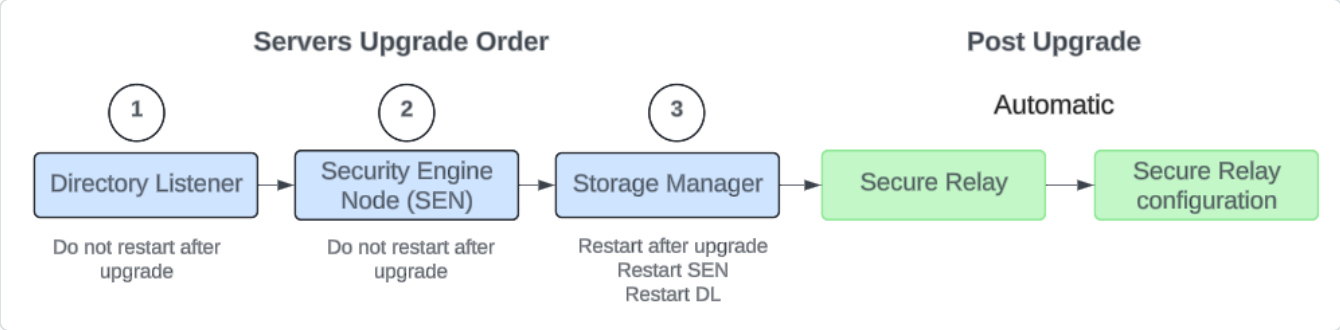
Note: You can upgrade to the next major release from any minor release.

Upgrade Order

- From **Tenable Identity Exposure 3.42** to **3.59**, proceed in the following order:



- From **Tenable Identity Exposure 3.59** to **3.59**, proceed in the following order:



Before you start

- **Ensure that your TLS certificates use OpenSSL 3.0.x**. See Pre-deployment Requirements for more information.
- **Take a snapshot of your environment before you upgrade**. If the upgrade fails, Tenable Identity Exposure support cannot perform a rollback, and this results in a fresh installation and causes you to lose your previous data. See Backups for complete information.
- **Back up and restore the Storage Manager**. Tenable strongly recommends that you back up the Storage Manager before you upgrade. For instructions on how to back up or restore MSSQL, see the official Microsoft documentation.
- **Consider the downtime**: Depending on your environment and the magnitude of the upgrade, downtime can range from minutes to several hours. Factor this into your scheduling and communication plan. Inform impacted users of the scheduled downtime and potential service disruption.
- **Download the executable programs** for Tenable Identity Exposure and Secure Relay from Tenable's Downloads site.
- **Run the installer as a local user or a domain user** who is a member of the **Local Administrators** group.
- **Restart your server** before launching the Tenable Identity Exposure installer for each component.

Upgrade Procedures

The following procedures upgrade the Tenable Identity Exposure components in **TLS with autogenerated and self-signed certificates (Default)**. For more information, see TLS Installation Types.

Note: The "No TLS" installation defaults to this mode.

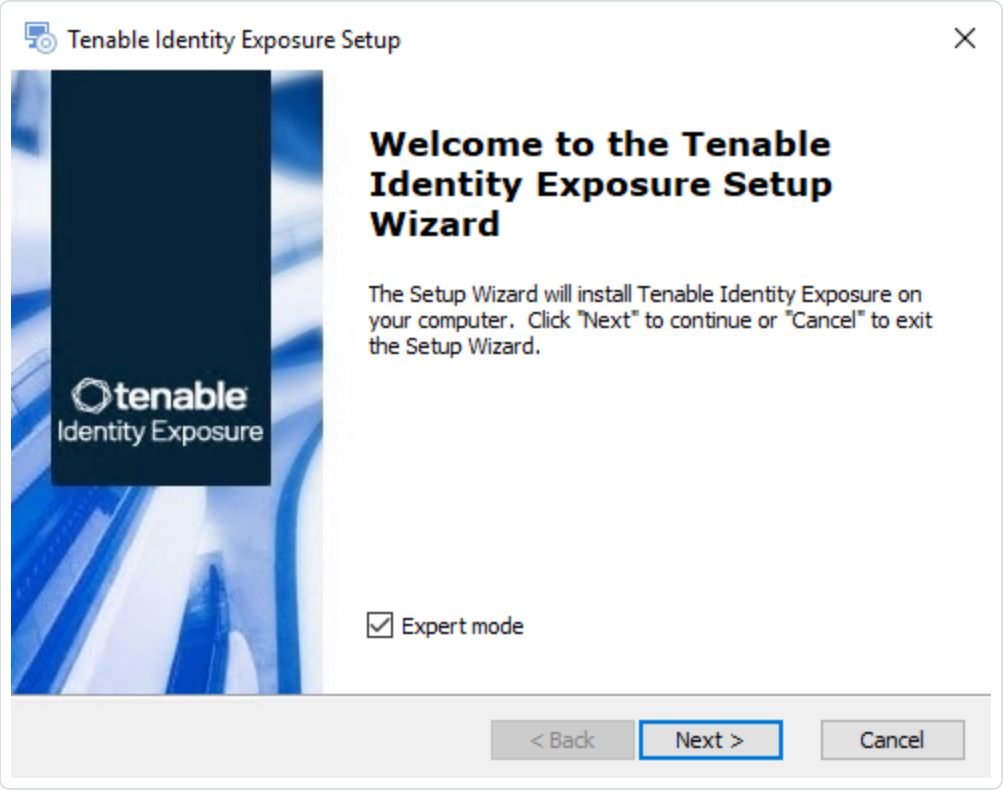
To upgrade the Directory Listener:

1. On the local machine, restart the server and run the **Tenable Identity Exposure 3.59** On-Premises installer.

   A welcome screen appears.

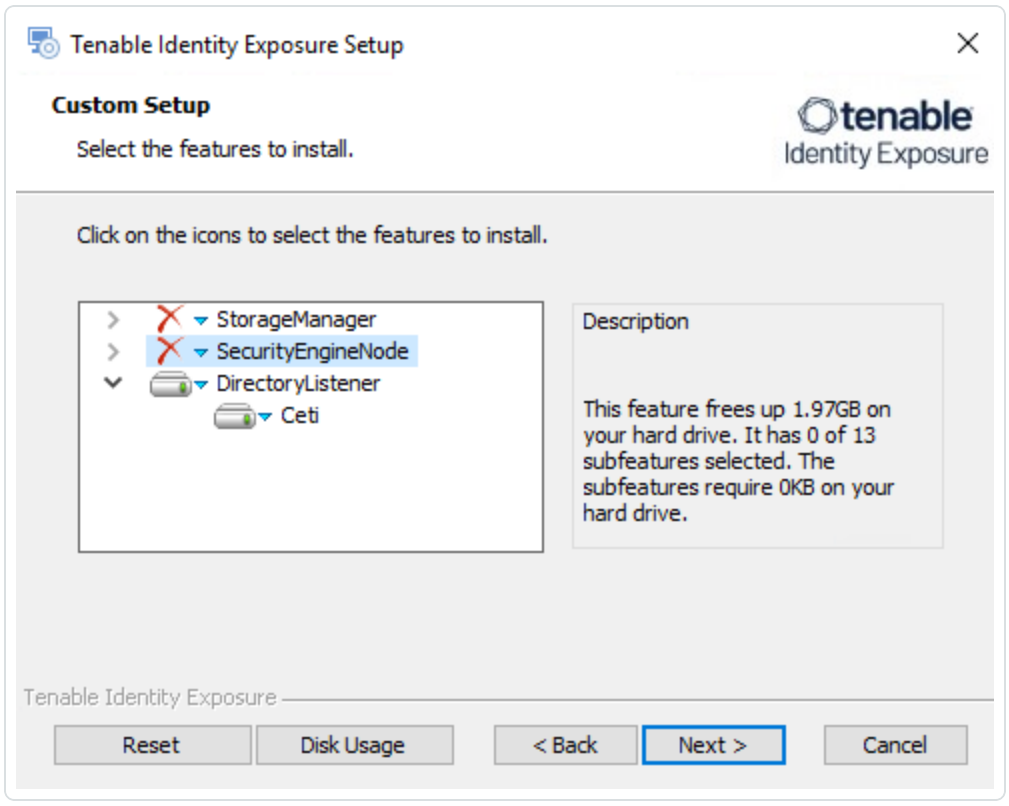
2. In the setup language box, select the language for the installation from the drop-down list and click **Next**.

   The **Setup Wizard** appears. The **Expert mode** checkbox is selected by default.



3. Click **Next**.

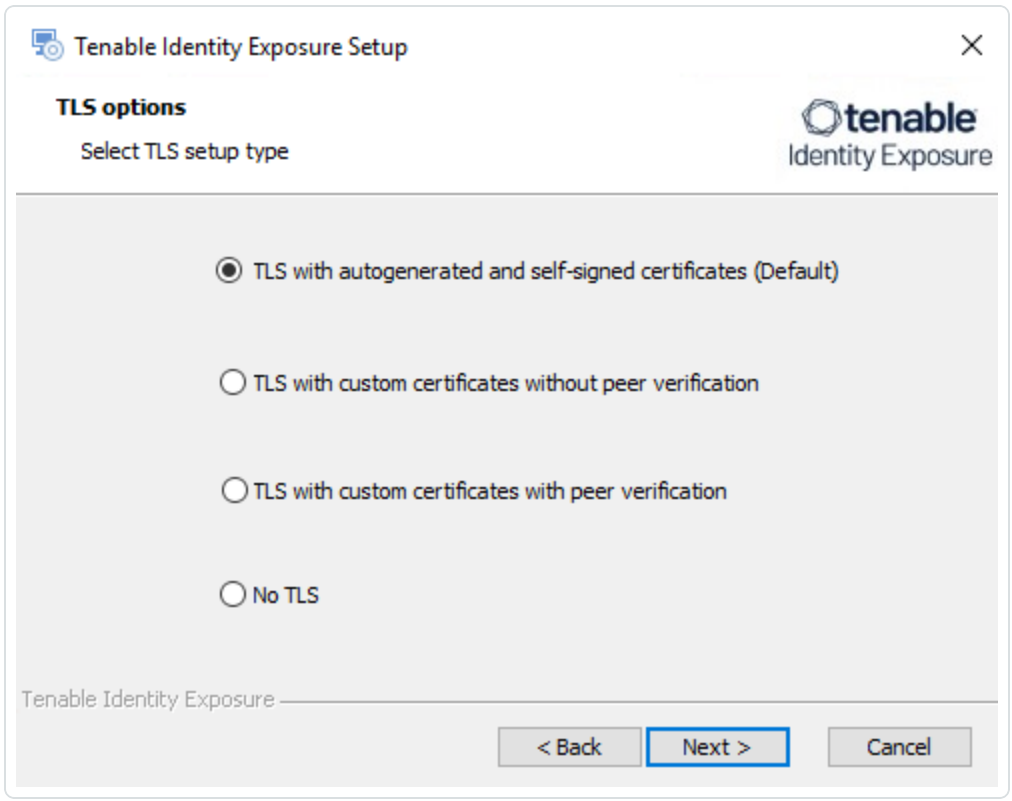
   The **Custom Setup** window appears.



4. The installation program automatically preselects the Directory Listener component based on your previous installation. Click **Next**.

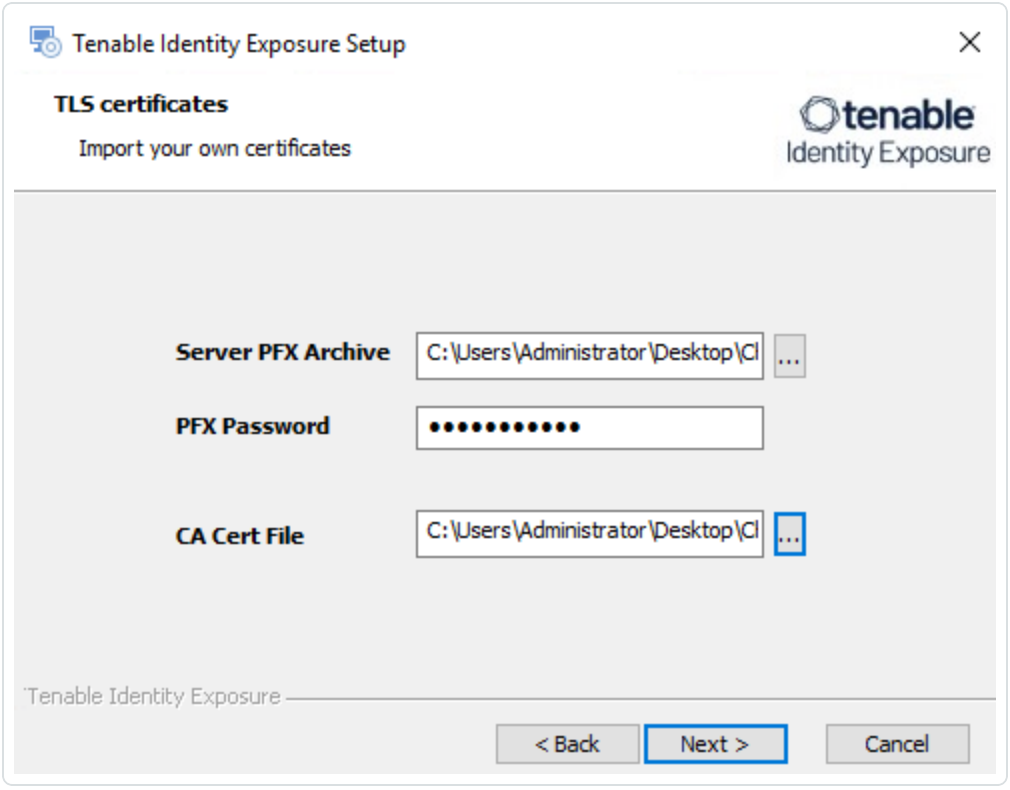
   The **TLS Options** window appears.

5. Select the **TLS with autogenerated and self-signed certificates (Default)** option.



Optional: If you select **TLS with custom certificates without peer verification** or **TLS with custom certificates with peer verification**, the next **TLS certificates** screen asks you to provide the following information:

- In the **Server PFX Archive** box, click **...** to browse to your PFX archive.
- In the **PFX Password** box, type the password for the PFX file.
- In the **CA Cert File** box, click **...** to browse to your CA certificate file.

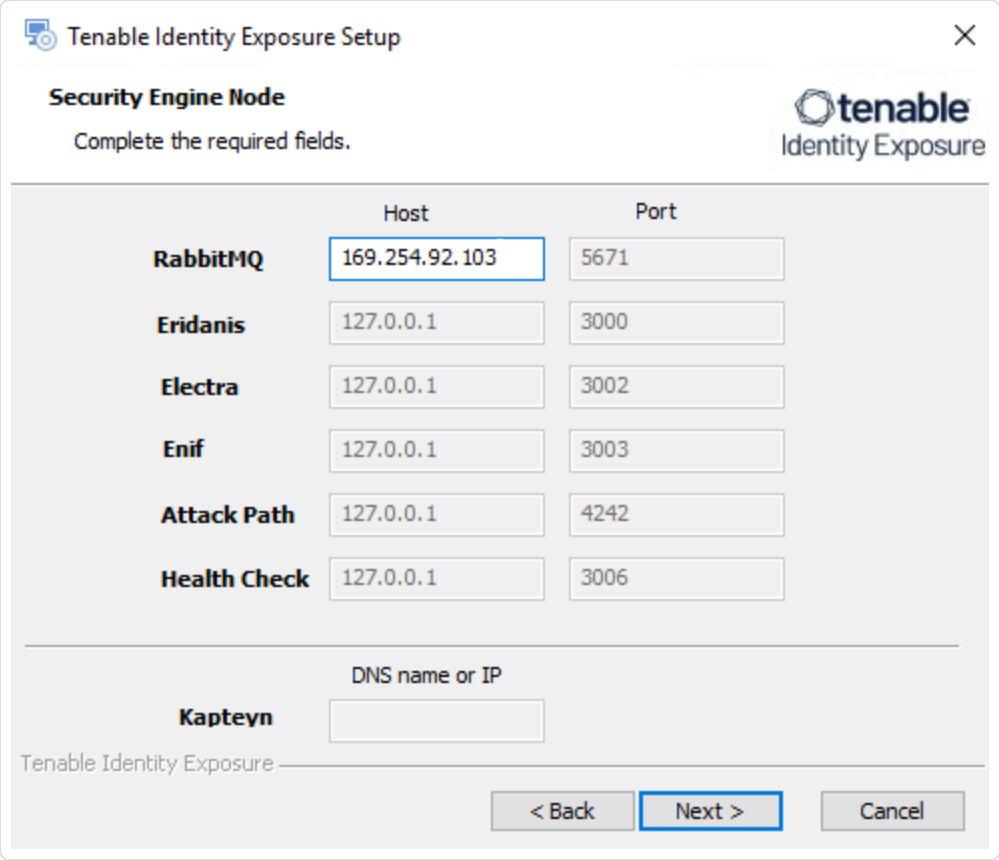


6. Click **Next**.

   The **Security Engine Node** window appears.

7. In the **Host** box for RabbitMQ, type the **IP address for the Security Engine Node** (**or the IP address for the Security Engine Node hosting RabbitMQ** if you use a split architecture.)

Caution: If you leave the default value "127.0.0.1" and click "Next", the installer fails and rolls back.

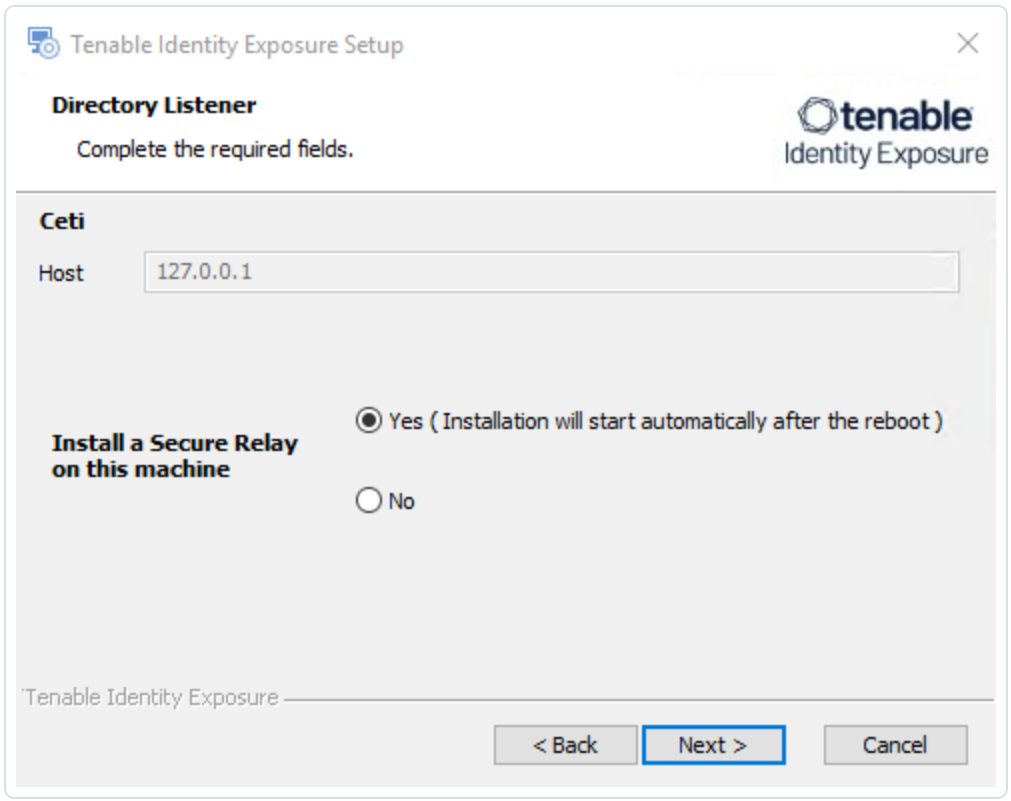


8. Click **Next**.

   The **Directory Listener** window appears.

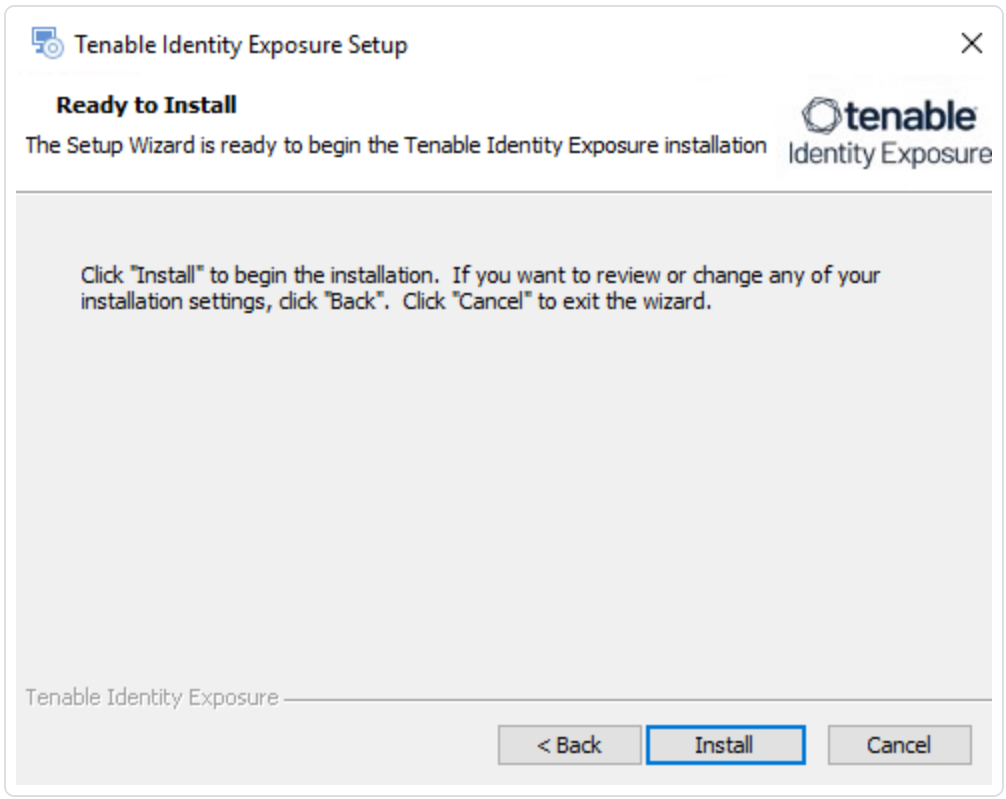
9. You have two options whether to install the Secure Relay on this Directory Listener:

   - **Yes** – After this installation completes and the Directory Listener reboots, the Secure Relay installer launches.
   - **No** – You select to install the Secure Relay at a later time **or on a separate server** (see Secure Relay Architectures for On-Premises Platforms.) A message shows you the location of the Secure Relay installer. **A Secure Relay is mandatory** whether you install it on the Directory Listener machine or on a separate machine.

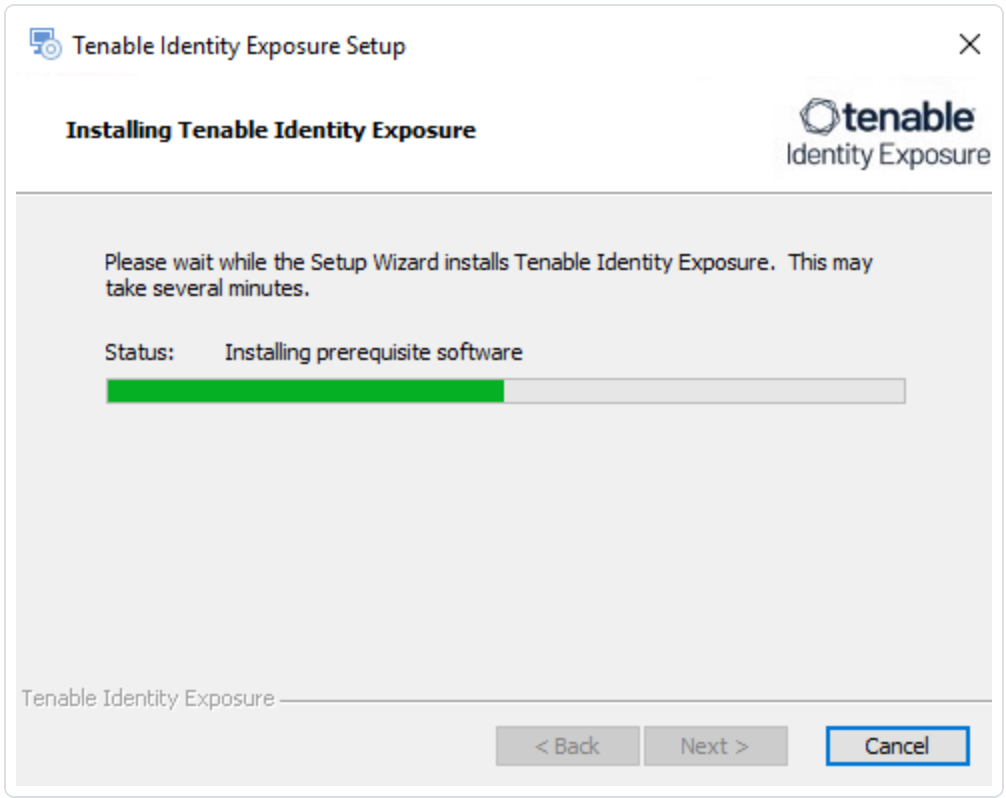


10. Click **Next**.

    The **Ready to Install** window appears.



11. Click **Install** to begin the upgrade.



After the upgrade completes, the **Completing the Tenable Identity Exposure Setup Wizard** window appears.

12. Click **Finish**.

    A dialog box asks you to restart your machine.

13. Click **No**.

    Caution: **Do NOT** reboot the machine now. Follow the restart order after the upgrade of all servers.

14. Upgrade the Security Engine Node (SEN).

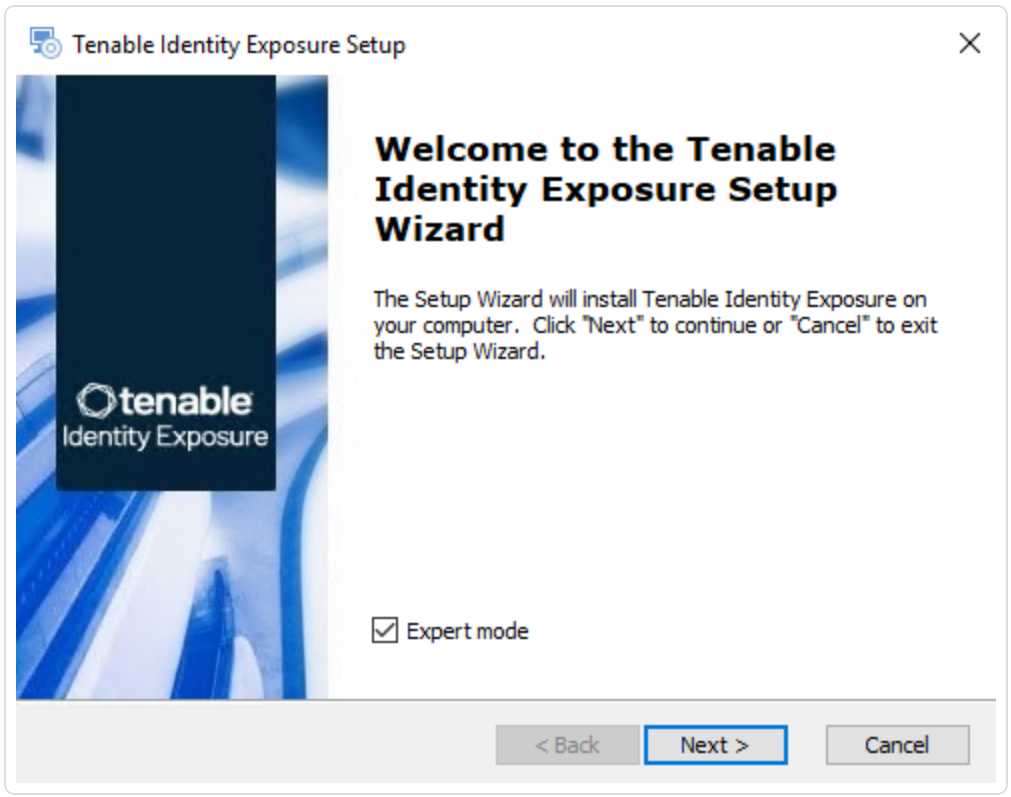
To upgrade the SEN:

1. On the local machine, restart the server and run the **Tenable Identity Exposure 3.59** On-Premises installer.

   A welcome screen appears.

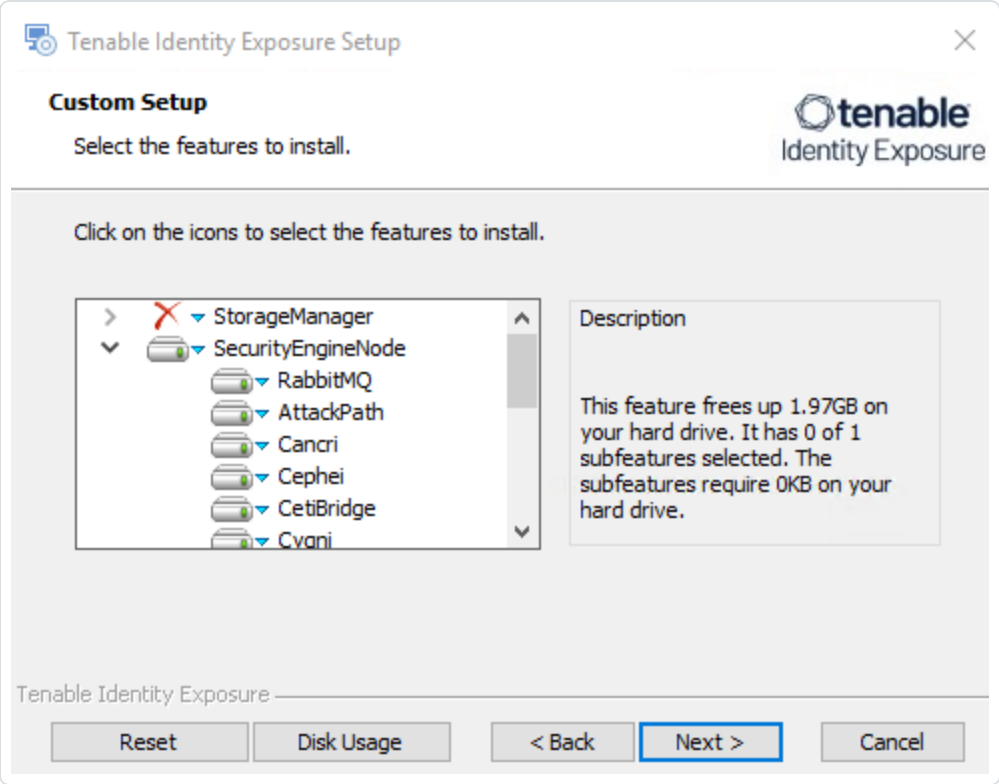
2. In the setup language box, click the arrow to select the language for the installation, and click **Next**.

   The **Setup Wizard** appears. The **Expert mode** checkbox is selected by default.



3. Click **Next**.

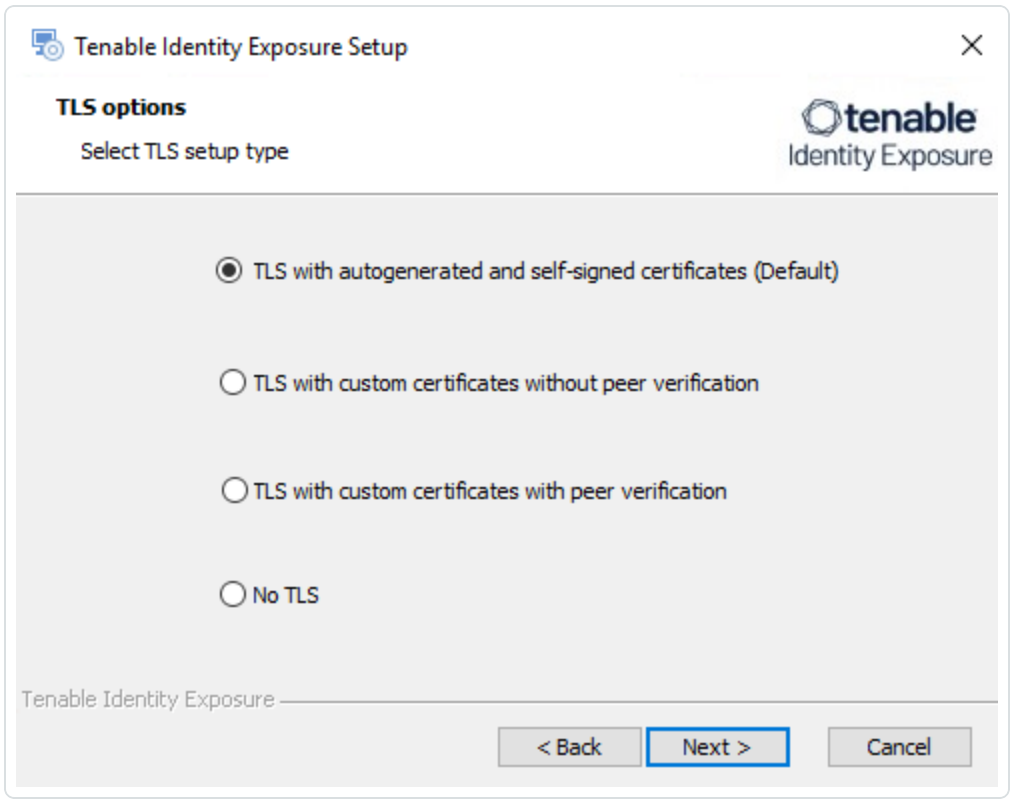
   The **Custom Setup** window appears.



4. The installation program automatically preselects the SEN component based on your previous installation. Click **Next**.

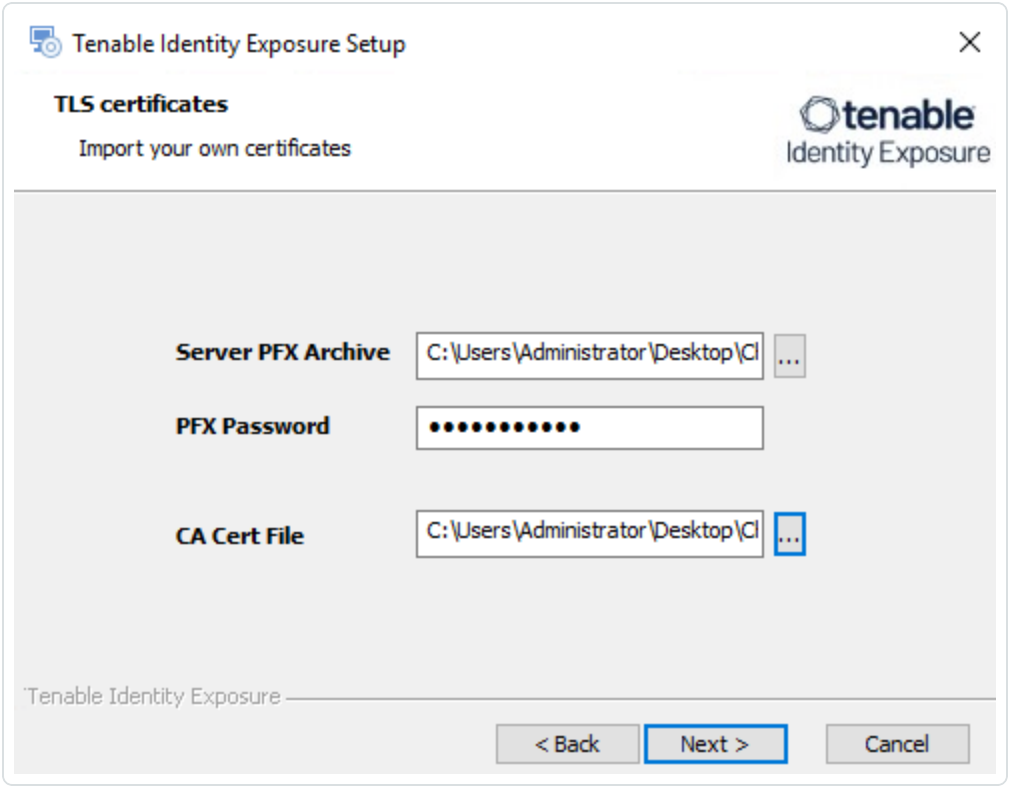
   The **TLS Options** window appears.

5. Select the **TLS with autogenerated and self-signed certificates (Default)** option.



Optional: If you select **TLS with custom certificates without peer verification** or **TLS with custom certificates with peer verification**, the next **TLS certificates** screen asks you to provide the following information:

- In the **Server PFX Archive** box, click **...** to browse to your PFX archive.
- In the **PFX Password** box, type the password for the PFX file.
- In the **CA Cert File** box, click **...** to browse to your CA certificate file.



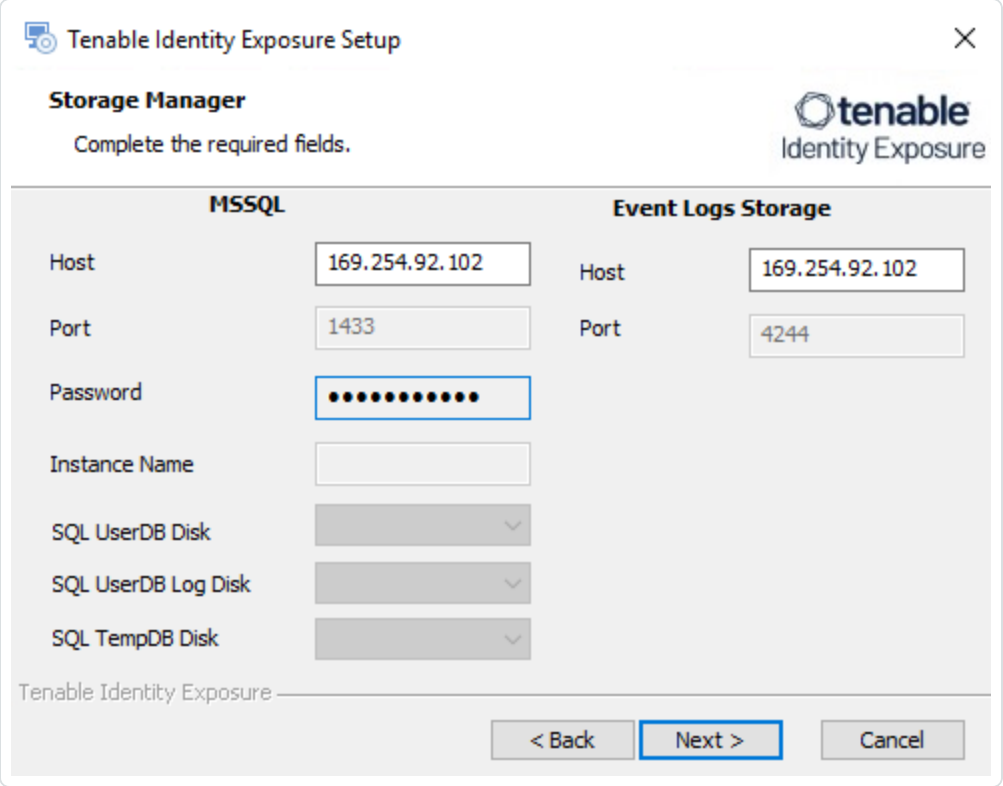
6. Click **Next**.

   The **Storage Manager** window appears.

7. Verify or enter the following information:

   - In the **Host** box, check that your MSSQL database's FQDN or IP address from your previous installation remains valid and correct it if necessary.
   - In the **Event Logs Storage** box, type the IP address of the machine storing your event logs, which is typically the same as the MSSQL database IP address.

> **Note**: If you changed the SA password since the previous installation, the installer requires that it follows the syntax described in Strong Passwords for the SQL Server.

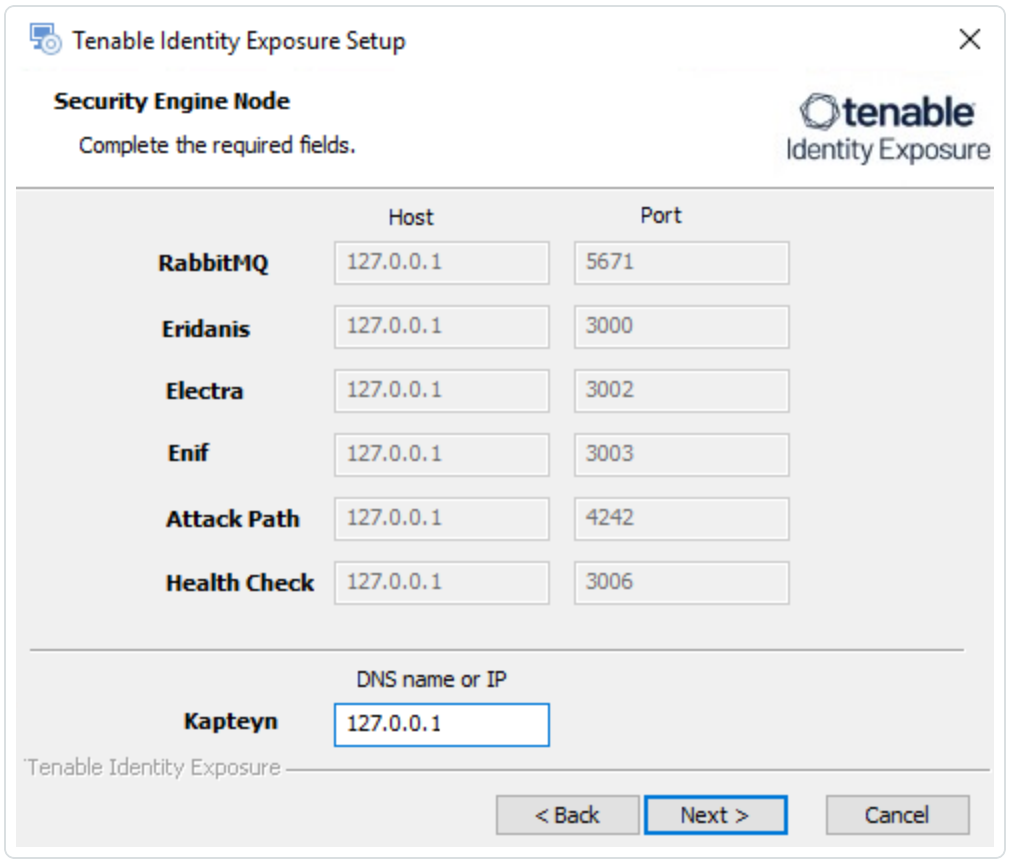


Caution: Remember to update the Event Logs Storage IP or hostname address during this step. Failing to do so leads to attack detection issues. If you have successfully completed this screen and upgraded the SEN, you must update the environment variables for `TENABLE_CASSIOPEIA_CYGNI_Service__EventLogsStorage__Host` and `TENABLE_CASSIOPEIA_EVENT_LOGS_DECODER_Service__EventLogsStorage__Host` from the **current value** to the accurate value for <**Storage Manager hostname or IP address**>. For more information, see the Troubleshooting knowledge base article.

8. Click **Next**.

   The **Security Engine Node** window appears.

9. In the **DNS name or IP** box, the installer shows the DNS name (preferred) or IP address of the web server that end users type to access Tenable Identity Exposure from your previous installation. Check that this remains valid and correct if necessary.



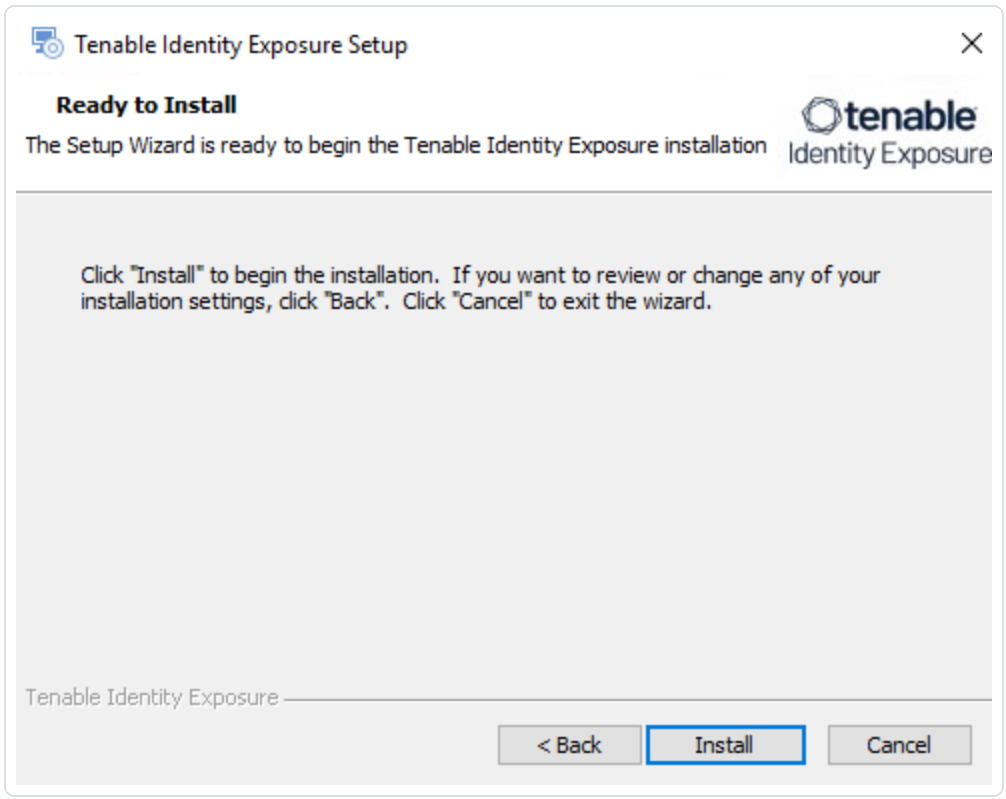
10. Click **Next**.

    The **Directory Listener** window appears.

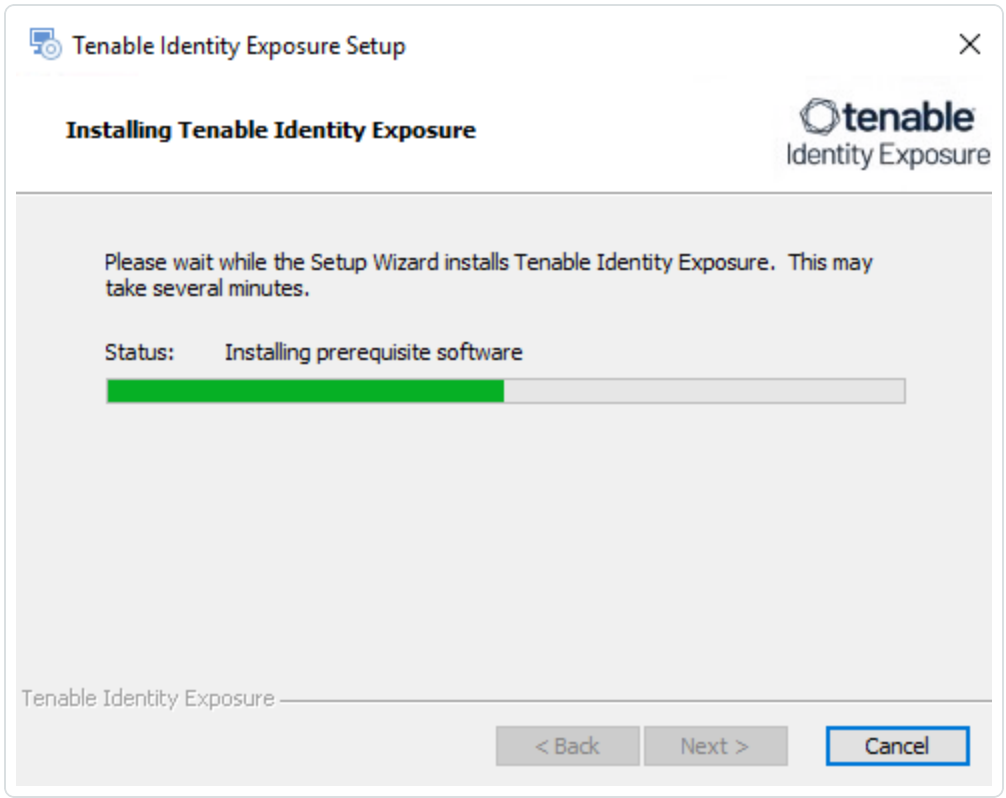
11. In the **Ceti** box, type the **IP address for the Directory Listener**.

12. Click **Next**.

    The **Ready to Install** window appears.



13. Click **Install** to begin the upgrade.



After the upgrade completes, the **Completing the Tenable Identity Exposure Setup Wizard** window appears.

14. Click **Finish**.

    A dialog box asks you to restart your machine.

15. Click **No**.

    > **Caution**: **Do NOT** reboot the server now. Follow the restart order after the upgrade of all servers.

16. Upgrade the Storage Manager.

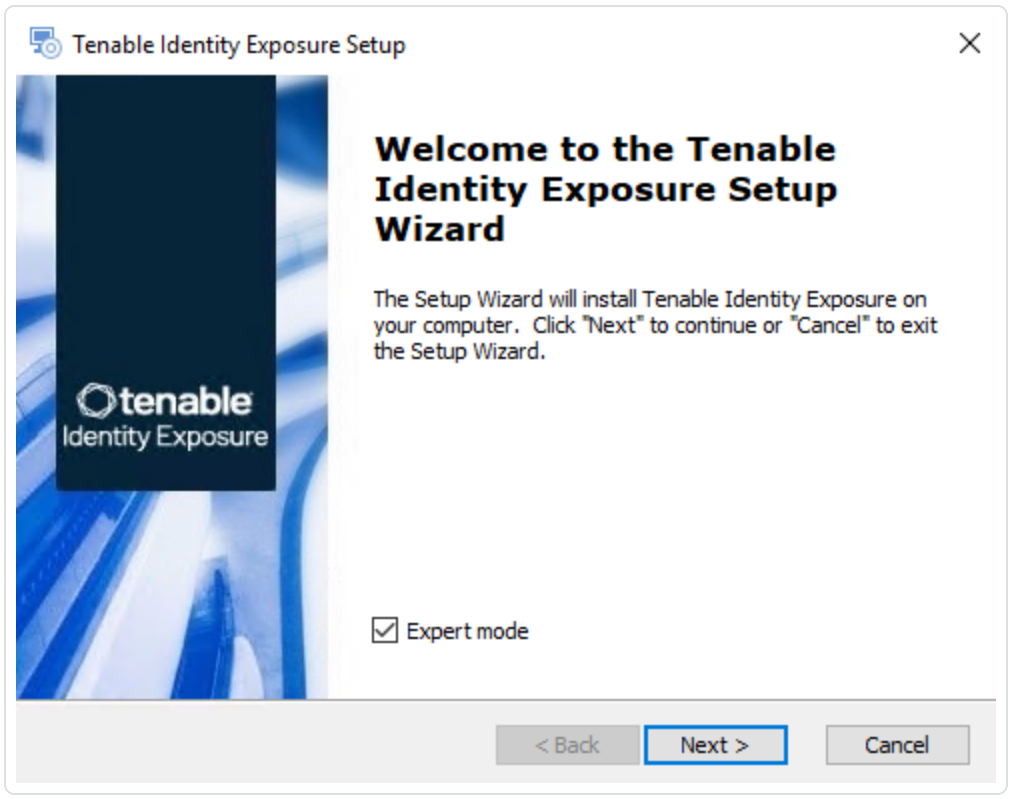
To upgrade the Storage Manager:

1. On the local machine, restart the server and run the **Tenable Identity Exposure 3.59** On-Premises installer.

   A welcome screen appears.

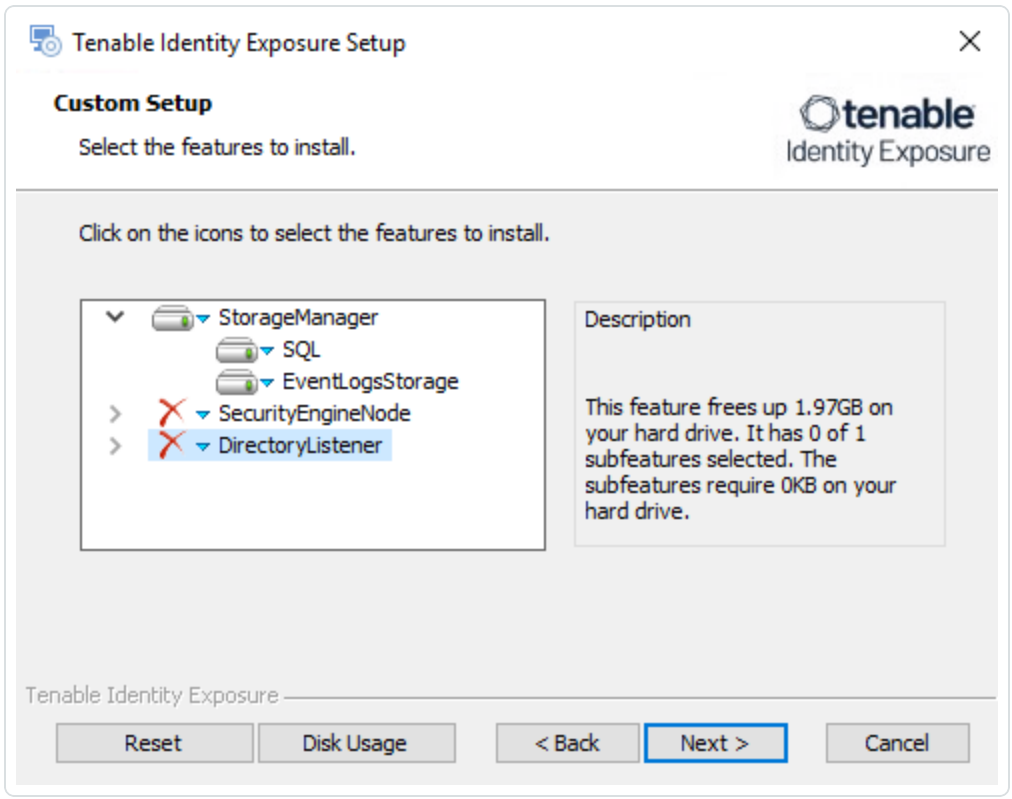
2. In the setup language box, click the arrow to select the language for the installation, and click **Next**.

   The **Setup Wizard** appears. The **Expert Mode** checkbox is selected by default.



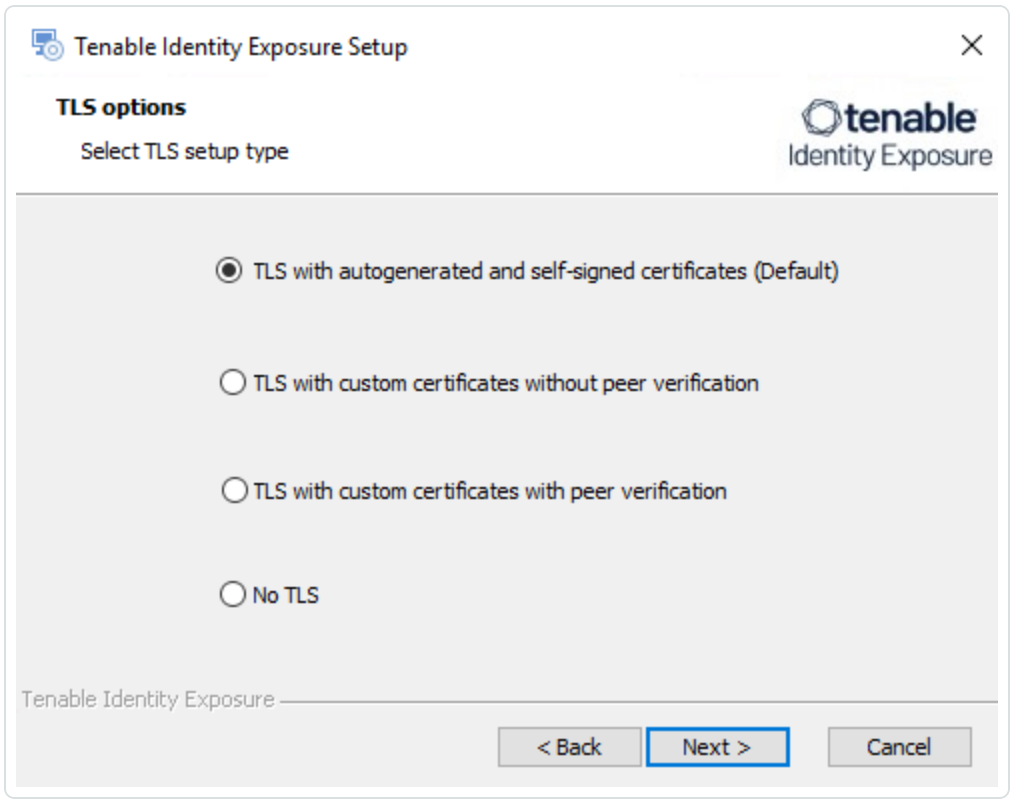
3. Click **Next**.

   The **Custom Setup** window appears. The installation program automatically preselects the Storage Manager component based on the previous installation.



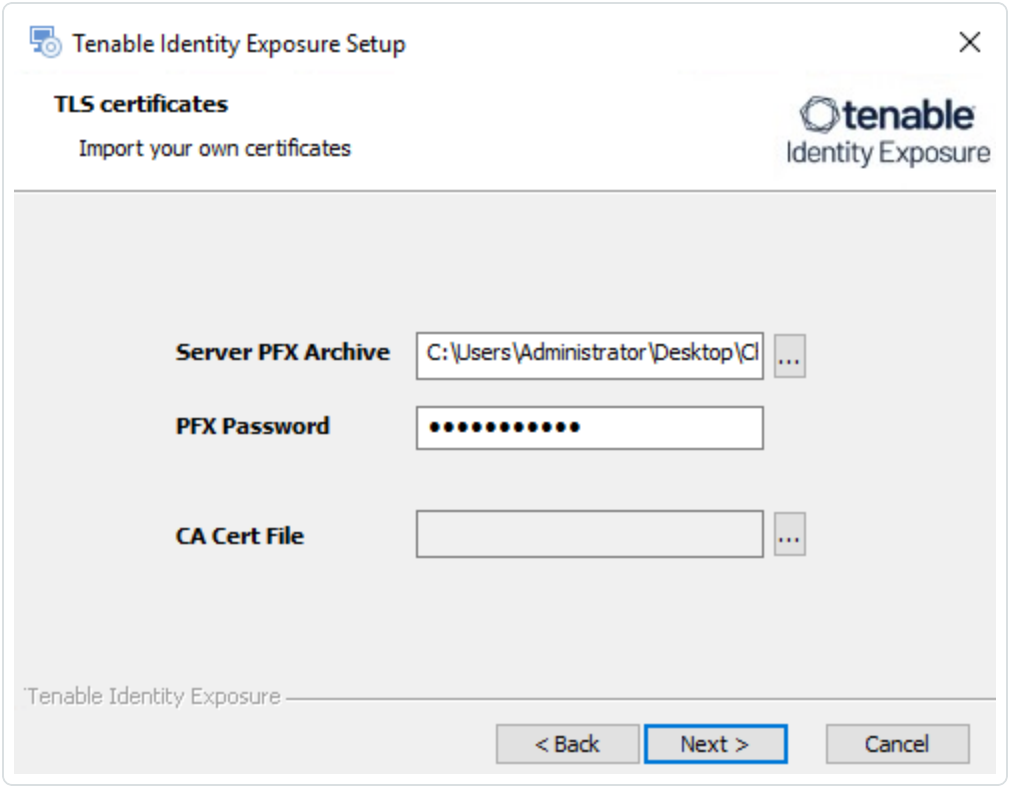
4. Click **Next**.
5. (Optional) Click **Browse** to change the installation folder location. Change only the drive letter.

   The **TLS Options** window appears.
6. Select the **TLS with autogenerated and self-signed certificates (Default)** option.



Optional: If you select **TLS with custom certificates without peer verification** or **TLS with custom certificates with peer verification**, the **TLS certificates** screen asks you to provide the following information:

- In the **Server PFX Archive** box, click **...** to browse to your PFX archive.
- In the **PFX Password** box, type the password for the PFX file.

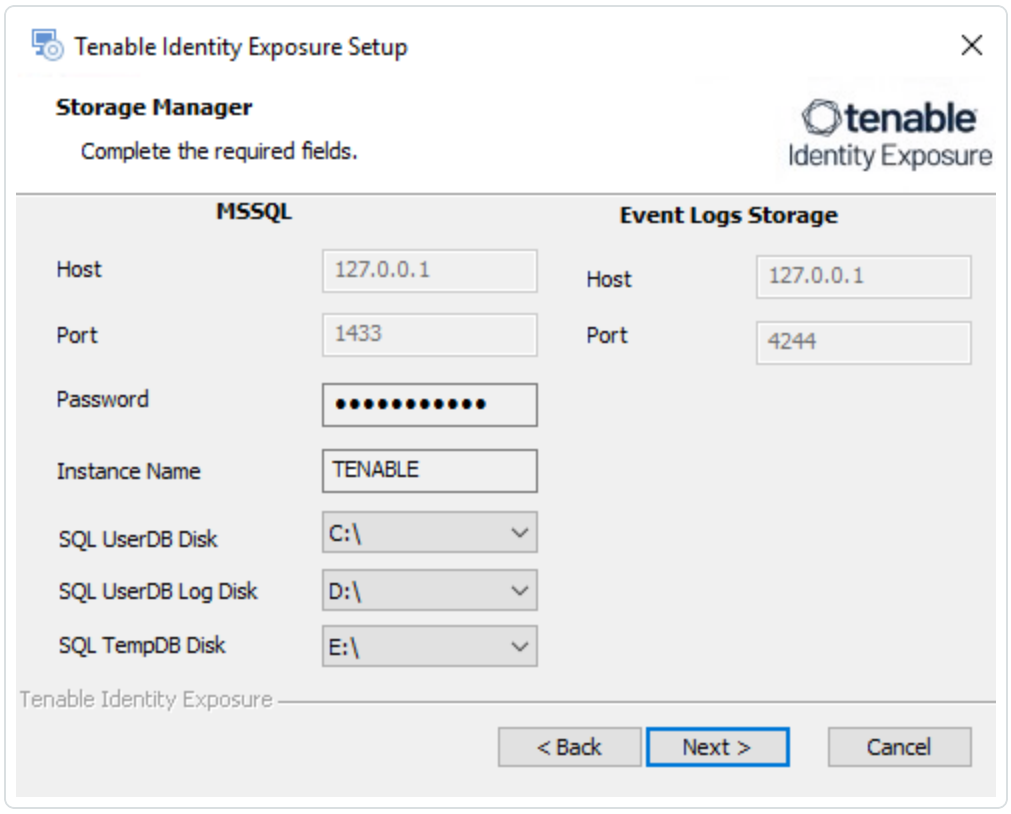


7. Click **Next**.

   The **Storage Manager** window appears.

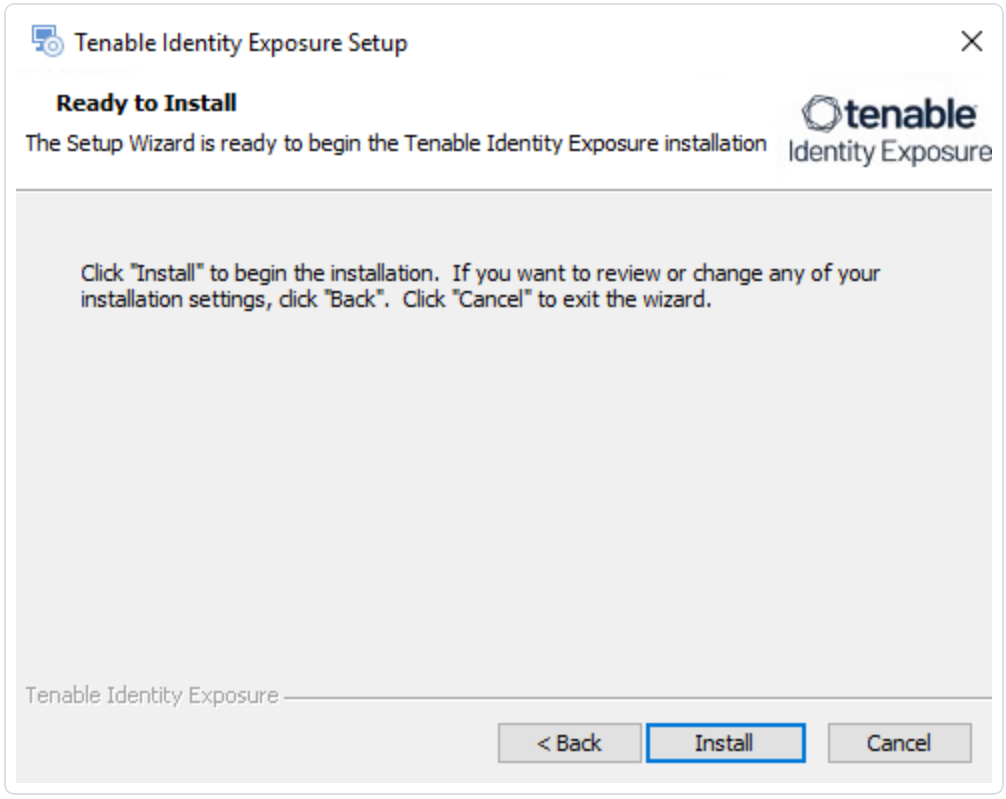
8. The installer reuses the information from your previous installation. Click **Next**.

   Note: If you changed the SA password since the previous installation, the installer requires that it follows the syntax described in Strong Passwords for the SQL Server.

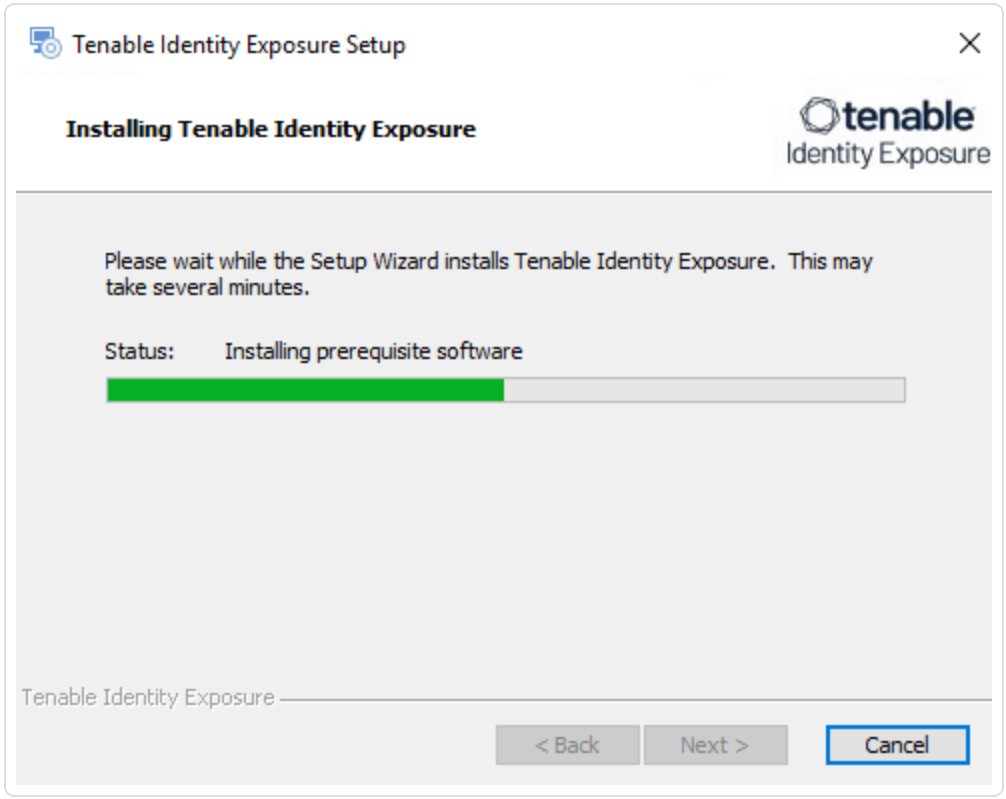

Tenable Identity Exposure Setup
Storage Manager
Complete the required fields.
tenable
Identity Exposure
MSSQL
Event Logs Storage
Host
127.0.0.1
Port
1433
Password
Instance Name
TENABLE
SQL UserDB Disk
C:\
SQL UserDB Log Disk
D:\
SQL TempDB Disk
E:\
Host
127.0.0.1
Port
4244
Tenable Identity Exposure
< Back
Next >
Cancel

9. Click **Next**.

   The **Ready to Install** window appears.



10. Click **Install** to begin the upgrade.



After the upgrade completes, the **Completing the Tenable Identity Exposure Setup Wizard** window appears.

11. Click **Finish**.

    A dialog box asks you to restart your machine.

12. Click **Yes**.

    The machine restarts.

13. Restart the SEN.
14. Restart the DL.
15. Install the Secure Relay for Tenable Identity Exposure 3.59 using a separate installer.

To install the Secure Relay:

1. Review Secure Relay Requirements.
2. Select Secure Relay Architectures for On-Premises Platforms.

3. Install the Secure Relay for Tenable Identity Exposure 3.59.

Restart Services

You restart services **after you finish installing or upgrading** the Storage Manager, Security Engine Node, and Directory Listener.

Restart Sequence

The restart sequence for services differs depending on whether it's an installation or upgrade:

- **New installation**: Directory Listener – Security Engine Node – Storage Manager
- **Upgrade**: Storage Manager – Security Engine Node – Directory Listener

Storage Manager

To restart the Storage Manager machine:

1. At the prompt from the installation program, click **Yes**.
2. Check that these Storage Manager services are running:
    - SQL Server (Tenable)
    - SQL Server Agent (Tenable)
    - `tenable_EventlogStorage1`

Security Engine Node

The databases must be running before you restart Security Engine Nodes (SEN) services.

To restart the SEN machine:

1. At the prompt from the installation program, click **Yes**.
2. If you have more than one SEN machine, restart the machines in this order:
    1. RabbitMQ
    2. Others (Eridanis, Kapteyn, etc.)

3. Cancri, EventLogsDecoder
4. Cygni

3. Check that the following SEN services are running:
   - `tenable_AttackPath1`
   - `tenable_Cancri`
   - `tenable_Cephei`
   - `tenable_CetiBridge`
   - `tenable_Cygni`
   - `tenable_Electra`
   - `tenable_Eltanin`
   - `tenable_Enif`
   - `tenable_Eridanis`
   - `tenable_EventLogsDecoder1`
   - `tenable_HealthCheck`
   - `tenable_Kapteyn`
   - `Rabbitmq`
   - `World Wide Web Publishing Services`

Directory Listener

Databases and Security Engine Nodes must be running before you restart Directory Listener services.

To restart Directory Listener services:

1. At the prompt from the installation program, click **Yes**.
2. Check that the following Directory Listener service is running:

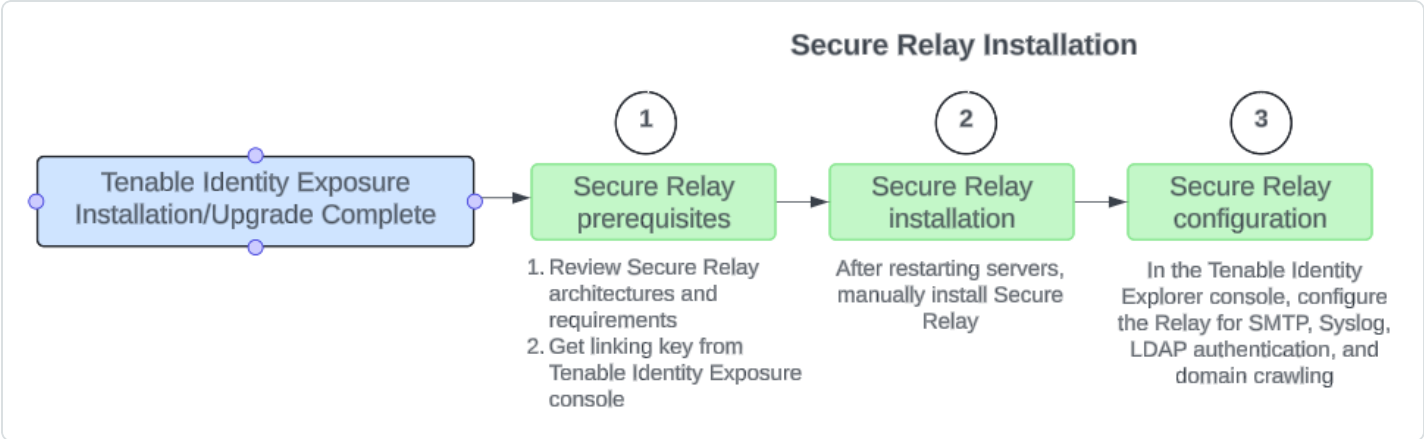
- `Tenable_ceti`
- `tenable_envoy_server`
- `tenable_envoy`
- `tenable_relay`

Secure Relay for Tenable Identity Exposure 3.59

You install the Secure Relay component **only after you install or upgrade** Tenable Identity Exposure.

As of version 3.59, the **Secure Relay** component takes over designated tasks in the Tenable Identity Exposure platform:

- Allows you to configure domains from which it forwards the data to the Directory Listener (DL) component which collects AD objects.
- Facilitates the setup and maintenance for large infrastructures through automatic updates: No longer needs multiple DLs that require simultaneous upgrades.
- Acts a bridge between the single DL and various endpoints, such as domain controllers, SMTP or SYSLOG servers or LDAP servers for in-product authentication.
- Ties to one or several domains. The DL can manage an unlimited number of Relays.
- Requires configuration in the Tenable Identity Exposure console, such as namings and mappings (domain, SMTP, SYSLOG, LDAP authentication).
- Supports the options to install the **Secure Relay on the DL server** or **separately from the DL**.
- Supports Split Security Engine Node (SEN) Services



Before you start

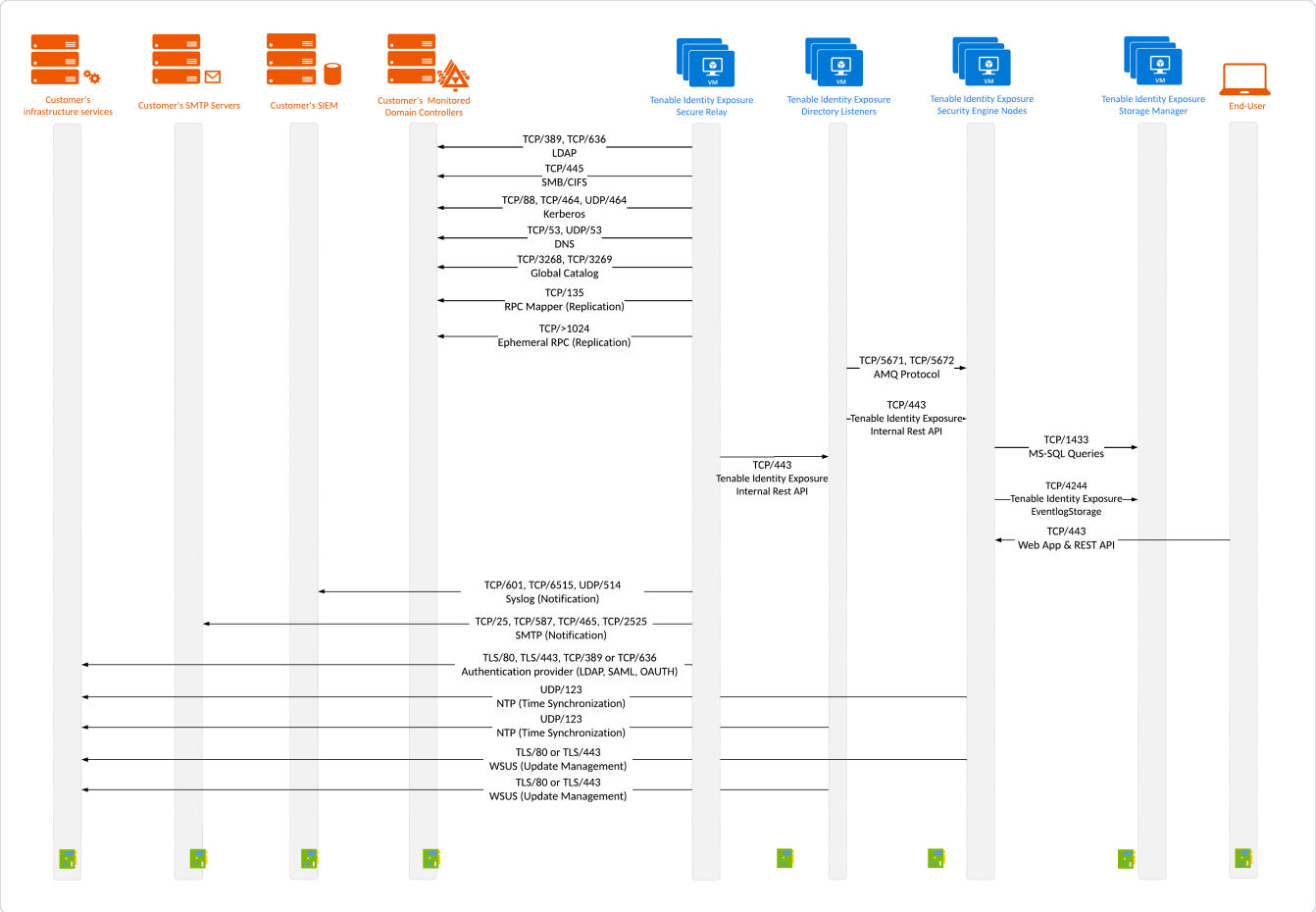
Follow these guidelines for the installation of or upgrade to Tenable Identity Exposure 3.59 with Secure Relay:

1. Review the Secure Relay Architectures for On-Premises Platforms and Secure Relay Requirements.
2. **Only one DL is supported** in version 3.59. When upgrading the Directory Listeners (DL):
    - **Keep only one DL** where you can optionally install one Relay. If you select this option, **combine the necessary resource requirements for the DL and Relay**. For more information, see Resource Sizing.
    - You must have **at least one Relay**. If you don't install it on the DL, then you have to provision a new machine to install this Relay.
    - Optionally, install Relays to replace other DLs if you previously used multiple DLs.

      For more information, see Secure Relay Architectures for On-Premises Platforms.
3. **Network requirements**:
    - In previous and current versions, the DL communicated to the SEN directly, using the AMQP(S) protocol.
    - In version 3.59, the Relays that replace the multiple DLs communicate with the only remaining DL over HTTPS.
    - Envoy is the reverse proxy.

Network flows for on-premises platform using Secure Relay

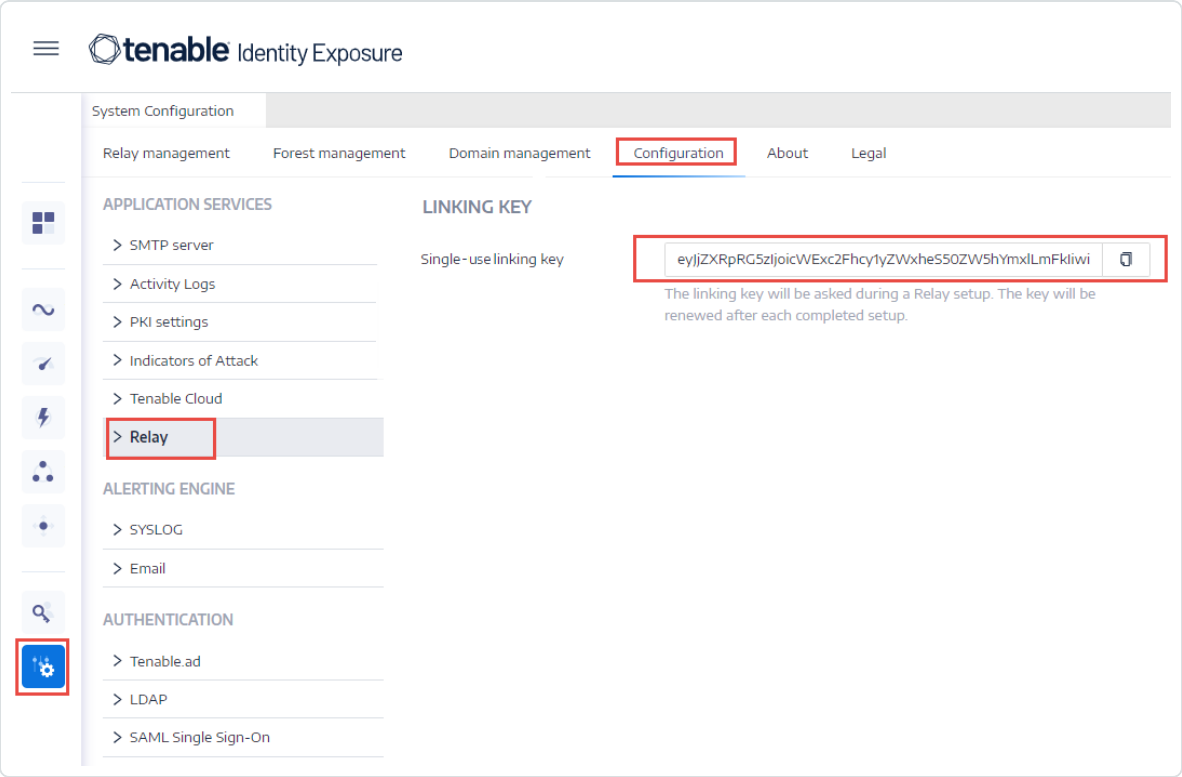
The following are network flows for an On-Premises platform using Secure Relay:



4. **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 the Tenable Identity Exposure console, click **System** on the left menu bar and select the **Configuration** tab > **Relay**.



2. Click to copy the linking key.

5. **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.

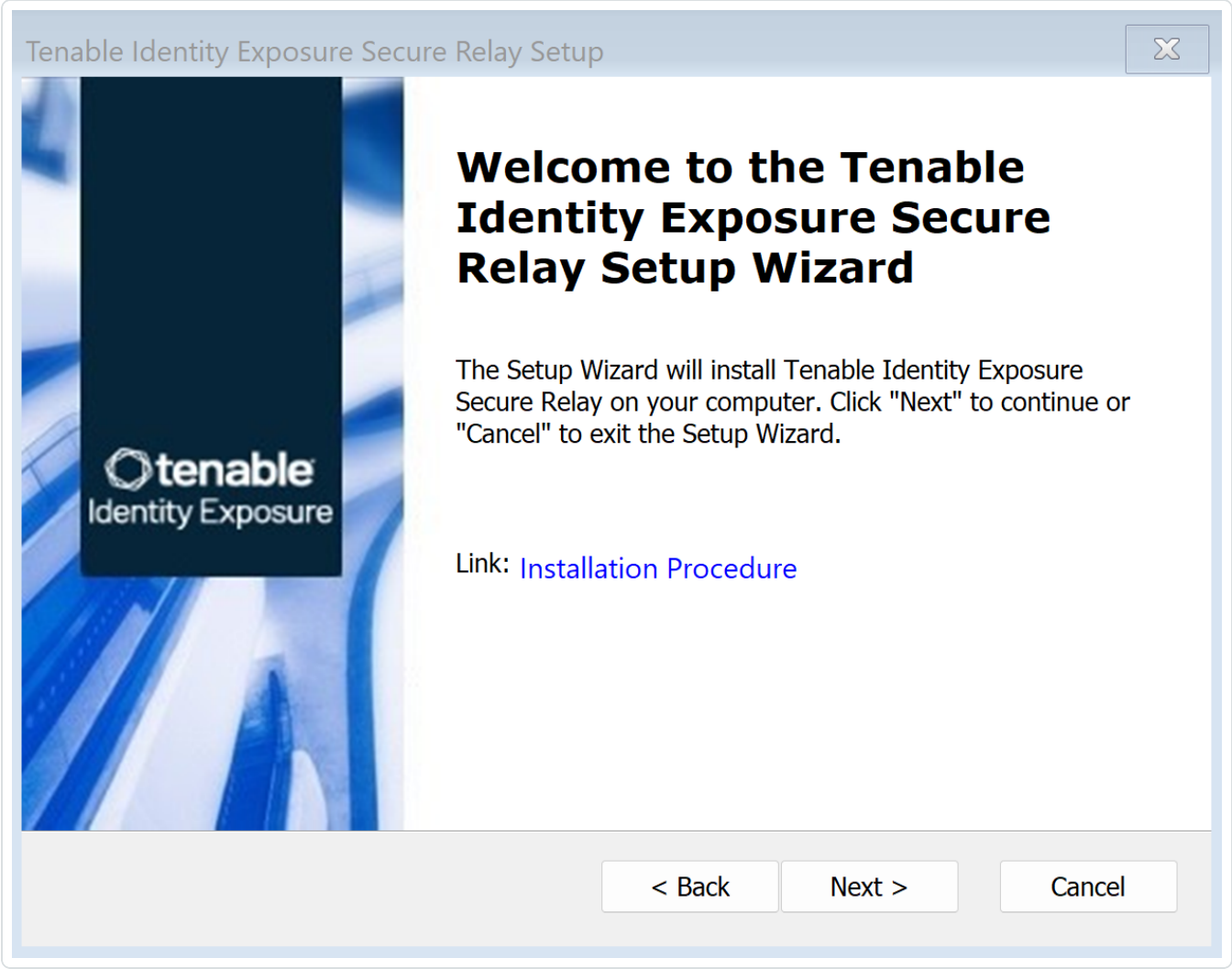
Installation procedure

Required User Role: Administrator on the local machine

To install the Secure Relay:

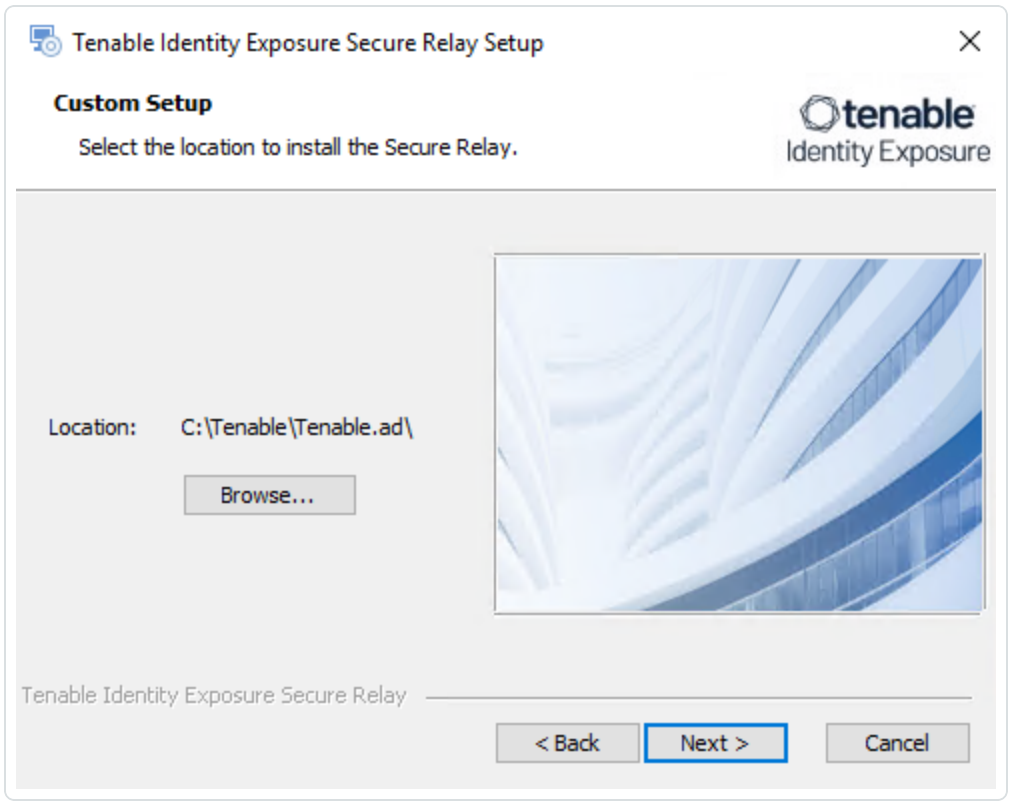
1. Download the executable program for Secure Relay from Tenable's Downloads site.
2. Double-click on the file `tenable.ad_SecureRelay_v3.xx.x` to start the installation wizard.

   The **Welcome** screen appears.



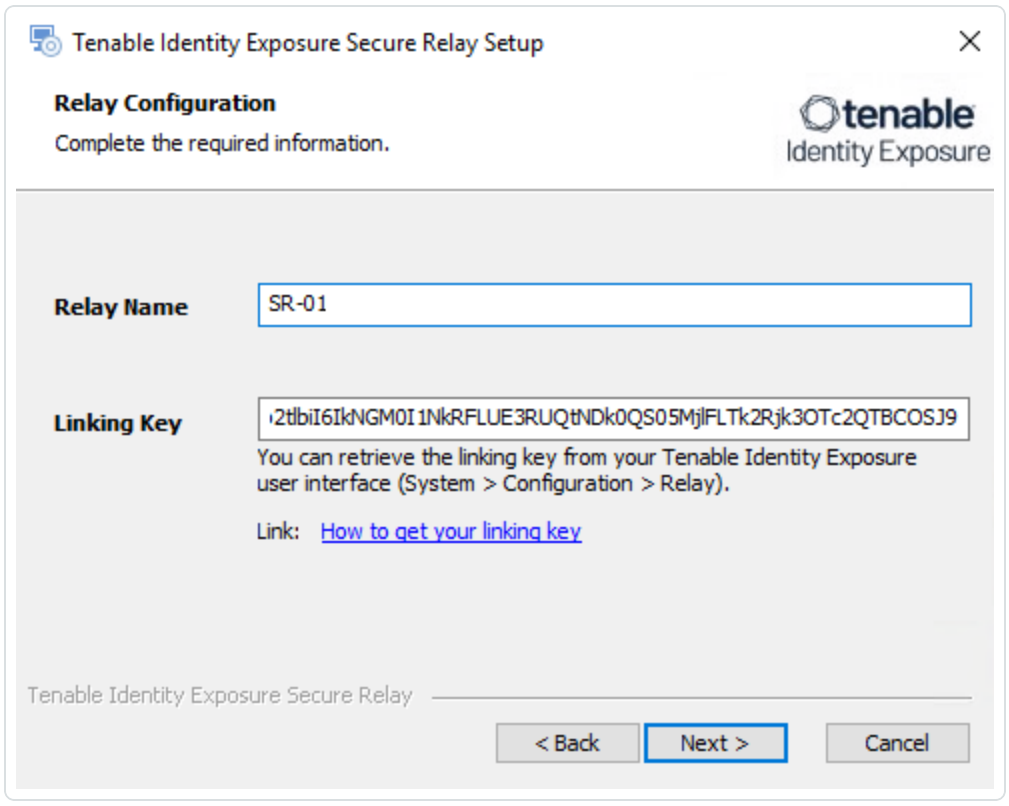
3. Click **Next**.

   The **Custom Setup** window appears.



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.



6. Provide the following information:

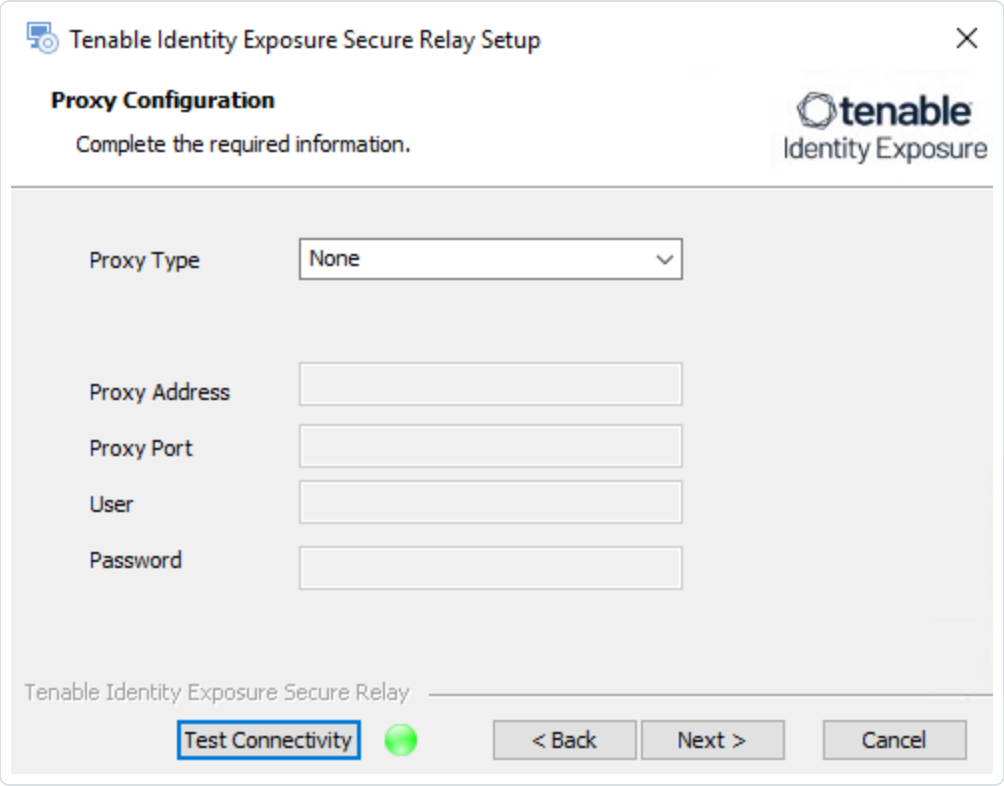
    a. In the **Relay Name** box, type a name for your Secure Relay.

    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:



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**.

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 6 new environment variables related to Secure Relay with names beginning with "'ALSID_CASSIOPEIA_" 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.

Relay configuration

- Configure the Relay

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.

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.

See also

- Troubleshoot Secure Relay Installation
- Secure Relay - FAQs

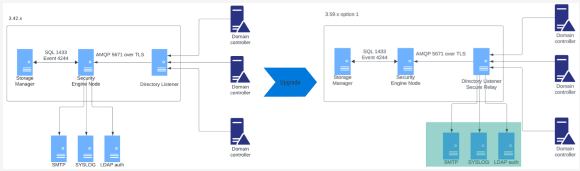
Secure Relay Architectures for On-Premises Platforms

Tenable Identity Exposure supports the following architectures comprising the Storage Manager (SM), Security Engine Node (SEN), Directory Listener (DL), and Secure Relay (SR):

- Standard 3 Servers with DL and SR on the Same Server
- Standard 3 Servers with DL and SR on a Separate Server
- Multiple DLs to a Single DL Running SR
- Multiple DLs to a New DL Communicating with SR(s)

Standard 3 Servers with DL and SR on the Same Server

This architecture transitions from a standard 3-servers architecture (SM, SEN, and DL) to one with a DL running the SR on the same server.

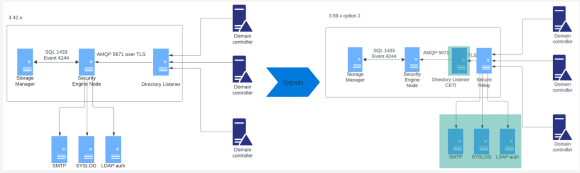
3.42	3.59
• The Security Engine Node: ◦ Sends email and Syslog alerts ◦ Provides LDAP authentication	• The Directory Listener runs the Secure Relay, which: • ◦ Sends email and Syslog alerts ◦ Provides LDAP authentication
	

Note: This architecture requires that you combine the required resources for the DL and SR in one virtual machine.

Standard 3 Servers with DL and SR on a Separate Server

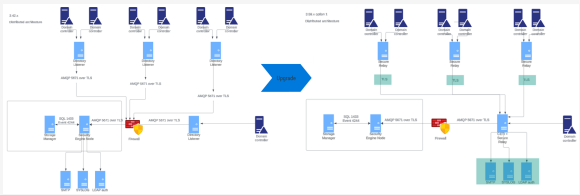
This architecture transitions from a standard 3-servers architecture (SM, SEN, and DL) to one with the DL and SR running on separate servers.

3.42	3.59
• The Security Engine Node:	• Requires **a new server for the Directory Listener**

◦ Sends email and Syslog alerts ◦ Provides LDAP authentication	• The Secure Relay: ◦ Replaces the Directory Listener ◦ Sends email and Syslog alerts ◦ Provides LDAP authentication
	

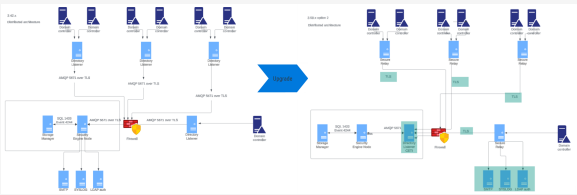
Multiple DLs to a Single DL Running SR

This architecture transitions from a multiple-DLs architecture to one with a single DL running the SR.

3.42	3.59
• Directory Listeners communicate with Security Engine using AMQP over TLS • The Security Engine Node: ◦ Sends email and Syslog alerts ◦ Provides LDAP authentication	The **first Directory Listener owns the Secure Relay** and acts as the "concentrator" for all deployed Secure Relays deployed (former Directory Listeners) and communicate with these using TLS. This Secure Relay: • Sends email and Syslog alerts • Provides LDAP authentication
	

Multiple DLs to a New DL Communicating with SR(s)

This architecture transitions from a multiple-DLs architecture to one with a new DL that communicates with Secure Relays (replacing old Directory Listeners).

3.42	3.59
• Directory Listeners communicate with Security Engine using AMQP over TLS • The Security Engine Node: ◦ Sends email and Syslog alerts ◦ Provides LDAP authentication	A **new server for the Directory Listener** acts as the "concentrator" for all deployed Secure Relays (former Directory Listeners) which communicate with the Directory Listener using TLS. The Secure Relay: • Sends email and Syslog alerts • Provides LDAP authentication
	

See also

Secure Relay for Tenable Identity Exposure 3.59

Configure the Relay

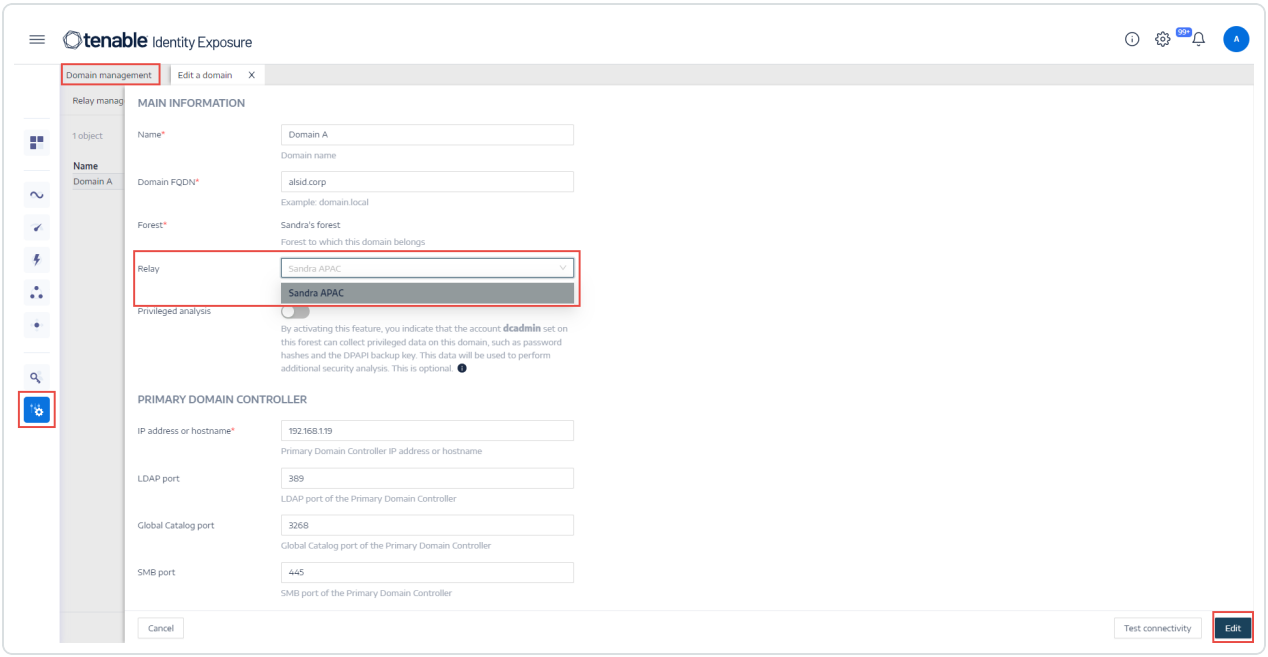
After installation and post-installation checks, you configure your Relay in Tenable Identity Exposure to link it to a domain and to set up alerts.

◦ Domain Mapping: Replace multiple-DL application settings or network environment variables with necessary domain settings (the number of edits may vary).

To map 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.



   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.

- Alert Mapping:
  - SMTP Configuration: Make necessary edits to SMTP Server Configuration.
  - Syslog Alerts: Configure Syslog Alerts (the number of edits may vary).
- LDAP Mapping: Implement Authentication Using LDAP .

See also

- Secure Relay - FAQs

Secure Relay - FAQs

I used to have multiple Directory Listeners (DLs). Can I still have multiple DLs?

No, Secure Relays replace multiple DLs). Tenable Identity Exposure now **only supports one DL**; multiple DLs create unknown issues.

I used to have only one machine for the DL, can I keep the same machine for the DL and the Secure Relay?

Yes, you can. However, make sure to combine the resource requirements for a DL and a Secure Relay. For example, if the RAM for a DL is 5 GB and for 1 GB for the Secure Relay, your machine must have 6 GB (5 GB + 1 GB).

You can also install the Secure Relay on a separate VM, as long as it can contact the DL.

What are the network flows that change between previous versions and this 3.59?

With the 3.59, in its simplest form, we add a Secure Relay between your Active Directory (AD) and the DL. That means:

- The communication between your AD and the Secure Relay is the same as the communication between your AD and the DL previously.
- The communication between the DL and the rest of the platform is the same as previously.
- What changes is that Tenable Identity Exposure uses HTTPS between one or more Secure Relays and the DL. You must allow this new network flow.

Where can I find the on-premises Secure Relay installer?

In the folder `C:\Tenable\Tenable.ad\DirectoryListener\Updates\`.

Should I use the Secure Relay installation package available on https://www.tenable.com/downloads or the one in the folder C:\Tenable\Tenable.ad\DirectoryListener\Updates\?

You can use either one as they are usually the same version. The one in the folder `C:\Tenable\Tenable.ad\DirectoryListener\Updates\` does not require a login to access the binary.

When installing/upgrading the DL, I selected "Yes" to the question "Install the Secure Relay after the DL?", but nothing's installed. What did I miss?

The Secure Relay installation launches after the DL server reboots, so make sure first and foremost that you did reboot after the DL installation/upgrade.

Other problems could arise from the AV/EDR blocking the installation process from running after the reboot. Make sure to review their full logs.

The timeframe to look for in these logs depends on the AV/EDR blocking the installation process, so make sure to check some time before (during the DL installation) and after the reboot.

When the relay installation fails, what elements should I collect?

Multiple elements need to be retrieved when installation fails, before any other attempt:

- The installation logs: Extract these from the MSI dialog box when a failure occurs.
- The Relay logs: Located in the `<install path>\SecureRelay\logs\Relay.log`.
- The Envoy logs: Located in the `<install path>\SecureRelay\logs\envoy.logs`.
- The `envoy.yaml` configuration file: Located at `<install path>\SecureRelay\envoy.yaml`. There's an API key that you can redact if necessary (although we also have it in the database).
- The environment variables: Fetched using one of the following commands:

```
(cmd.exe) set
(powershell.exe) ls env: | fl
```

See also

- Troubleshoot Secure Relay Installation

Logs for Troubleshooting

Tenable Identity Exposure provides debug logs for troubleshooting and understanding platform behavior.

The following are some of the common logs:

- Installation/upgrade logs
- Platform logs
- IoA script installation/upgrade logs

Installation/Upgrade Logs

If the installation program cannot install Tenable Identity Exposure on a machine, you can forward the log file to our support (https://community.tenable.com/s/).

This log file is in your `%tmp%` folder, and its name always starts with “MSI” followed by random numbers, such as `MSI65931.LOG`.

To generate log files in another location (for example, if you placed the installer on the desktop):

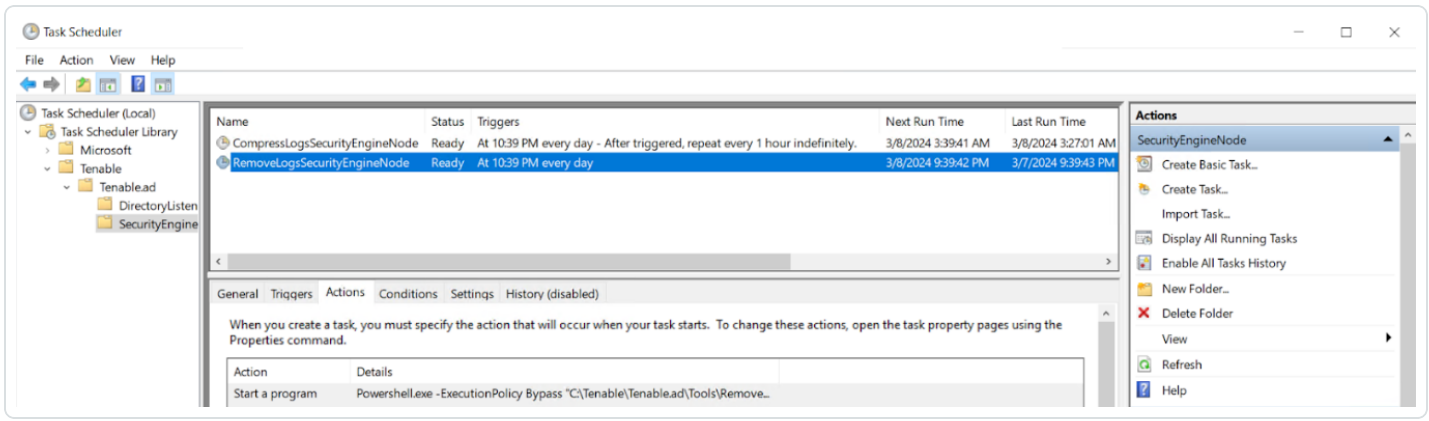
1. In the command line of the local machine, type cd desktop.
2. Type .\installername.exe /LOGS "c:\<path>\logsmsi1.txt".

Platform Logs

Tenable Identity Exposure generates log files for the various services on the individual installation.

- From the Directory Listener server – `<Installation Folder>\DirectoryListener\logs`
- From the Security Engine Node server – `<Installation Folder>\SecurityEngineNode\logs`
- From the Storage Manager server – `<Installation Folder>\StorageManager\logs`
- From the Directory Listener server and or Standalone Secure Relay server – `<Installation Folder>\SecureRelay\logs`

The default platform log files rotate when they reach a size of 100 MB each and then get compressed. These tasks automatically generate during installation in the Windows Task Scheduler. The following is an example of the tasks on the Security Engine Node node.



IoA Script Installation/Upgrade Logs

The Indicator of Attack (IoA) script creates a log file (example `Register-TenableIOA-xxxx.log`) in the same location as the script. You can review it there is any error or issue during the installation.

Log Retention Periods

- **Short-term retention**: Keep debug logs for a short period such as 7 days after they are generated. This allows you to diagnose recent issues while minimizing storage consumption.
- **Long-term archiving**: Consider archiving a subset of debug logs for longer periods for compliance or troubleshooting purposes. You can store them to a safe location or compress them for efficient space utilization.

Troubleshoot Secure Relay Installation

Removal of configuration file by EDR or anti-virus during installation

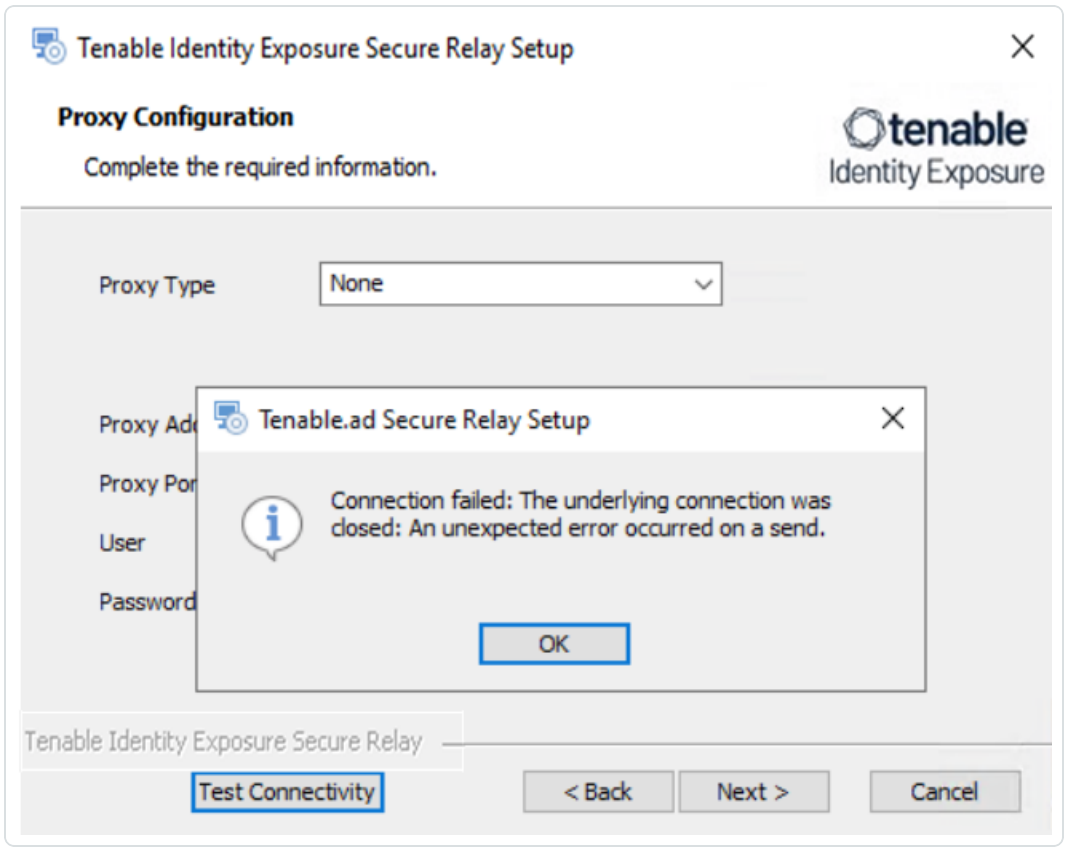
- **Cause**: During the installation of Secure Relay, Endpoint Detection and Response (EDR) software or anti-virus programs may interfere with the process by automatically removing the `envoy.yaml` configuration file. This file is essential for the Secure Relay to function correctly. If it is removed, the installation fails.
- **Error message**: If you suspect that the installation failure is caused by EDR or anti-virus software removing the `envoy.yaml` file, you can confirm this by checking the MSI error log. The MSI error log is generated in the TEMP folder on your system. Look for the following error message: `Error: The file envoy.yaml is missing.`

If this error appears in your log, it indicates that the `envoy.yaml` file was removed during the installation process, likely by security software.

- **Fix**: To resolve this issue and ensure a successful installation, follow these steps:
  1. Whitelist the installation folder or configuration file:
     - Configure your EDR or anti-virus software to exclude the following directory from scans and removal actions: `[Install_path]\Tenable.ad\SecureRelay\`
     - Alternatively, you can whitelist the `[Install_path]\Tenable.ad\SecureRelay\envoy.yaml` file if excluding the entire folder is not an option.
  2. Reattempt Installation: After adding the necessary exclusions, rerun the Secure Relay installation.

Installation failure of multiple Secure Relays and a Secure Relay on a standalone server

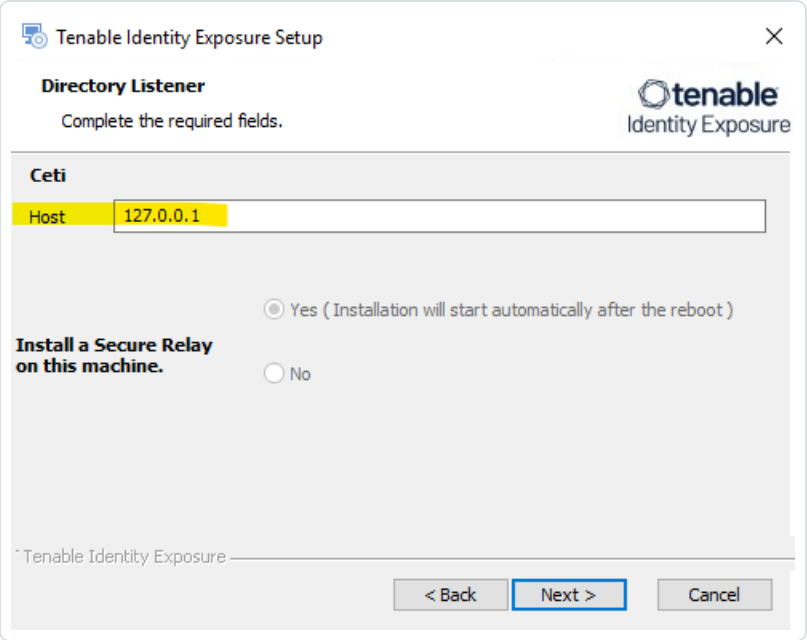
- **Cause**: During upgrade, the installer does not pick up the environment variable for the Ceti host IP address and defaults to "127.0.0.1".
- **Error message** – Connection failed due to an unexpected error during transmission.



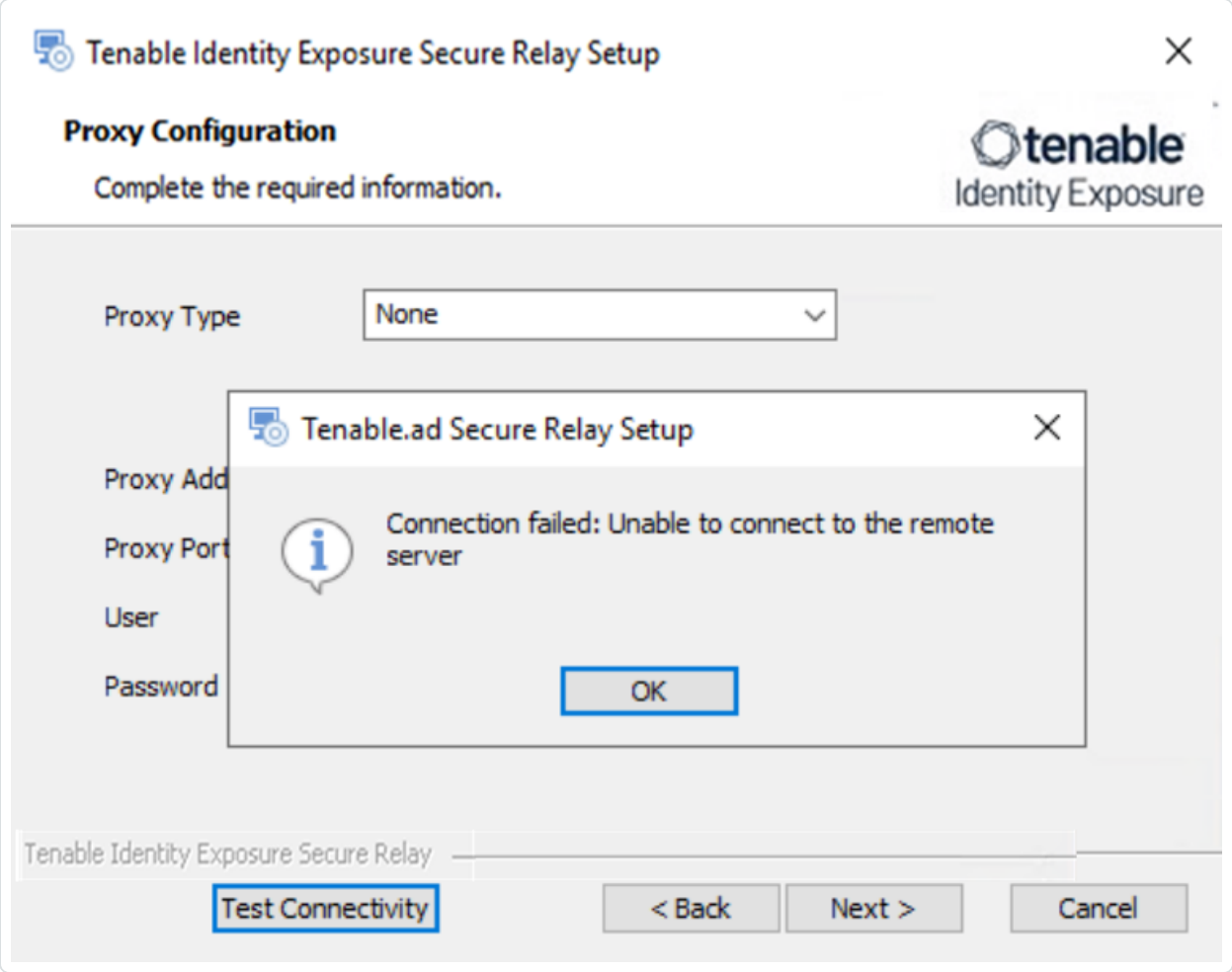
- **Fix**:
  1. Verify the environment variable 'TENABLE_CASSIOPEIA_CETI_Service__Broker__Host' on the Directory Listener server.
  2. Ensure that it is **set to the IP address of the Security Engine Node**. If the variable is set to the default '127.0.0.1', it causes the Secure Relay installation to fail.
  3. After you update the environment variable 'TENABLE_CASSIOPEIA_CETI_Service__Broker__Host', **restart the Ceti service**.
  4. **Begin the Secure Relay installation again**. Otherwise, it rolls back and leaves the Relay and Envoy services installed and block any further installation.

Invalid CetiDNS name

- **Cause**: The IP Address of the Ceti Server was not set during the upgrade or installation of the Security Engine Node server. The installer defaults to “127.0.0.1”:



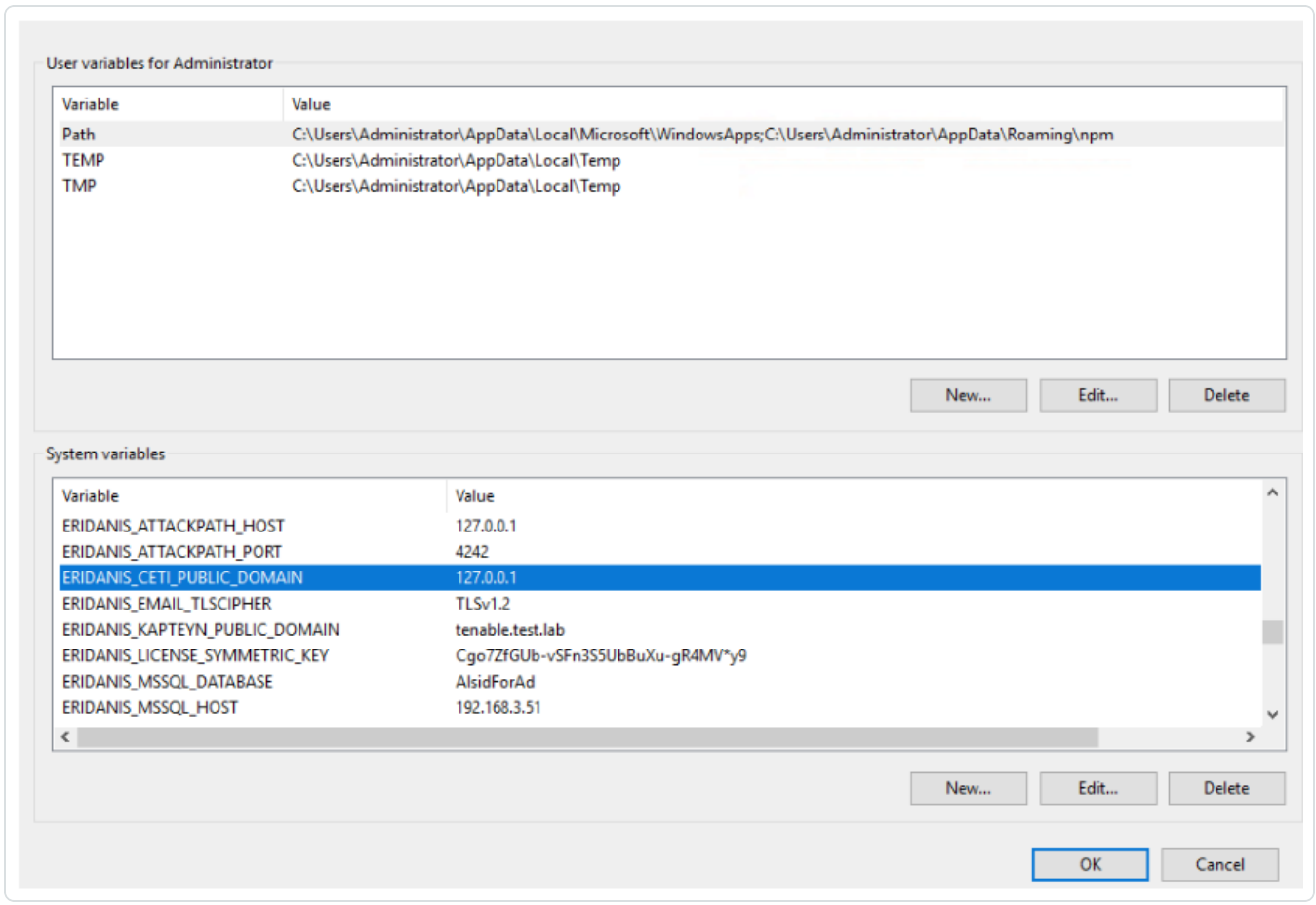
- **Error message** – Connection failed: Unable to connect to the remote server.



For the "tenable_envoy_server" service in a paused state: Identify the application currently occupying the port `0.0.0.0:443` using the PowerShell command `netstat -anob | findstr 443`. If you find another application, either remove it or stop it to resolve the conflict and allow proper functioning of the "tenable_envoy_server" service.

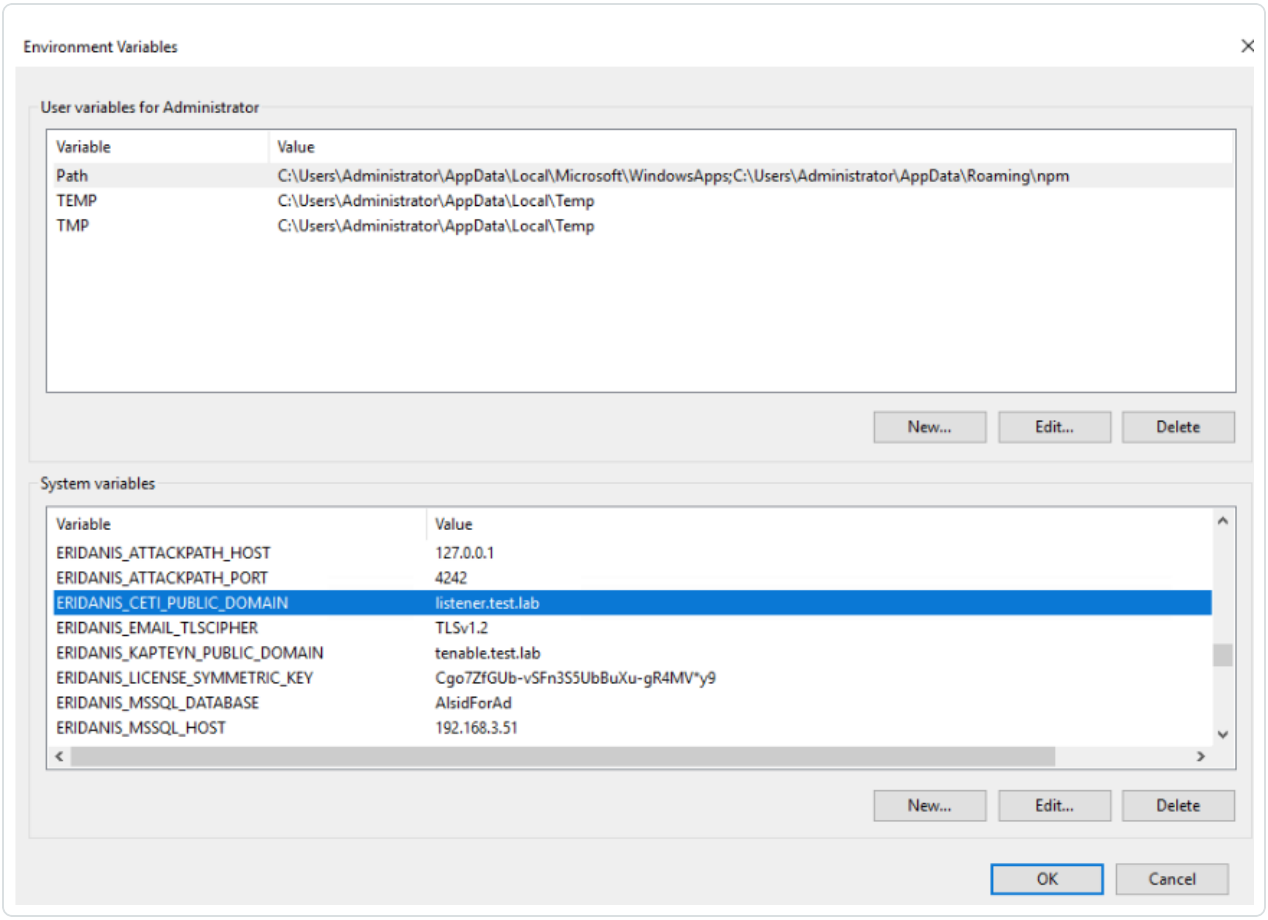
Fix:

1. Log into the Security Engine Node server.
    - If you use a split Security Engine Node architecture, log into the server that runs the Eridanis service.
2. Open Environment Variables and locate the variable name `ERIDANIS_CETI_PUBLIC_DOMAIN`.

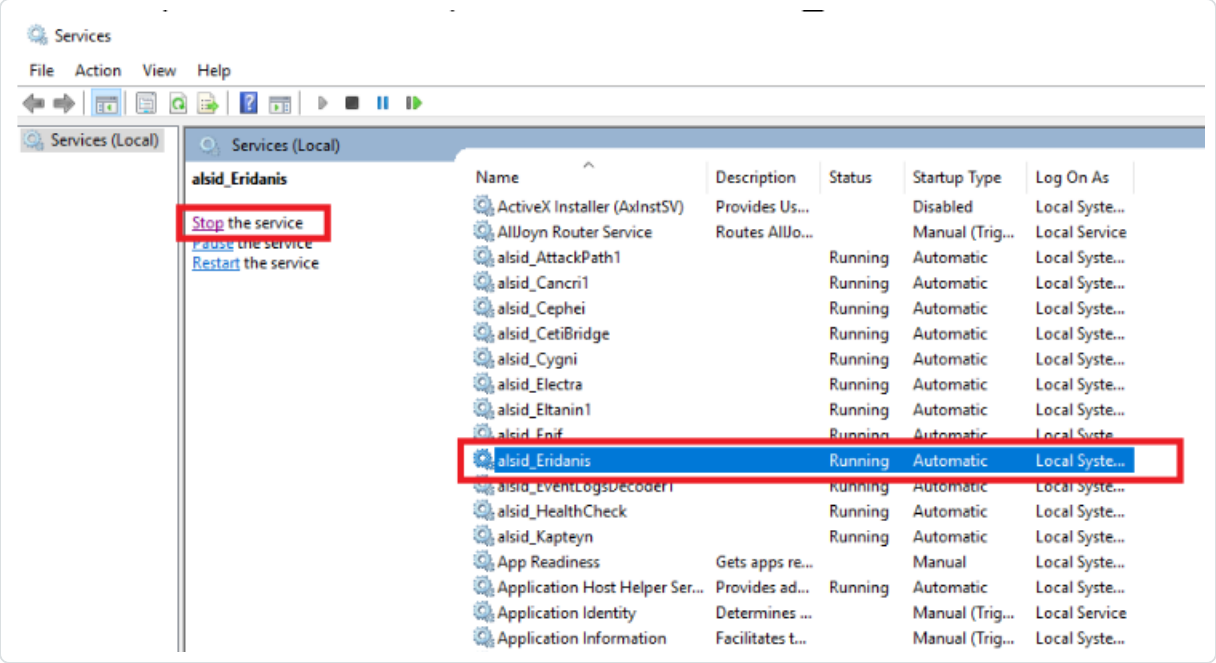


3. Edit the variable value for `ERIDANIS_CETI_PUBLIC_DOMAIN` to insert the **IP address or hostname of the Directory Listener**:
    - Update the environment variable `ERIDANIS_CETI_PUBLIC_DOMAIN` to match the IP address or hostname of the Directory Listener. This synchronization facilitates seamless communication between the components deployed on separate servers.
    - The Variable value for “ERIDANIS_CETI_PUBLIC_DOMAIN” changes from `127.0.0.1`

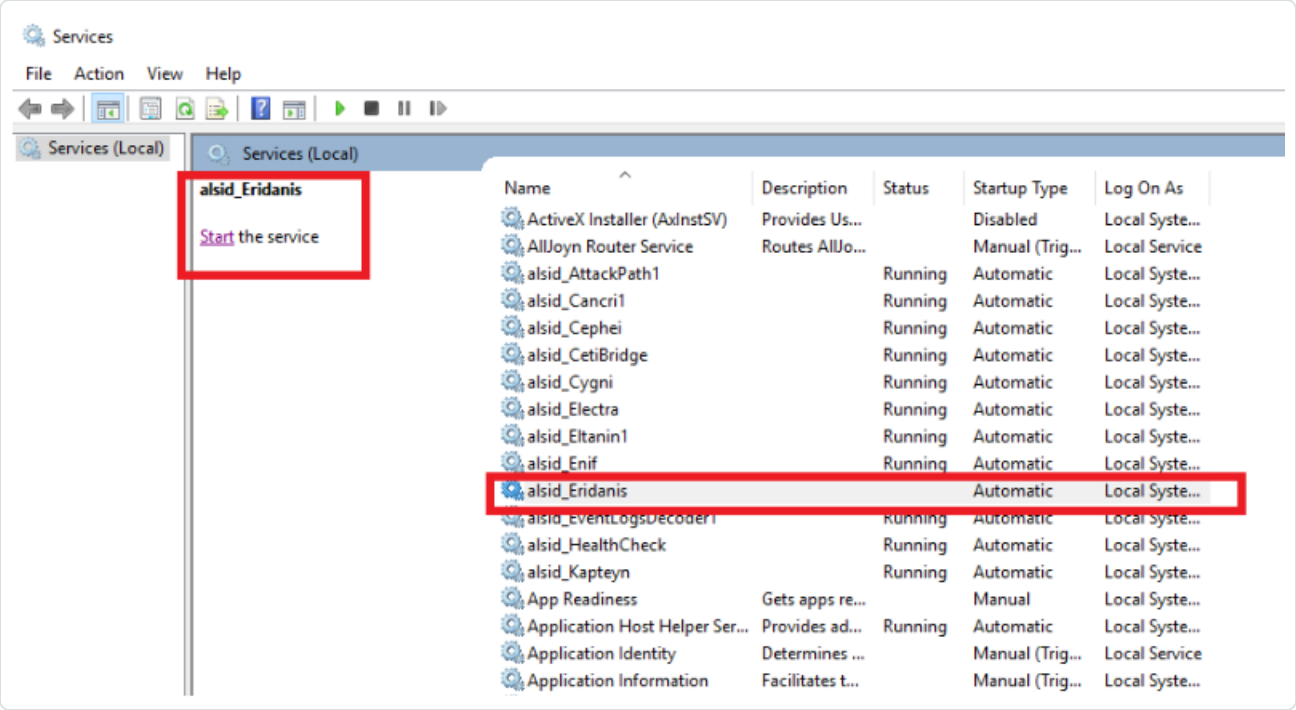
to the IP address or hostname of the Directory Listener `listener.test.lab`.



4. Open Services and stop the service `tenable_Eridanis`.



5. Start the service `tenable_Eridanis`.

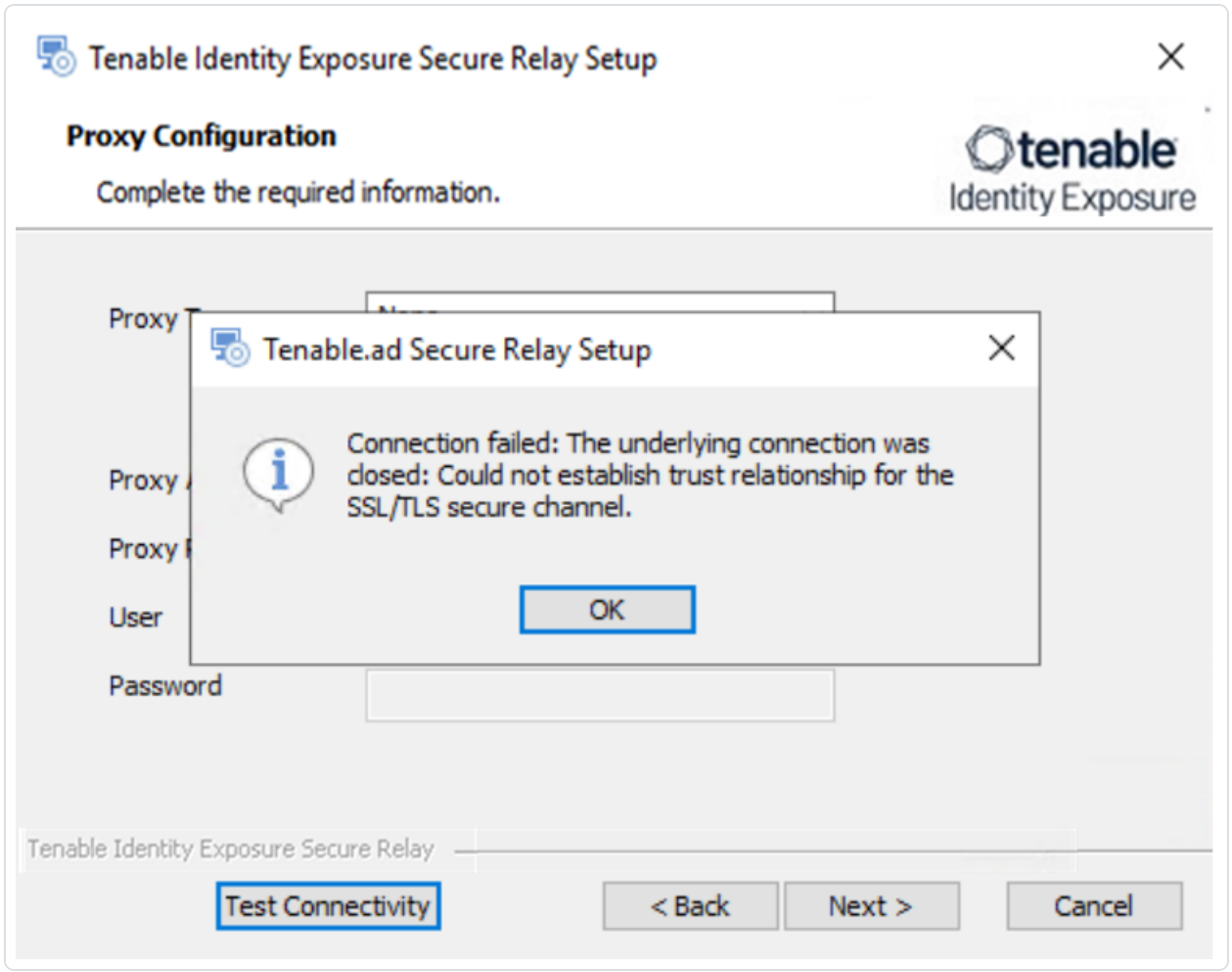


6. Log into the Secure Relay server. Exit the Secure Relay installer if it is already open and begin the Secure Relay installation again.

> **Caution**: Be sure to **exit the installer** and start a fresh installation. If you do not exit the installer and continue with the installation, it breaks the installation process, and you can't proceed further (blocker).

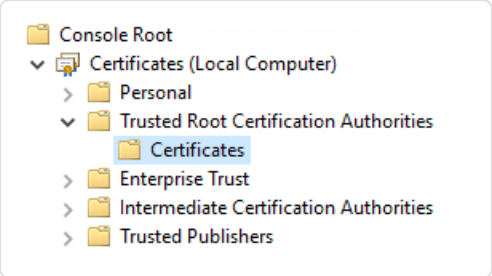
No "Trust Relationship" for SSL/TLS secure connection

- **Cause**: The installer cannot find the CA certificates on the local server.
- **Error message** – Connection failed: The underlying connection was closed: Could not establish a trust relationship for the SSL/TLS secure channel.



- **Fix**:

1. Access the source system (Directory Listener server) or repository where trusted CA certificates reside and locate the trusted CA certificates, typically in directories such as:
    - Default self-signed certificate location: `"installation_drive":\Tenable\Tenable.ad\DefaultPKI\Certificates\ca`
    - Custom certificate location: `"installation_drive":\Tenable\Tenable.ad\Certificates`
2. Copy the trusted CA certificate files from the source system (Directory Listener server) to the local server (Secure Relay server).
3. Import the certificates into the trusted certificate store of the Secure Relay server.



4. After a successful import, **exit the Secure Relay installer and begin the installation again**.

    Caution: Be sure to **exit the installer** and start a fresh installation. If you do not exit the installer and continue with the installation, it breaks the installation process, and you can't proceed further (blocker).

Start Using Tenable Identity Exposure

After you deploy Tenable Identity Exposure, this section walks you through the key steps to begin using Tenable Identity Exposure effectively.

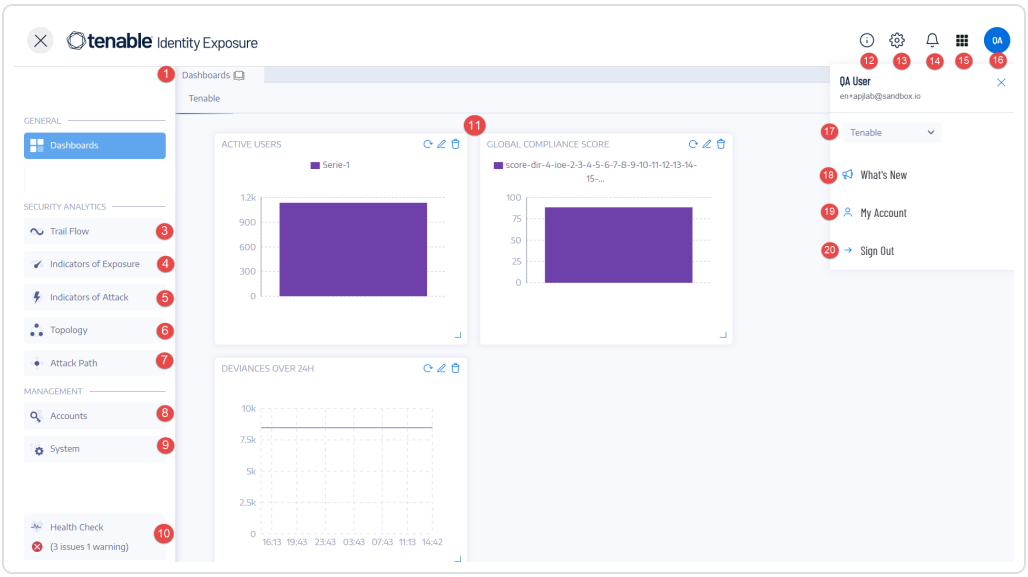
Tip: For additional information on Tenable Identity Exposure, review the following customer education materials:

- Tenable Identity Exposure Introduction (Tenable University)

Each section contains links to more detailed descriptions and instructions for the related task.

1. ## Log in and navigate the user interface

   - Log in to Tenable Identity Exposure portal. The home page opens, as shown in this example.
   - Your initial login is `hello@tenable.ad` and the password is `verySecure1.`
   - Expand or collapse the side navigation bar:
     - To expand: click the ☰ menu at the top left of the window.
     - To collapse: click the ✕ at the top left of the window.



   - Navigate the Tenable Identity Exposure User Portal.

2. ## Enable Indicators of Exposure (IoE) for an Active Directory Domain

   Before you configure Indicators of Exposure, you must have or create an Active Directory service account with the appropriate permissions. While Tenable Identity Exposure does not require administrative privileges for security monitoring, some containers require manual configuration to allow read access for the service account user.

   > For complete information, see Access to AD Objects or Containers

1. Log in to the Tenable Identity Exposure web portal with administrative credentials such as the default "hello@tenable.ad" account.
2. Click the menu icon on the top left to expand the navigation panel, then click **System** in the left panel.

Add a Forest:

1. In the **Forest Management** tab, click **Add a Forest**.
2. Provide a display name for the forest (e.g. Tenable).
3. Enter the login and password for the service account to connect to all domains in this forest.
4. Click **Add**.

   For complete details, see Forests.

Add a Domain:

1. Click **Add a Domain**.
2. Provide a display name for the domain to monitor (e.g. HQ).
3. Enter the fully qualified domain name (e.g. sky.net).
4. Select the corresponding forest from the drop-down list.
5. If using SaaS with Secure Relay, select the relay to handle this domain.
6. Enable the "Privileged Analysis" toggle if the account has required privileges.
7. If you enable **Privileged Analysis**, optionally enable **Privileged Analysis Transfer** for Tenable Cloud.
8. Provide details for the Domain Controller with Primary Domain Controller Emulator FSMO role:
   - IP address or hostname
   - Leave LDAP, Global Catalog, and SMB ports with pre-filled default values

9. Click **Test Connectivity** at the bottom.
10. If successful, click **Add**.

    In the Domain Management view, you'll see columns for LDAP Initialization, SISFul Initialization, and Honey Account Configuration statuses showing a circular loading icon until initial crawling completes.

    For complete details, see Domains.

Monitor initialization:

1. Switch to the **Trail Flow** view. After a few minutes, data begins to flow in once analysis starts.
2. Return to **System** > **Domain Management**.
3. Wait for green icons indicating LDAP and SYSVOL initialization completed.

   You have now enabled Indicators of Exposure monitoring for this domain. Notifications on the web portal appear within minutes/hours depending on environment size.

Review exposure data:

1. Click **Indicators of Exposure** in the left menu to see all indicators triggered for the added domain.
2. Click on an indicator to view deviant object details causing non-compliance.
3. Close the details and go to **Dashboards** to see the environment metrics.

3. **Deploy Indicators of Attack (IoA) for a domain**

To deploy IoAs, you must first perform three configurations as described below:

1. The IoA script is mandatory for all attack scenarios.
2. The Honey Account configured to detect specific attacks such as Kerberoasting.

3. Sysmon installation on all Domain Controllers of the monitored domain to detect attacks like OS Credential Dumping.

Tenable Identity Exposure provides the IoA script, its command line, and the Honey Account configuration command line. However, you must perform these prerequisites directly on the Domain Controllers or an administrative machine with appropriate rights.

> For complete information, see Indicators of Attack Deployment.

Configure Attack Scenarios:

1. Log in to the Tenable Identity Exposure web portal using administrative credentials (e.g., hello@tenable.ad).
2. Navigate to **System** > **Configuration** > **Indicators of Attack**.
3. Select the attack scenarios you want to enable for your environment.
4. Select the checkbox below the domain name to enable all available attack scenarios.
5. Click **Save** at the bottom right.
6. Click **See Procedure** at the top.

   A window appears, showing the procedure to deploy the IoA engine.
7. Use the toggle to enable or disable the automatic updates feature.
8. Click the first **Download** button to download the PS1 file.
9. Click the second **Download** button to download the JSON file.
10. Note where the location where you downloaded the installation files.
11. Locate the field labeled **Run the following PowerShell** commands.
12. Copy the contents of the text field and paste them into a text file.
13. Copy the PS1 and JSON files to a Domain Controller or an administrative server with appropriate rights.

14. Start the Active Directory module for Windows PowerShell as an administrator and navigate to the folder hosting the files.
15. Paste the command copied from the Tenable Identity Exposure web portal and press Enter.
16. Open the Group Policy Management console and find the GPO named "Tenable.ad" linked to the Domain Controller's OU.

For the detailed procedure, see Install Indicators of Attack.

Configure the Honey Account:

1. Return to the Tenable Identity Exposure web portal.
2. Navigate to **System** > **Domain Management** tab.
3. Click the **+** icon under **Honey Account Configuration Status** to the right of your domain (available once the other two statuses are green).
4. In the **Name** search box, type the name of the account to use as a honey pot.
5. Select the distinguished name of the object from the drop-down list.
6. Copy the contents of the command line text field and paste them into a text file.
7. Go back to the server where you ran the IoA script.
8. Open or start a PowerShell command line as an administrator.
9. Paste the command copied from the Tenable Identity Exposure web portal and press Enter.
10. Confirm that the command line ran properly.
11. Return to the Tenable Identity Exposure web portal and click the **Add** button at the bottom.

    After a few seconds, the Honey Account Configuration status should show a green dot.

For the detailed procedure, see Honey Accounts.

Install Sysmon:

The Tenable Identity Exposure web portal does not provide automatic deployment for Sysmon. See Install Microsoft Sysmon for the required Sysmon configuration file. You can install Sysmon manually as shown in the documentation or by GPO.

> For the detailed procedure, see Install Microsoft Sysmon.

4. ### Configure Microsoft Entra ID for Tenable Identity Exposure:

Tenable Identity Exposure also supports Microsoft Entra ID alongside Active Directory with specific IoEs for Entra ID identities.

> For complete information, see Configuring Microsoft Entra ID as an Identity Provider.

Create the Entra ID application:

1. Log in to the Azure Admin Portal at portal.azure.com with appropriate credentials.
2. Click on the **Azure Active Directory** tile, then **App Registrations** from the left menu.
3. Click **New Registration** and provide an application name (e.g., "Identity Exposure App").
4. Click **Register** at the bottom.
5. On the app's Overview page, note down the "Application (client) ID" and "Directory (tenant) ID".
6. Click **Certificates & secrets** in the left menu.
7. Click **New client secret**, provide a description, and set expiration per policy.
8. Click **Add**, then save the displayed secret value securely.
9. Click **API permissions** and **Add a permission**.
10. Select **Microsoft Graph**, then **Application Permissions**.
11. Add the following permissions: `Audit Log.Read.All`, `Directory.Read.All`, `IdentityProvider.Read.All`, `Policy.Read.All`, lReports.Read.All,

`RoleManagement.Read.All`, `UserAuthenticationMethod.Read.All`.

12. Click **Add permissions** and **Grant admin consent**.

Configure Tenable Vulnerability Management:

1. Connect to the Tenable Vulnerability Management web portal with the proper account.
2. Click **Menu** > **Settings** > **Credentials**.
3. Click **Create Credential** and select the **Microsoft Azure** type.
4. Provide a name, description, paste in the Tenant ID, Application ID, and Client Secret.
5. Click **Create**.
6. Click **Menu** > **Settings** > **My Account** > **API Keys**.
7. Click **Generate**, review the warning, and click **Continue**.
8. Copy the Access Key and Secret Key values.

Configure Tenable Identity Exposure:

1. Connect with a Global Administrator account.
2. Click **Menu** > **System** > **Configuration** > **Tenable Cloud**.
3. Toggle **Activate Microsoft Entra ID Support** to enable it.
4. Enter the Access Key and Secret Key generated earlier.
5. Click the checkmark to submit the API keys successfully.
6. Click the **Tenant Management** tab and **Add a Tenant**.
7. Provide a name for the Azure AD tenant.
8. Select the Azure credential created earlier.
9. Click **Add**.

Monitor and review findings:

1. Tenable Identity Exposure scans the tenant. To see the next scan time, hover over **Scan Status**.
2. When the first scan ends, a green icon appears in the **Scan Status** column.
3. Click **Indicators of Exposure** in the left menu.
4. Use tabs to filter between AD and Azure AD indicators.
5. Toggle **Show All Indicators** to see all available indicators.
6. Three tabs provide **Indicator details**, **Tenant Findings**, and **Recommendations**.
7. Review potential exposure risks and remediation guidance.

5. ### Set up and use IoEs in your environment

Tenable Identity Exposure uses Indicators of Exposure to measure the security maturity of your Active Directory and assign severity levels to the flow of events that it monitors and analyzes.

> For complete information about IoEs, see Indicators of Exposure.

Access IoEs:

1. Sign in to Tenable Identity Exposure.
2. Click the icon on the top left to expand the panel.
3. Click **Indicators of Exposure** on the left side to see the IoEs.

   The default view shows configuration items in your environment that are potentially vulnerable, rated by severity: Critical, High, Medium, and Low.

View all IoEs:

- Click the toggle to the right of **Show All Indicators**.
  - You can see all the IoEs available in your Tenable Identity Exposure instance. Any item that shows no domain is an item where you do not have that exposure.

- To the right of **Show All Indicators**, you can see **Domain**. If you have multiple domains in your environment, click on it and select the domains to view.

Search IoEs:

- Click **Search an Indicator** and type a keyword, such as "password".

  All IoEs related to passwords appear.

Review IoE details:

- To see additional information about an indicator, click on it.
  - The detailed view starts with an executive summary of the particular exposure.
  - It then lists documents related to it and known attacker tools that can expose this particular item.
- To the right, you see **Impacted Domains**.
  - Click the **Vulnerability Details** tab to read additional information about the checks done for this IoE.
  - Click the **Deviant Objects** tab to see the list of objects and reasons that triggered the exposure.
  - If you expand an object in the list, you can see more details about what caused the deviance.

Create queries:

1. To create a query, click **Type an Expression** and enter a Boolean query for an item. You can also click the filter icon to the left to build a query.
2. Set the start and end dates, choose domains, and search for ignored items by clicking the **Ignore** toggle.

   > For complete procedures, see Search Deviant Objects.

Ignore/Export deviant objects:

- You can hide objects in the list by ignoring them.
  - Select one or more objects, then click **Select an Action** at the bottom of the page.
  - Select Ignore **Selected Objects** and click **OK**.
  - Choose the date until which you want to ignore the selected objects.
  - You can stop ignoring objects the same way, using the **Stop Ignoring Selected Objects** option.
- To export the list of all deviant objects for this indicator as a CSV file, click the **Export All** button.

> For complete procedures, see Deviant Objects.

Remediation recommendations:

- Click the **Recommendations** tab to see recommendations on how to remediate this indicator.

> See also Remediate Deviances from Indicators of Exposure for remediation use cases.

6. ### Track configuration changes in AD using the Trail Flow

The Trail Flow displays the real-time monitoring and analysis of events affecting your ad infrastructures. It allows you to identify critical vulnerabilities and their recommended courses of remediation.

> For complete information, see Trail Flow and Trail Flow Use Cases.

Access the Trail Flow:

1. Sign into Tenable Identity Exposure.
2. Click the icon on the top left to expand the navigation bar.
3. Click **Trail Flow**.

Navigate the Trail Flow page:

The Trail Flow page opens with a list of events, including the source type, object path, domain, and date.

1. Click the date box in the upper right to indicate the dates that you are searching for.
2. Click **Domain** to change which Active Directory servers or forests.
3. Click the pause button in the upper right corner to pause or restart Trail Flow capture.

Create queries:

There are two ways of creating queries for your search: manually or by using the wizard.

- To filter events manually, type an expression in the search box to refine results using the Boolean operators.

  > For complete information, see Search the Trail Flow Manually.

- To use the search wizard:

  1. Click the magic wand icon on the left.
  2. Follow the prompts to create and combine query expressions.

  > For complete information, see Search the Trail Flow Using the Wizard and Customize Trail Flow Queries

View event details:

Once you've identified an important event:

1. Click on the event. This will bring up the attributes of the change on that object.
2. Hover over the blue dot icon on the left to compare the values before and at the event.
3. Hover over items to see additional information.
4. Click **See Whole Value** and click the button to copy that information to the clipboard.

Identify configuration changes:

One of the challenges of Active Directory server cybersecurity is the large number of configuration changes that do not impact cyber exposure. To identify configuration changes:

1. Click the magic wand icon.
2. Enable **Deviant Only**.
3. Click **Validate**.

View cyber exposure items:

Notice that the events have a red diamond symbol next to them. Click on an event to see information regarding the configuration change. An additional tab is available labeled "Deviances". Click on it to see the specific cyber exposure items that were created or resolved.

7. ### Identify potential attacks on AD using IoAs

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

> For complete information, see Indicators of Attack.

Access IoAs:

1. Sign into Tenable Identity Exposure.
2. Click the icon at the top left to expand the navigation bar.
3. Click **Indicators of Attack**.

Filter the timeline:

By default, you see the timeline of attack detection for today. To change the filter:

- Click **Day**, `Month`, or **Year**.
- To change the time frame, click the calendar icon and select the appropriate time frame.

Filter the view:

You can filter the view on specific domains or IoAs using the selector on the right side of the portal.

1. Click **Domains** to view the choices and make selections.
2. Click **X** to close.
3. Click **Indicator**s to view the choices and make selections.
4. Click **X** to close.

As an example, let's focus on what happened in 2022:

1. Click the **Year** button and select "2022".
2. Click the red and yellow bar in the timeline.
3. You can now see a new view with the top three critical and top three medium attacks detected that month.
4. Close the view by clicking outside the black box.

View details of detected attacks:

Below the timeline, you see a card for the monitored domain on which the attack was detected.

- Click the **Sort By** drop-down.
- You can sort the card by domain, indicator criticality, or forest.
- To search for a specific domain or attack, use the search box.

- By default, you only see a card for the domain under attack. Toggle the view to see each domain by switching **Show Only Domains Under Attack** from **Yes** to **No**.

Customize the chart:

A card contains two types of information: a chart and the top three attacks.

1. To change the chart type, click the pencil icon at the top right of the card.
2. Select either **Attack Distribution** or **Number of Events**.
3. Click **Save**.

Viewing incident details:

To see more details about the attack that was detected:

- Click the card to see incidents related to the domain.
- To filter, use the search box, select a start or end date, specific indicators, or toggle the **No/Yes** box to show or hide closed incidents.
- To close incidents, select an alert, click the **Select an Action** menu at the bottom, select **Close Selected Incidents**, and click **OK**.
- To reopen an incident, select an alert, click the **Select an Action** menu, select **Reopen Selected Incidents**, and click **OK**.

View attack details and Yara detection rules:

- Click on an attack to open the detail view. In the description panel, there is the incident description of the attack, MITRE ATT&CK framework information, and additional resources with links to external websites.
- Click the Yara detection rules panel to see an example of a rule that can perform malware research in detection tools.
- Export the list of incidents by clicking **Export All**. CSV is the only format available.

Notification and alerts:

The Bell icon on the top right shows a notification when Tenable Identity Exposure detects an attack. These attacks appear in the attack alerts tab.

8. ### Set up and use alerts

The Tenable Identity Exposure alerting system helps you identify security regressions or attacks on your monitored Active Directory. It pushes analytics data about vulnerabilities and attacks in real-time through email or Syslog notifications.

> For complete procedures, see Alerts.

Configure the SMTP Server:

1. Connect to Tenable Identity Exposure.
2. Click **System** > **Configuration**.
3. Configure the SMTP server from this menu.

Create email alerts:

1. Under **Alerting Engine**, click **Email**.
2. Click the **Add an Email Alert** button.
3. In the **Email Address** box, type the recipient's email address.
4. In the **Description** box, type a description for the address.
5. From the **Trigger the Alert** drop-down list, select **On Changes**, **On Each Deviance**, or **On Each Attack**.
6. From the **Profiles** drop-down, select the profiles to use for this email alert.
7. Check the **Send Alerts When Deviances** box to send email notifications when a system reboot triggers alerts.
8. From the **Severity Threshold** drop-down, select the threshold at which Tenable Identity Exposure will send alerts.
9. Select the indicators for which to send alerts.

10. Select domains for alerts:

    a. Click **Domains** to select the domains for which Tenable Identity Exposure sends out alerts.

    b. Select the forest or domain and click the **Filter on Selection** button.

11. Click the **Test the Configuration** button.

    A message confirms that Tenable Identity Exposure sent an email alert to the server.

12. Click the **Add** button.

    A message confirms that Tenable Identity Exposure created the email alert.

Create Syslog alerts:

1. Click on **Syslog** and then click the **Add Syslog Alert** button.
2. In the Collector **IP Address or Hostname** box, type the server IP or hostname of the server receiving the notifications.
3. In the **Port** box, type the port number for the collector.
4. From the **Protocol** drop-down, select either UDP or TCP.
5. If you choose TCP, select the **TLS** option checkbox to enable TLS security protocol.
6. In the **Description** box, type a brief description for the collector.
7. Choose one of the three options for triggering alerts: **On Changes**, **On Each Deviance**, or **On Each Attack**.
8. From the **Profiles** drop-down, select the profiles to use for this Syslog alert.
9. If you want to send alerts after a system reboot or upgrade, check **Send alerts when deviances are detected during the initial analysis phase**.
10. If you set alerts to trigger on changes, type an expression to trigger the event notification.
11. Click the **Test the Configuration** button.

    A message confirms that Tenable Identity Exposure sent a Syslog alert to the server.

12. Click **Add**.

    A message confirms that Tenable Identity Exposure created the Syslog alert.

9. ### Set up dashboards in the Tenable Identity Exposure portal

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

> For complete information, see Dashboards.

Access dashboards:

1. Sign into Tenable Identity Exposure.
2. Click the icon on the top left to expand the navigation bar.

Create a custom dashboard:

1. Go to **Dashboards** and click **Add**.
2. Click **Add a Dashboard**.
3. Give it a name and click **OK**.

Add widgets to the dashboard:

1. Click **Add** in the upper right corner.
2. Select **Add a Widget on this Dashboard** or click the button in the middle of the screen.
3. Choose the type of widget (bar charts, line charts, or counters).

Configure a line chart widget:

1. Click **Line Charts**.
2. Name the widget, e.g., "Deviances in the Last 30 Days".
3. Choose the type of data (users count, deviances count, or compliance score).

4. Select **Deviances** and set it for one month.
5. Click **No Indicator** and select which indicators to use.
6. Name the data set, e.g., "Critical".
7. Add other data sets as needed (e.g., for medium and low).
8. Click **Add**.

Add a bar chart widget:

1. Click **Bar Chart**.
2. Name it **Compliance** and choose the compliance score data type.
3. Select all indicators.
4. Name the data set, e.g., "IoE".
5. Click **Add**.

Add a counter widget:

1. Click **Counter**.
2. Name the widget, e.g., "Users", and set the type of data to **User Count**.
3. Choose the status **All** and select the domain.
4. Name the data set and click **Add**.

10. **View Attack Paths**

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

> For complete information, see Attack Path.

Access the Attack Path feature:

1. Sign into Tenable Identity Exposure.
2. Click the menu icon on the top left to expand the navigation bar.
3. In the **Security Analytics** section, click **Attack Path.** The Attack Path feature has three modes:
    - Attack Path
    - Blast Radius
    - Asset Exposure

Use the Blast Radius mode:

1. In the search box, type the name of the account (e.g., "John Doe").
2. Select the account from the list and click the magnifying glass icon.
3. Explore the blast radius from the selected compromised account.
4. Filter and view nodes as needed.
5. Hover over endpoints to view the attack path.
6. Toggle the option to show all node tooltips.
7. Use the zoom bar to adjust the view.
8. To change the search object, click the **X** next to the account name and perform a new search.

Use the Asset Exposure mode:

1. In the search box, type the name of the sensitive server (e.g., "srv-fin").
2. Select the object from the list and click the magnifying glass icon.
3. Explore the asset exposure to the selected sensitive server.
4. Use similar options as in Blast Radius mode.
5. Hover over paths to view details.

6. Toggle the option to show all node tooltips.
7. Adjust the view using the bottom bar.

Use the Attack Path mode:

1. In the starting point search box, type the name of the compromised account (e.g., "John Doe").
2. Click the account name.
3. In the arrival point search box, type the name of the sensitive asset (e.g., "s or v-fin").
4. Click the asset name.
5. Click the magnifying glass icon.
6. Explore the available attack paths between the compromised account and the sensitive asset.
7. Use similar options as in Blast Radius and Asset Exposure modes.

Additional capabilities:

- **Who has control over my privileged assets**: Shows all user and computer accounts that have an attack path leading to a privileged asset.
- **What are my privileged assets**: Lists tier zero assets and accounts with potential attack paths leading to those assets.
- Switch between tabs to view the lists.
- Click the magnifying glass icon next to an item to switch the view.
- Click the blue arrow and dot icon to open the asset exposure view filtered to show only this asset.

Interpret results:

1. Use the Attack Path feature to confirm hypotheses and visualize dangerous attack paths between entities.

2. Take remediation actions to close identified attack paths.

Essential Basics in Tenable Identity Exposure

This section covers the essential, day-to-day tasks that most users need to know to get started and take full advantage of Tenable Identity Exposure.

Whether you're new to the product or just need a refresher on the basics, you'll find step-by-step instructions here for common operations like authentication, navigating the workspace, setting preferences and notifications, using dashboards and widgets, exploring identities with the Exposure Center, visualizing data trails with Trail Flow, and understanding Indicators of Exposure and Indicators of Attack.

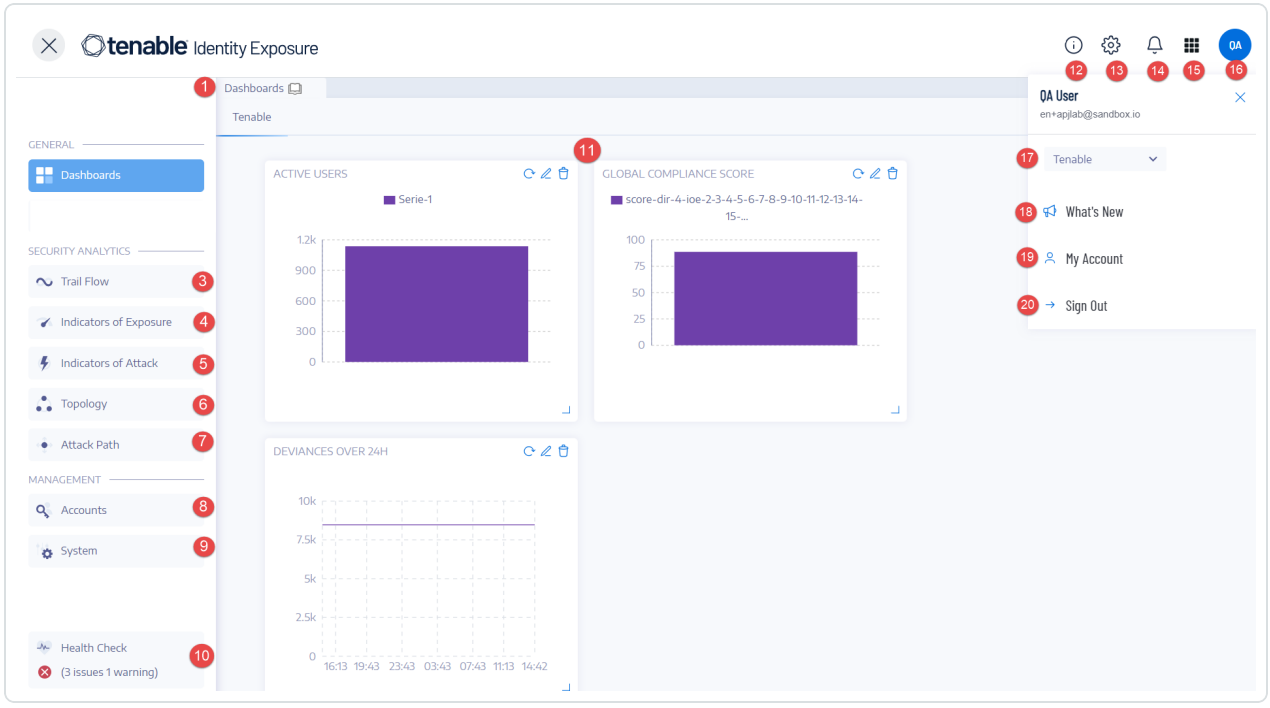
To find information related to a specific task, click on the relevant topics in the menu pane on the left side of the screen.

Tenable Identity Exposure User Portal

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 ✕ 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	-	-
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.

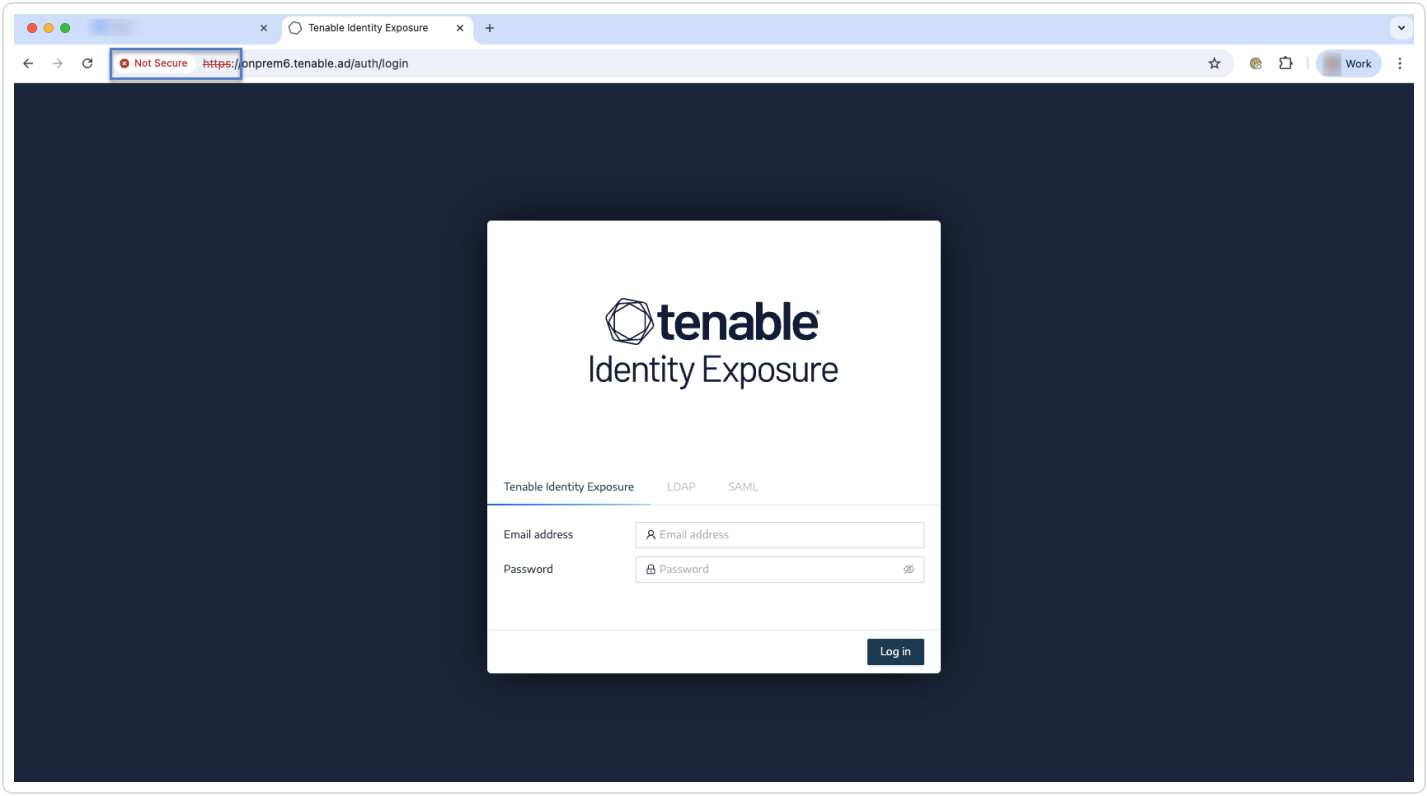
		• Attack Path: Anticipates privilege escalation techniques to reach an asset from a specific entry point. • Asset Exposure: Measures an asset's vulnerability using asset exposure visualization and tackles all escalation paths.
8, 9	Management **Required User Role**: Organizational User with appropriate 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 Configuration and Administration.
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,

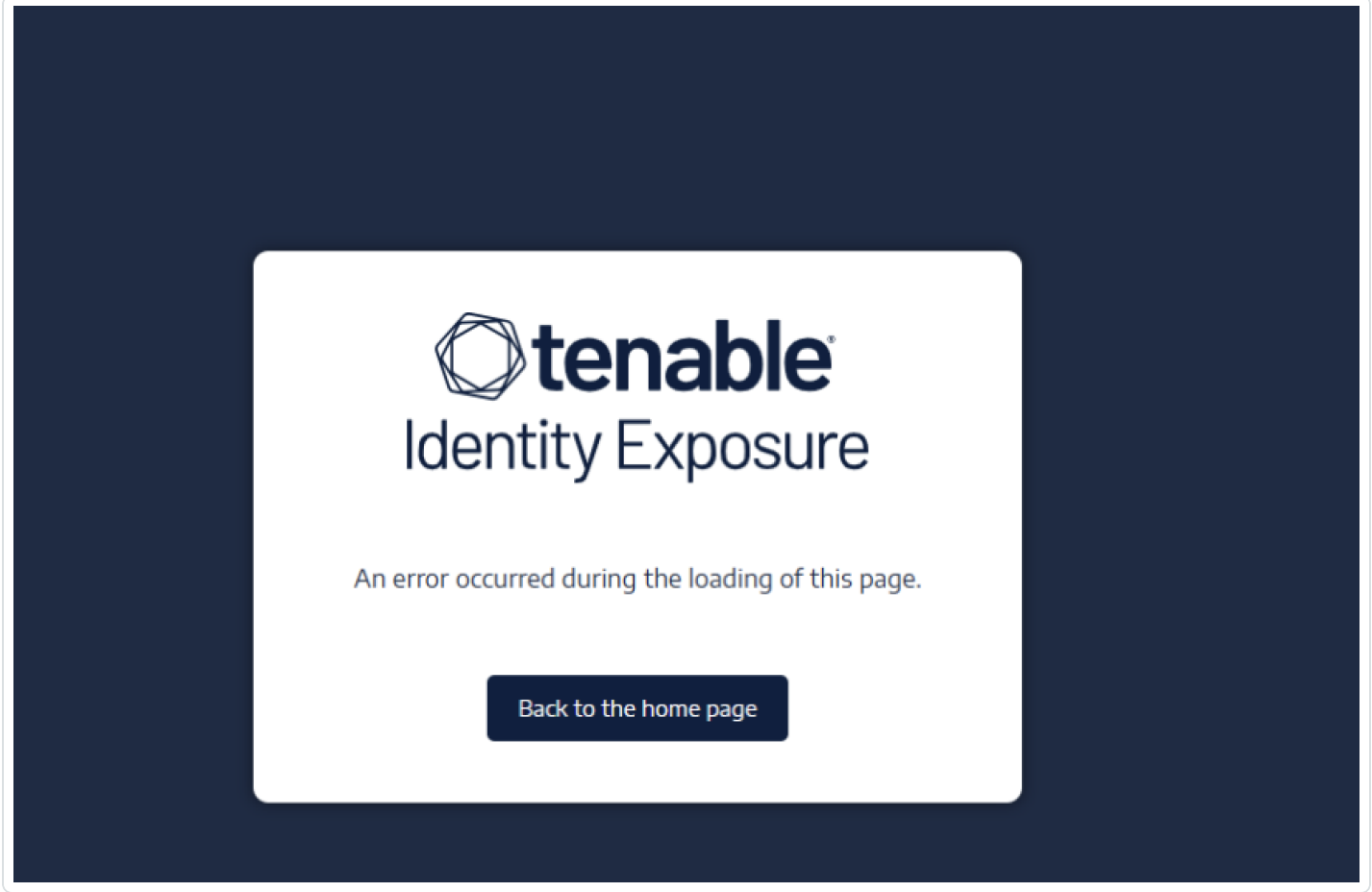
		forest and domain management, license, user and role management, profiles, and activity logs.
14	Notifications (Bell)	A bell icon and badge counts notify you of attack alerts and/or exposure alerts waiting for your acknowledgment.
15	Access the Workspace	Click this icon to switch between applications 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.

Trusted Certificates

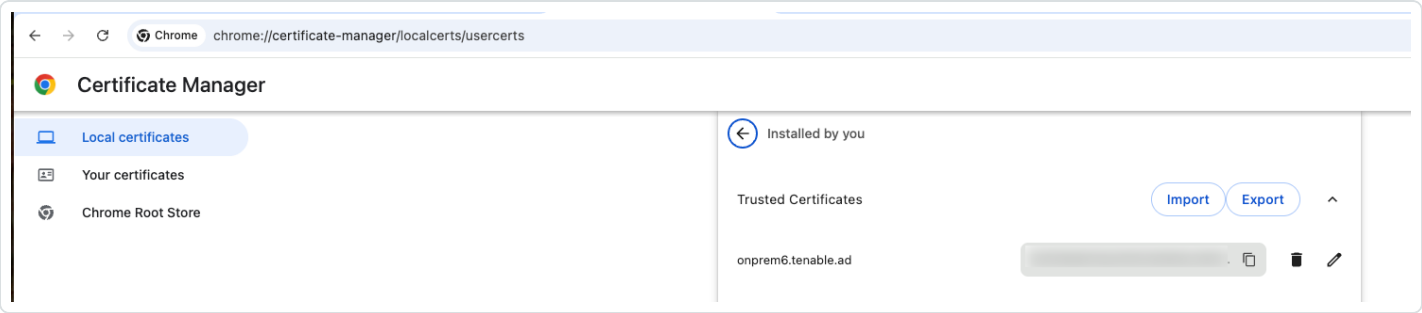
If the browser used to log in to Tenable Identity Exposure does not trust the Tenable Identity Exposure certificate, there may be errors when logging in or when navigating the user interface. To ensure that there are no errors, you must use a trusted Web Certificate for the domain or import the Tenable Identity Exposure certificate into the browser's Trusted Certificates.

The following example shows a login error.


Tenable Identity Exposure
Not Secure
https://onprem6.tenable.ad/auth/login
Work
tenable
Identity Exposure
Tenable Identity Exposure
LDAP
SAML
Email address
Email address
Password
Password
Log in


tenable
Identity Exposure
An error occurred during the loading of this page.
Back to the home page

The following image shows the manual import of the certificate to the Chrome browser's Trusted Certificates.



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

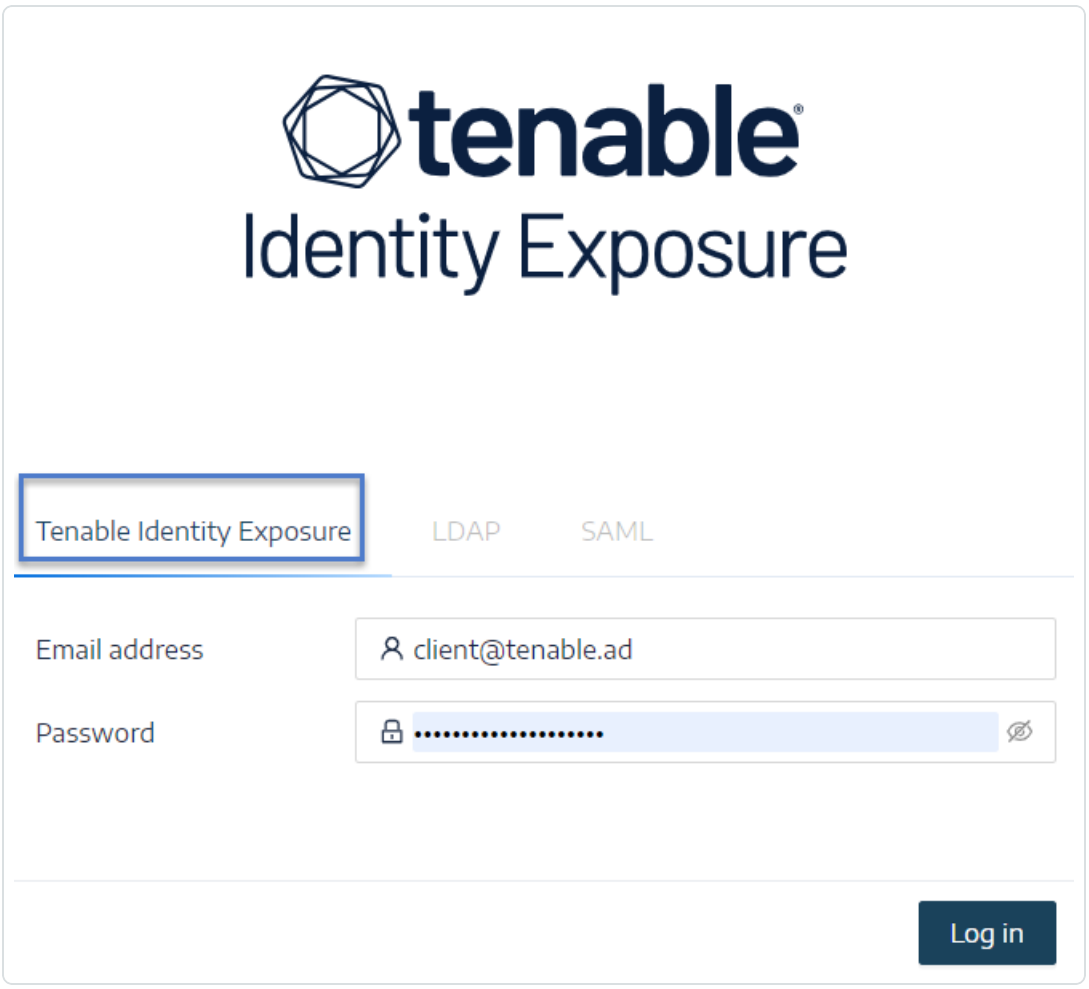
Note: Your initial credentials with the username `hello@tenable.ad` and the password `verySecure1.`

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.



2. Click the **Tenable Identity Exposure** tab.
3. Type your email address.
4. Type your password.
5. Click **Log in**.

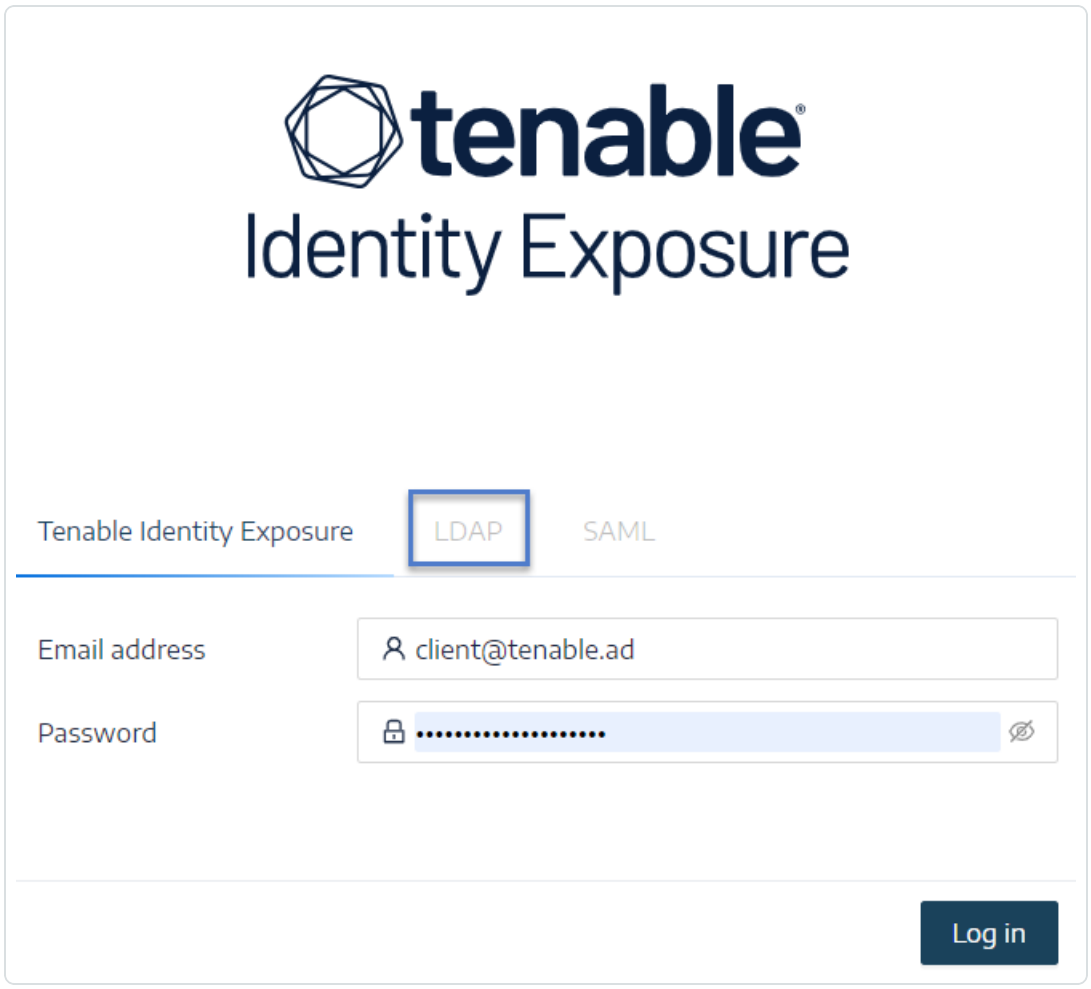
   The Tenable Identity Exposure page opens.

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.



2. Click the **LDAP** tab.
3. Type your LDAP account name.
4. Type your LDAP password.
5. Click **Log in**.

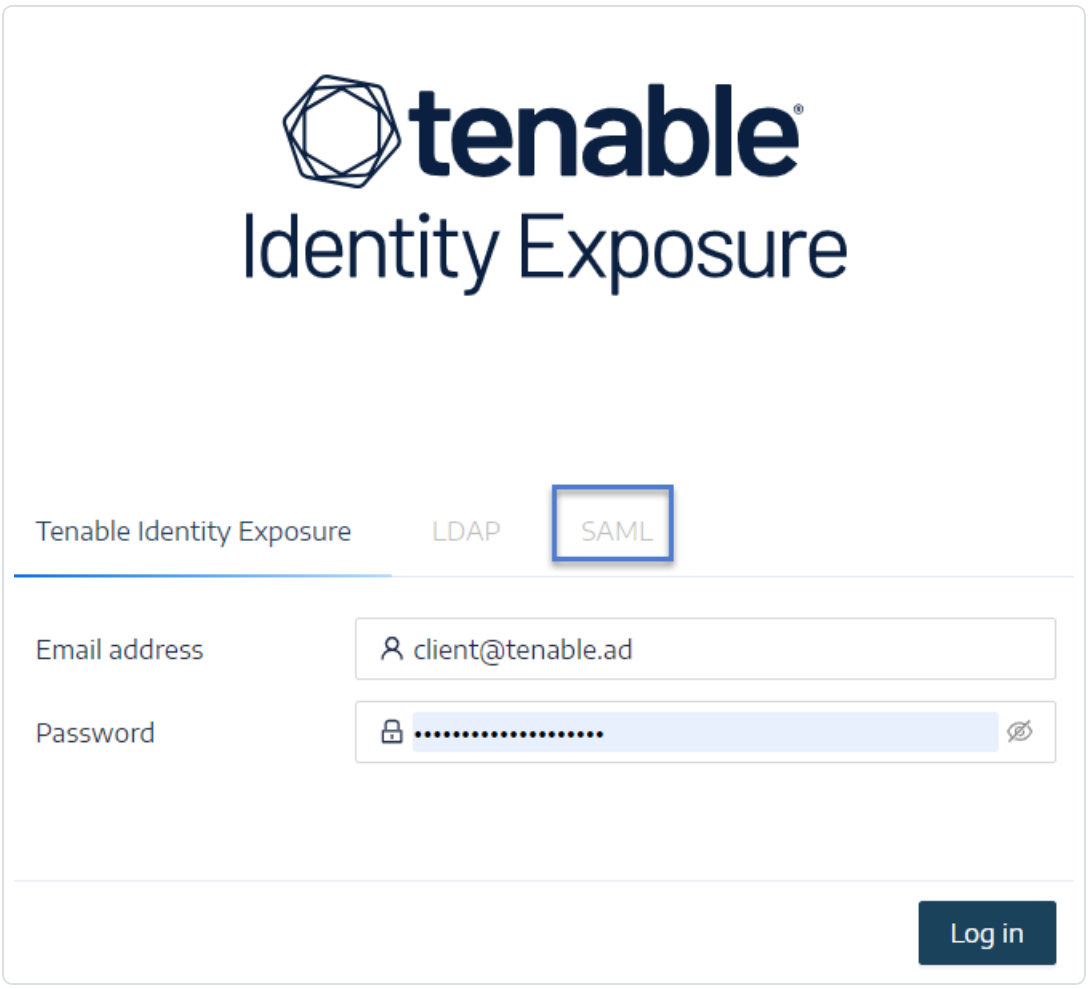
   The Tenable Identity Exposure page opens.

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.

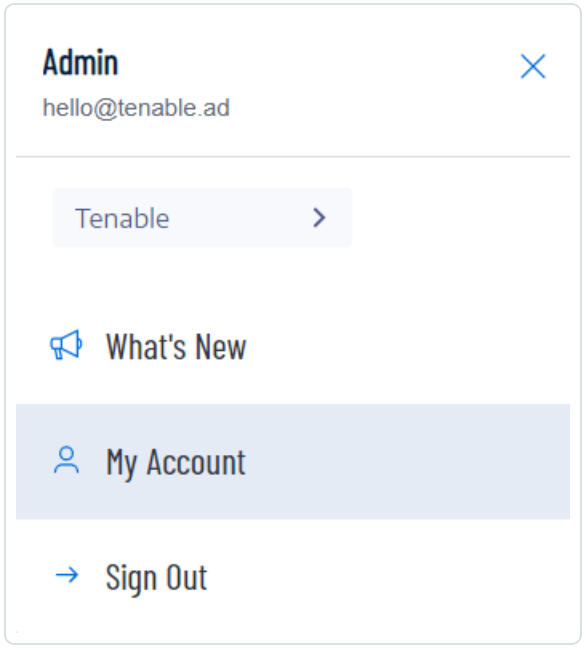
To reset your password after the first login:

When logging in for the first time with the `hello@tenable.ad` account, Tenable Identity Exposure prompts you to reset your default 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.

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

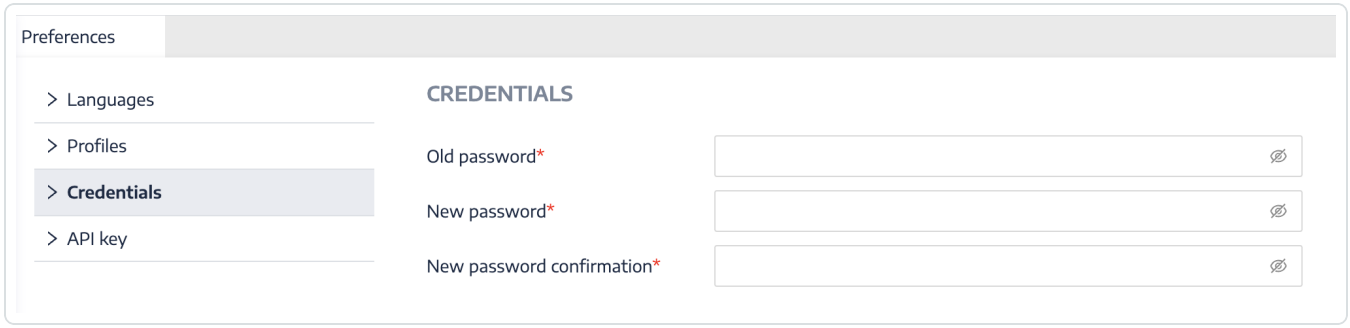
   A submenu appears.



2. Select **My Account**.

   The **Preferences** page appears.

3. Under **Preferences**, click **Credentials**.



4. In **Old password**, type the old password.

5. In **New Password**, type a new password. Adhere to the following password complexity rules, which align with those required for Tenable One accounts:
    - Must be at least 12 characters long.
    - Must contain at least one of each of the following:
        - Uppercase letter (A-Z)
        - Lowercase letter (a-z)
        - Number (0-9)
        - Special character (e.g., !, @, #, $)
    - Cannot contain the string `verysecure` to prevent the reuse of the previous default password `verySecure1!`.
6. In the **New password confirmation** box, retype the new password.
7. Click **Save**.

    A message confirms that Tenable Identity Exposure changed your password.

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.

The **Workspace** menu, which appears in the top navigation bar, allows you to quickly switch between your Tenable applications from any page.

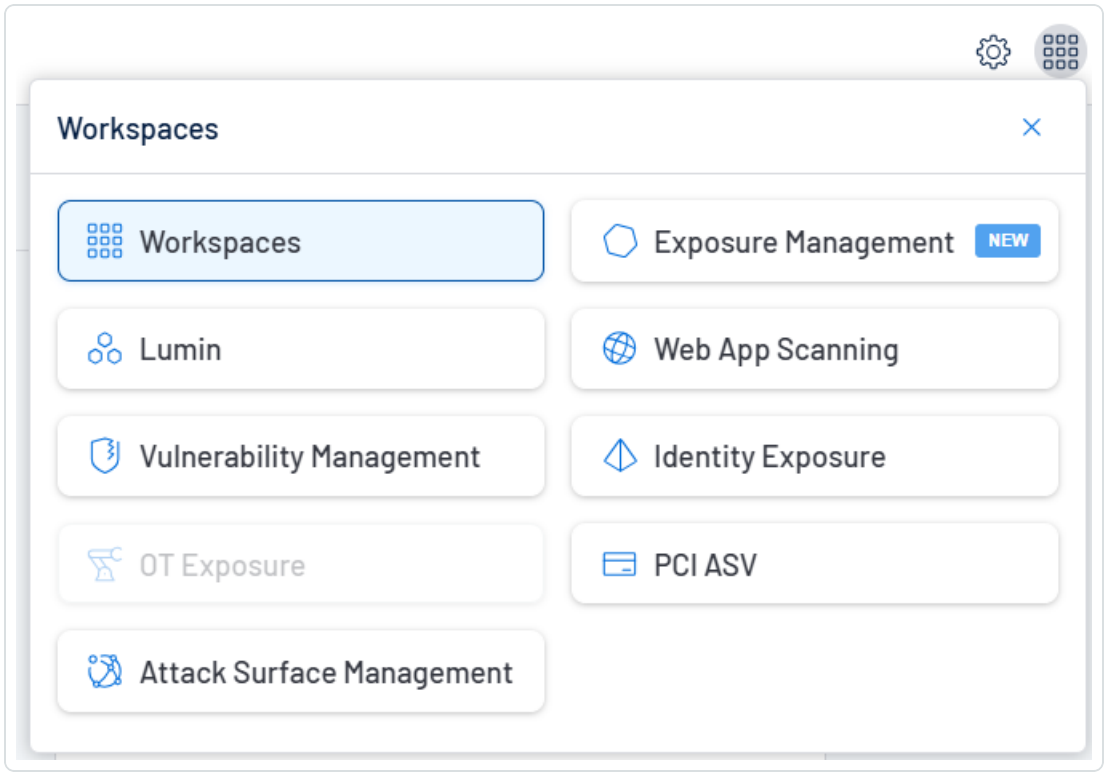
Important: Tenable disables application tiles for expired applications. Tenable removes expired application tiles from the **Workspace** page and menu 30 days after expiration.

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.

Workspace Page

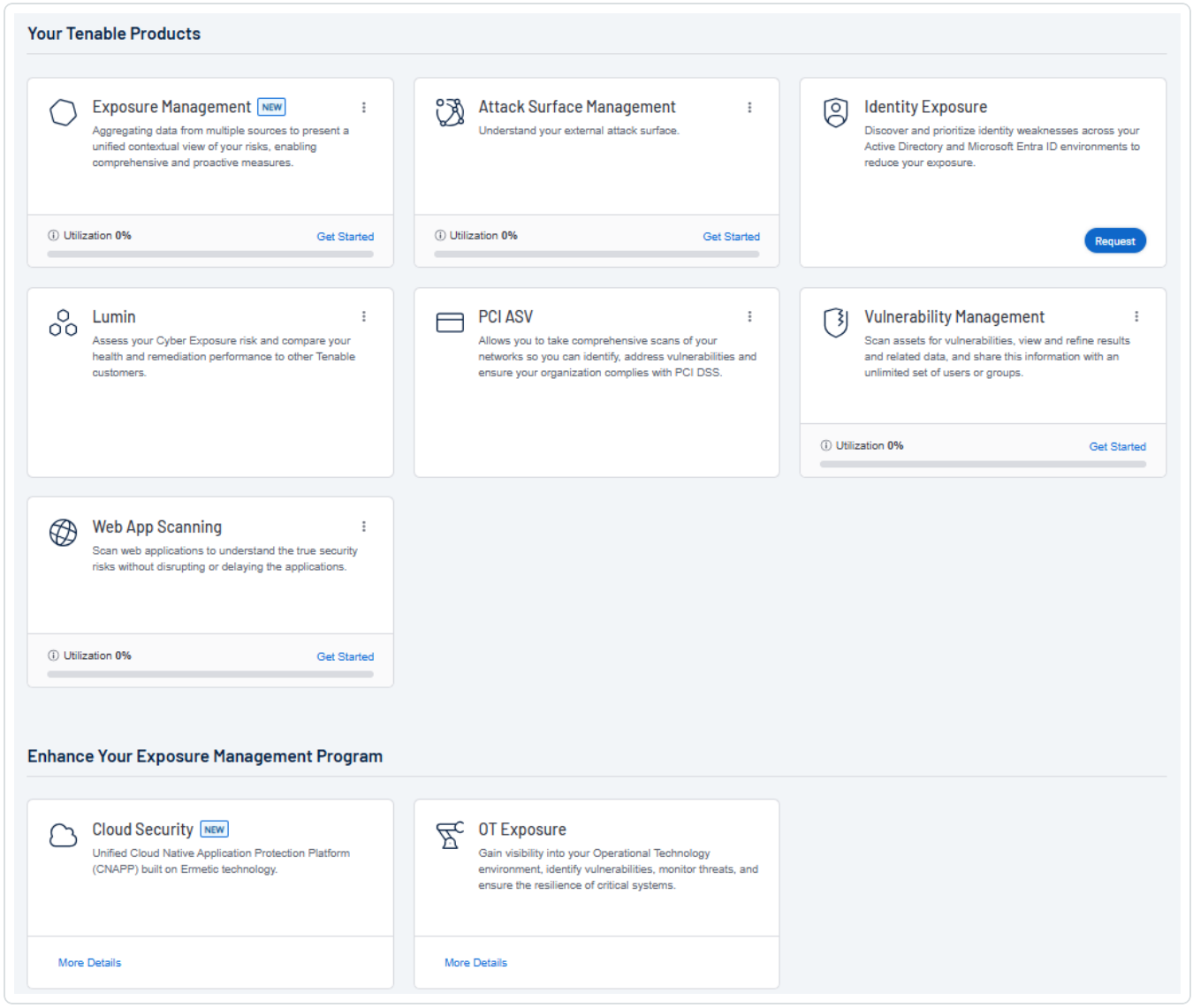
To view the Workspace page:

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

   The **Workspace** menu appears.

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

The **Workspace** page appears.



On the **Workspace** page, you can do the following:

- Where applicable, at the bottom of a tile, view the percentage of your license utilization for the application. Click **See More** to navigate directly to the **License Information** page for the selected application.

  Tip: For more information on how Tenable licenses work and how assets or resources are licensed in each product, see Licensing Tenable Products.

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

   A menu appears.

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

   A menu appears.

2. Click **Remove Default Login Page**.

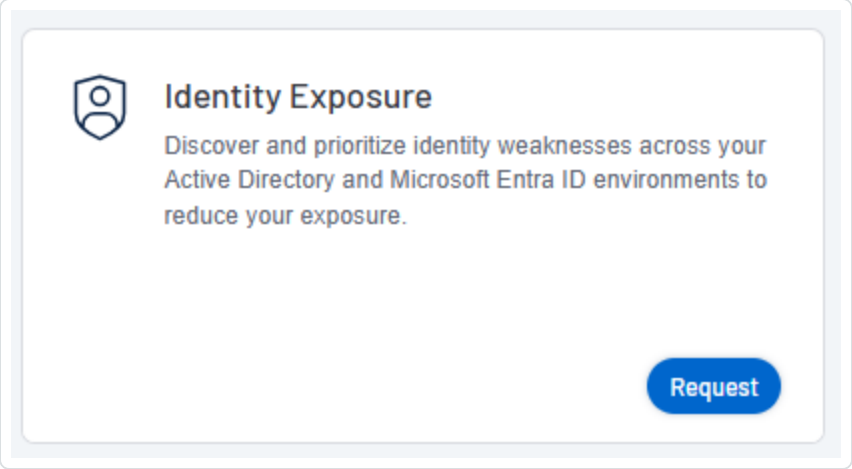
   The **Workspace** page now appears when you log in.

- **Request Access to a Tenable application:**

Some applications, like Tenable Identity Exposure, require you to request access to the application. You can do this directly via the **Workspace** page.

To request access to a Tenable application:

1. In the lower-right corner of the tile, click **Request**.



You navigate directly to the request page for the selected application.

User Preferences

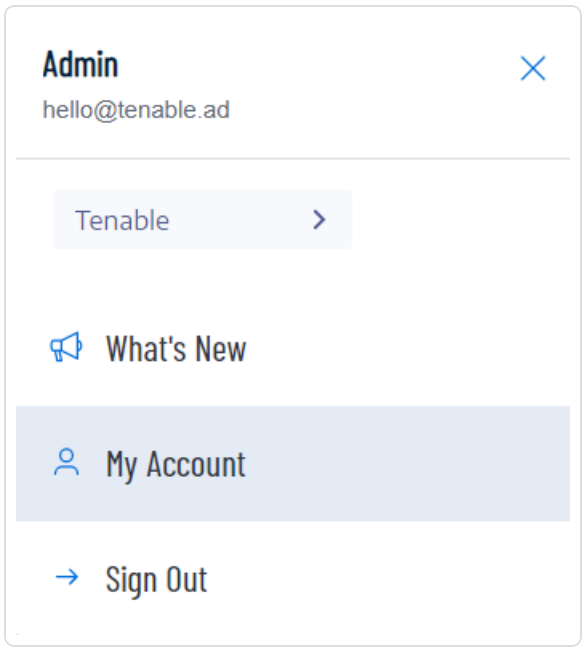
You can set your user preferences in Tenable Identity Exposure.

- 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. In **Old password**, type the old password.

c. In **New Password**, type a new password. Adhere to the following password complexity rules, which align with those required for Tenable One accounts:

- Must be at least 12 characters long.
- Must contain at least one of each of the following:
  - Uppercase letter (A-Z)
  - Lowercase letter (a-z)
  - Number (0-9)
  - Special character (e.g., !, @, #, $)
- Cannot contain the string `verysecure` to prevent the reuse of the previous default password `verySecure1!`.

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

e. 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:

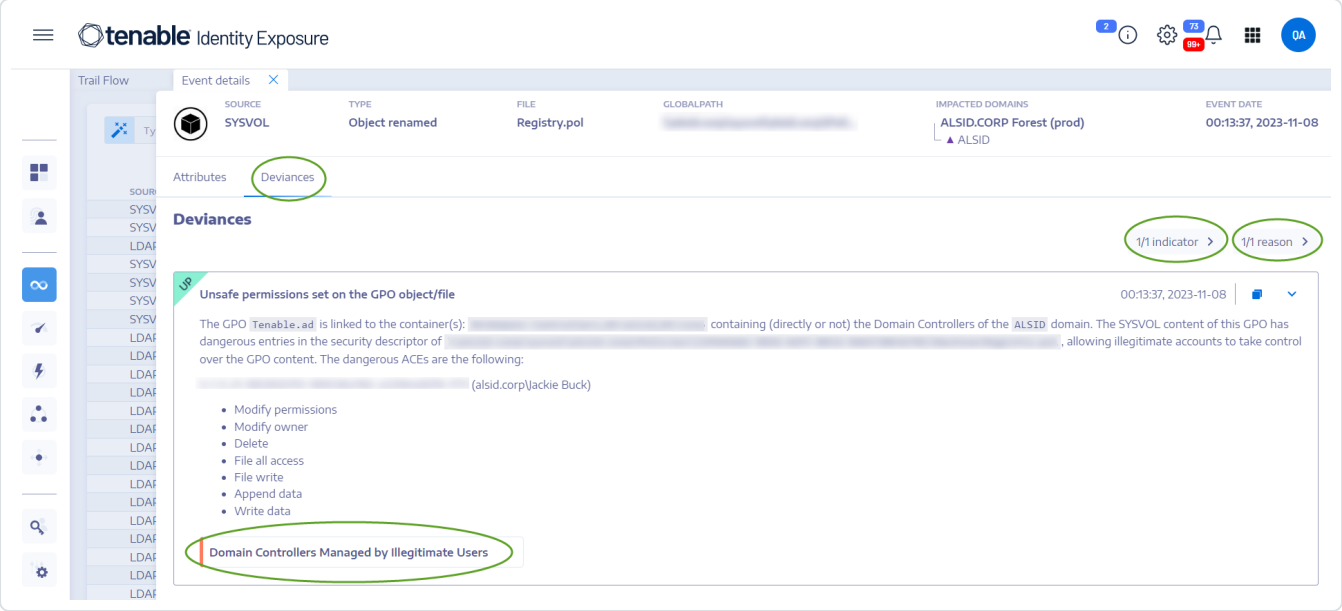
1. Select an alert from the list and click **Actions> See the deviance**.

   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.



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:

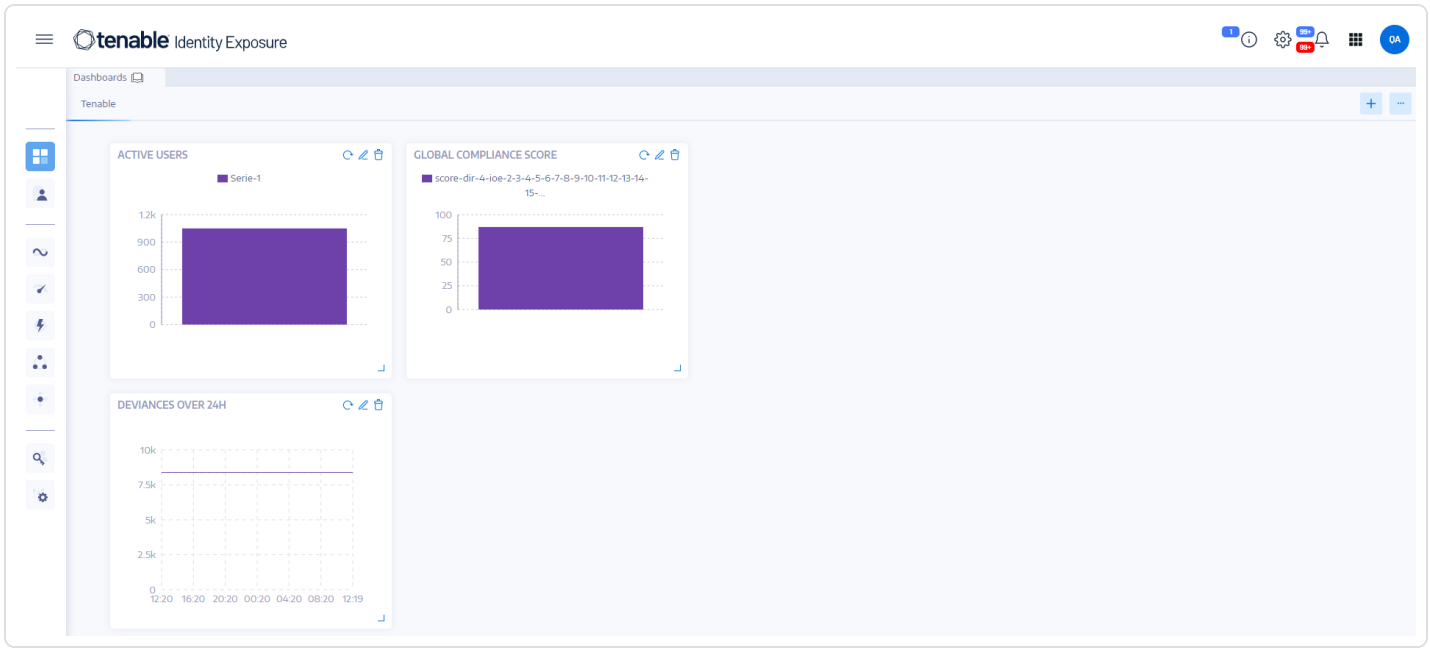
After you view the alert, you can archive it.

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.

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



Key Dashboard Features

- **At-a-glance overview**: Get a rapid pulse check on your security state, with key metrics like compliance score, top risks, and user activity trends displayed prominently.
- **Drilling down into details**: Dive deeper into specific areas with interactive widgets that break down risk factors by severity, user category, and other relevant criteria.
- **Customizable focus**: Build personalized dashboards tailored to your priorities, using pre-built templates or crafting your own layouts. For example, for creating a dashboard for popular misconfiguration against common recurring IoEs:
    - Ensure SDProp Consistency
    - Domain Controllers Managed by Illegitimate Users
    - Dangerous Kerberos Delegation
- **Real-time monitoring**: Stay informed of emerging threats and suspicious activity with continuous updates and alerts.
- **Actionable insights**: Gain practical recommendations for remediation, prioritized based on severity and potential impact.

Dashboard Templates

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.

See also

- Dashboards
- Video tutorial on dashboards

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.

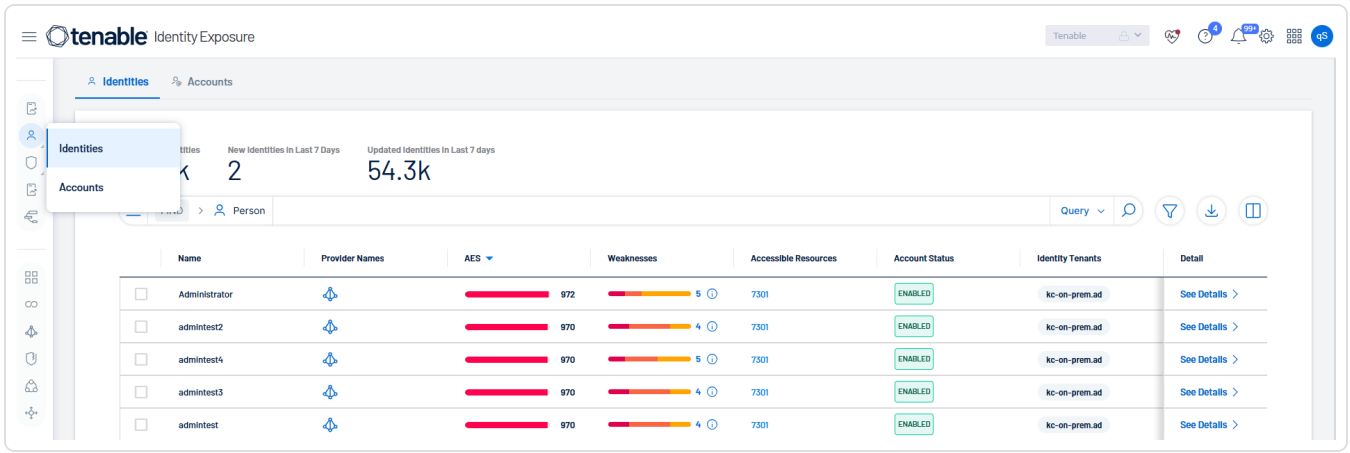
Tenable Identity Exposure's Identity Explorer view unifies identities across both Active Directory and Microsoft Entra ID . This view shows the Identity Risk Score (beta) for each listed asset and the potential reach of compromised identities.

To access the Identity Explorer:

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

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

  The **Identity Explorer** pane opens.



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

- **Name** – Name of the user account under the identity provider.
- **Provider Names** – The Identity Provider.
- **AES** – Asset 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.

- **Weaknesses** – The percentage of aggregated weaknesses from the accounts linked to the identity, rated from 1 (low) to 5 (critical).
- **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.

The Trail Flow tracks the following events:

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

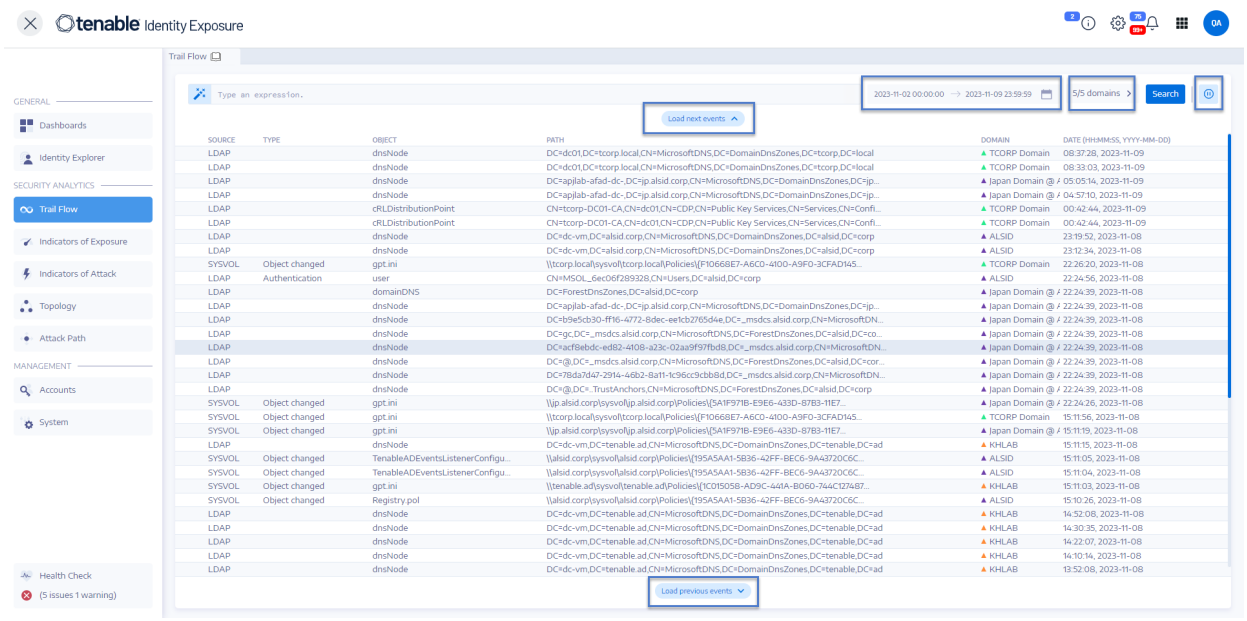
Tenable Identity Exposure offers these capabilities to leverage the Trail Flow data:

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

To access the Trail Flow:

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

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



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**

How does the data appear in the Trail Flow?

1. When you perform an action within your Active Directory (AD) interface, such as:
   - Creating a new user account
   - Modifying a user's group membership
   - Resetting a password
   - Disabling an account
   - Enabling an account
   - Deleting an account
   - Moving an object
   - Modifying permissions

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

See also

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

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

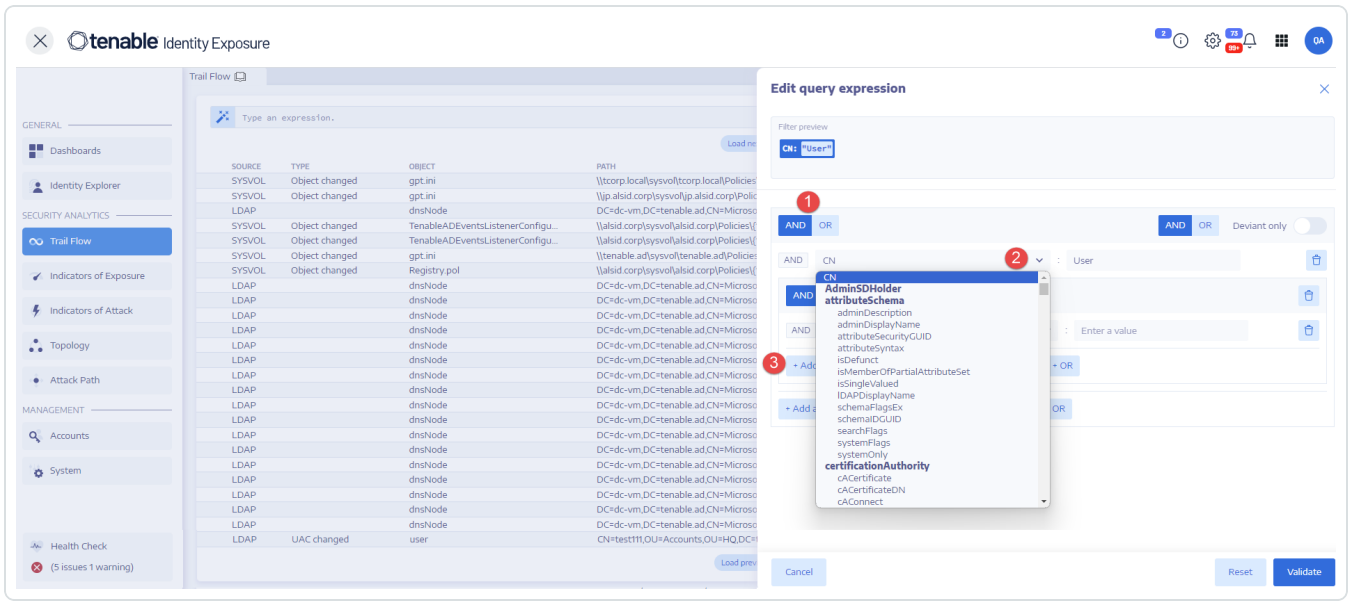
The search wizard allows you to create and combine query expressions.

- 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.



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**.

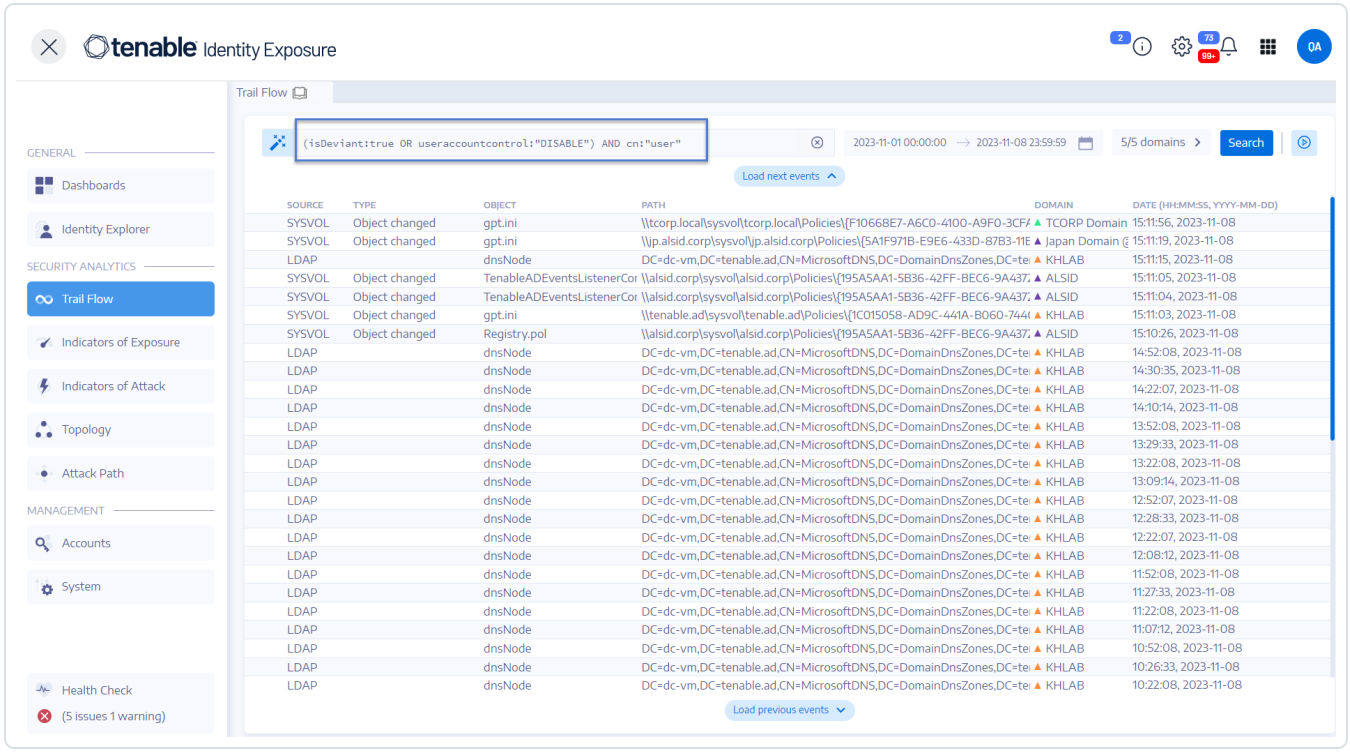
    Tenable Identity Exposure updates the list with the results matching your search criteria.

Tip: To search using other criteria, you can Search the Trail Flow Using the Wizard

Example:

The following example searches for:

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

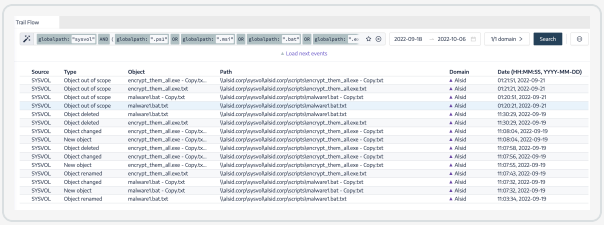


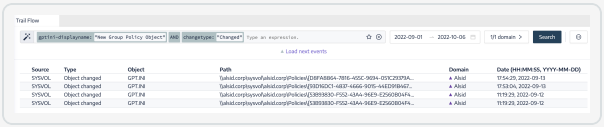
Customize Trail Flow Queries

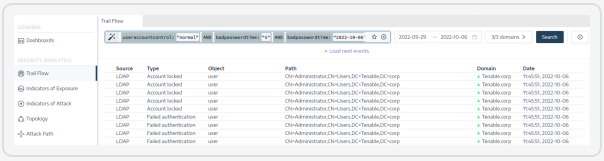
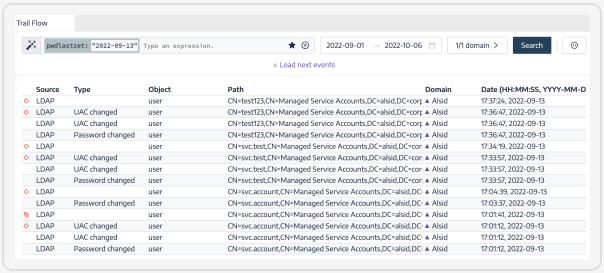
The Trail Flow allows you to extend Tenable Identity Exposure capabilities beyond the default monitoring of Indicators of Exposure and Indicators of Attack. You can create custom queries to retrieve data quickly and also use the query as a custom alert that Tenable Identity Exposure can send to your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

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

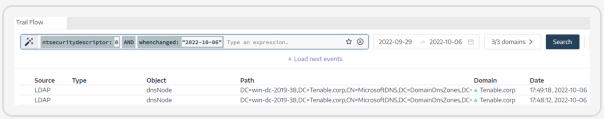
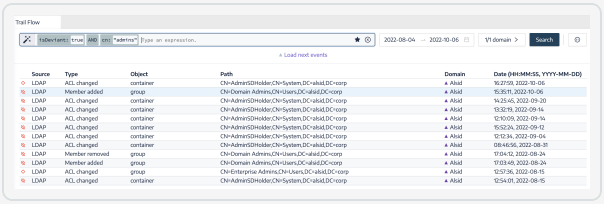
Use Case	Description
GPO Startup and Shutdown binaries and Global SYSVOL path monitoring	Monitors for scripts in the boot startup path and/or the Global SYSVOL replication path. Attackers often use these scripts to abuse native AD services to proliferate ransomware quickly across an environment. • **Scripts 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")`
	
	 

Modifications of GPO Configuration	Monitors for modifications to GPO configurations. Attackers often use this method to downgrade security settings to aid in persistence and/or account takeover. • **GPO monitoring query:** `gptini-displayname:"New Group Policy Object" AND changetype:"Changed"` 
Failed Authentication and Password Reset	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>"`
	
	 
	
	• **Password reset query:**
	
	`pwdlastset:"<DATE_TIME_STAMP"`
	
	 

Object Permissions Added, Removed, or Changed	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"`

	
Changes to Admins Resulting in a Deviance	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"` 

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.



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

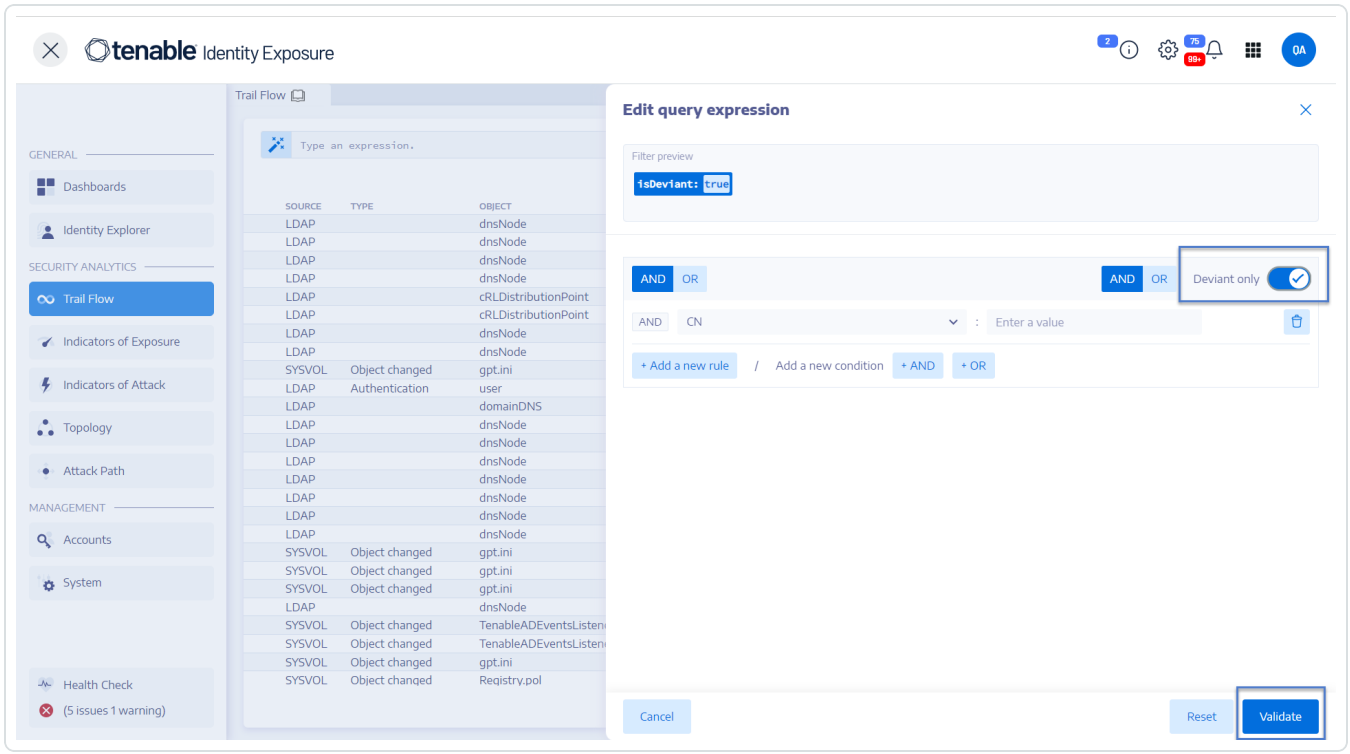
Display Deviant Events

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

To display only deviant events:

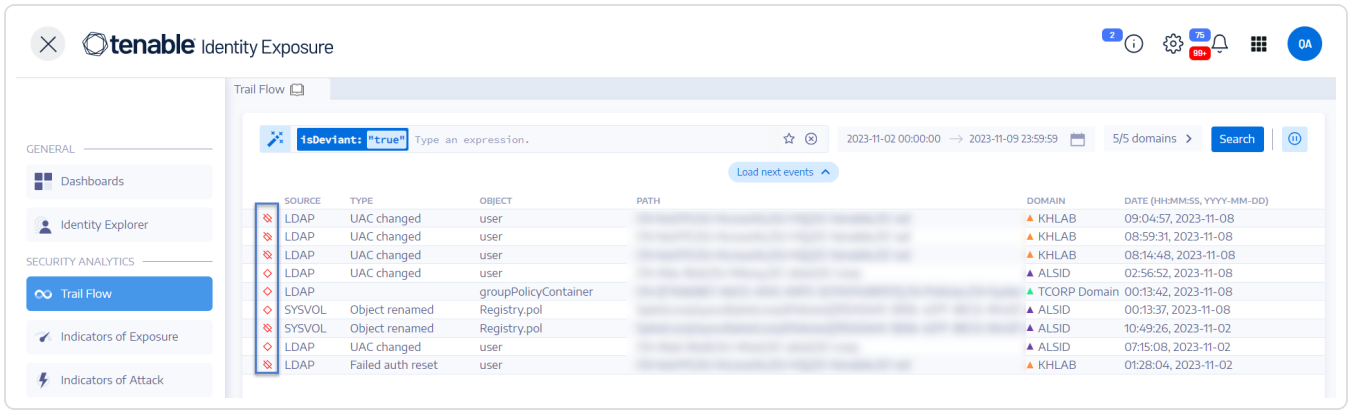
1. In Tenable Identity Exposure, click **Trail Flow** to open the Trail Flow page.
2. Click the icon next to the Search box.

   The **Edit Query Expression** pane opens.



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.



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.

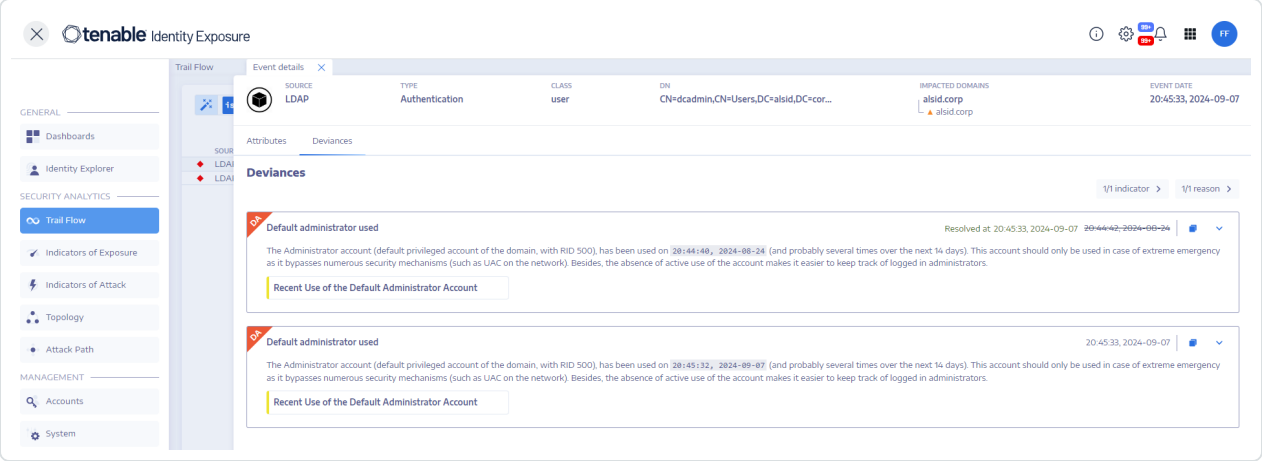
To view event details:

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. For more information, see Indicators of Exposure.



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.

Tenable Identity Exposure ties a deviance to a root object and can link it to multiple incriminating attributes. When you resolve one of these attributes, Tenable Identity Exposure resolves the deviance on the root object. It then creates a new deviance for the root object, keeping the same reason but including only the unresolved attributes.

For example, Tenable Identity Exposure ties a deviance to object **A** for a single reason that connects to multiple related objects (**B**, **C**, and **D**). When you resolve the incriminating attribute on object **C**, Tenable Identity Exposure resolves the deviance on object **A**. Then, it creates a new deviance for object **A**, linking it to the same reason but including only objects **B** and **D**.

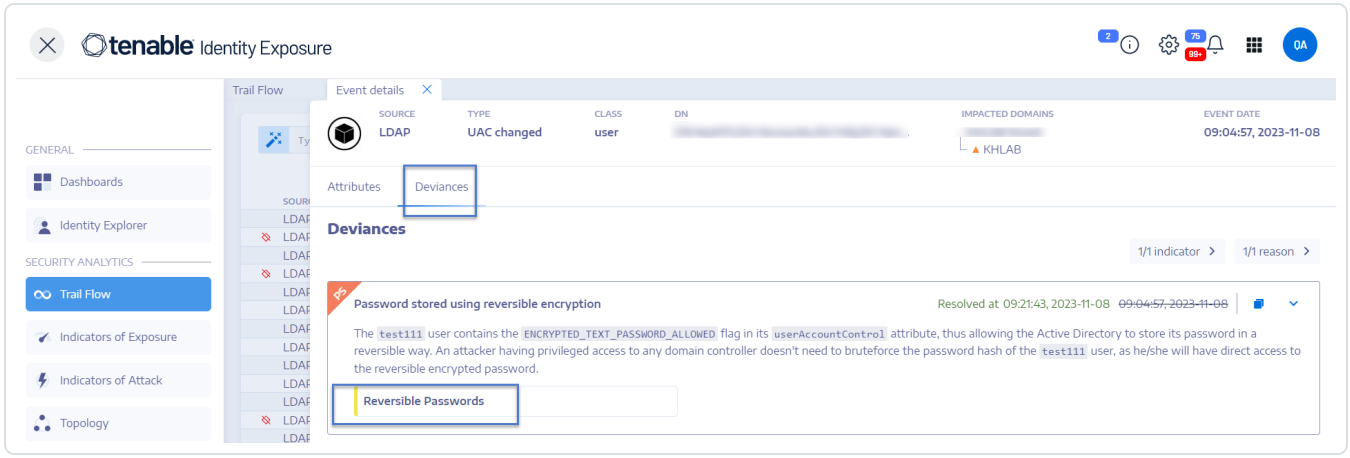
During this process, Tenable Identity Exposure can generate a Trail Flow event that shows multiple deviances as resolved and reopened at the same timestamp.

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.



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.

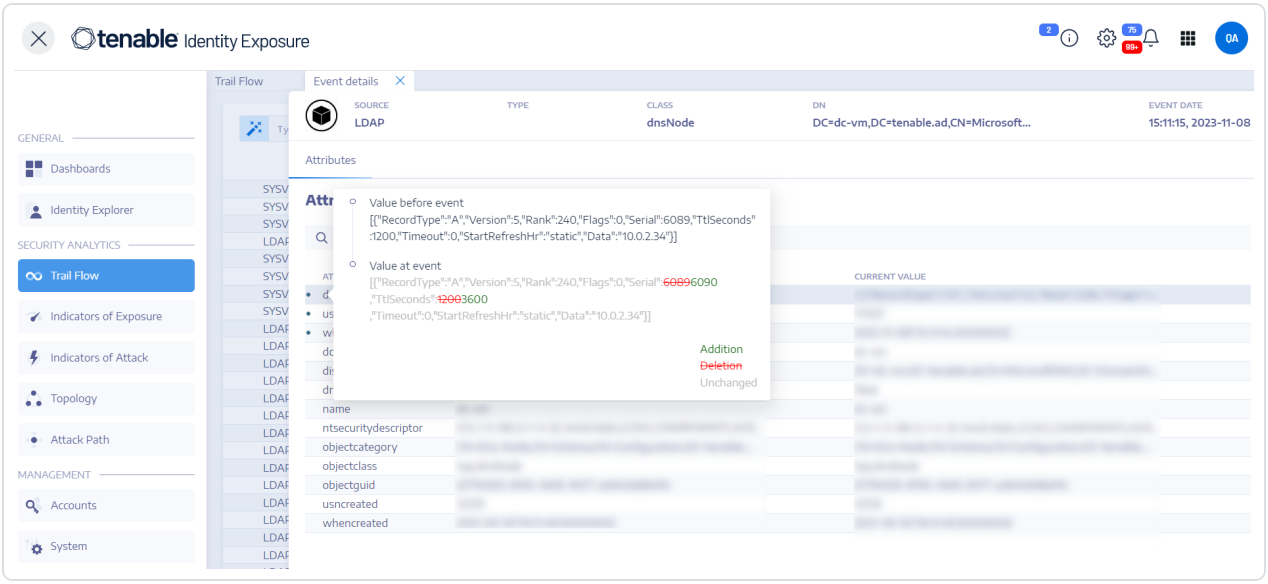
   The **Trail Flow** page opens with a list of events

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**



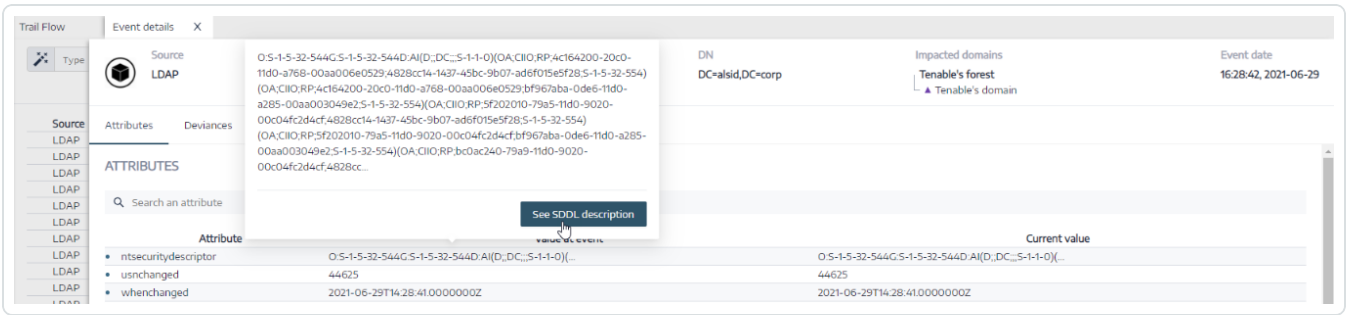
Attribute "ntsecuritydescriptor"

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.

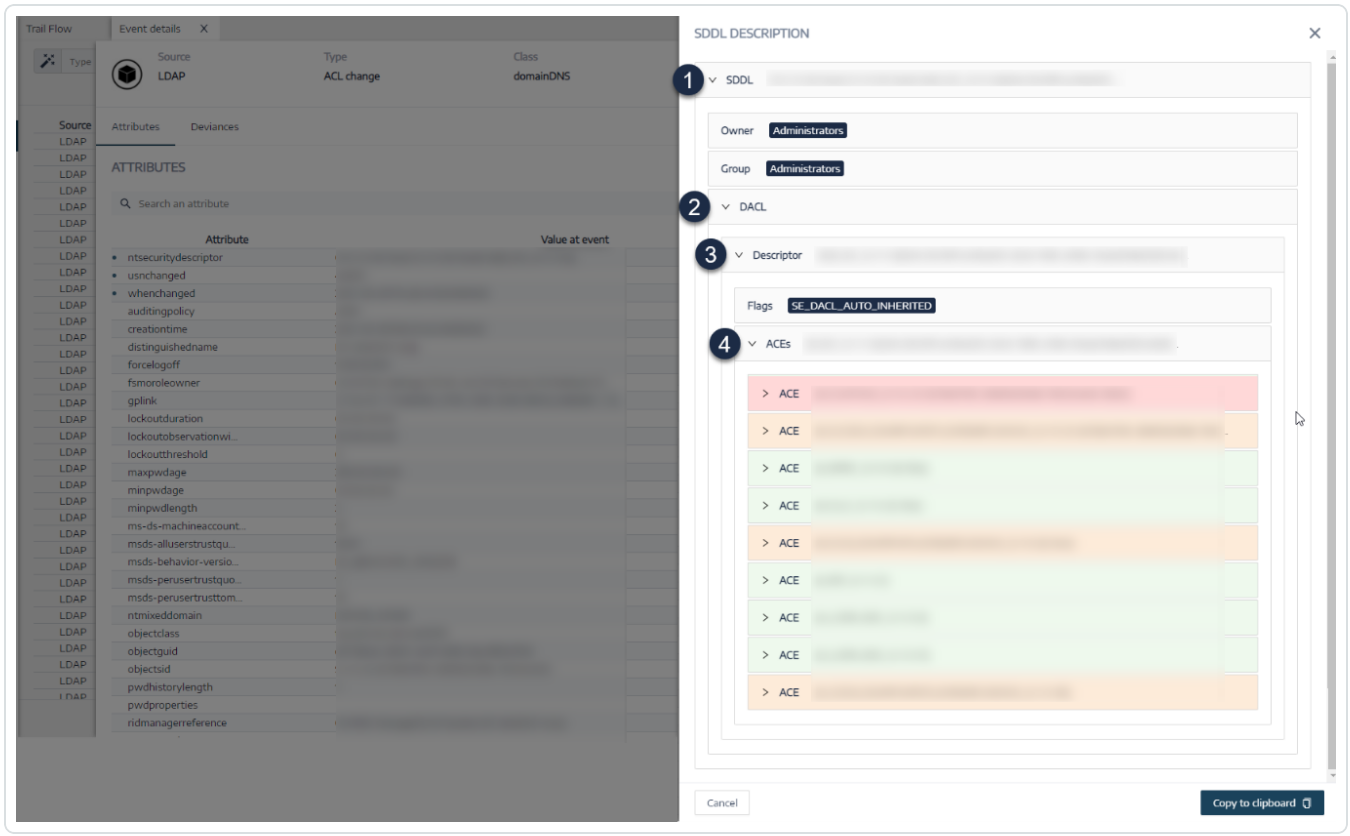
   The **Event details** pane opens.
3. Hover over the `ntsecuritydescriptor` attribute entry (Value at event or Current value column) **.



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

   The n**SDDL Description** pane opens.

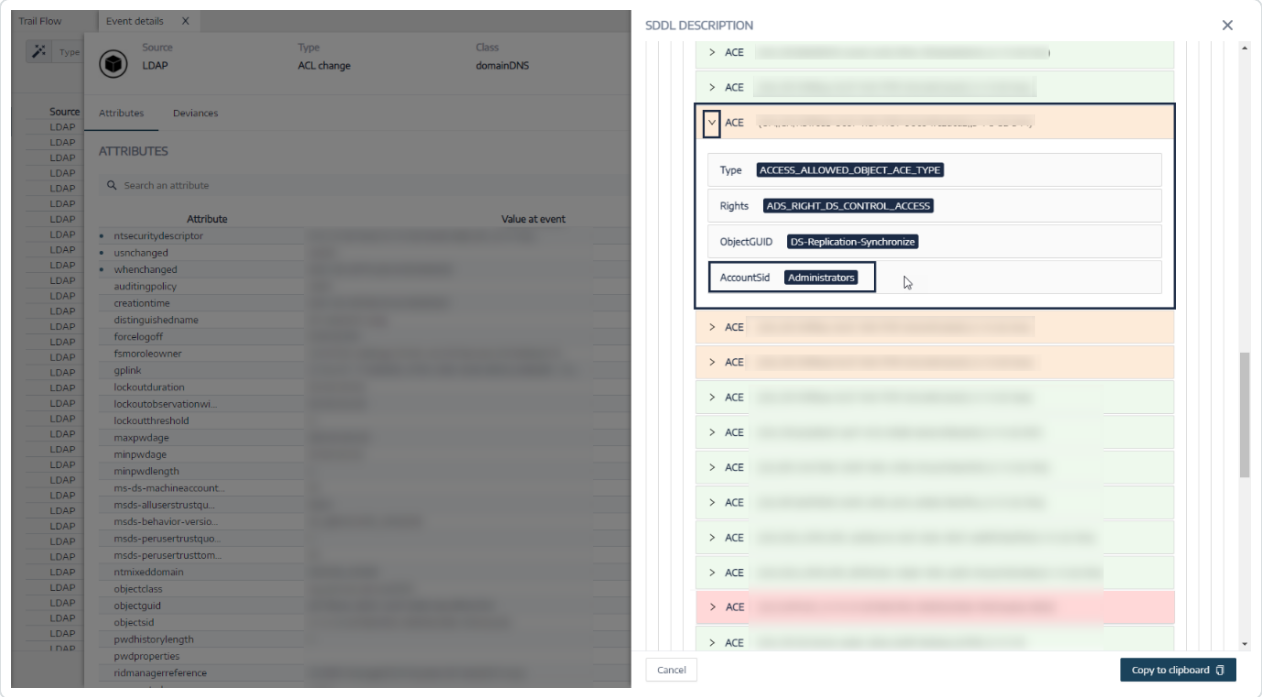
5. Click on the arrows on the left of the SDDL (1), DACL (2), and Descriptor (3) to expand the description:



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.



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

Trail Flow Use Cases

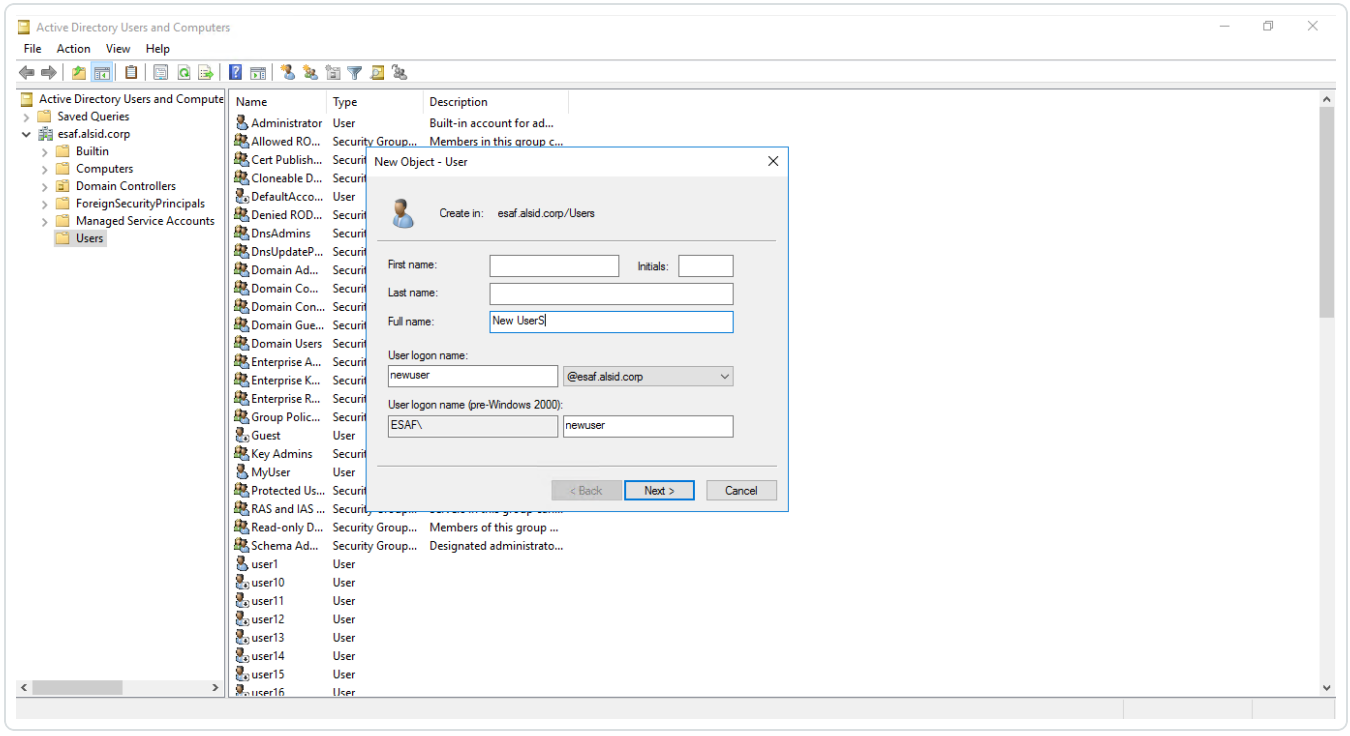
To understand the Trail Flow behavior, two examples illustrate how an operation that you perform in your Active Directory (AD) interface reflects in the Trail Flow page.

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.

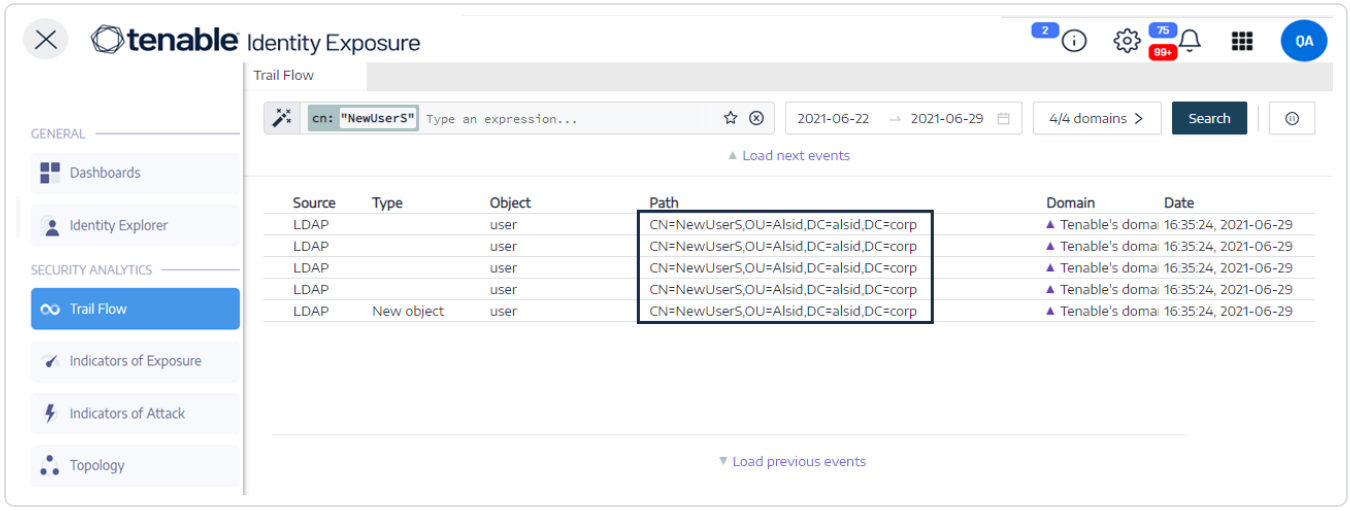
Note: These examples are not exhaustive and cannot cover every possible situation.

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.

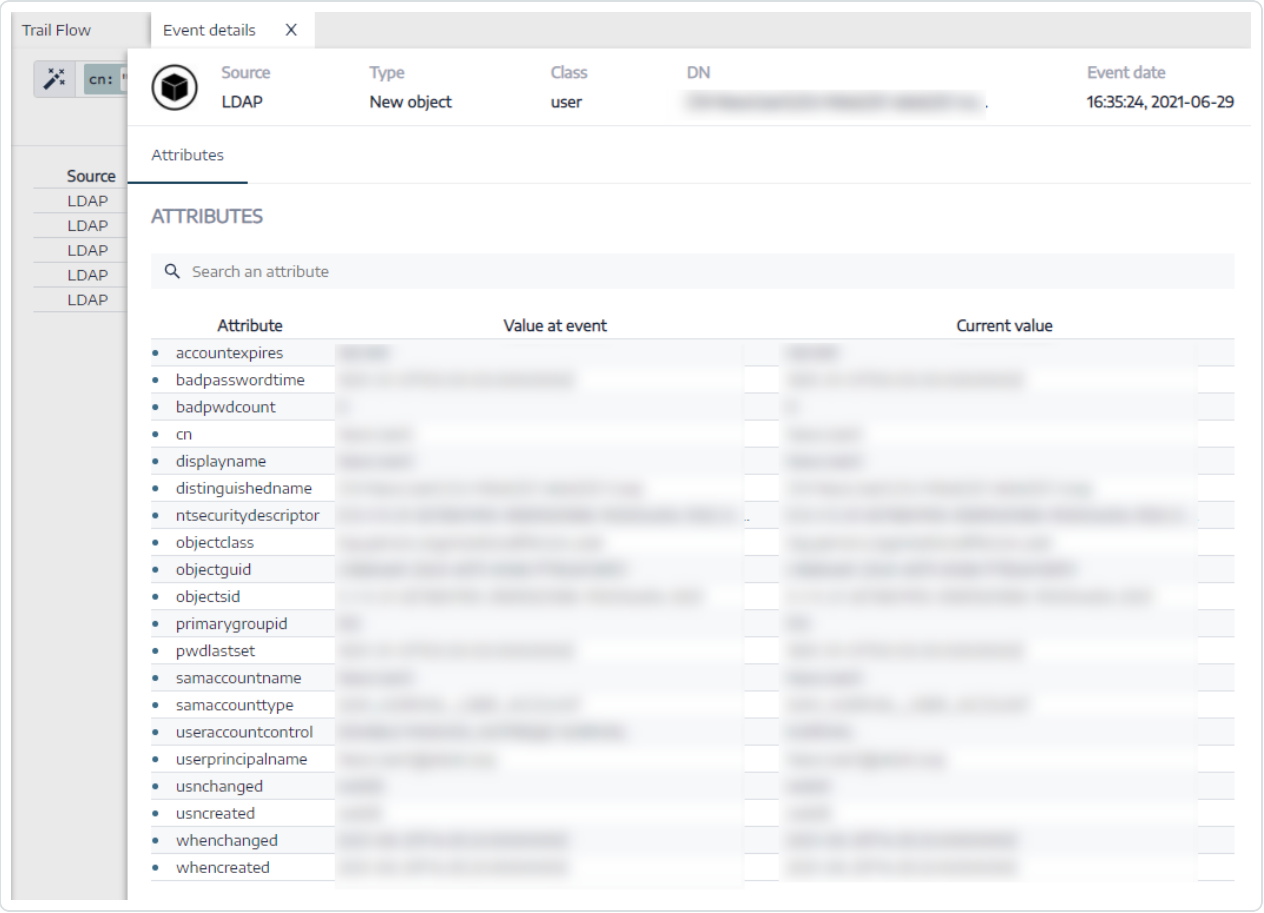


- On the end-user side, Tenable Identity Exposure updates the **Trail Flow** page. See the **Type** column indicating *New object*.



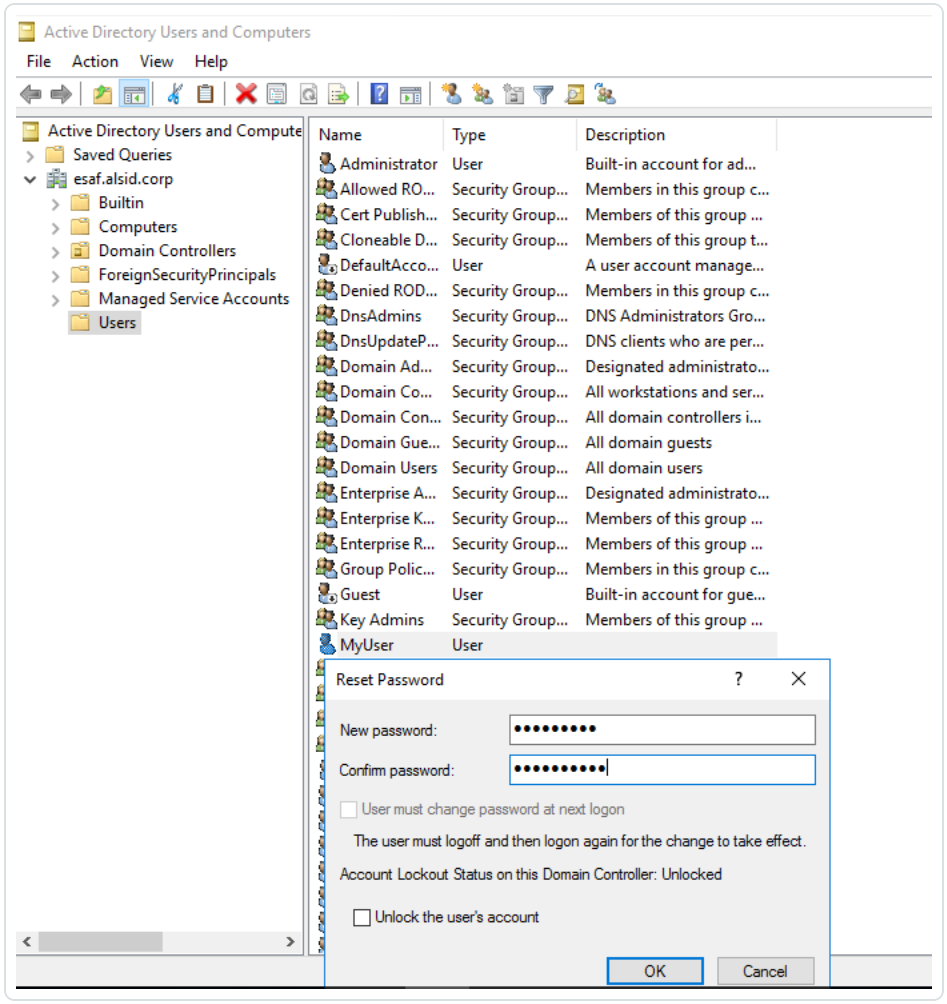
- The **Event details** page also reflects this change. The blue dots on the left of the attribute names indicate that an update occurred.

  For more details on attributes, see View Event Details.

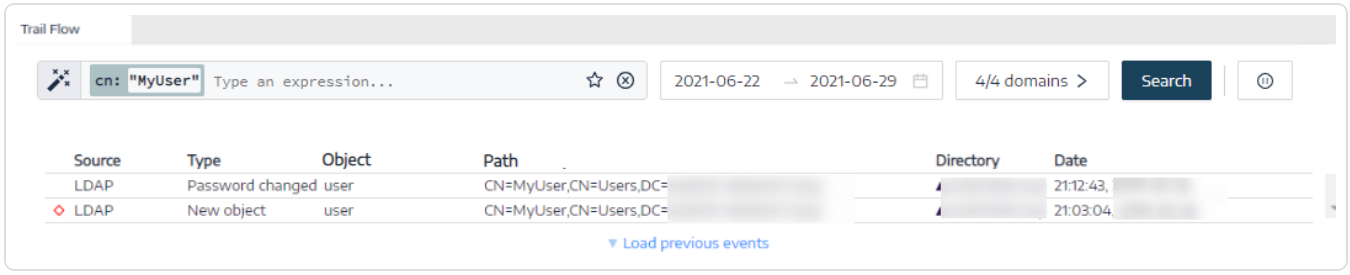


What happens in the Trail Flow when you change an AD user's password?

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

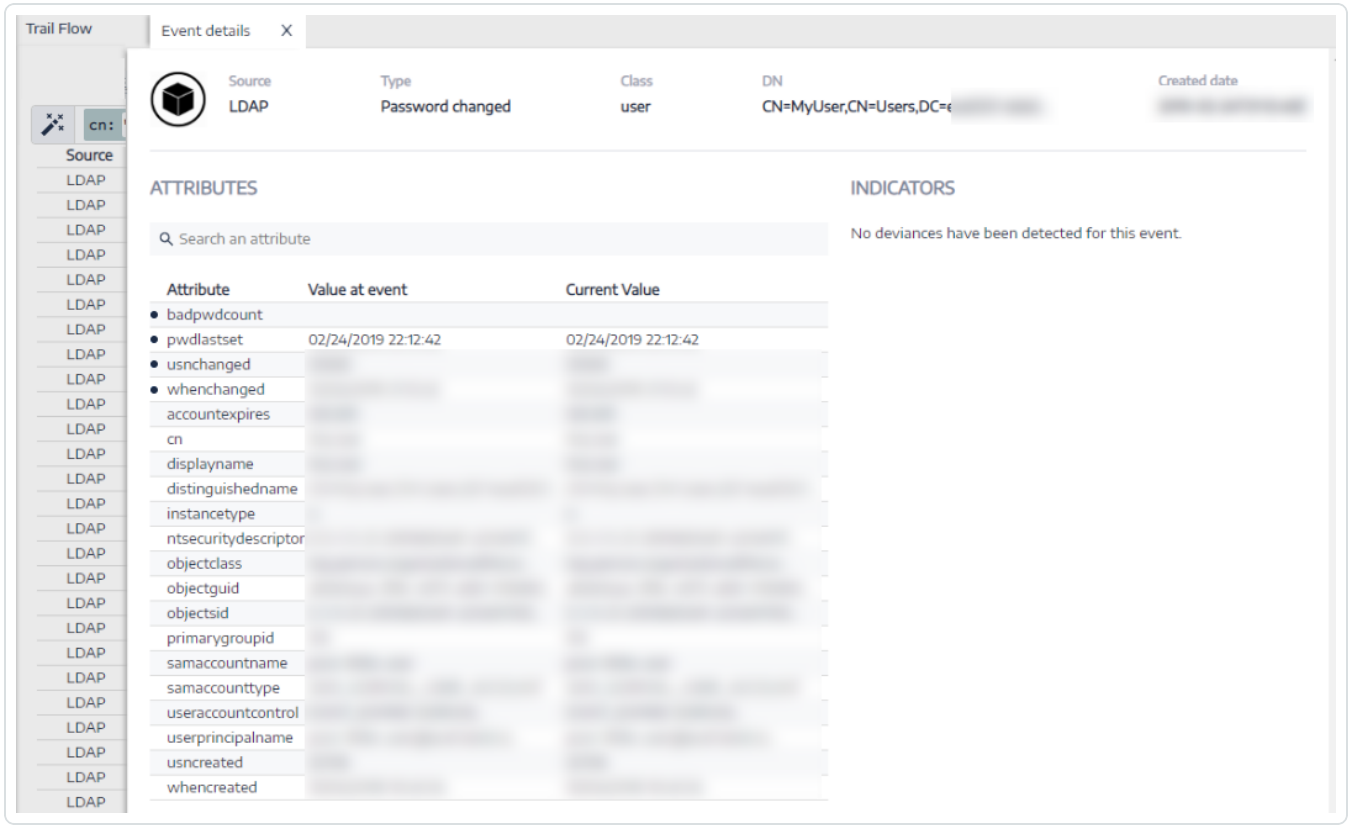


- On the end-user side, Tenable Identity Exposure updates the **Trail Flow** page. See the **Type** column indicating "Password changed."



- 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.



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.

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

To display IoEs:

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

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

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

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

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

The data from the IoE include:

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

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.

Deviance Resolution and Detection Date

Tenable Identity Exposure sometimes uses a different resolution or detection date from the actual event date. This happens because Tenable Identity Exposure stores the most recent event date affecting each Active Directory (AD) object during the caching process.

When Tenable Identity Exposure detects and resolves a deviance affecting an AD object, it assigns the most recent event date for that object as the resolution date.

For instance, when a user's group membership changes, Tenable Identity Exposure records the event date for the group, not the user. If the deviance impacting the user gets resolved through a group membership change, Tenable Identity Exposure will use the user's last recorded event date, not the date of the group membership change.

See also

- Indicator of Exposure Details
- Deviant Objects
- Search Deviant Objects
- Ignore a Deviant Object or a Reason (Deviance)
- 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.

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 or a Reason (Deviance)
- 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.

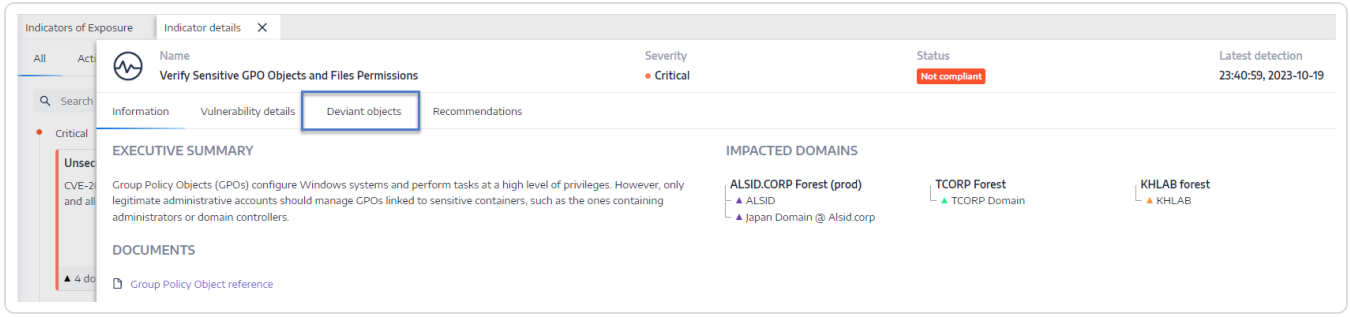
To display deviant objects:

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.

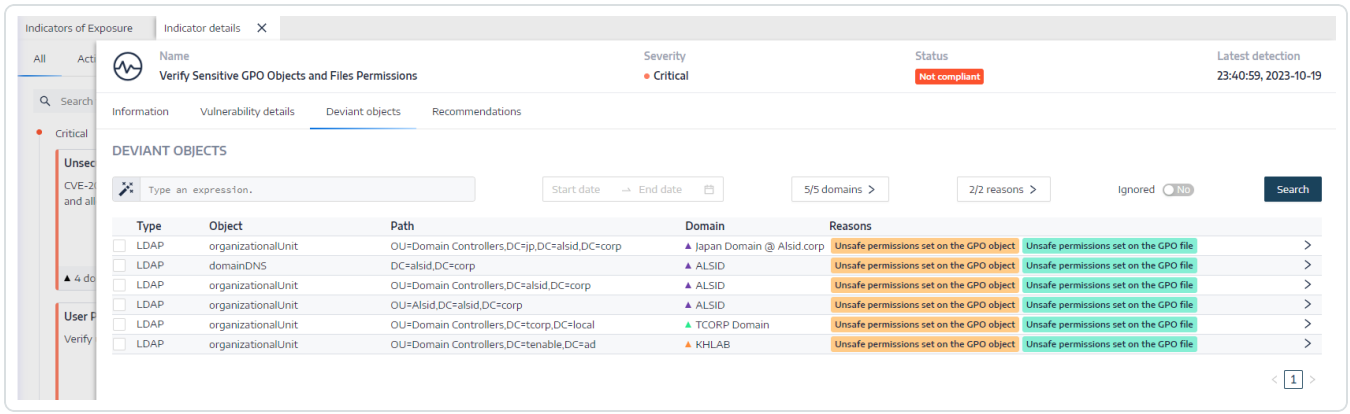
2. Click on any **Indicators of Exposure** tile on the page.

   The **Indicator details** pane opens.



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

   The list of deviant objects associated with the IoE appears.



   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 or a Reason (Deviance)
- Incriminating Attributes

Search Deviant Objects

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

Wizard Search

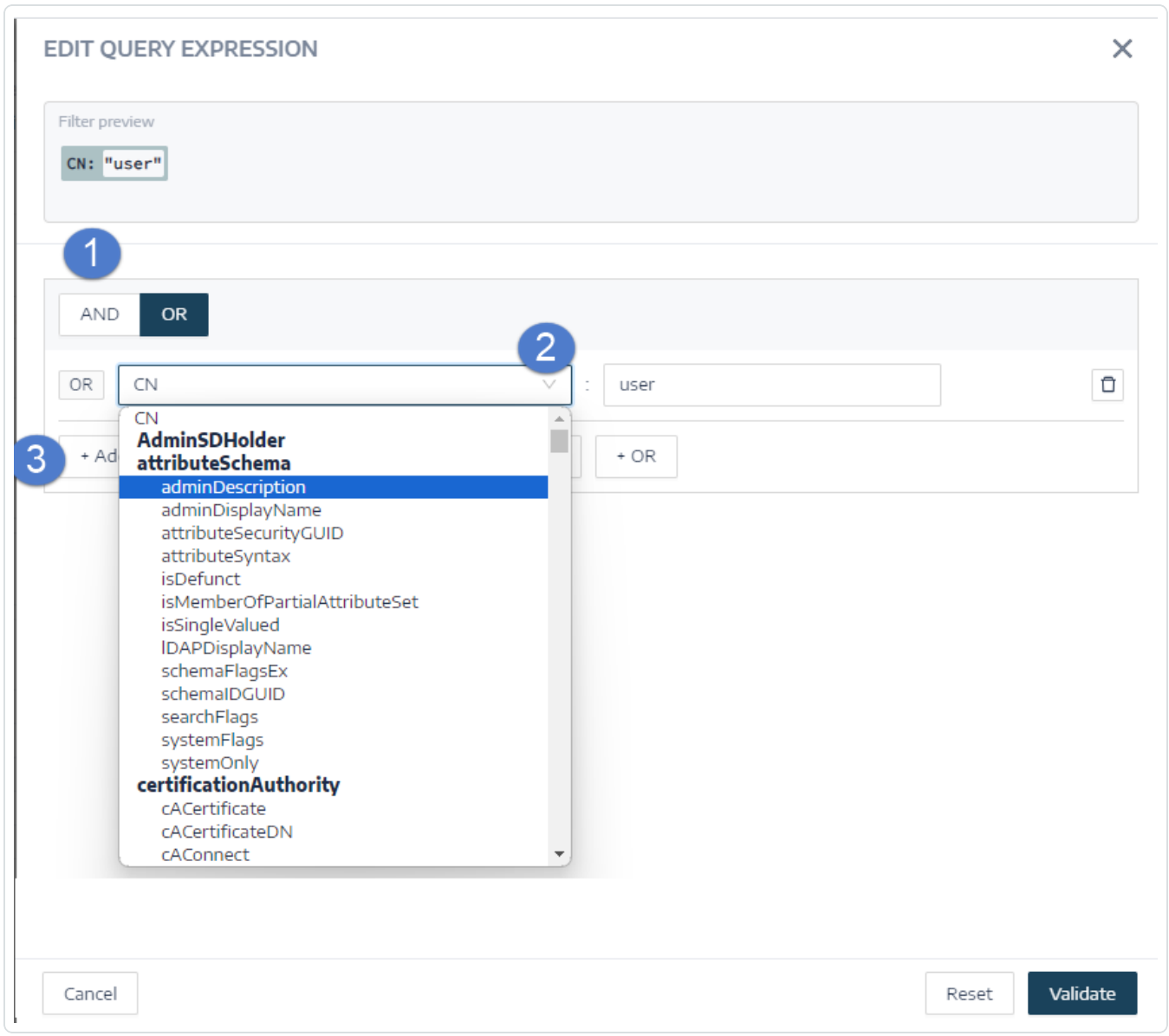
The search wizard allows you to create query expressions.

- 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.



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.

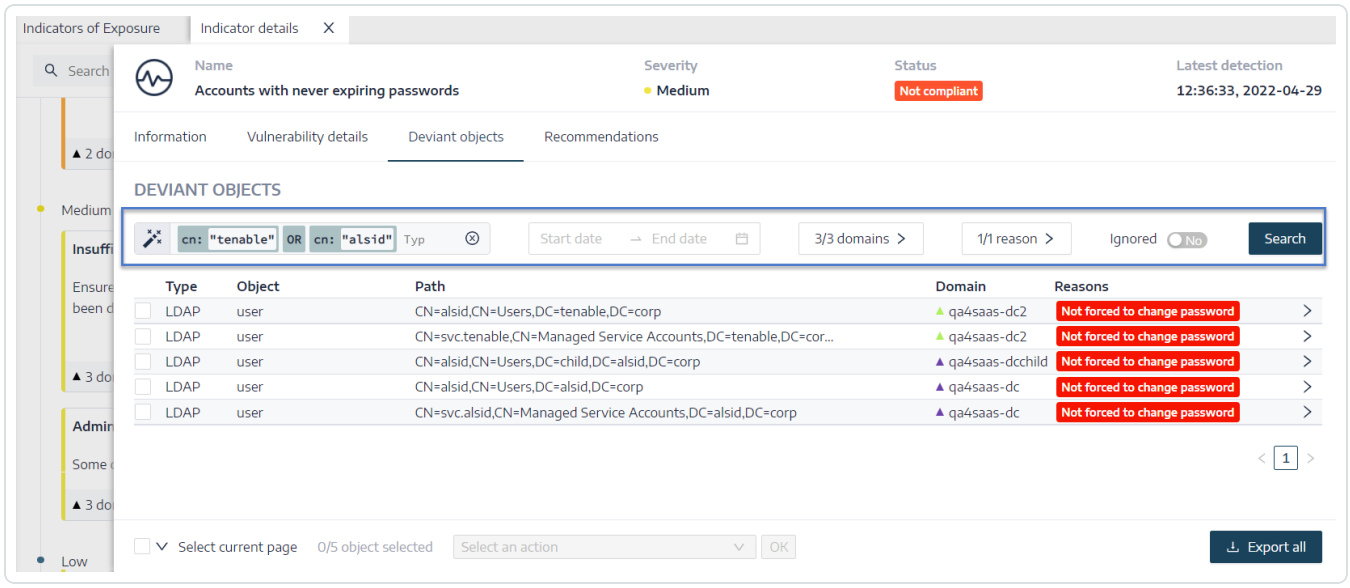
6. Click **Validate** to run the search or **Reset** to modify your query expressions.

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.



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 or a Reason (Deviance)
- Incriminating Attributes

Ignore a Deviant Object or a Reason (Deviance)

In Tenable Identity Exposure, a **deviant object** refers to any object in the Active Directory (AD) that exhibits abnormal or risky behaviors, such as improper configurations or permissions, which could potentially expose security vulnerabilities. These objects are identified through Tenable's Indicators of Exposure (IoE), which identify deviations from best practices and security norms.

A **reason**, also known as a "**deviance**," is the specific attribute or factor that makes an object deviant. Multiple reasons may contribute to why the IoE flagged an object as deviant. For example, an object could be marked deviant due to incorrect file permissions, misconfigurations, or risky delegation, each of which represents a distinct "reason."

In summary:

- **Deviant Object**: An AD object flagged for risky or abnormal behavior.
- **Reason/Deviance**: The specific attribute or factor that causes the IoE to flag the object.

These reasons are critical to understanding the underlying security weaknesses associated with each deviant object.

Ignoring a deviant object

When you choose to ignore a deviant object, you also ignore all associated reasons or deviances.

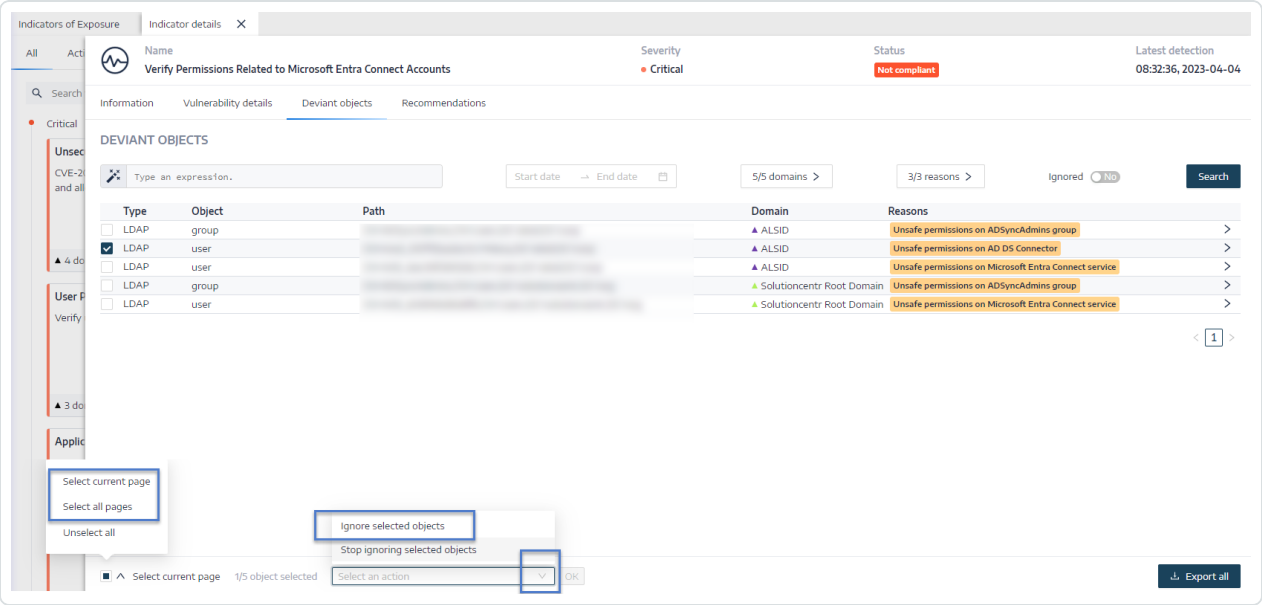
This can be useful for reducing clutter in the interface when certain flagged objects are not of immediate concern.

However, ignoring these objects does not resolve the underlying issues; it simply prevents them from appearing in reports or investigation screens for the specified timeframe.

To ignore deviant objects:

1. In Tenable Identity Exposure, display the list of Deviant Objects
2. Select the check boxes 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.



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.

Ignoring a reason or "deviance"

When you choose to ignore a specific reason (or "deviance") in Tenable Identity Exposure, the IoE stops alerting you about that particular issue, but it doesn't resolve the problem itself.

The ignored deviance no longer appears in the active monitoring dashboard, effectively silencing the alert for that specific reason.

However, other deviances related to the same object continue to trigger alerts unless you also ignored them individually.

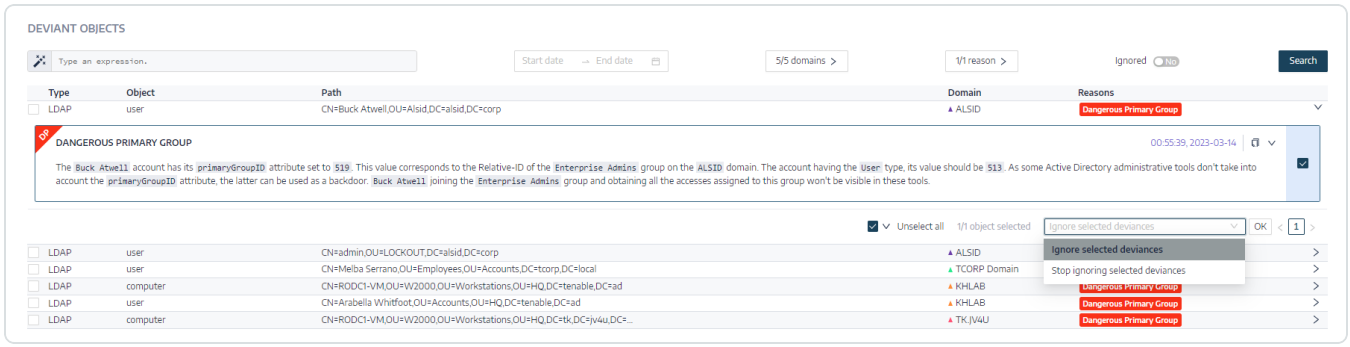
To ignore a reason ("deviance"):

1. In Tenable Identity Exposure, display the list of Deviant Objects

   A list of deviant objects appears.
2. Identify a deviant object and click on the arrow (>) at the end of the line.

   The view expands to show the details of the reason.

3. Click the checkbox at the end of the line. If there are several reasons, select the ones to ignore or click **Select all** to ignore all associated reasons.



4. Click **OK**.

   The **Ignore selected deviances** pane appears.

5. Click the **Ignore until** box to display the calendar and select a date until which Tenable Identity Exposure must ignore the deviance.

6. Click **OK**.

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

To show ignored deviances:

1. Click the **Ignored** toggle to **Yes**.

   The list of deviant objects updates with an expanded view for all reasons. The ignored reasons show the  icon.

2. Select the ignored reason and click Stop ignoring selected deviance from the drop-down list.

3. Click **OK**.

   The pane "Stop ignoring selected deviances " appears.

4. Click **OK**.

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

See also

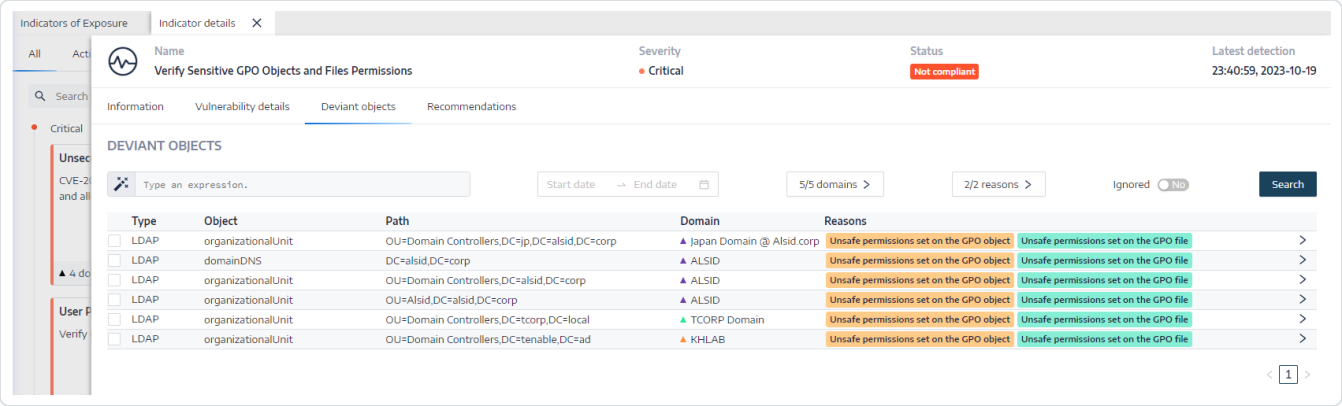
- Indicators of Exposure
- Indicator of Exposure Details
- Deviant Objects
- Search Deviant Objects
- Incriminating Attributes

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.

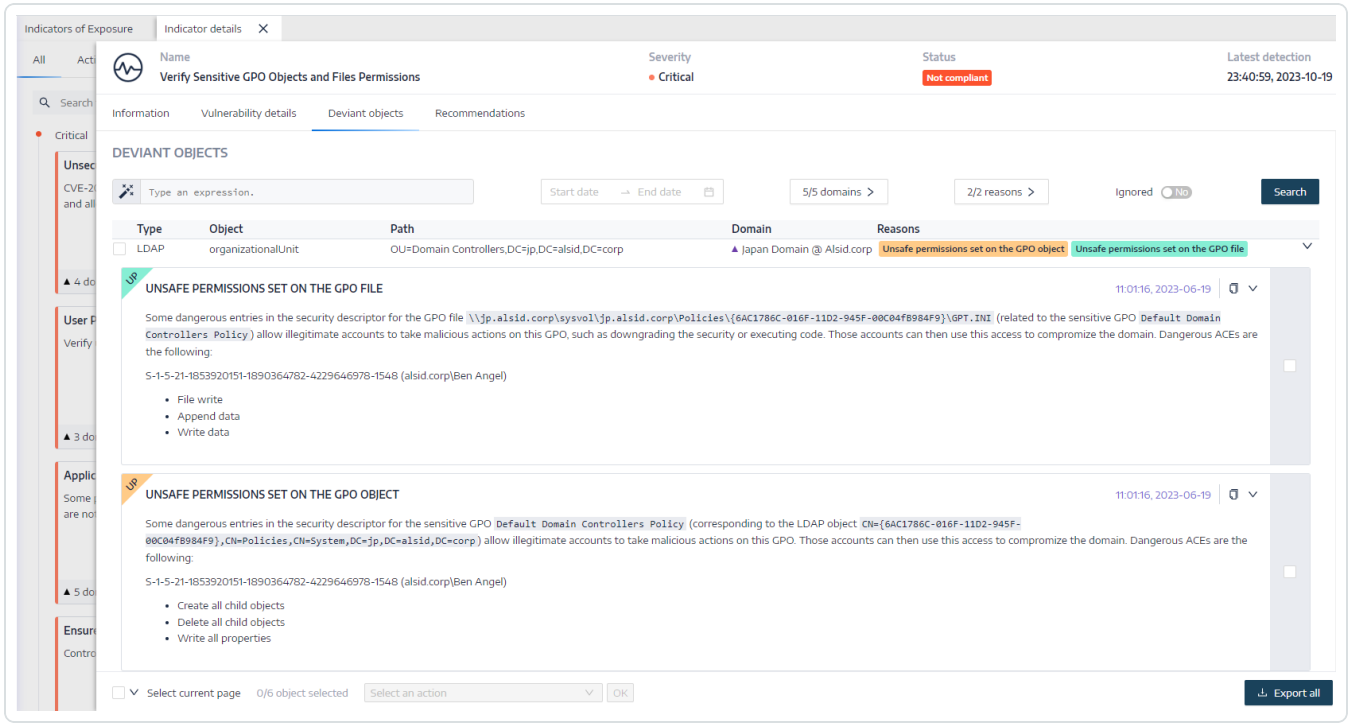
To see incriminating attributes:

1. Display the list of Deviant Objects



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

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



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 or a Reason (Deviance)

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.

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.

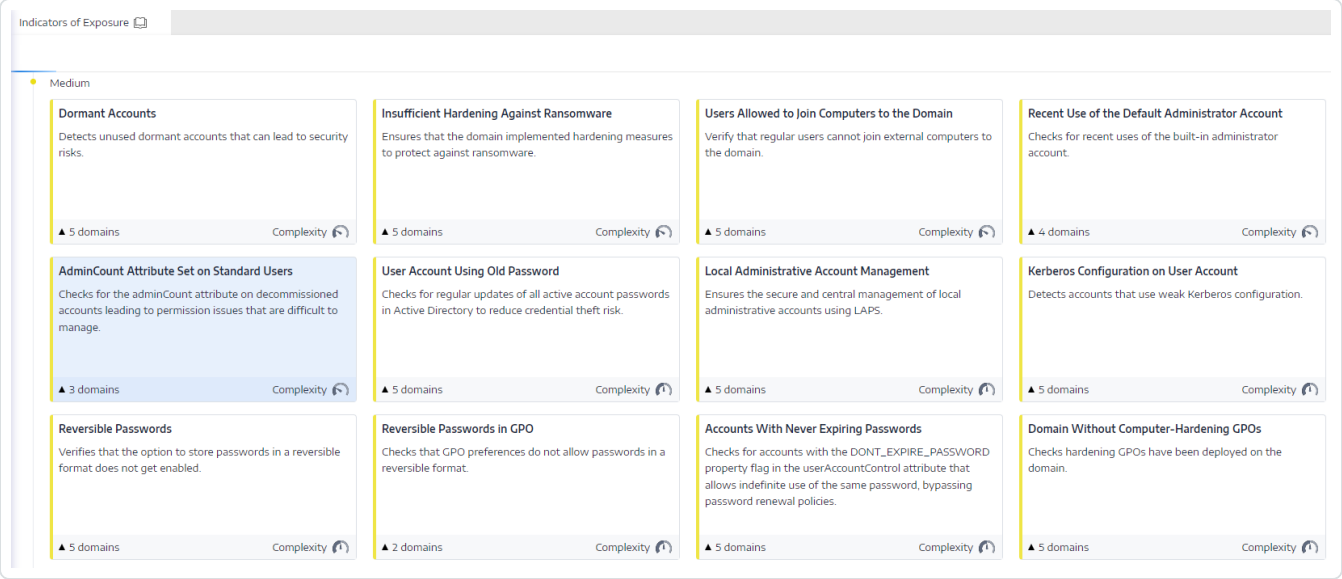
This medium-level IoE only reports on active user accounts and groups with this attribute and excludes privileged groups with legitimate members that have the `adminCount` attribute set to `1`.

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.

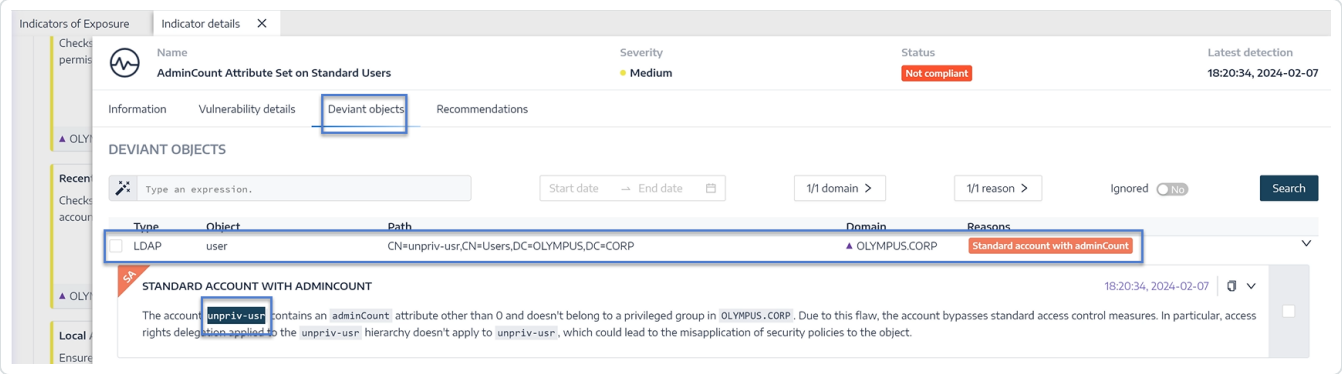
   By default, Tenable Identity Exposure shows only the IoEs that contain deviant objects.

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



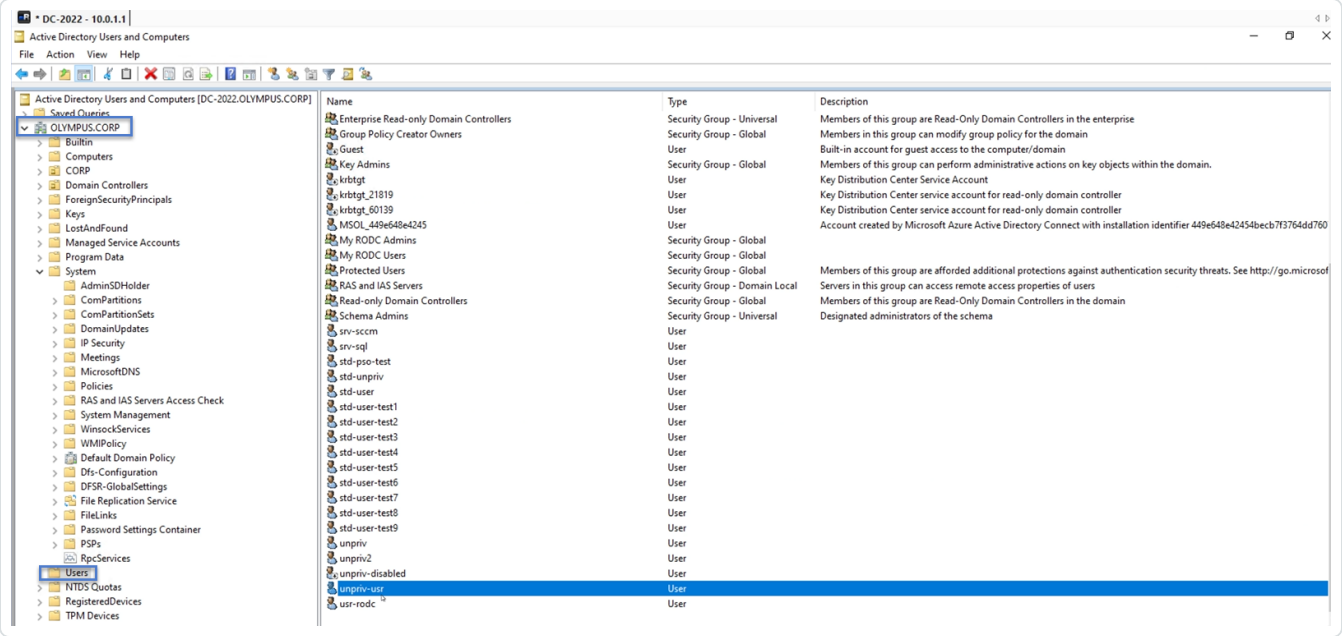
The **Indicator details** pane opens.

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`)



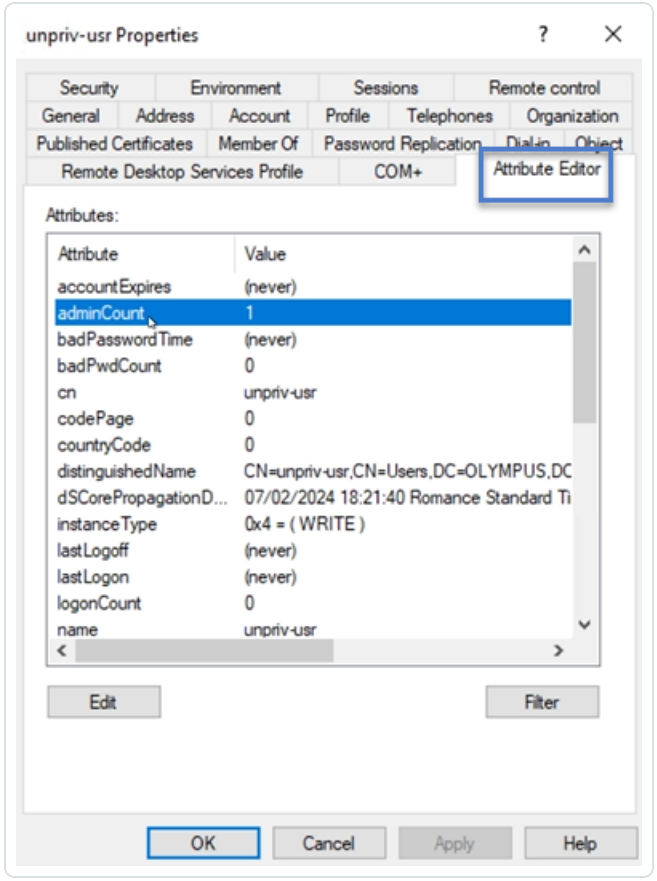
4. In Remote Desktop Manager (or similar tool), locate the domain name and navigate to **Users** and the account that Tenable Identity Exposure flagged.

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

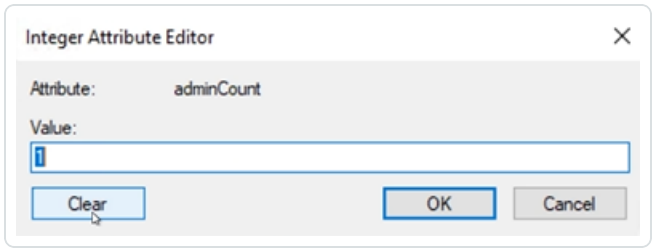


5. Click on the account name to open its **Properties** dialog box and select the **Attribute Editor** tab.

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



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



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.

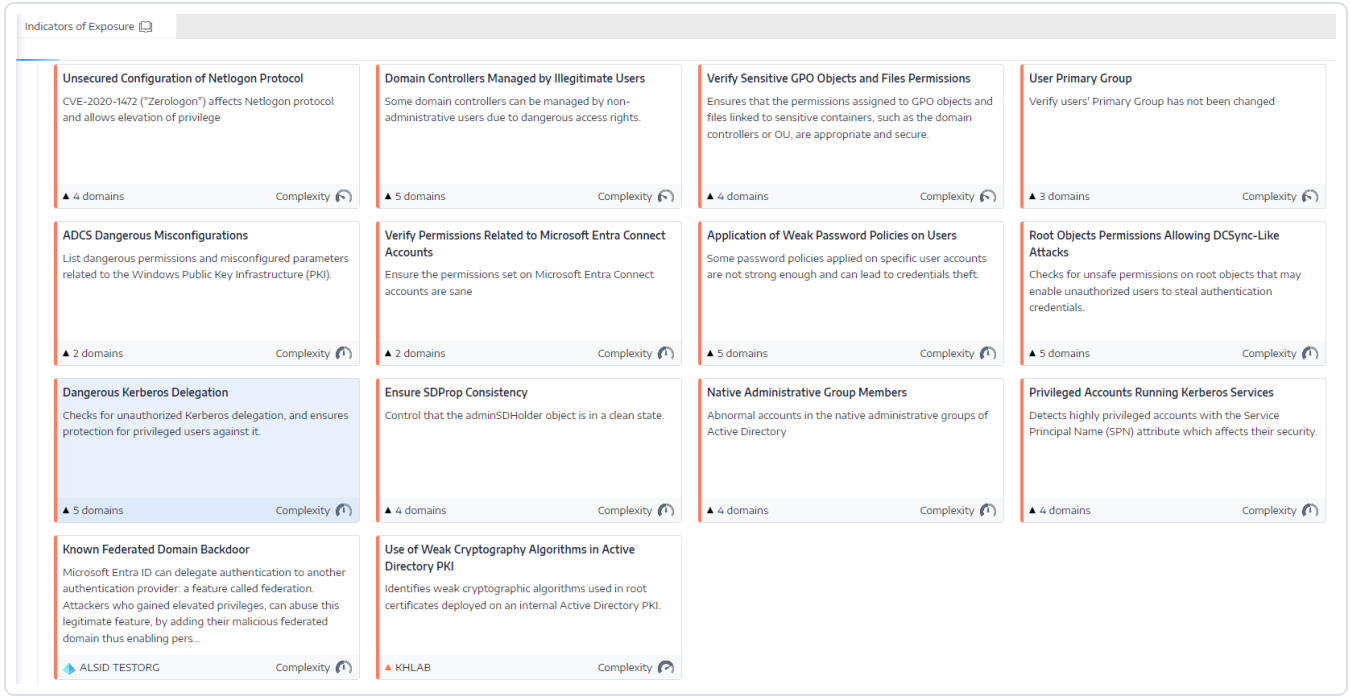
This critical-level IoE reports all accounts with delegation attributes and excludes disabled accounts. Privileged users should not have delegation attributes. To protect these user accounts, add them to the "Protected Users" group or mark them as "Account is sensitive and cannot be delegated".

To add the account to the "Protected Group":

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

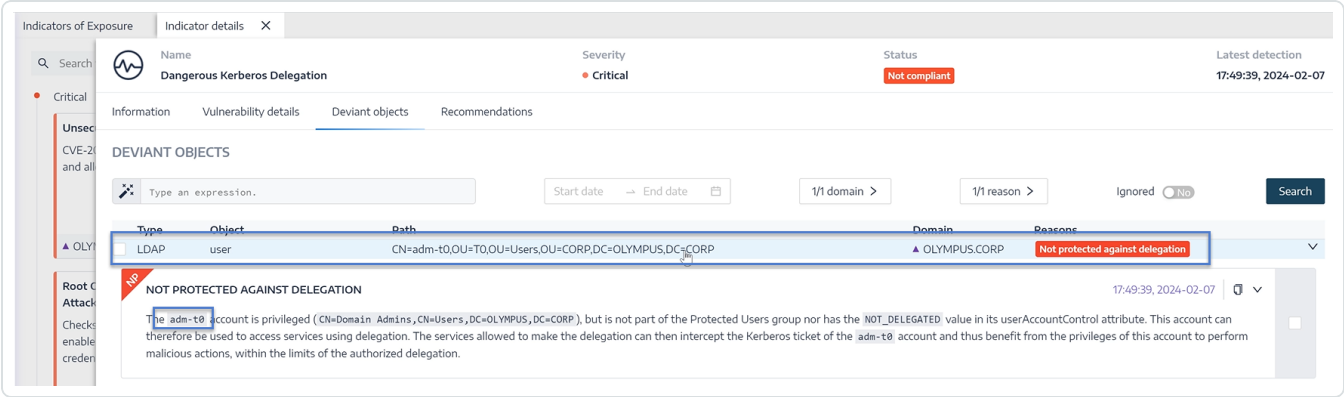
   By default, Tenable Identity Exposure shows only the IoEs that contain deviant objects.

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



   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`)

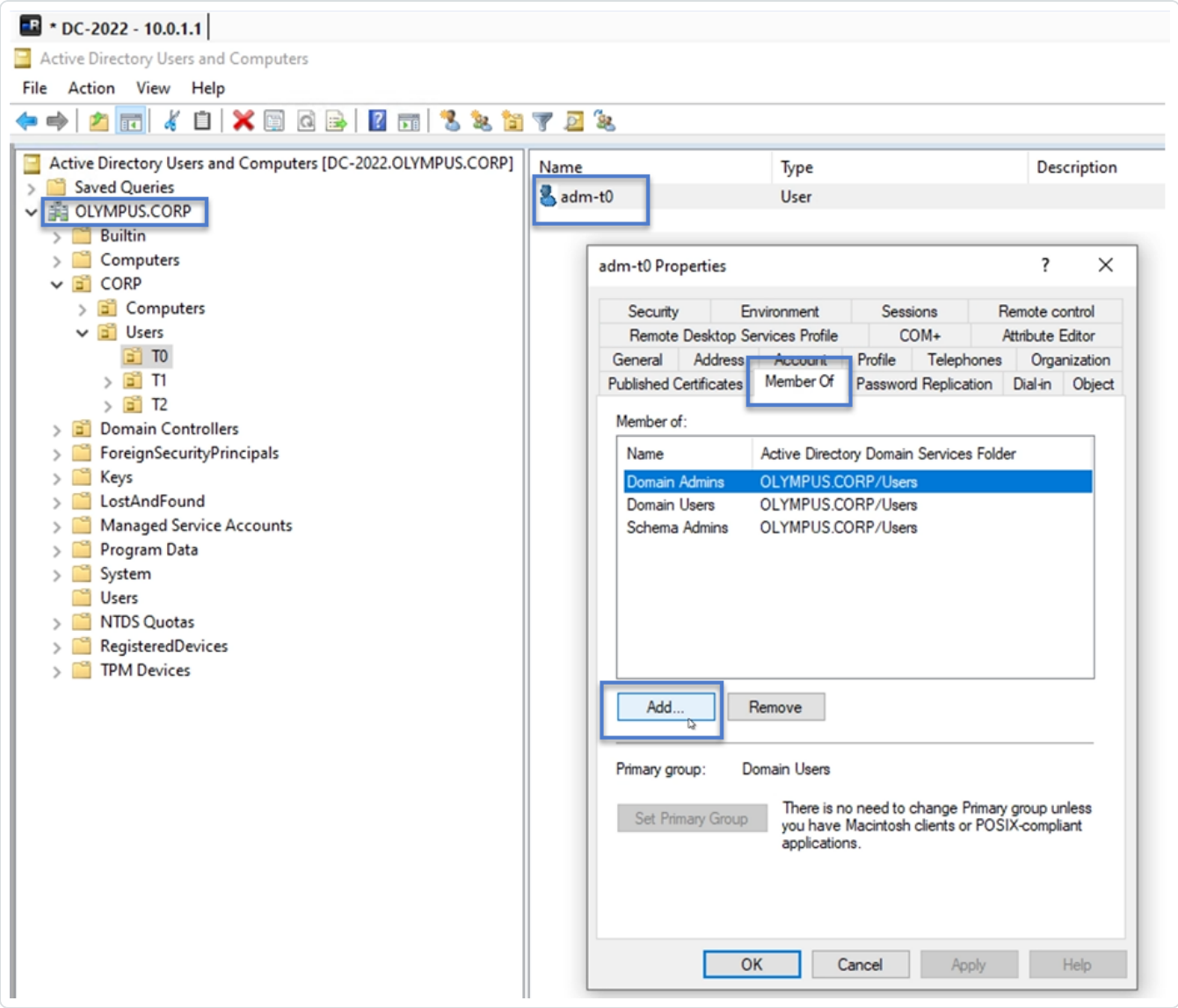


4. In Remote Desktop Manager (or similar tool), locate the domain name and navigate to the domain and account that Tenable Identity Exposure flagged.

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

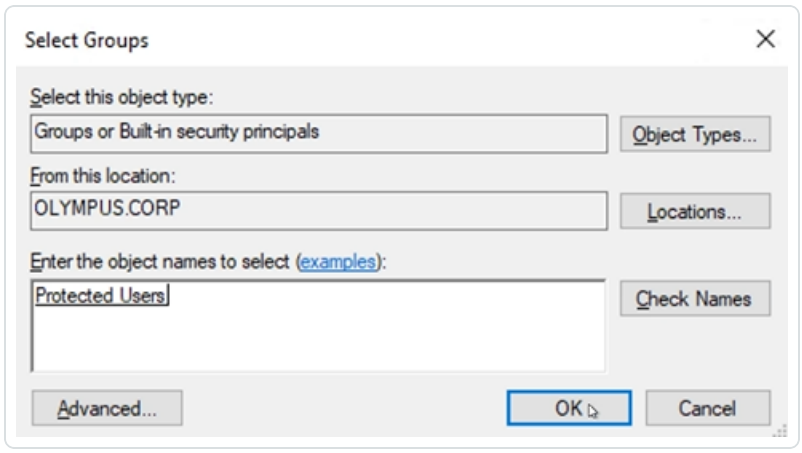
5. Click on the account name to open its **Properties** dialog box and select the **Member Of** tab.

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



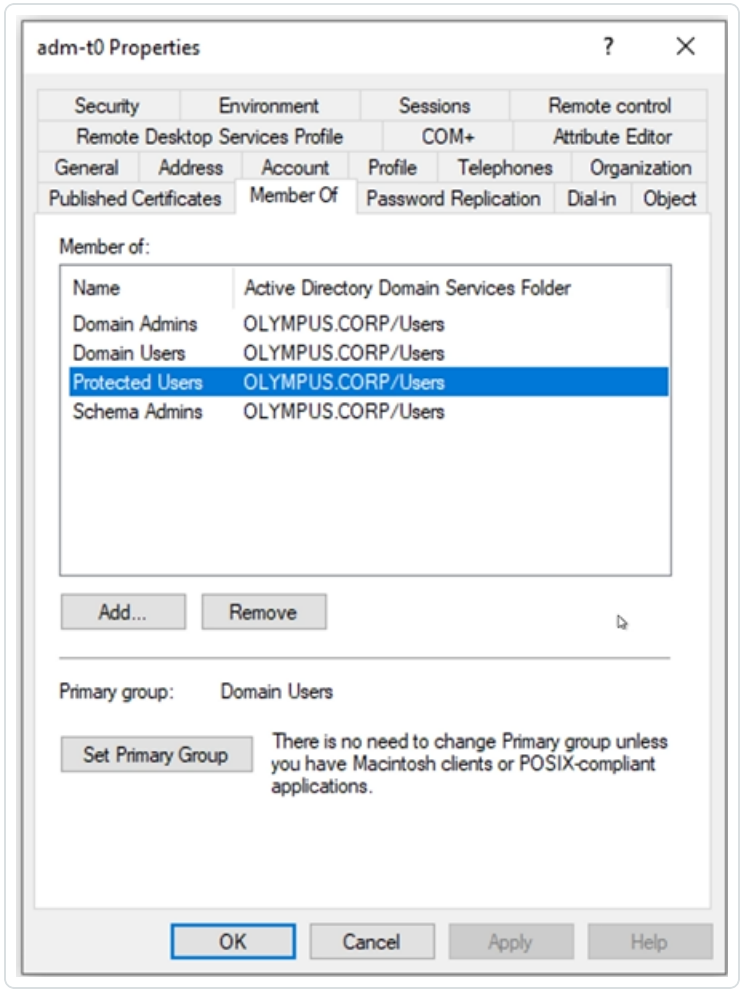
The **Select Groups** dialog box appears.

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



8. Click **OK** to close the dialog box.
9. In the **Properties** dialog box, click **Apply**.

   The new group appears on the member list.



10. Click **OK** to close the dialog box.
11. In Tenable Identity Exposure, return to the Indicator details pane and refresh the page.

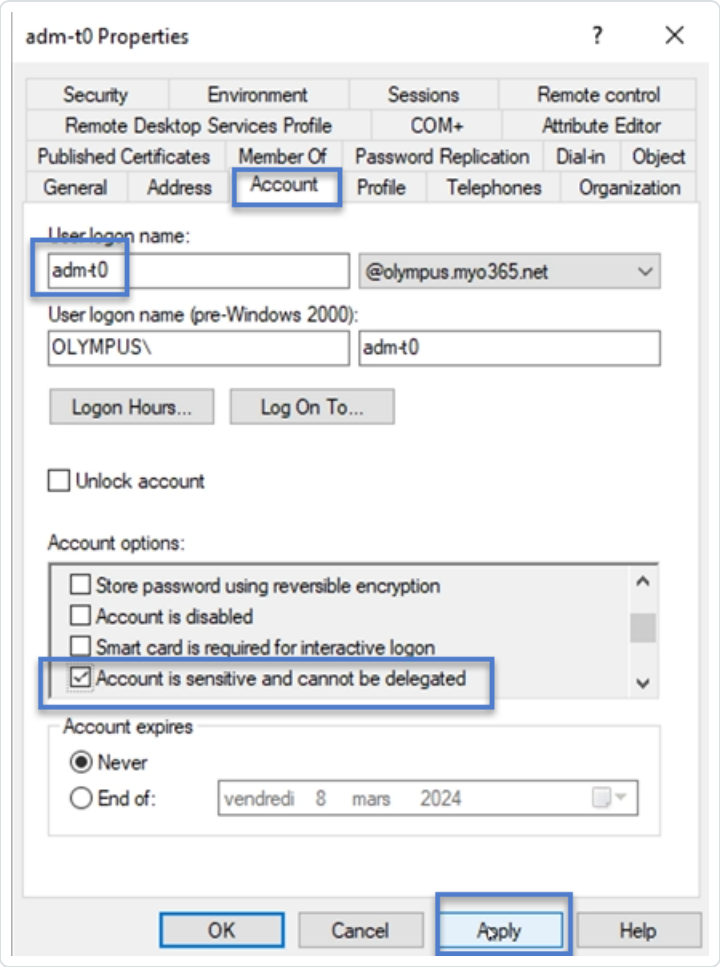
    The deviant object no longer appears in the list.

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**.



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.

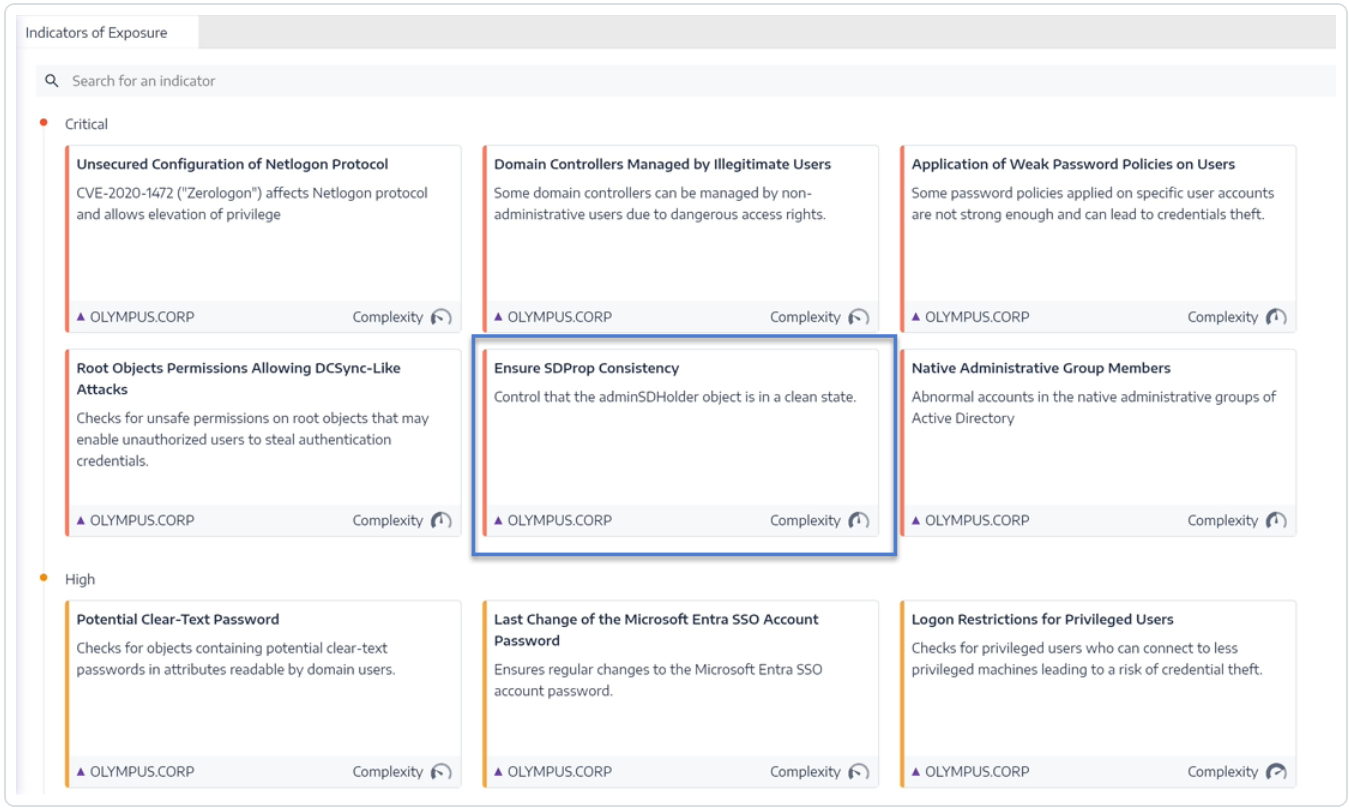
This critical-level IoE checks that the permissions set on the `adminSDHolder` object allow only privileged access to administrative accounts.

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.

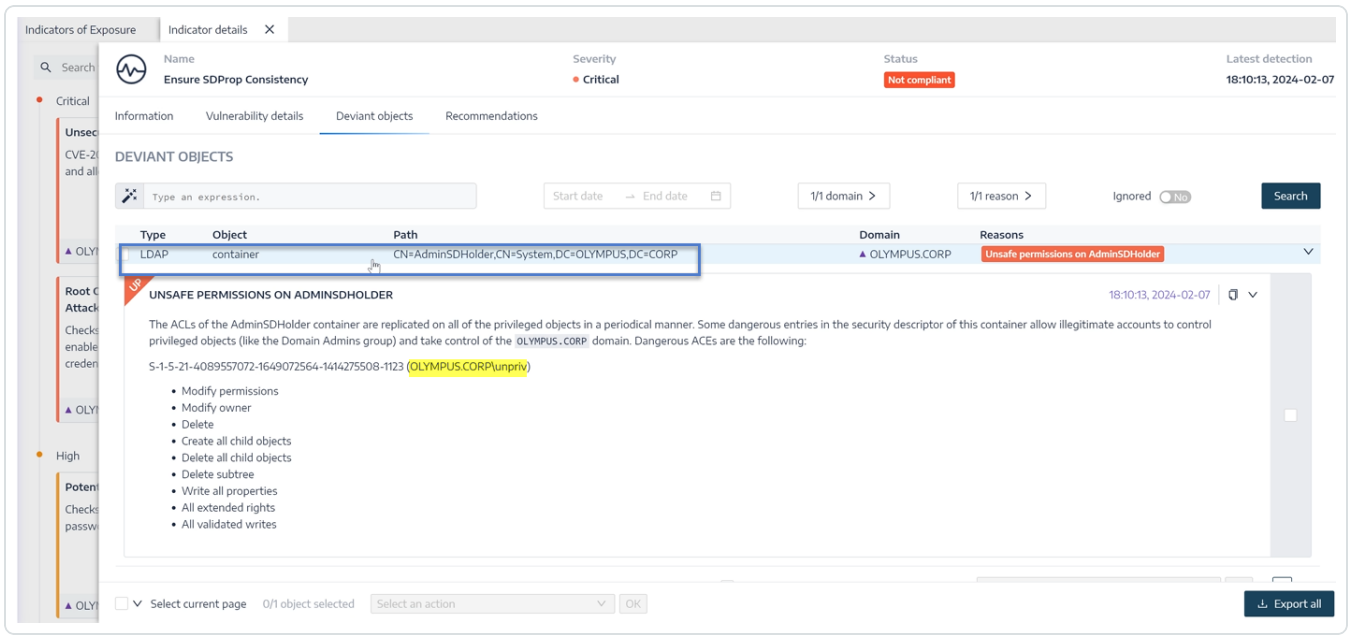
   By default, Tenable Identity Exposure shows only the IoEs that contain deviant objects.

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



   The **Indicator details** pane opens.

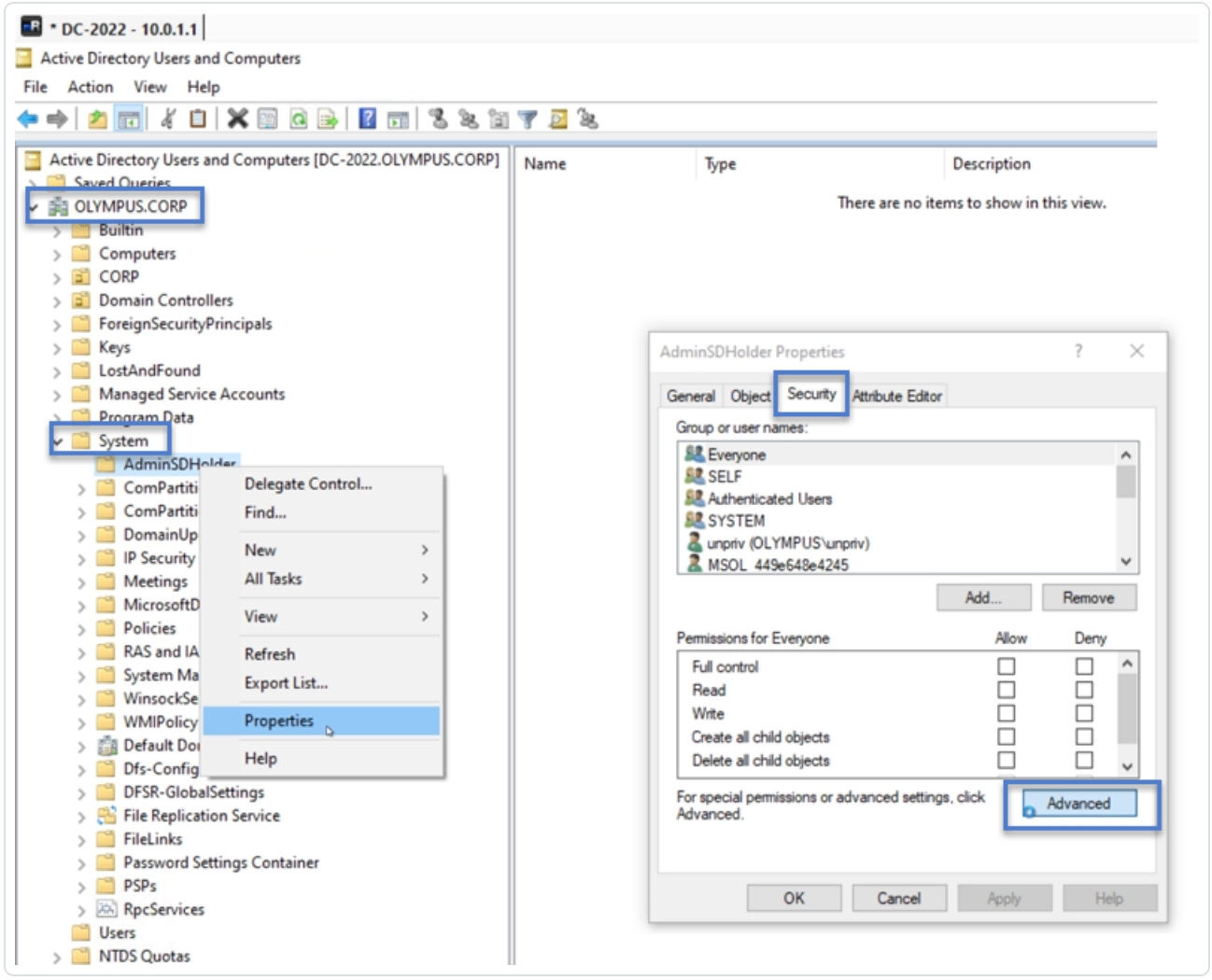
3. Hover over and click on the deviant object to show its details. Note the domain name and the associated permission that Tenable Identity Exposure flagged. (In this example: `OLYMPUS.CORP .\unpriv`)



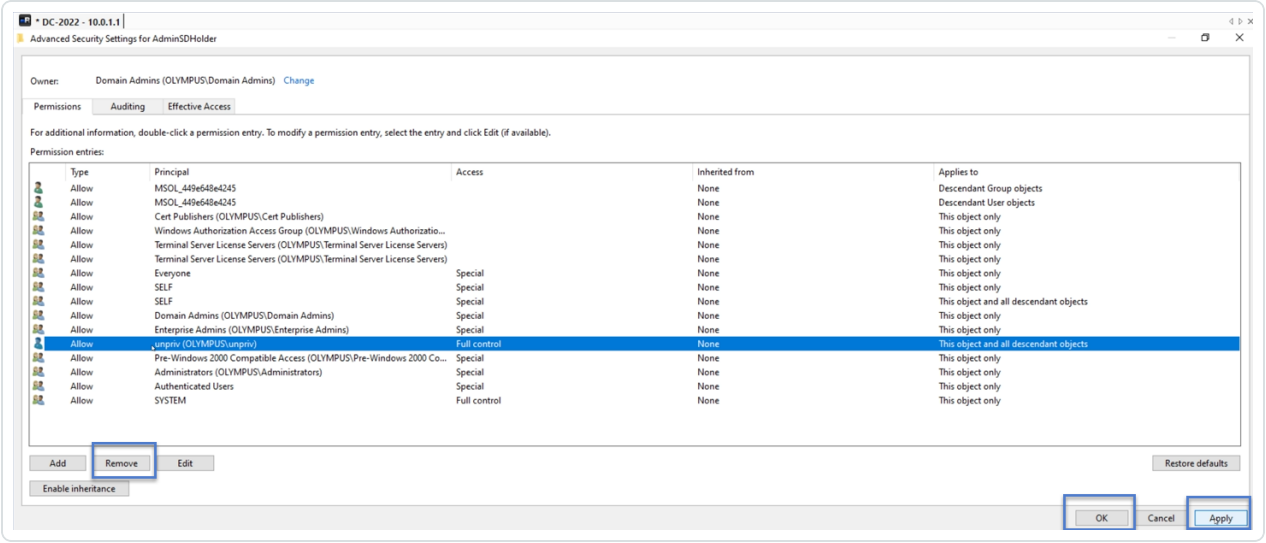
4. In Remote Desktop Manager (or similar tool), locate the domain name and navigate to **System** > **AdminSDHolder**.

> **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.



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.

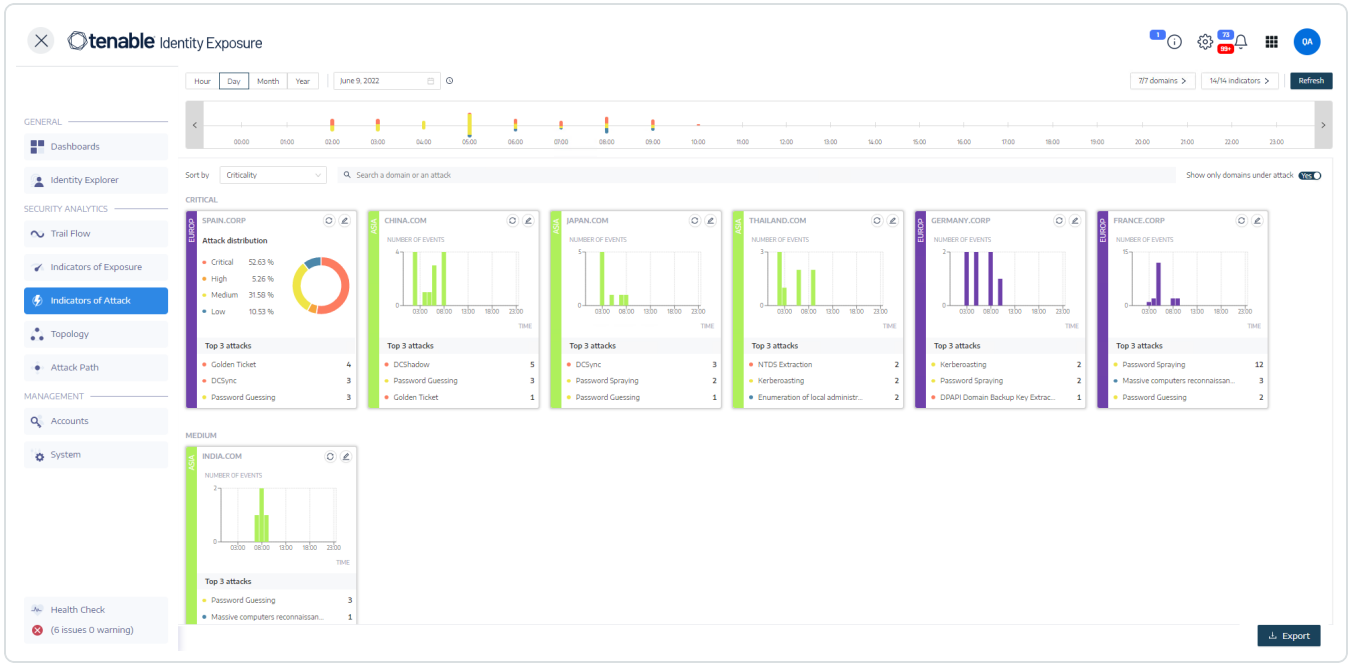
For more information about specific IoAs, see the Indicators of Attack Reference Guide (requires Tenable Downloads site login.)

> **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.

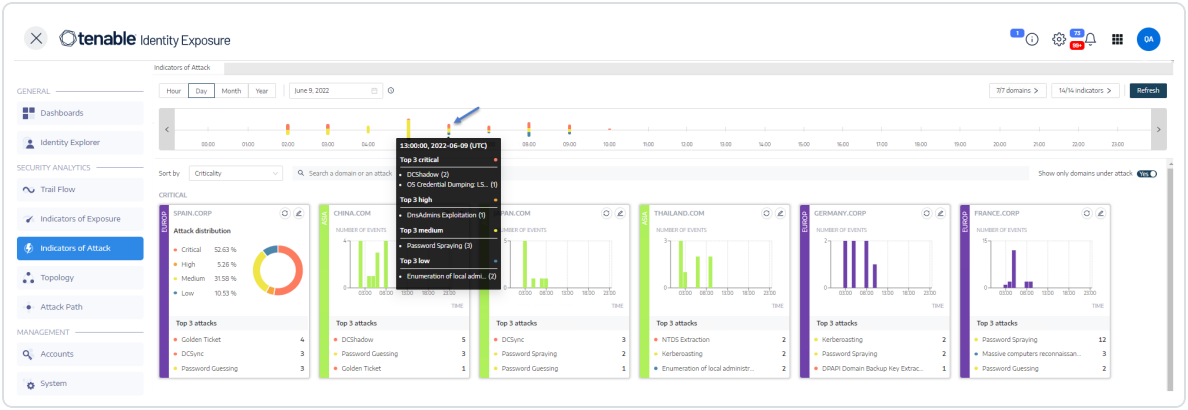
To view Indicators of Attack:

- 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.



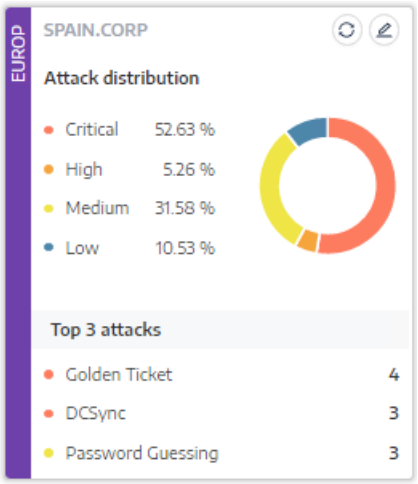
To change the chart type:

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.



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



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.

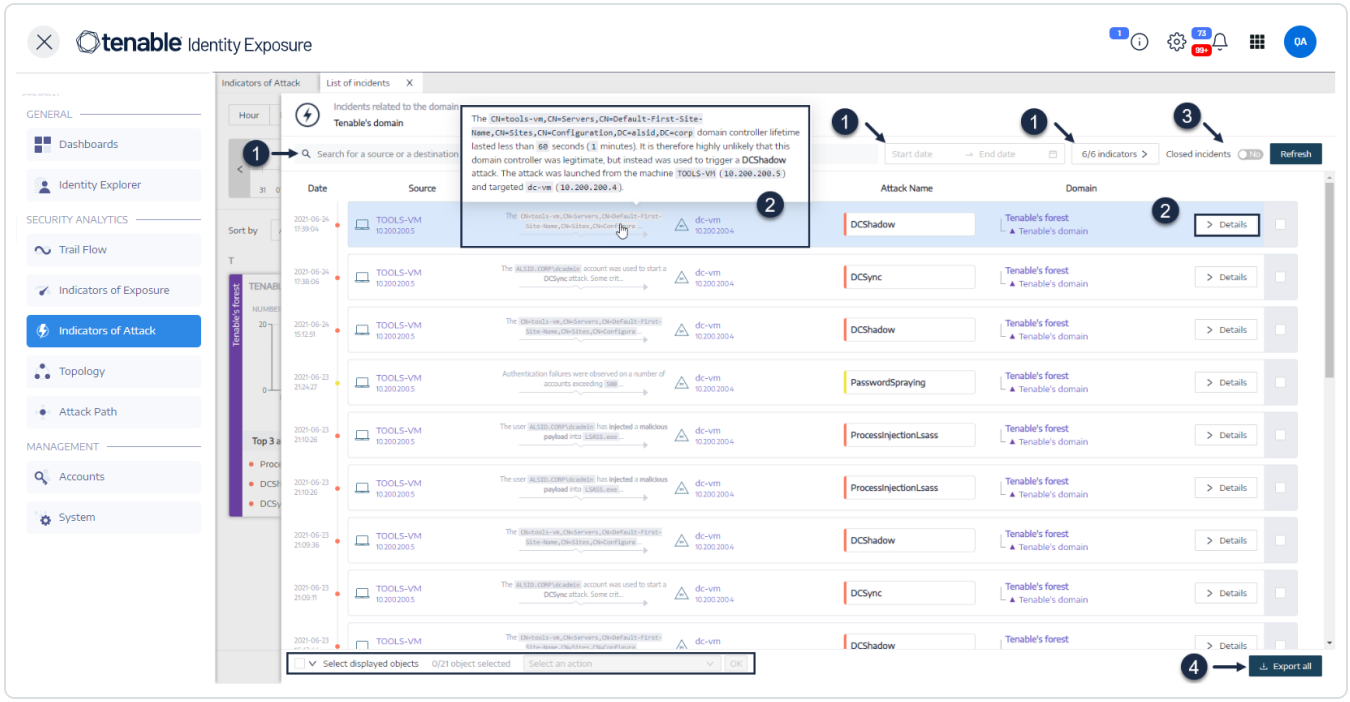
To view attack incidents:

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.



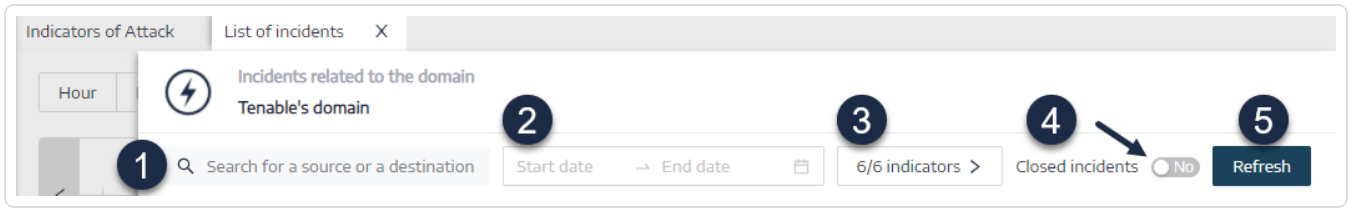
3. From this list, you can do any of the following:

   - Define search criteria to search for specific incidents (**1**).
   - Access detailed explanations on the attacks affecting the AD (**2**).
   - Close or reopen an incident (**3**).
   - Download a report showing all incidents (**4**).

To search for an incident:

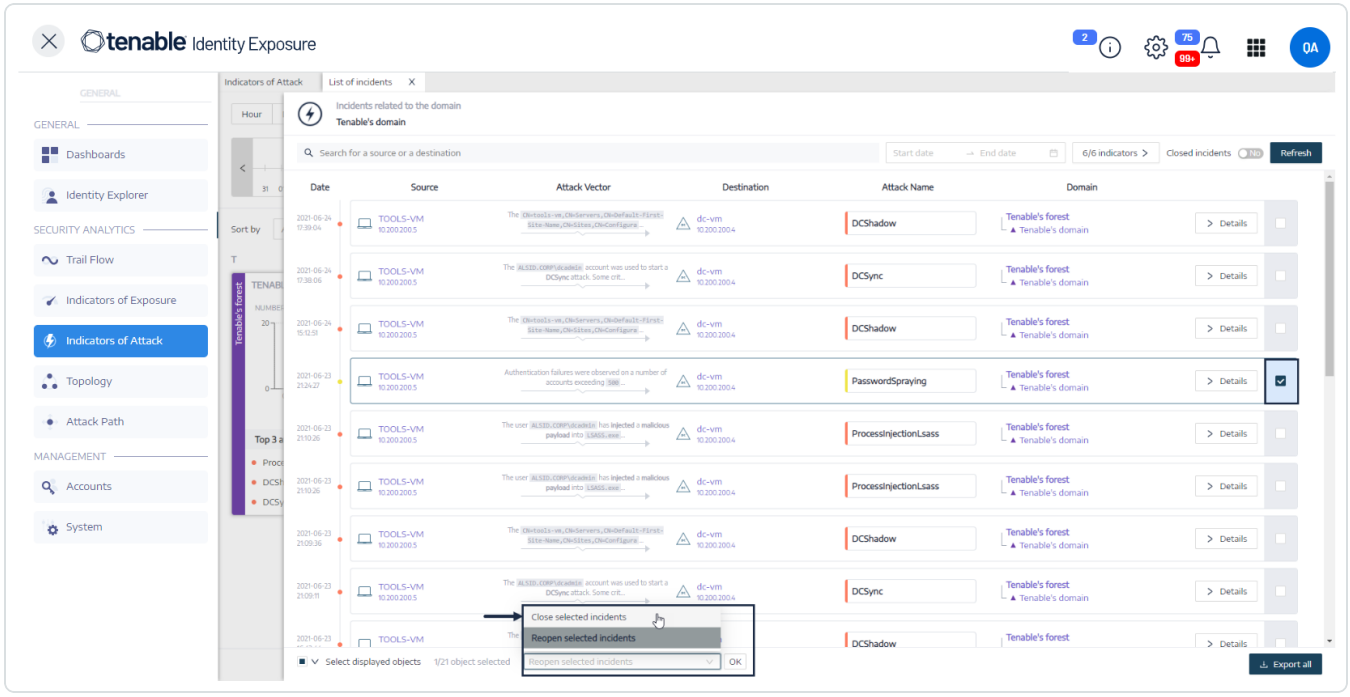
1. In the **Search** box, type the name of a source or destination.
2. Click the date picker to select a start date and end date for the incident.
3. Click **n/n Indicators** to select the related indicators.
4. Click the **Closed Incidents** toggle to **Yes** to limit the search to closed incidents.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



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**.

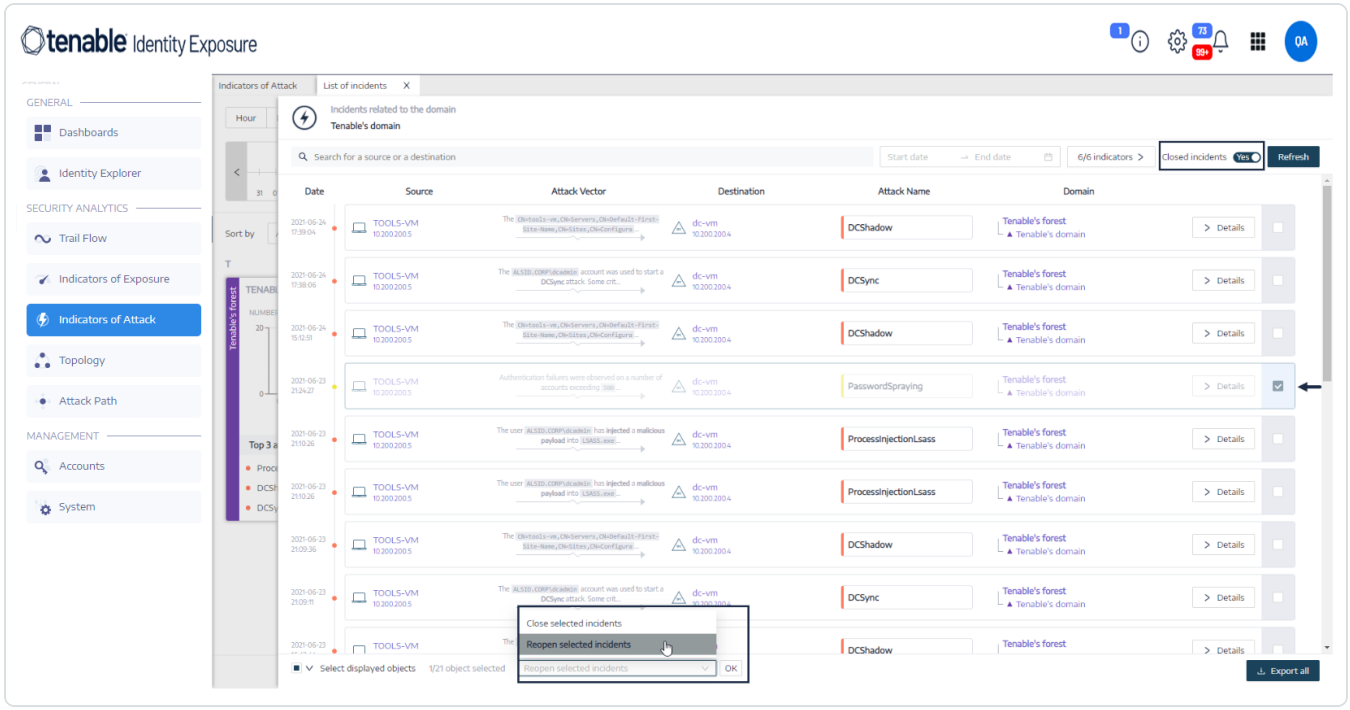
   A message confirms that Tenable Identity Exposure closed the incident and no longer shows it.

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.



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**.

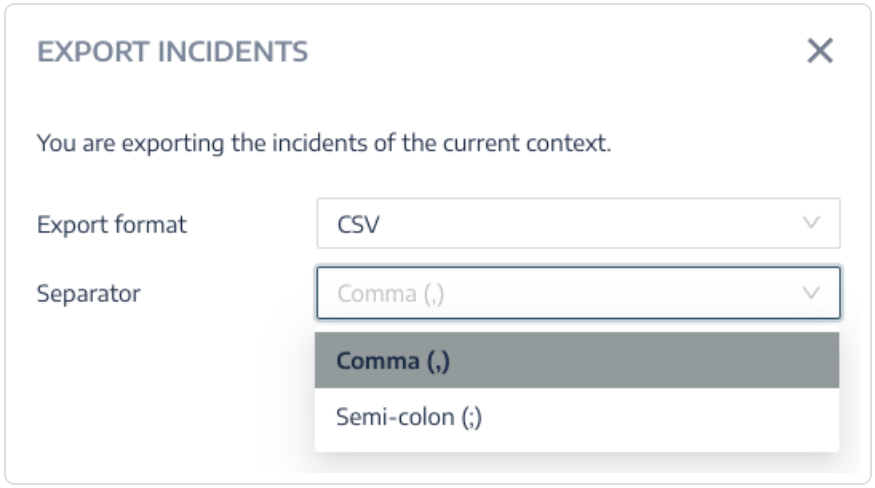
To export incidents

1. In the **List of incidents** pane, click the **Export All** button at the bottom.

   The **Export Incidents** side panel opens.

2. From the **Separator** drop-down list box, select a separator for the exported data: **comma** or **semicolon**.

   Tenable Identity Exposure exports the data in CSV format for download.



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.

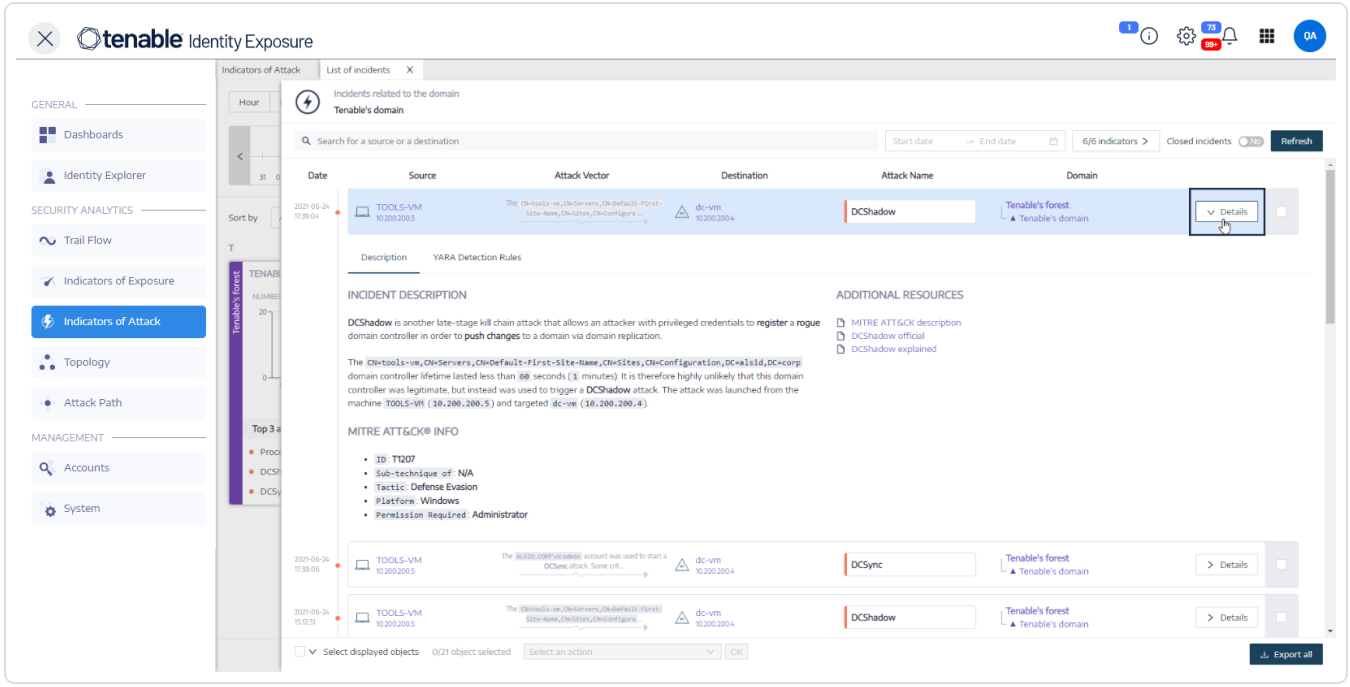
Tip: Tenable Identity Exposure can show a maximum of five panes when you click on several interactive elements (links, action buttons, etc.) in the **List of incidents**. To close all panes simultaneously, click anywhere on the page.

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**.



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.

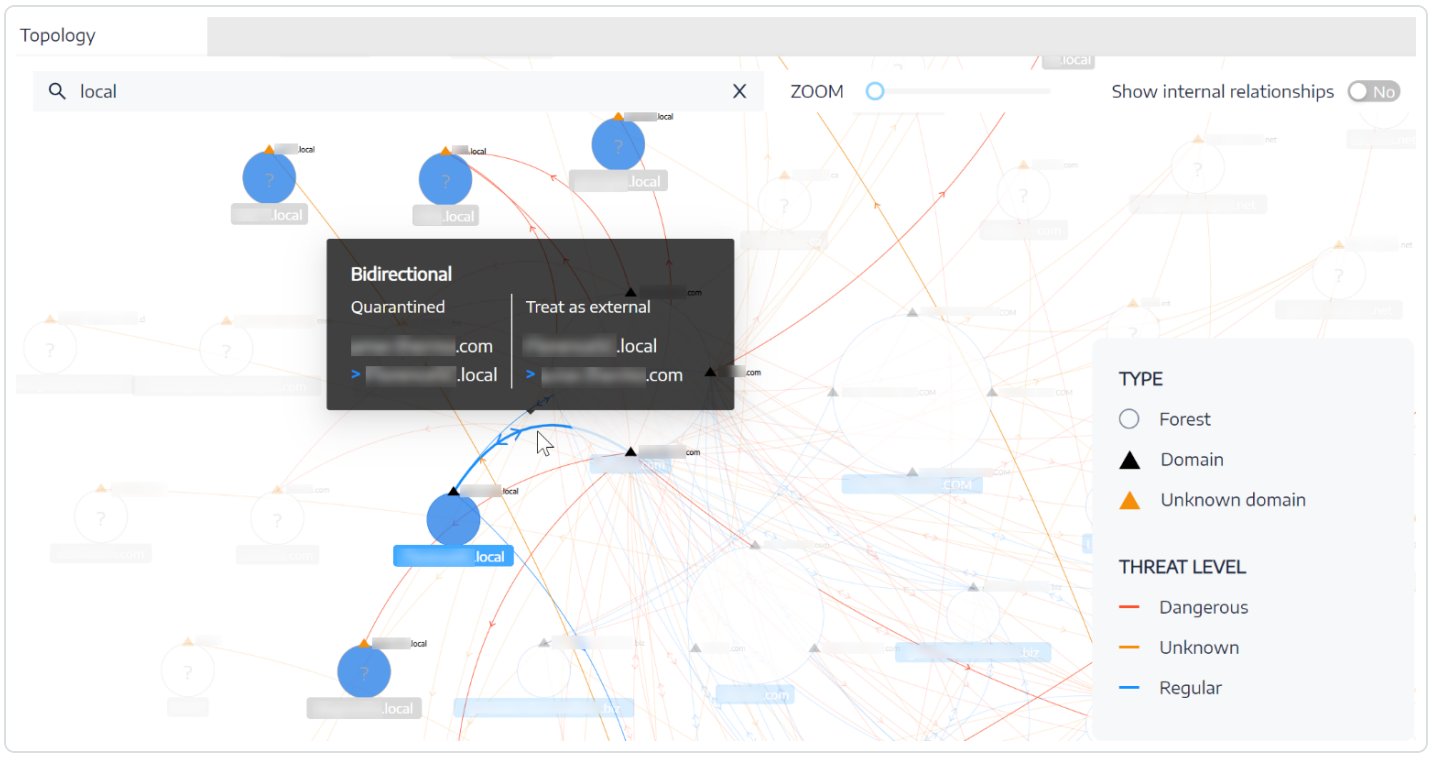
> **Note**: YARA is the name of a tool primarily used in malware research and detection. It provides a rule-based approach to create descriptions of malware families based on textual or binary patterns. A description is essentially a YARA rule name, where these rules consist of sets of strings and a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



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

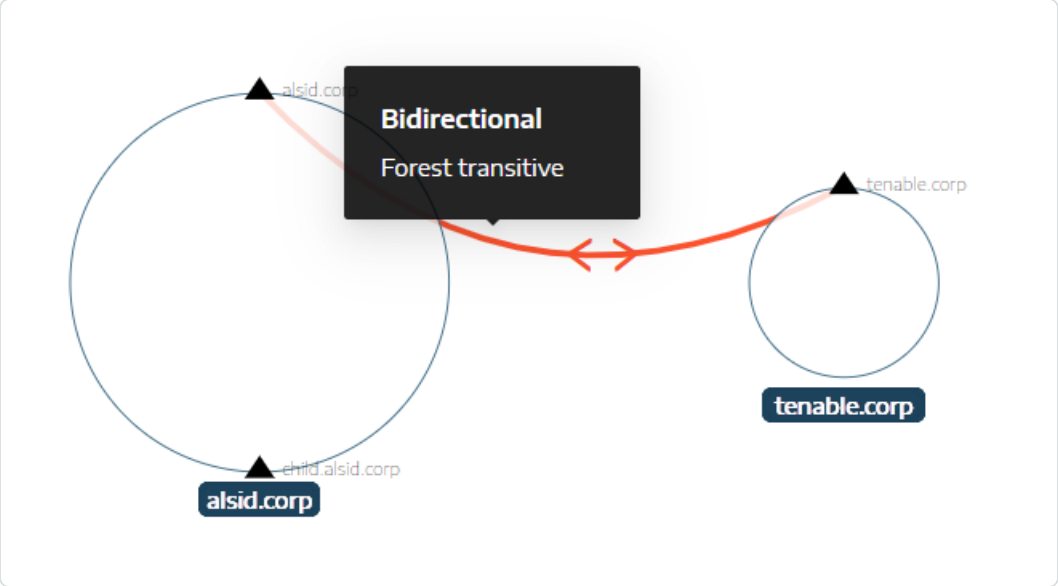
Trust Relationships

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.



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:

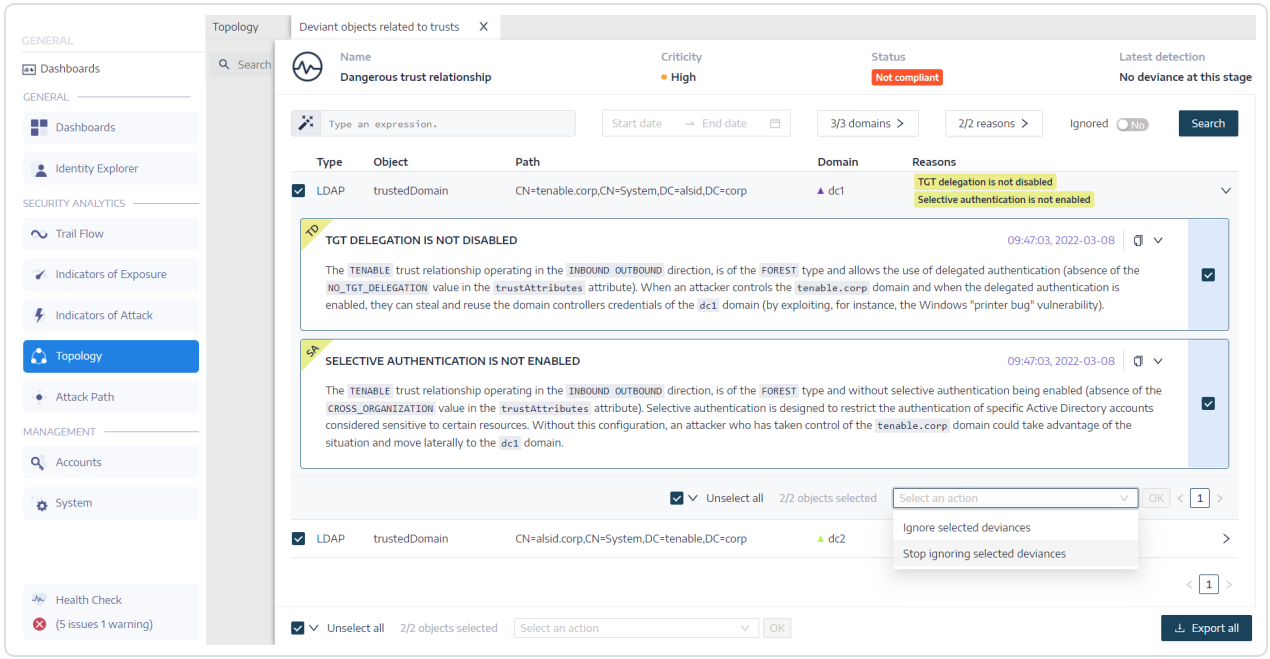
- **Red** for dangerous trusts
- **Orange** for regular trusts
- **Blue** for unknown trusts

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.



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.

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

Benefits of using Attack Path in Tenable Identity Exposure:

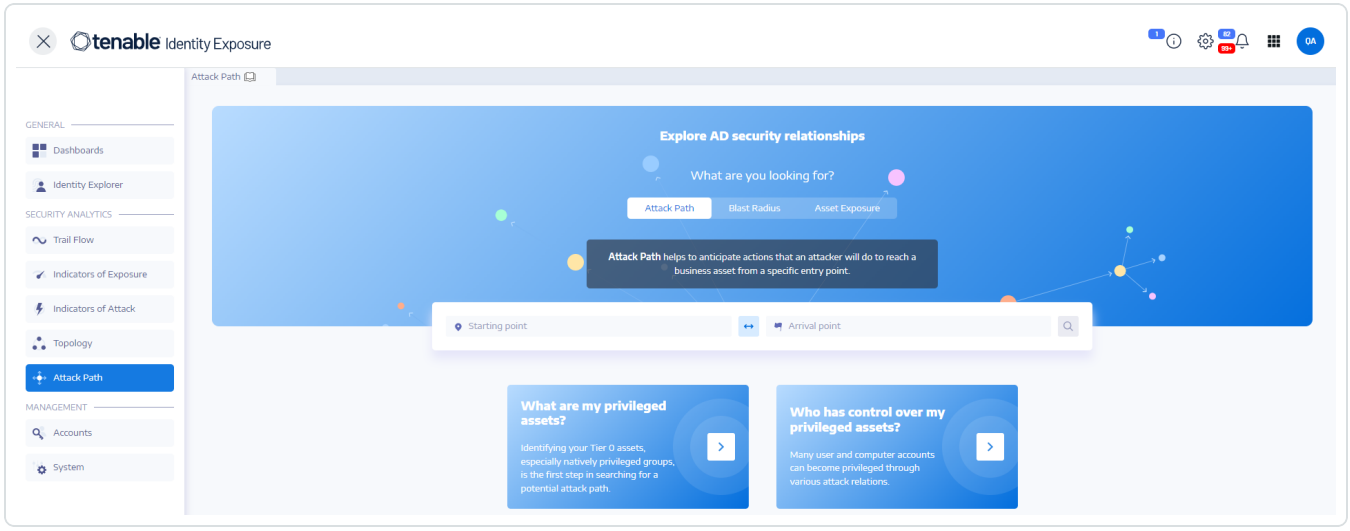
- **Proactive security**: It helps anticipate and address potential attack vectors before they are exploited.
- **Prioritization**: It guides towards focusing security efforts on the most critical vulnerabilities and attack paths.
- **Visualization**: It provides a clear and easy-to-understand representation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

To display the Attack Path:

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

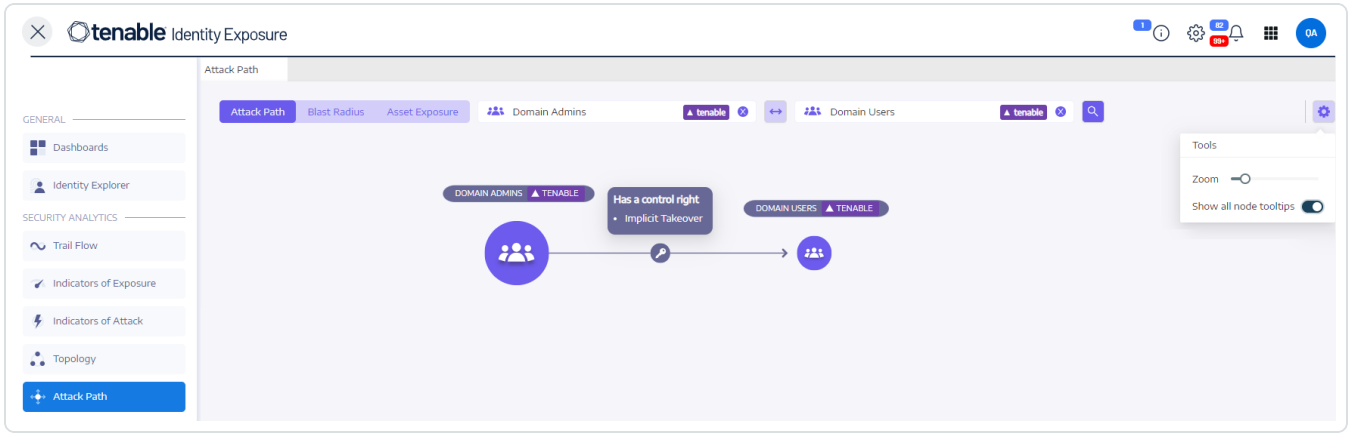
1. In Tenable Identity Exposure, click **Attack Path** on the sidebar menu.

   The **Attack Path** pane appears.



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:

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

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

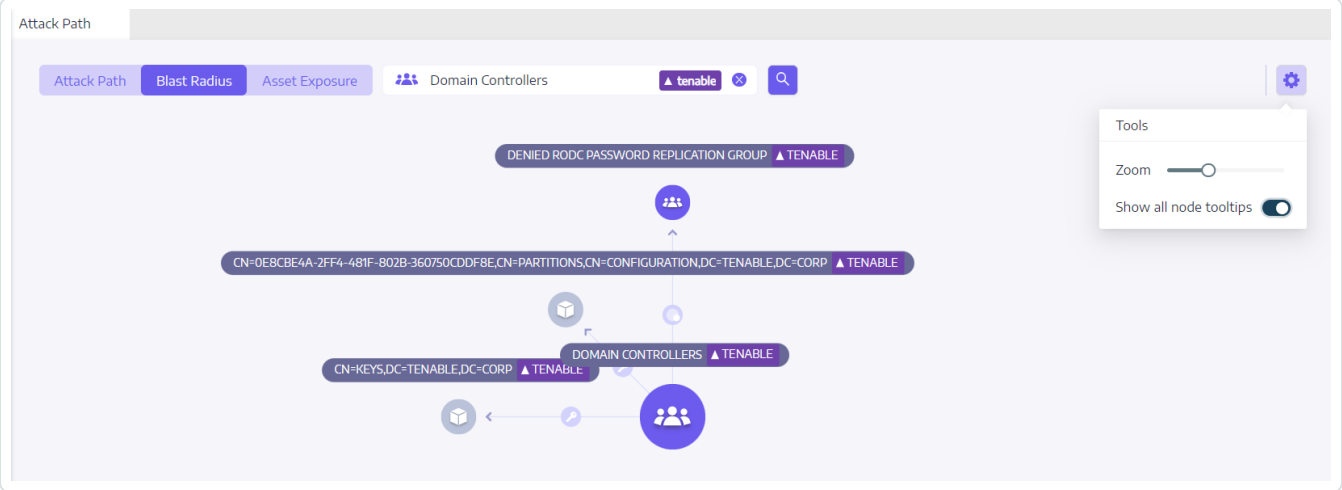
   The **Attack Path** pane appears.

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

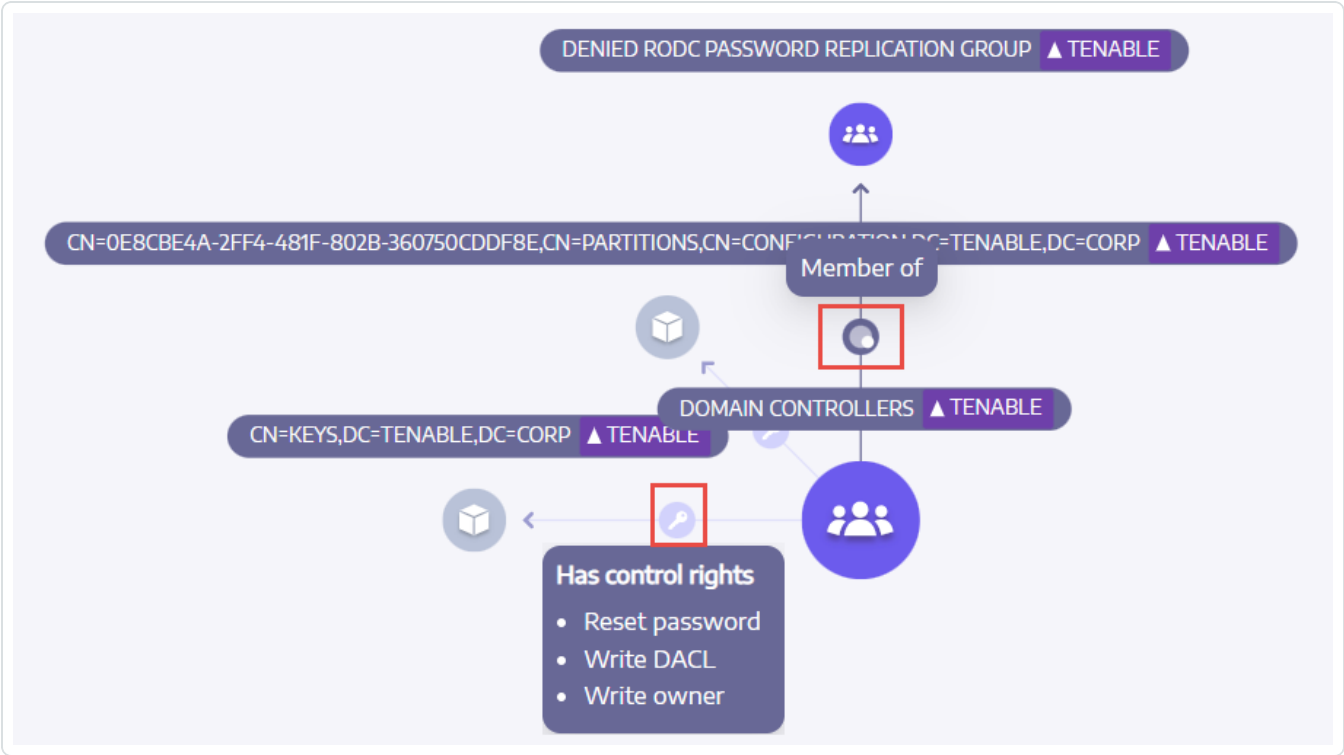
3. In the **Search for an object** box, type the name of an asset.

4. Click the icon.

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



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



To display the Asset Exposure:

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

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

   The **Attack Path** pane appears.

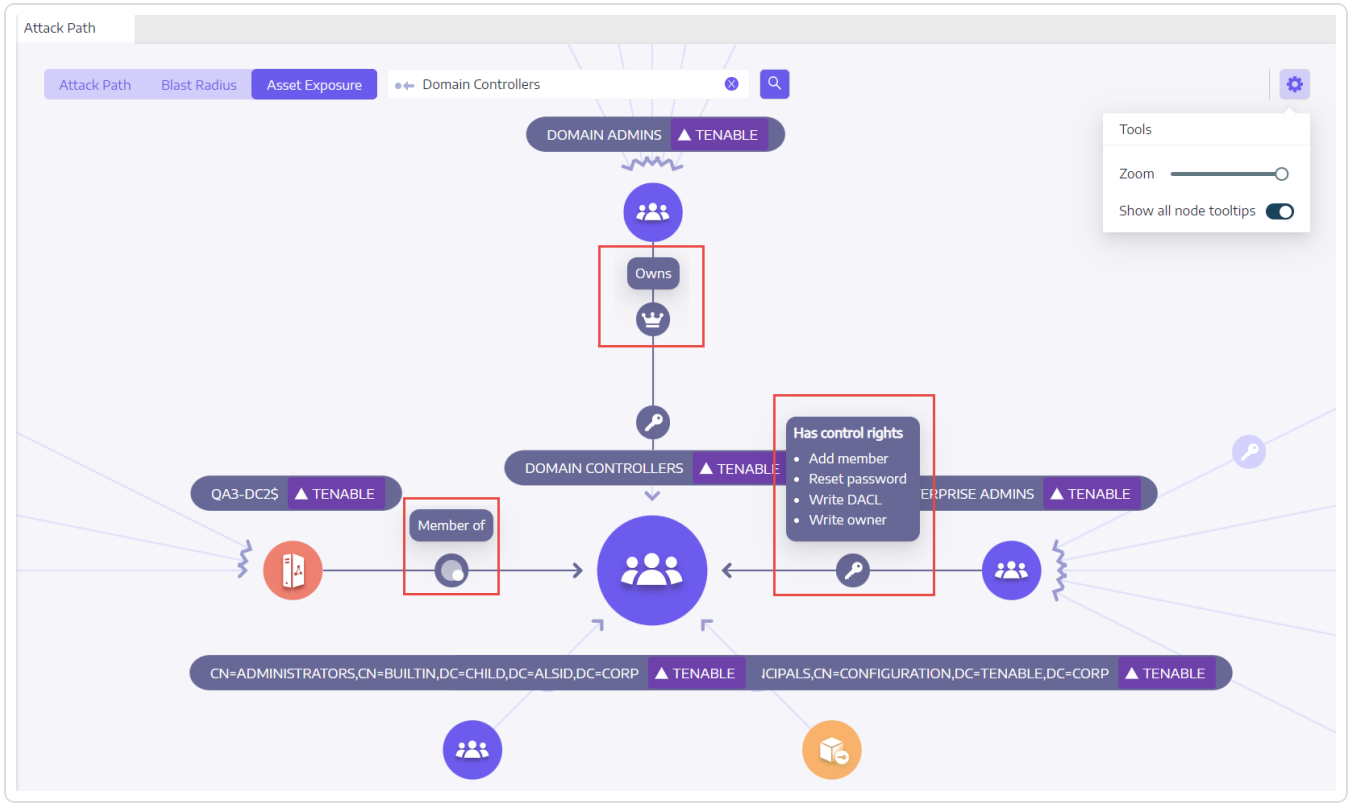
2. In the banner, click **Asset Exposure**.

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

4. Click the icon.

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

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

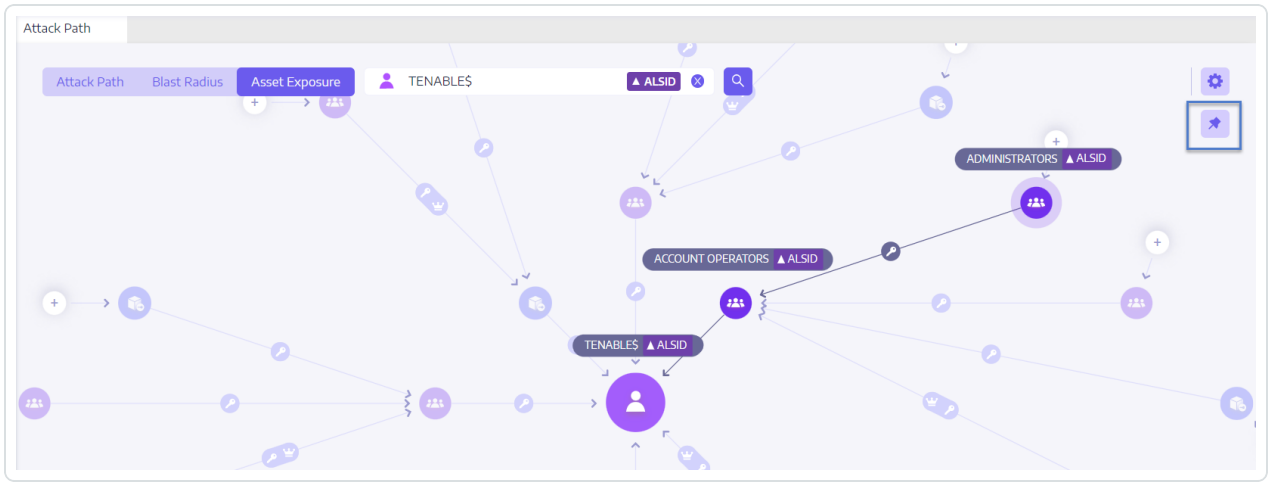


To pin an attack path:

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.

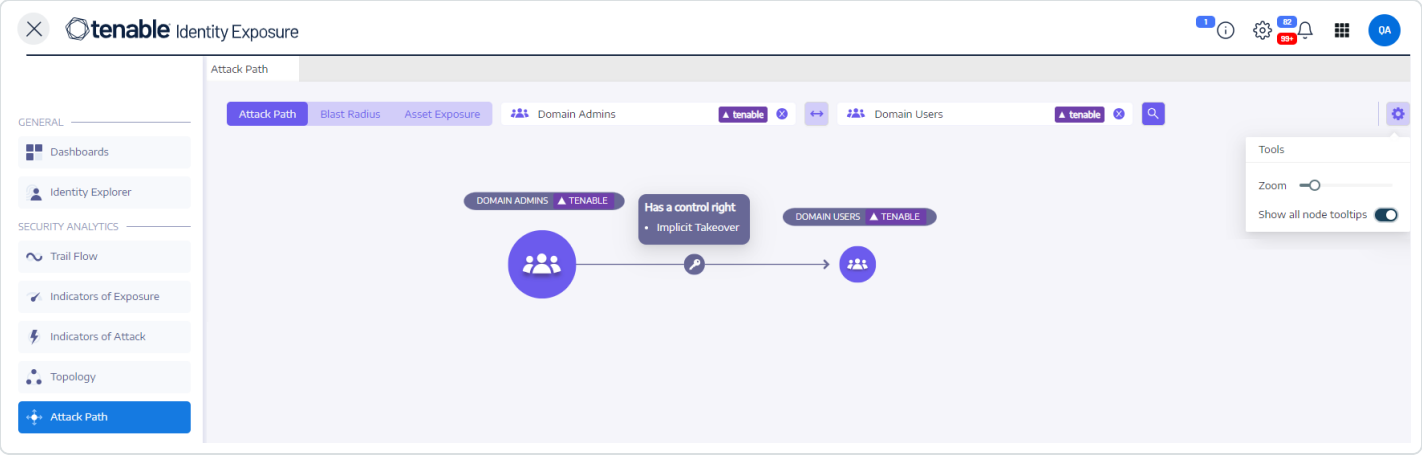


See also

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

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.

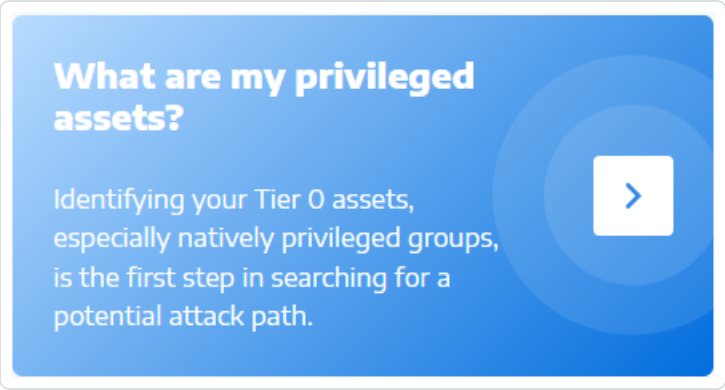
Tenable Identity Exposure lists your Tier 0 assets and accounts with potential attack paths leading to that asset.

To list Tier 0 assets:

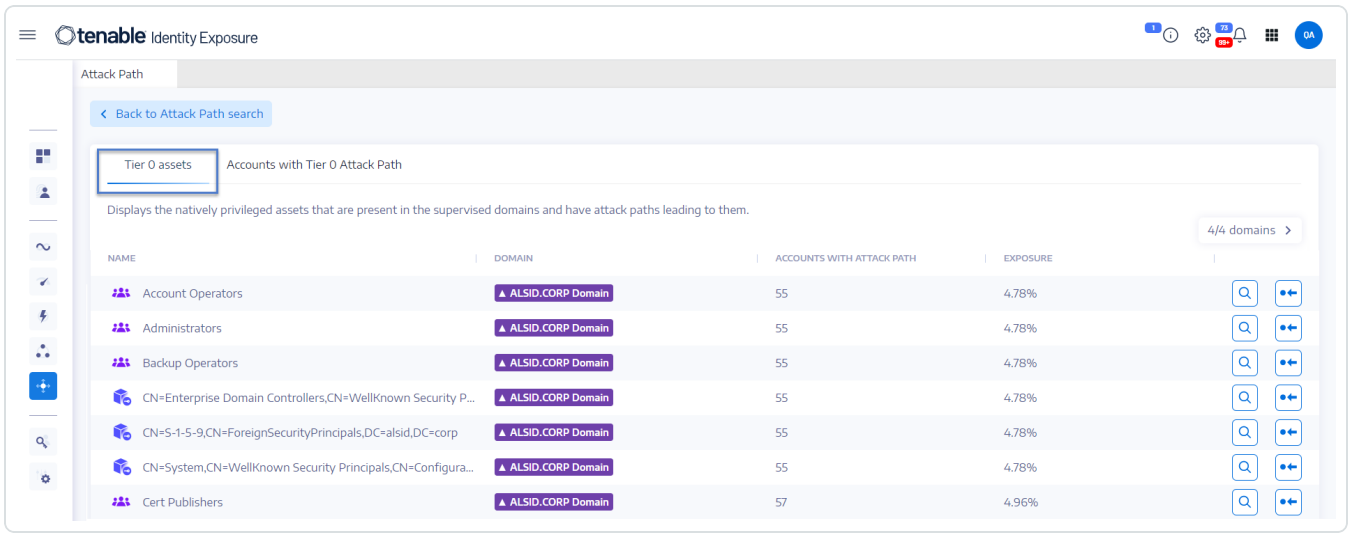
1. In Tenable Identity Exposure, click on the Attack Path icon in the left navigation bar.

   The **Attack Path** pane opens.

2. Click on the tile "**What are my privileged assets?**".

   Tenable Identity Exposure shows a list of Tier 0 assets in your AD.



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.

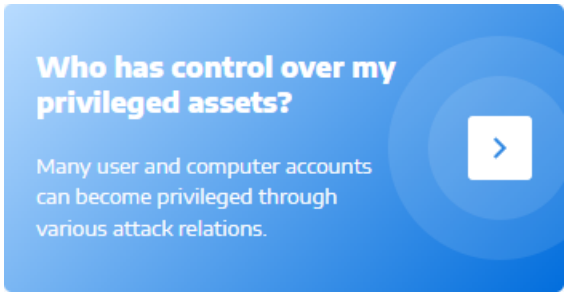
For more information, see Identifying Tier 0 Assets.

To show assets with attack paths:

1. In Tenable Identity Exposure, click on the Attack Path icon in the left navigation bar.

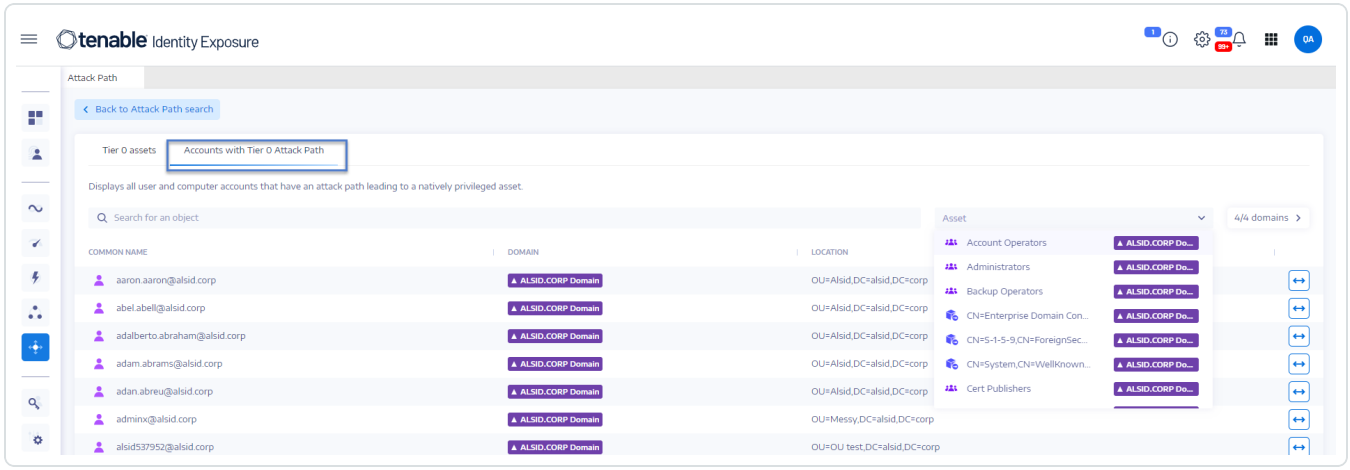
   The **Attack Path** pane opens.

2. Click on the tile "**Who has control over my privileged assets?**".

   Tenable Identity Exposure shows all user and computer accounts that have an attack path

leading to a Tier 0 asset.



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:

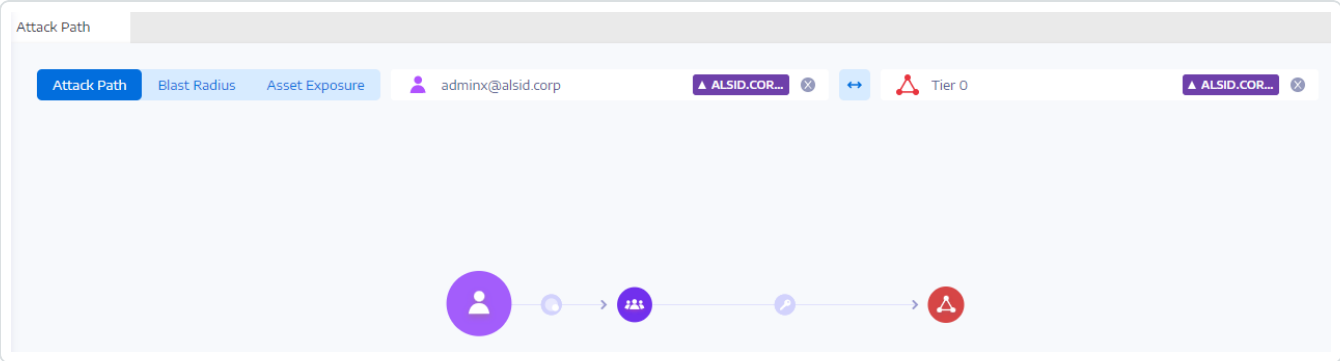
   - In the **Search** box, type the name of a forest or domain.
   - Select the **Expand all** box and select the forest or domain that you want.
2. Click **Filter on selection**.

   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	LDAP		LDAP object that has its `objectClass` attribute containing the class `organizationalUnit`. Avoid

(OU)			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 (DC)	LDAP		LDAP object that has its `objectClass` attribute containing the class `computer` and its `primaryGroupID` 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.

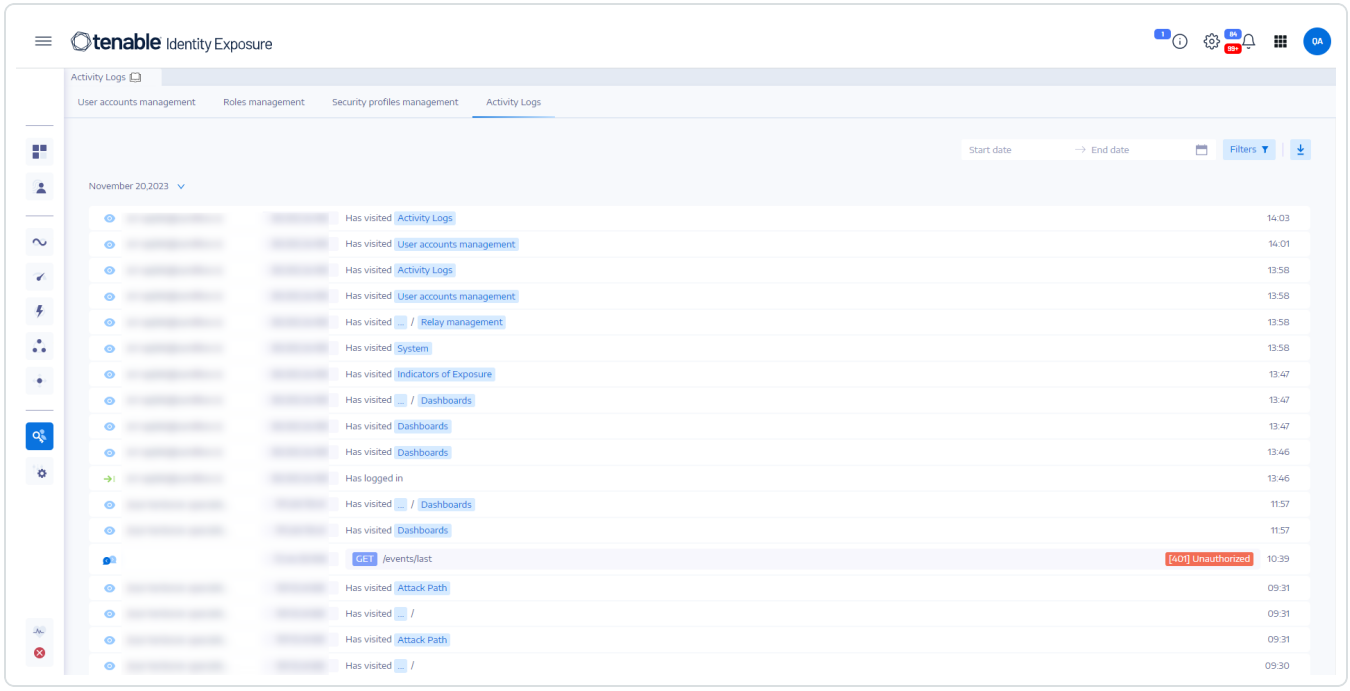
To view the activity logs:

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.



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.

SAML Authentication and Impersonation Entries

Because Tenable Identity Exposure uses SAML authentication to connect with Tenable Cloud, actions performed by Tenable Identity Exposure are logged as impersonation events.

Each request that Tenable Identity Exposure sends to Tenable Cloud appears in the Activity Logs as if it were performed by the service account established for the SAML connection.

In these entries:

- **Actor** – the Tenable Cloud account used to log into Tenable Identity Exposure through the target account
- **Target** – shows the account associated with the SAML redirection

As a result, the Activity Logs may display a large number of impersonation events. This behavior is expected and reflects how the SAML integration manages authentication, not an issue with account security.

Privileged Entity Definitions

Tenable Identity Exposure uses the concept of **"privileged"** entities in various Indicators of Exposure, Indicators of Attack, and other features. The definition of privileged entities differs between Active Directory and Entra ID:

Active Directory

Privileged entities may encompass **privileged users**, **privileged computer accounts**, **privileged service accounts**, **privileged groups**, **privileged security principals**, etc. Privileged entities include the (Local) System and KRBTGT (Kerberos Ticket Granting Ticket) users and all direct or indirect (transitive) members of the following natively privileged groups, which are identified internally by their well-known RID/SID, regardless of their names.

- Account Operators
- Administrators
- Backup Operators
- Cert Publishers
- Domain Admins
- Domain Controllers
- Enterprise Admins
- Enterprise Domain Controllers
- Enterprise Key Admins
- Enterprise Read-Only Domain Controllers
- Group Policy Creator Owners
- Key Admins
- Print Operators

- Read-Only Domain Controllers
- Replicators
- Schema Admins
- Server Operators

Entra ID

- A **privileged entitlement** or **permission** is one identified as such by Microsoft.
- A **privileged role** is an Entra role containing at least one privileged permission as defined by Microsoft.
- **Privileged entities** (users, groups, or service principals) are those assigned directly or indirectly (transitively via a role-assignable group) to any privileged Entra role.

Tenable Identity Exposure Configuration and Administration

The options and capabilities outlined in this section are geared towards administrators and advanced users looking to customize, optimize, and maintain their Tenable Identity Exposure installation or deployment.

You'll find specialized instructions here on topics like managing Active Directory, configuring Indicators of Attack deployment, authentication settings, user accounts, security profiles, roles, forests, domains, and alerts. This section also covers running health checks, using the reporting center, integrating with Microsoft Entra ID (formerly Azure AD), licensing, and troubleshooting.

To find information related to a specific task, click on the relevant topics in the menu pane on the left side of the screen.

> **Permission**: These tasks require administrative access privileges.

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 PowerShell console, run the following commands to grant access to Active Directory objects or containers:

  Note: You must run these commands on each domain that Tenable Identity Exposure monitors.

  ```
  #Set Service Account
  $serviceAccount = "<SERVICE_ACCOUNT>"

  #Don't Edit after here
  $domain = Get-ADDomain
  @($domain.DeletedObjectsContainer, "CN=Password Settings
  Container,$($domain.SystemsContainer)") | ForEach-Object {
      & dsacls $_ /takeownership
      & dsacls $_ /g "$($serviceAccount):LCRP" /I:T
  }
  ```

  where `<__SERVICE_ACCOUNT__>` refers to the service account that Tenable Identity Exposure uses.

Alternatively, if PowerShell is not available, you can also execute these commands for each container:

```
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:

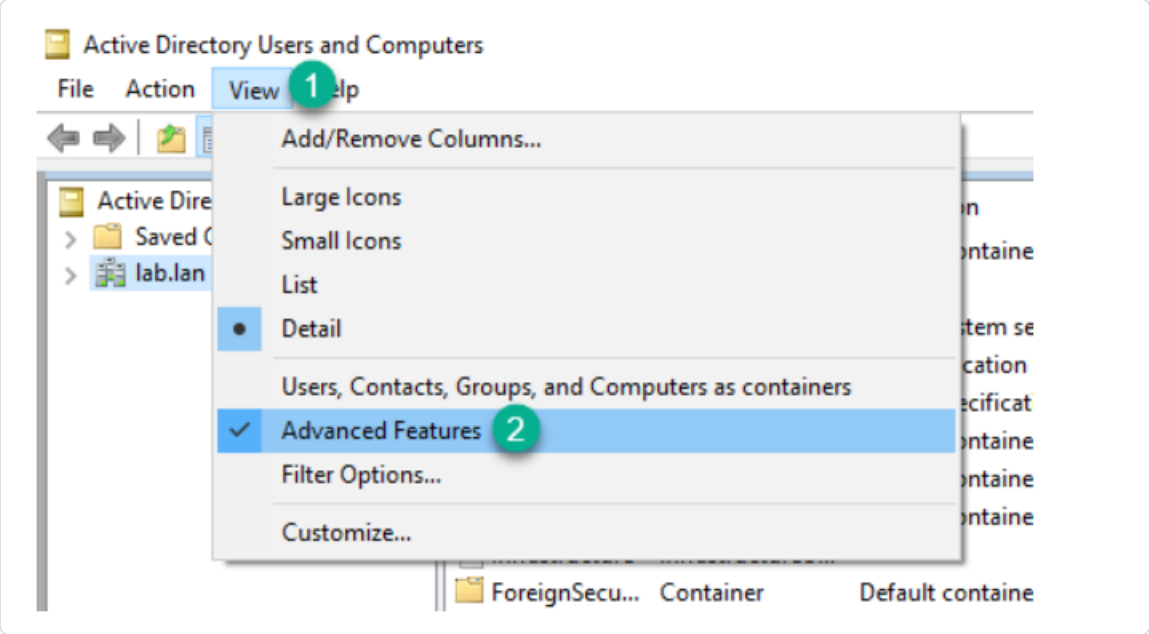
```
dsacls "<__DOMAIN_ROOT__>"  /g "<__SERVICE_ACCOUNT__>:CA;Replicating Directory Changes" "<__
SERVICE_ACCOUNT__>:CA;Replicating Directory Changes All"
```

  Where:

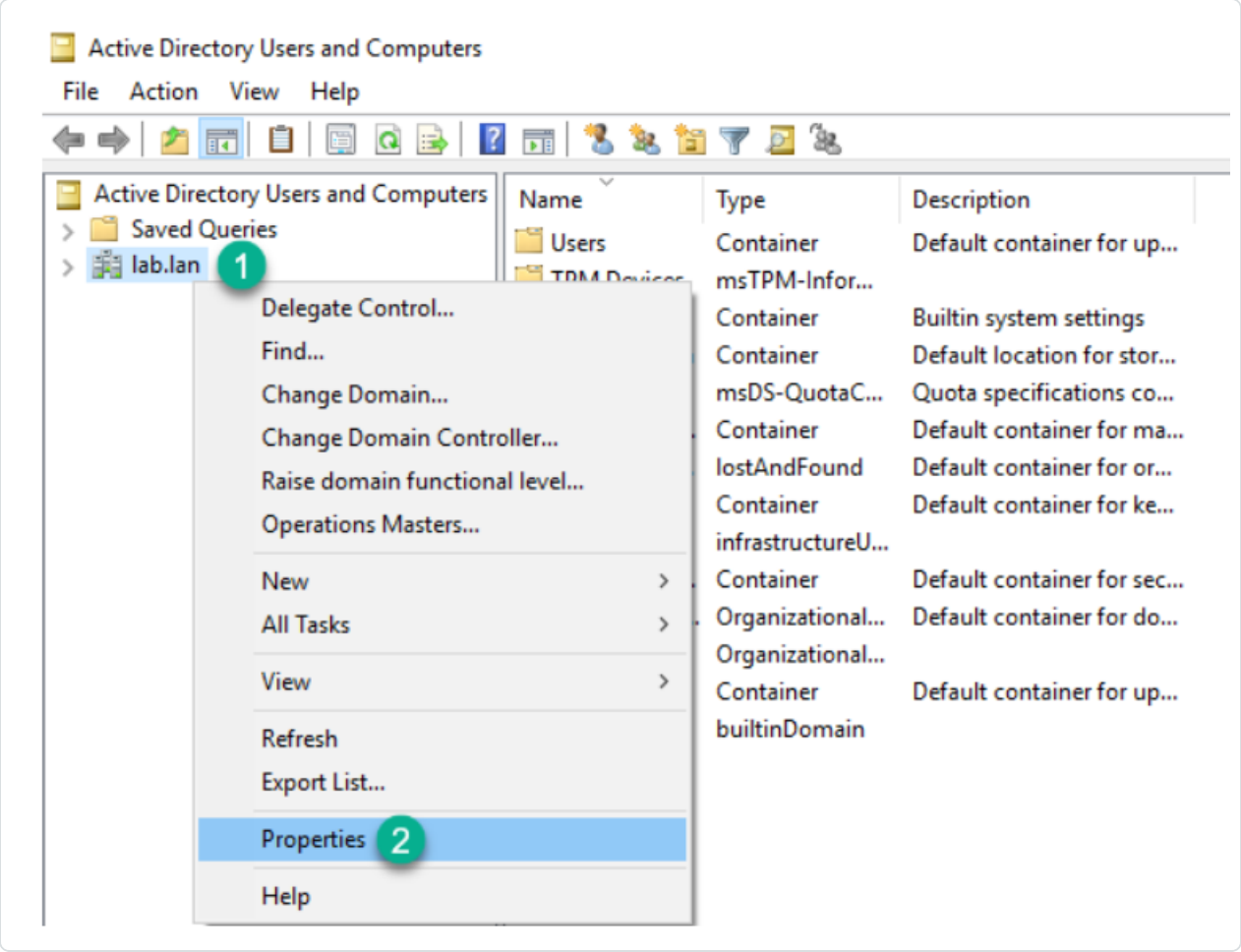
  - `<__DOMAIN_ROOT__>` refers to the Distinguished Name of the root of the domain. Example: `DC=<DOMAIN>,DC=<TLD>`
  - `<__SERVICE_ACCOUNT__>` refers to the service account that Tenable Identity Exposure uses. Example: `DOMAIN\tenablead`.

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**.

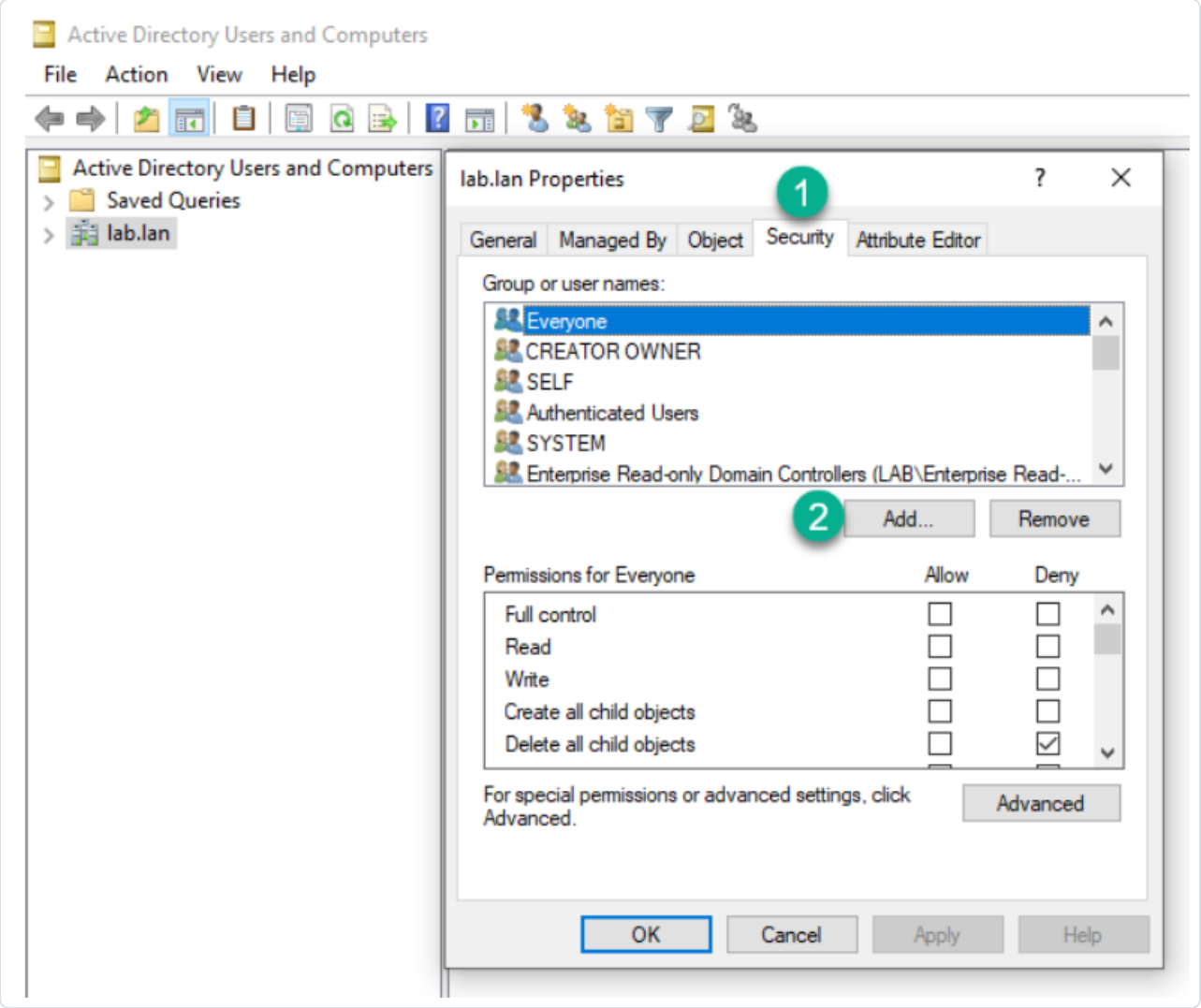


3. Right-click on the domain root and select **Properties**.



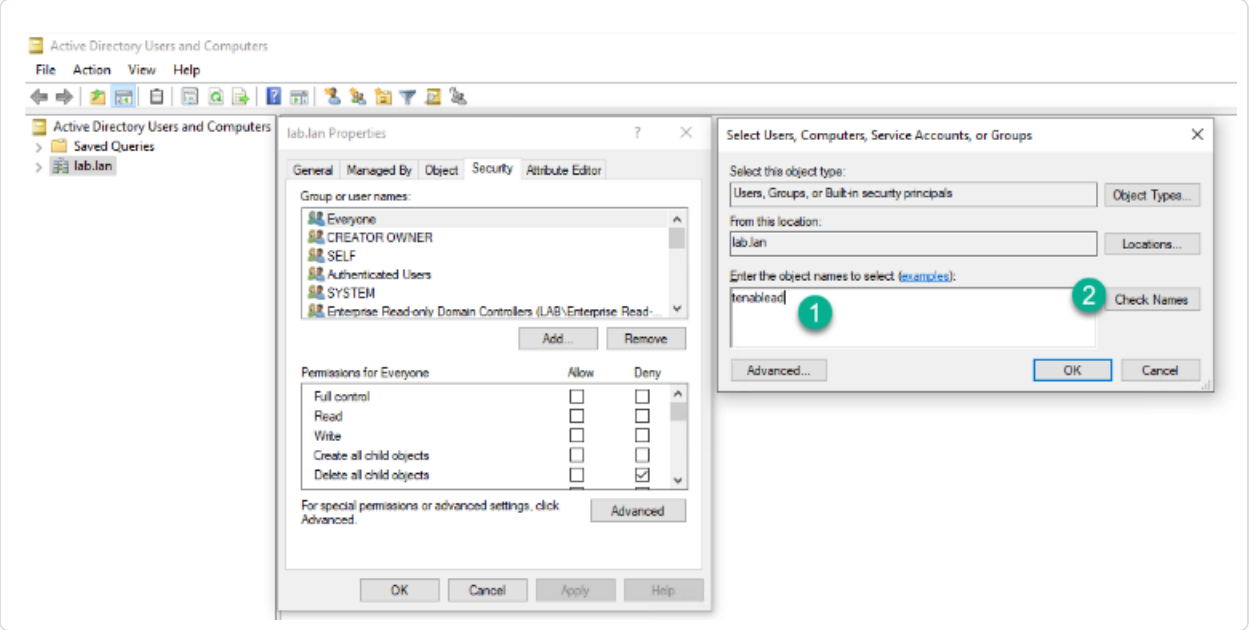
The domain root's properties pane opens.

4. Click the **Security** tab and click **Add**.

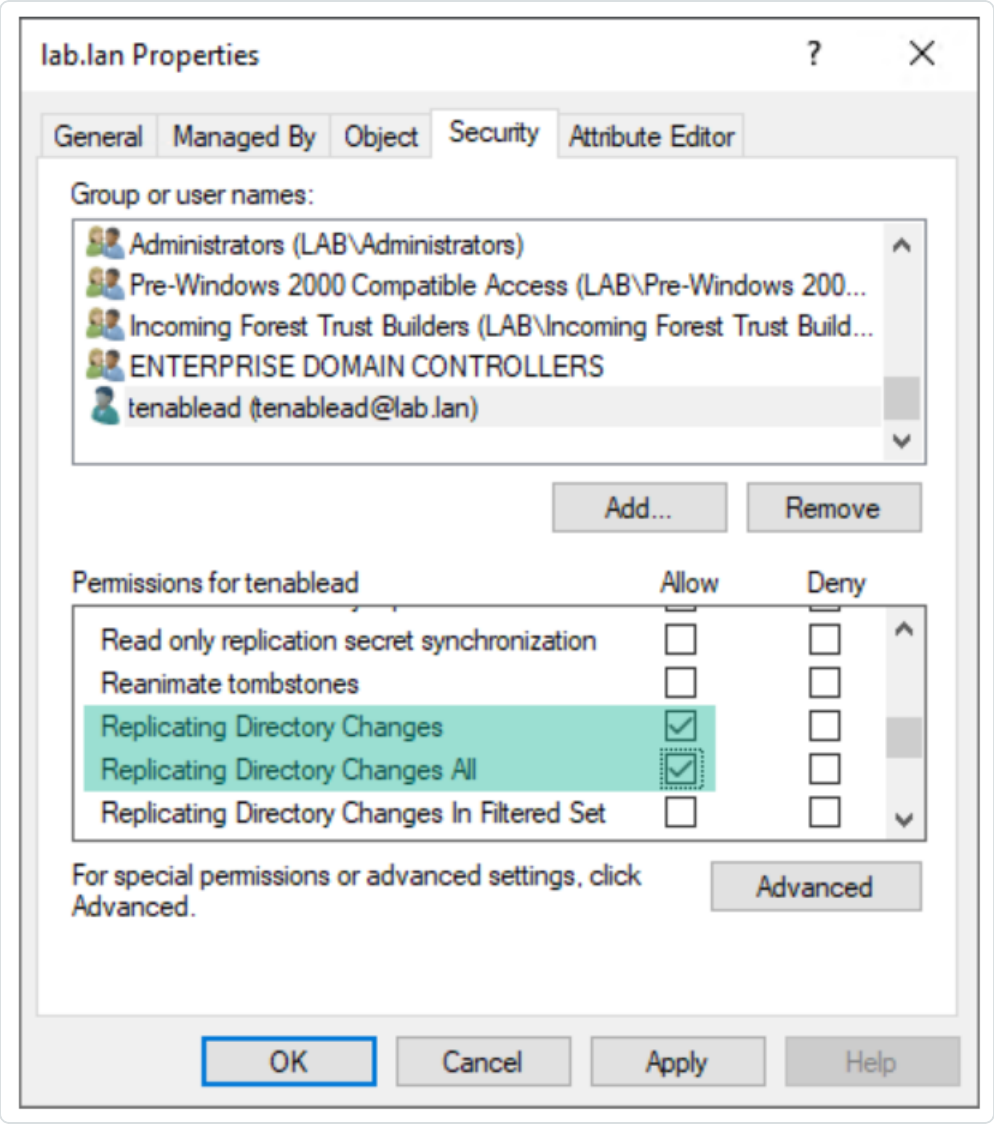


5. Locate the Tenable Identity Exposure service account:

> **Note**: in a forest with multiple domains environment, the service account may be in a different Active Directory domain.



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*.



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.

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.

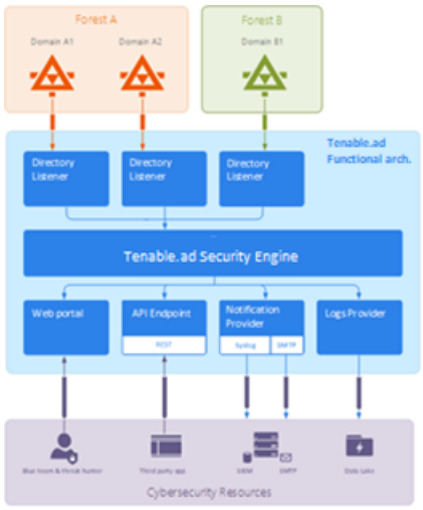
Tenable Identity Exposure uses a regular user account with no administrative permissions to connect to standard APIs for its security monitoring feature.

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.

  To do this, run the following PowerShell command on the target machine (DC) where you plan to deploy the IoA module:

  ```
  if (-not (Get-Module -ListAvailable -Name GroupPolicy)) {
      Write-Error "The GroupPolicy module is not installed or not available on this machine. This is a requirement for this script and the IOAs to run, please install it and run this script again."
  }
  ```

  Any error appearing in your console indicates that this requirement is not validated in your current environment.
- 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.
- **Dedicated SMB share** – If you use the dedicated SMB share instead of SYSVOL to store event logs files:
  - You must have SMBv2 or above enabled to install and run the IoA module. SMBv1 is a legacy protocol which Tenable Identity Exposure does not support for security reasons.
  - This requirement also applies to its normal operating conditions. If you install the module under the correct configuration and subsequently revert to SMBv1-only, the IoA module disables itself until you restore the proper SMB configuration (SMBv2 or above).

To check your SMB configuration on your Domain Controllers, follow the instructions from the official Microsoft documentation.

- Your domain controllers must be able to communicate with your PDCe (Primary Domain Controller emulator) using the SMB protocol.

- 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.

Note: You must redeploy the IoA installation script after each new release of a major version of Tenable Identity Exposure.

Note: The recommended version of PowerShell is 5.1.

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.

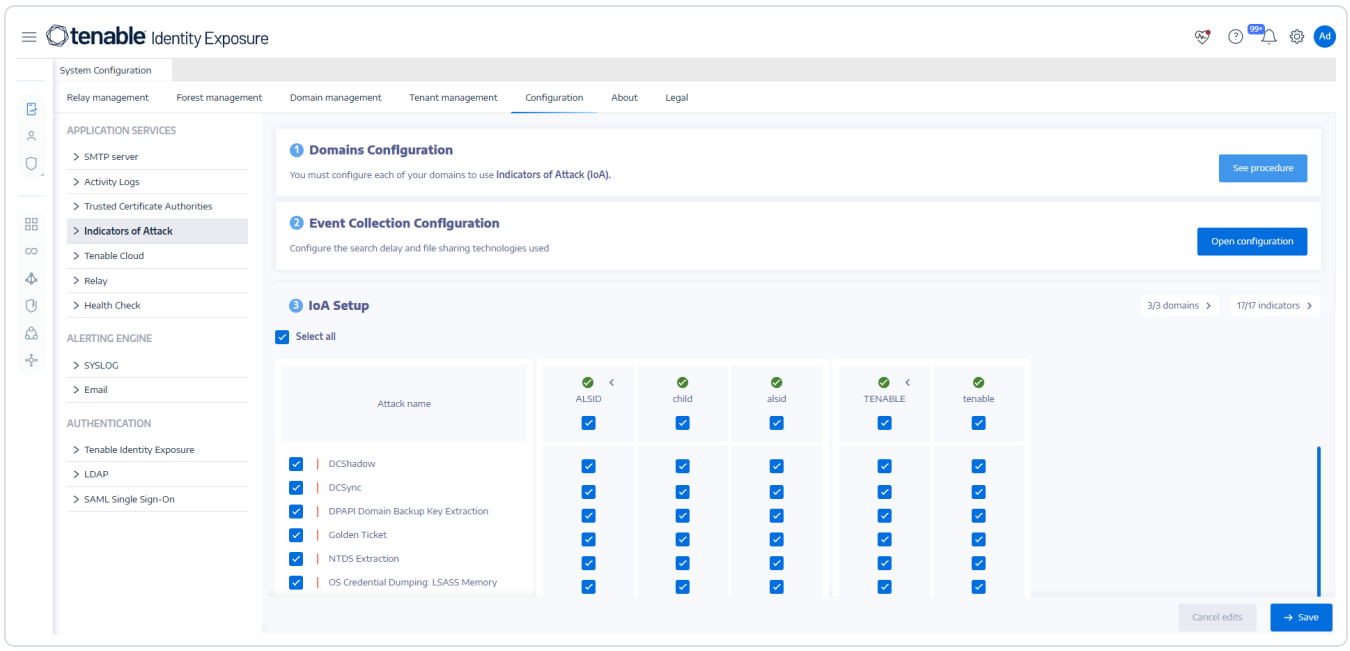
To configure domains for IoAs:

1. In Tenable Identity Exposure, click **System** on the left menu bar and the **Configuration** tab.

   The **Configuration** pane appears.

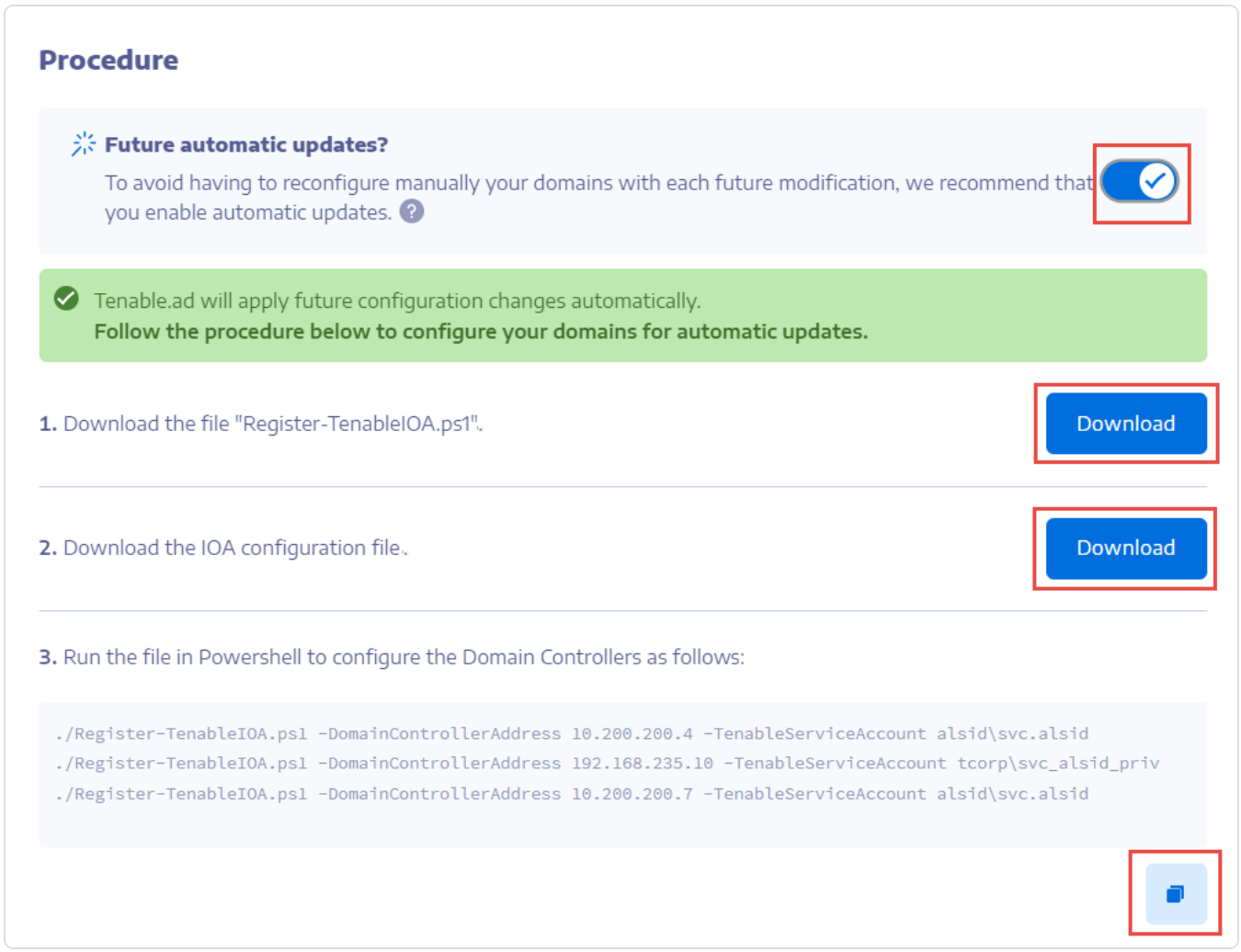
2. Click **Indicators of Attack**.

   The IoA configuration pane appears.



3. In **(1) Domains Configuration**, click **See Procedure**.

   A procedure window opens.



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.

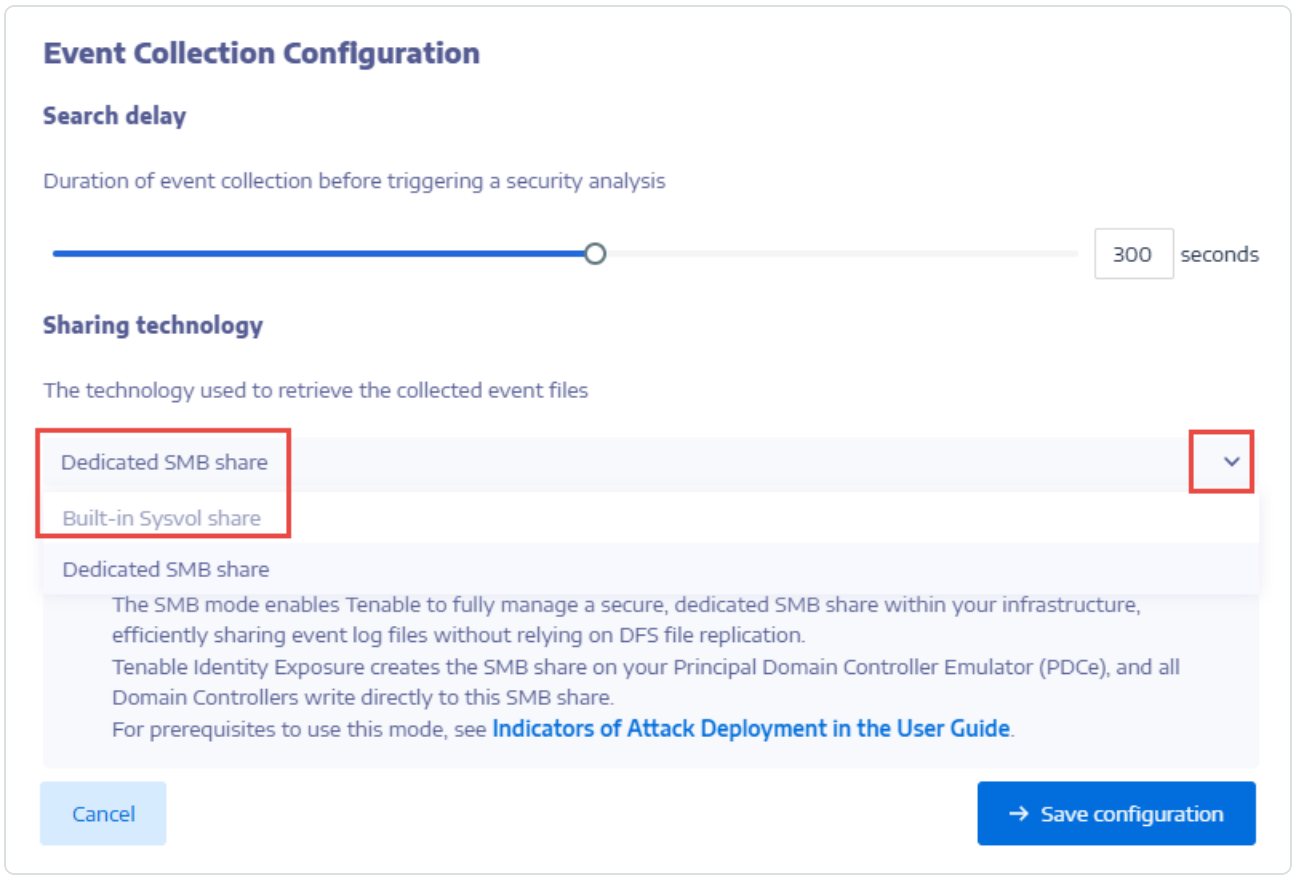
8. Click outside the procedure window to close it.
9. Open a PowerShell terminal with administrative rights and run the commands to configure your domain controllers for IoAs.

> **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 select an event collection configuration:

1. In **(2) Event Collection Configuration**, click **Open Configuration**.

   A configuration window appears.



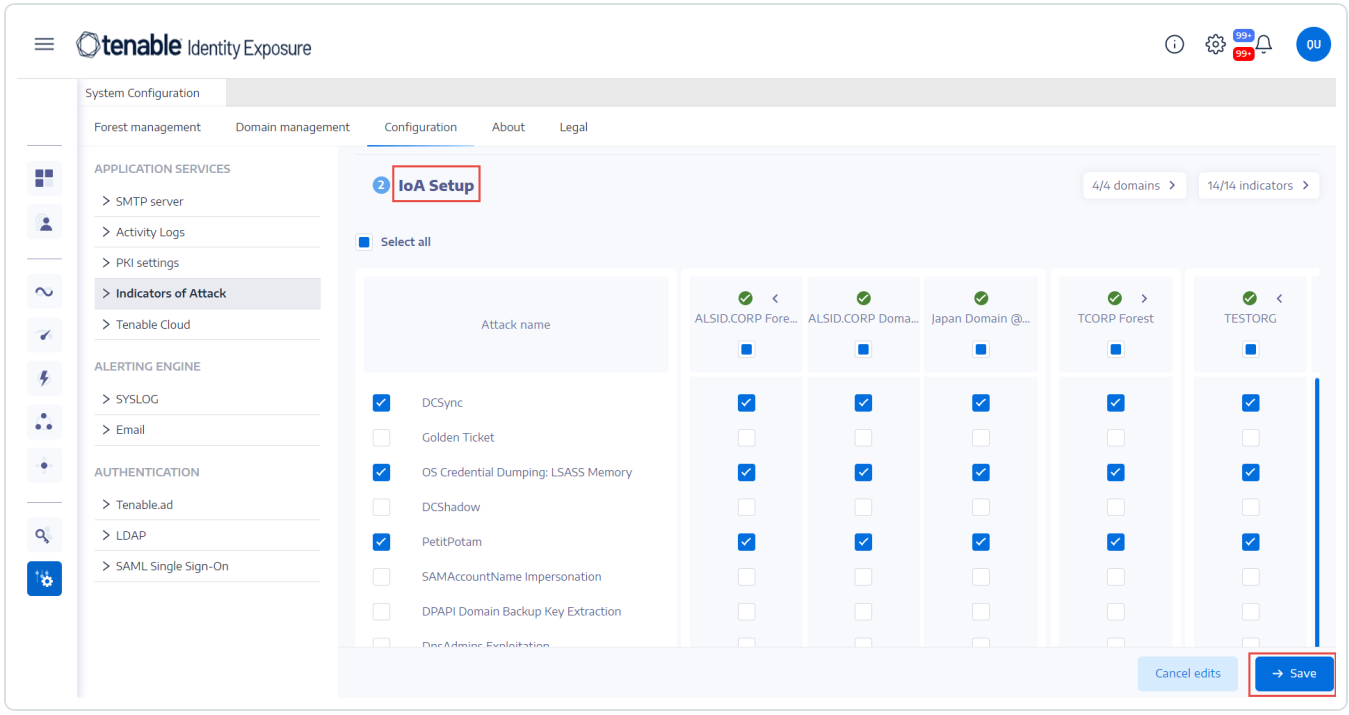
2. Under **Search delay**, move the slider to select the duration of event collection before triggering a security analysis.
3. Under **Sharing technology**, click the drop-down arrow to select one of the following:
    - **Dedicated SMB share** – Tenable Identity Exposure creates the SMB share on your Principal Domain Controller Emulator (PDCe), and all Domain Controllers write directly to this SMB share. For prerequisites to use this mode, see Indicators of Attack Deployment.
    - **Built-in SYSVOL share** – Event logs files stored on the SYSVOL share will be available across all Domain Controllers as part of the DFSR mechanism.

    > **Note**: After installation of the IoA module, you can switch between SMB and SYSVOL modes at any time, provided you observe the prerequisites for SMB mode as indicated in Indicators of Attack Deployment.

    > **Note**: Two domain health checks help you assess the status of the IoA modules. For more information, see Health Checks.
4. Click **Save configuration**.

To set up your IoAs:

1. In the IoA configuration pane, under **IoA Setup,** select the IoAs you want in your configuration.

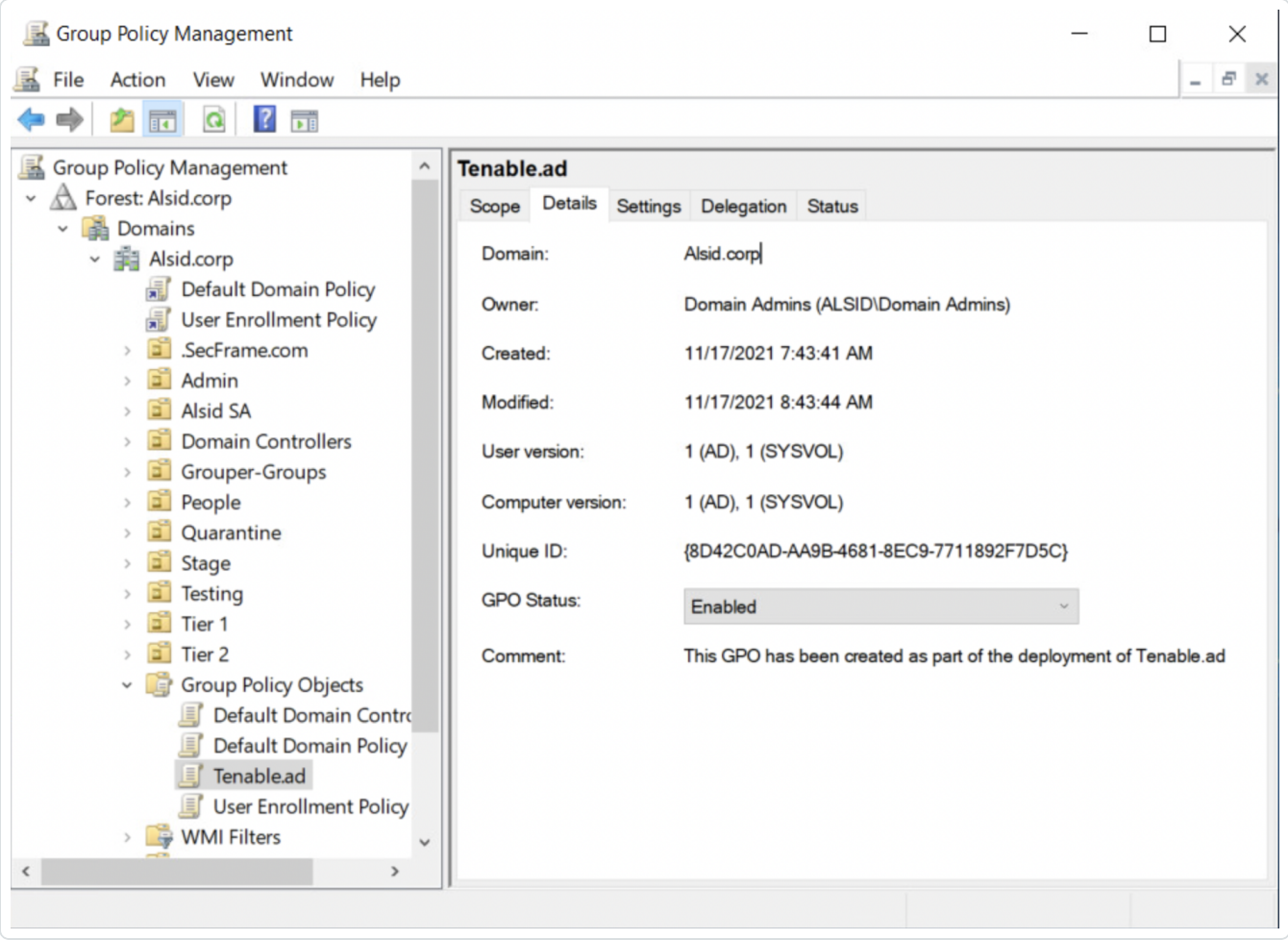


Tip: The **Zerologon Exploitation** Indicator of Attack (IoA) dates from 2020. If all of your domain controllers (DCs) received updates within the past three years, they are protected from this vulnerability. To determine the required patches for securing your DCs against this vulnerability, consult 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.

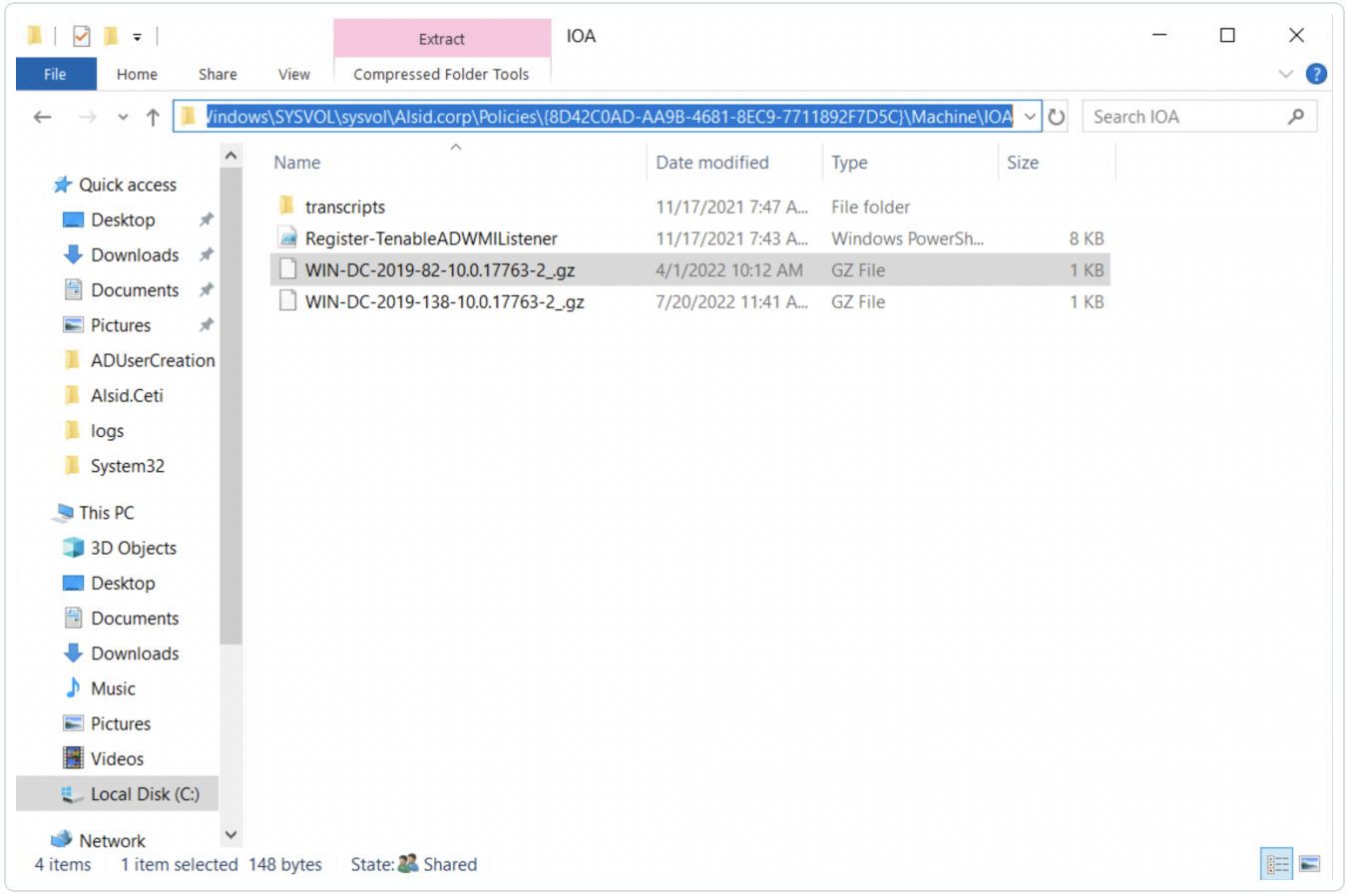
2. Click **Save**.
    - If you enabled **Future automatic updates**, Tenable Identity Exposure saves and automatically updates your new configuration. Allow a few minutes for this update to take effect.
    - If you did not enable **Future automatic updates**, a procedure window appears to guide you 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:



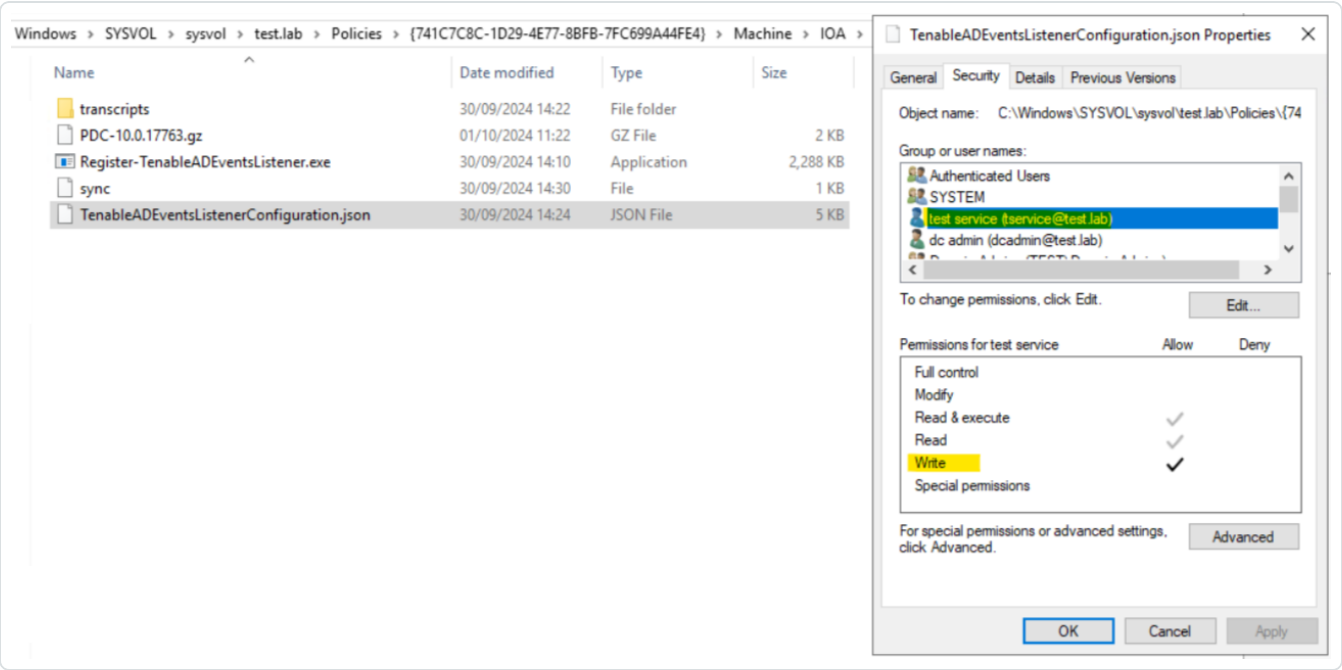
2. Go to the path `C:\Windows\SYSVOL\sysvol\alsid.corp\Policies\{GUID}\Machine\IOA` and check that the `.gz` file exists for **all domain controllers** before you test the IoAs:



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 `TenableADEventsListenerConfiguration.json` file 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 active for the Tenable service account.



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:

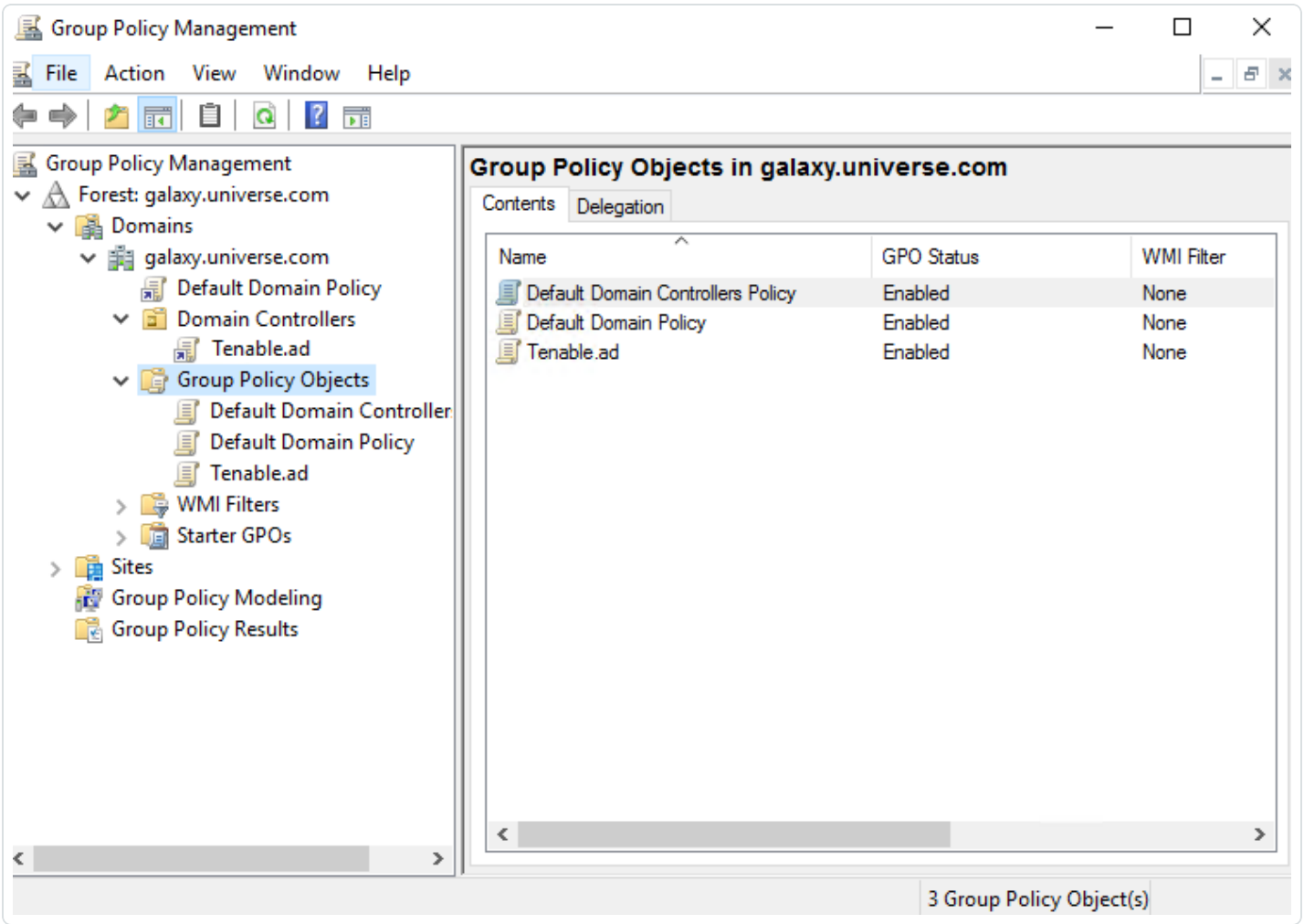
Message	Remediation
"Tenable Identity Exposure cannot write to the configuration file because the target folder `<targetFolder>` does not exist. This indicates that the IoA module deployment may have failed."	Uninstall the script and click "See procedure" for instructions to re-install the script.
"Tenable 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.



Installation Script (Tenable Identity Exposure v. 3.59 and later)

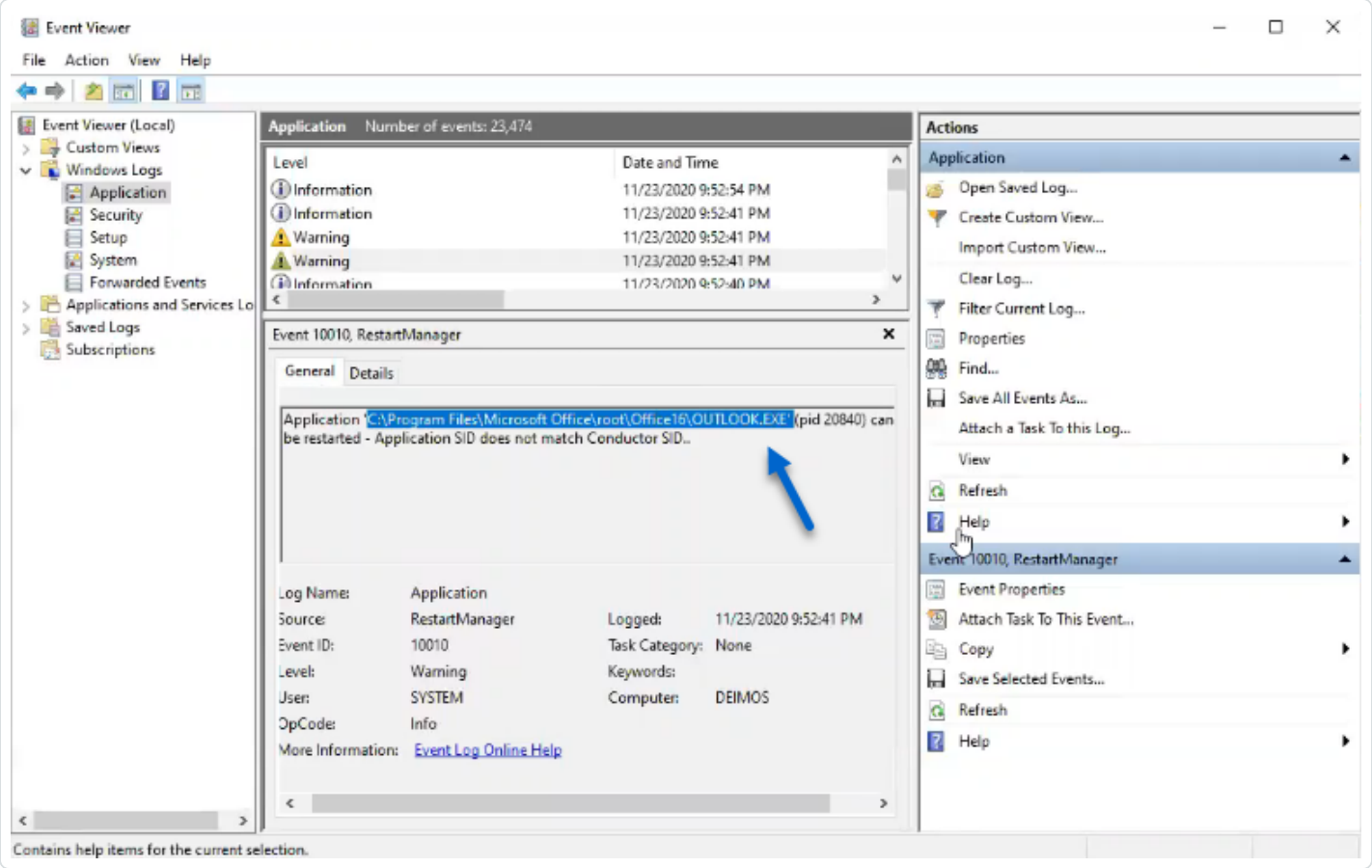
The GPO contains PowerShell scripts that all DCs execute locally to collect data of interest, as follows:

- 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.
- Dedicated SMB share:
    - The event listener captures event logs, buffers them, and periodically flushes them to a file stored on a dedicated SMB share hosted on your PDCe. Tenable Identity Exposure automatically maintains and secures this SMB share through the event listener. Each Domain Controller writes to a single file on the dedicated SMB share on the PDCe SMB.
    - Tenable Identity Exposure's platform listens to SMB updates on this dedicated share to collect event data, perform security analyses, and 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.



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	GPO Manage	Creates the `Tenable.ad` (default name) GPO and links it to the Domain Controllers OU.

	Identity Exposure's IoA deployment	ment	
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 produce	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.

	r		
6	Collect event logs messages	DC local system	• **SYSVOL** mode – 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_GUID}\Machine\IOA<DC_name>`). • **SMB** mode ◦ The physical path where the files reside by default is `SmbShareLocation` on the PDCe, which defaults to `C:\Tenable\IdentityExposure\IOALogs`. You can modify this parameter as needed, with instructions available in the documentation on IoA installation script parameters. ◦ The network path that the listeners use to send files is `\\{PDCe_HOSTNAME}\TIE-IOA-Logs$`, where `{PDCe_HOSTNAME}` represents the hostname of the PDCe.
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. 3.29 and later)

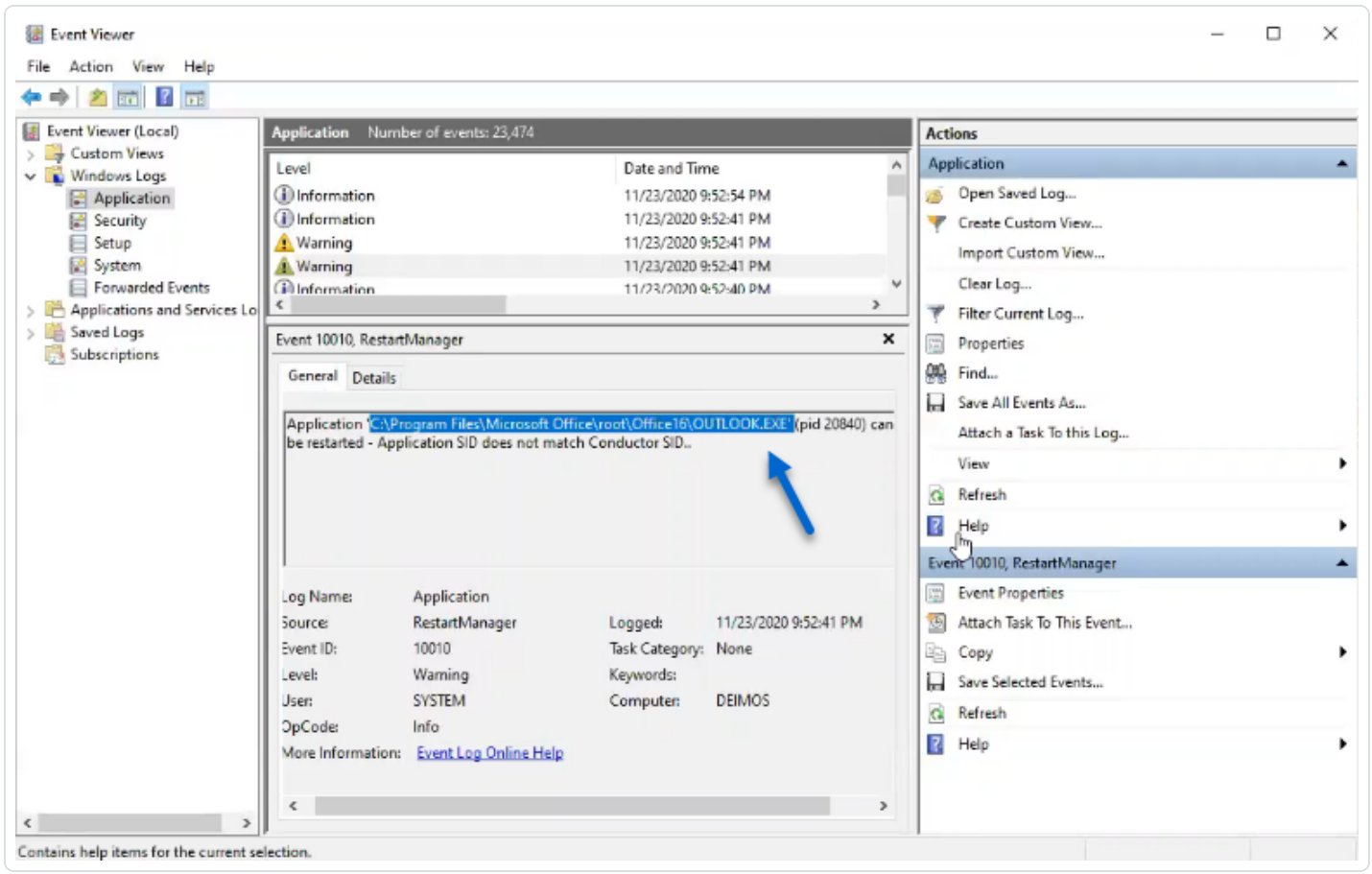
The GPO contains PowerShell scripts that all DCs execute locally to collect data of interest, as follows:

- 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.



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)

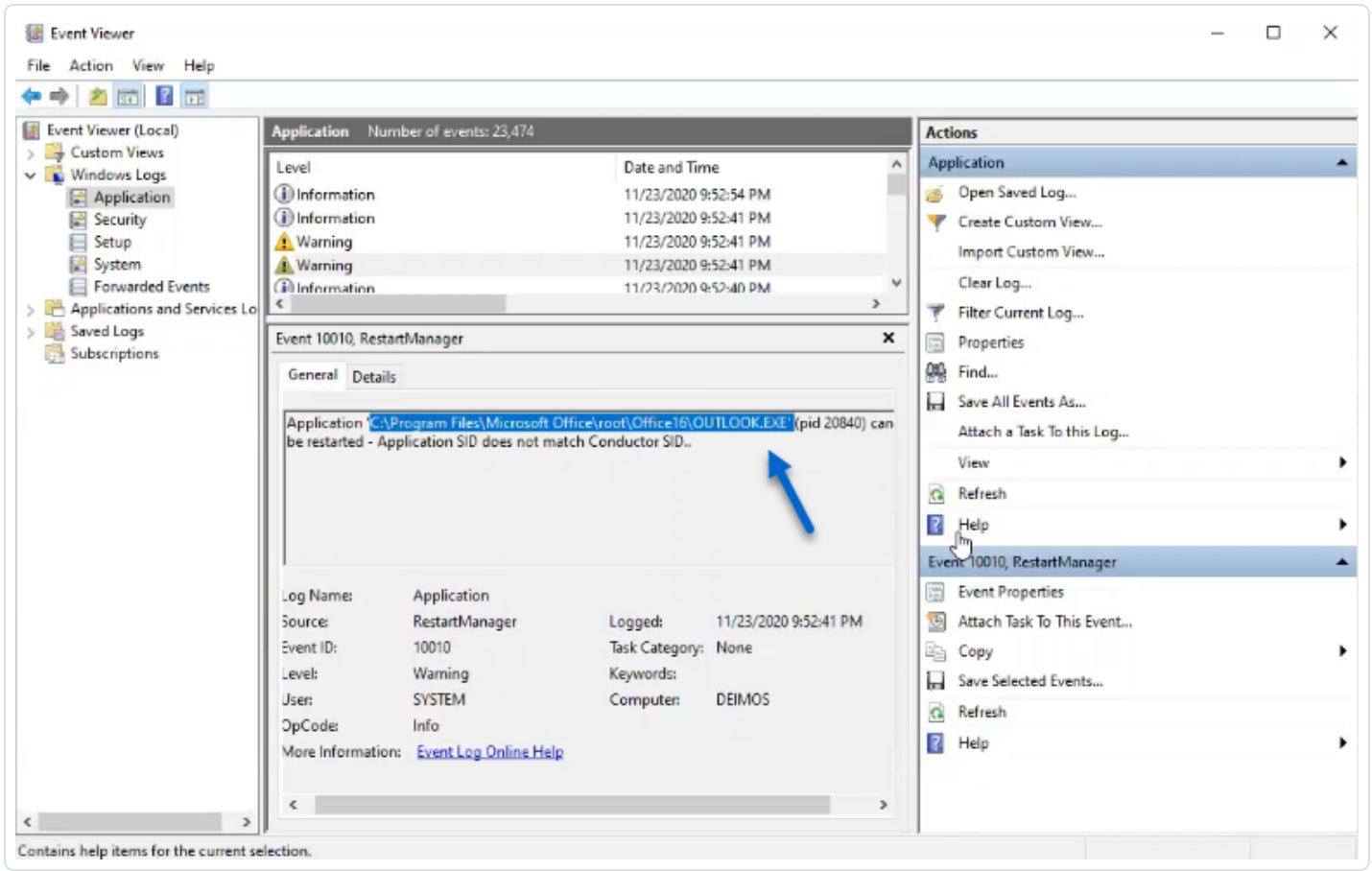
The GPO contains PowerShell scripts that all DCs execute locally to collect data of interest, as follows:

- 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.



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

- 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.

Limitations 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 .

> **Note**: SMB mode provides a solution for slow or unreliable Distributed File System replication performance by allowing Tenable to manage and utilize a dedicated, secure SMB share. For more information on how to use the dedicated SMB share, see Indicators of Attack Deployment and Install Indicators of Attack.

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:

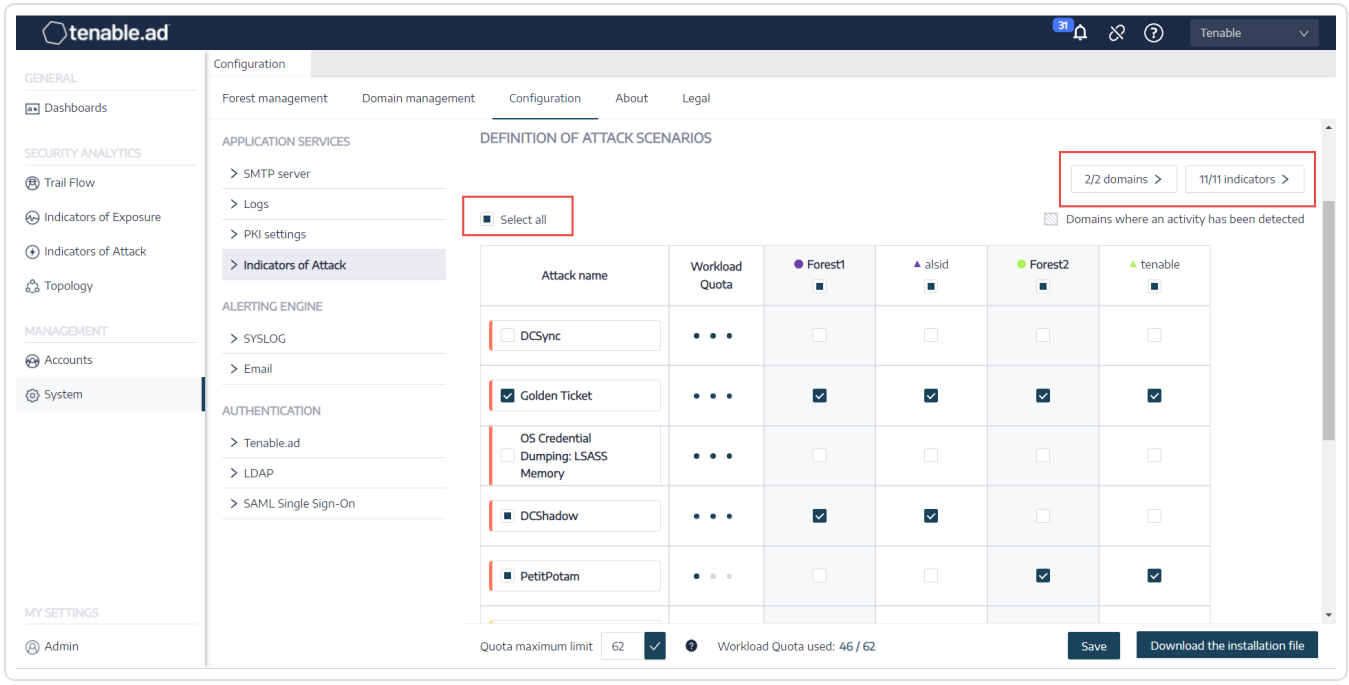
- In **Data Entities**, "Read" access for:
  - All Indicators of Attack
  - All domains
- In **Interface Entities**, access for:
  - Management > System > Configuration
  - Management > System > Configuration > Application Services > Indicators of Attack
  - Management > System > Configuration > Application 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.



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**.

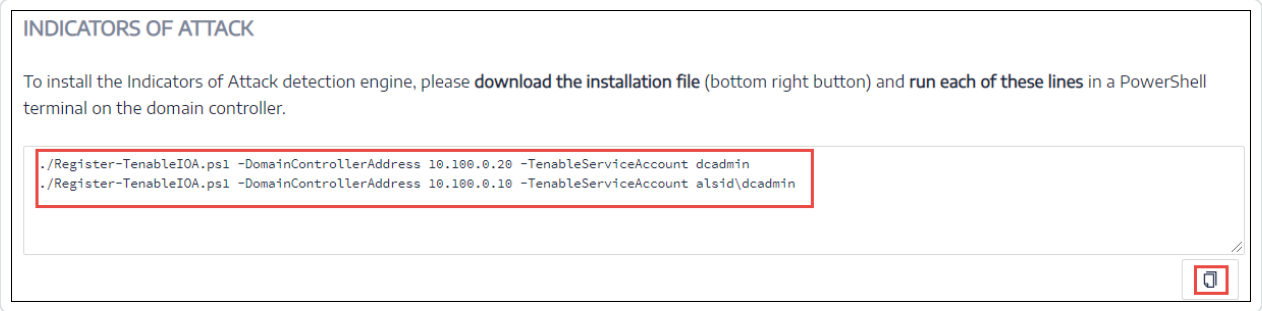
   A message confirms that Tenable Identity Exposure updated the Indicator of Attack configuration.
7. Click **Download the installation file**.

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.



    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.

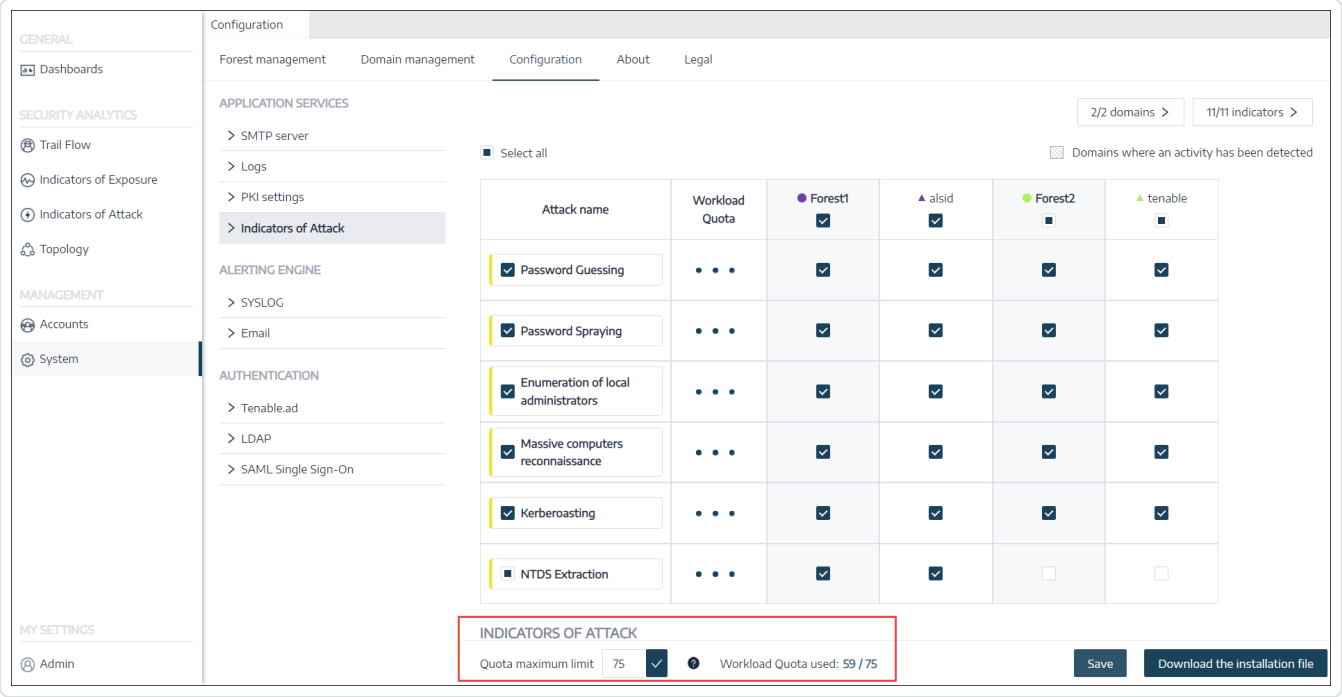
To modify the workload quota limit:

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.



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.

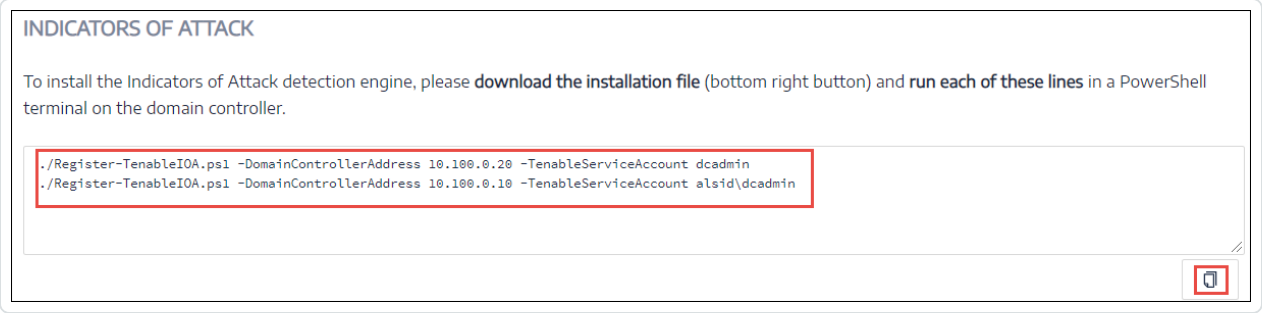
8. Click **Download the installation file**.

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.



   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
```

You have now completely uninstalled the IoAs. However, their registry entries may persist if another GPO doesn't define them. Below are the registry entries that the Massive Computers Recon IoA used (these may vary based on your specific IoA configuration):

- `HKLM\MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0\AuditReceivingNTLMTraffic (value: 2)`
- `HKLM\MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0\RestrictSendingNTLMTraffic (value: 1)`
- `HKLM\MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\AuditNTLMInDomain (value: 7)`

To remove these registry entries, run the following PowerShell script on all your domain controllers:

```
Remove-ItemProperty -Path "HKLM:\System\CurrentControlSet\Control\Lsa\MSV1_0" -Name
"AuditReceivingNTLMTraffic"
Remove-ItemProperty -Path "HKLM:\System\CurrentControlSet\Control\Lsa\MSV1_0" -Name
"RestrictSendingNTLMTraffic"
Remove-ItemProperty -Path "HKLM:\System\CurrentControlSet\Services\Netlogon\Parameters" -Name
"AuditNTLMInDomain"
```

Manual Removal of Outdated GPO Folders from SYSVOL

In some cases, when reinstalling the IoA GPO, older folders may remain in the SYSVOL directory due to a Microsoft feature. If the Directory Listener recognizes these outdated folders as the IoA folder, it can lead to detection failures.

Perform the following procedure to ensure a clean removal of outdated IoA GPO folders, preventing detection issues during reinstallation.

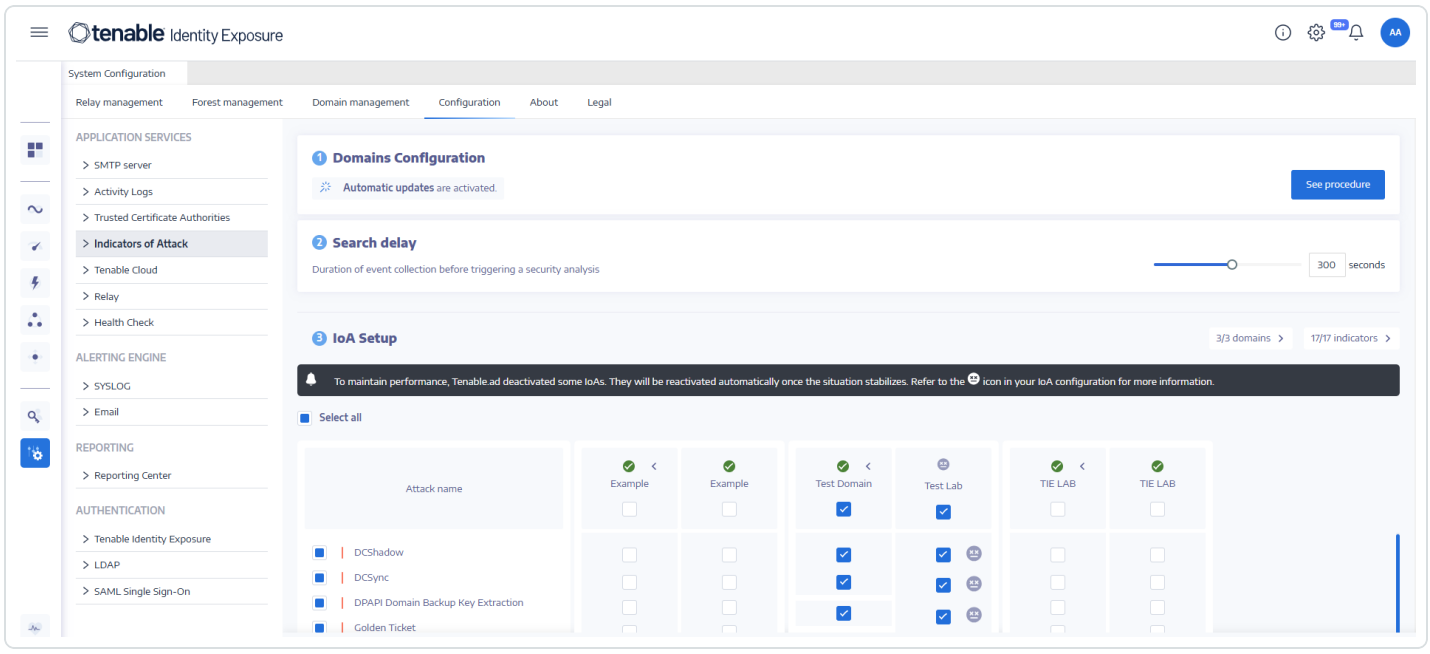
To remove outdated IoA GPO folders:

1. Identify the latest IoA GPO GUID: Determine the GUID (Globally Unique Identifier) of the latest installed IoA GPO.
2. Review the logs (`tenable_Ceti.log` located in the directory `C:\Tenable\Tenable.ad\DirectoryListener\logs`) to identify which folder it recognizes as the IoA folder.
3. Delete manually any outdated IoA folders from the SYSVOL directory that do not match the latest IoA GPO GUID.
4. Restart the `tenable_Ceti` Service.
5. Repeat steps 2-4 until the Directory Listener recognizes the correct IoA folder with the latest GUID.

Deactivated Indicators of Attack

Occasionally, Tenable Identity Exposure may temporarily deactivate some Indicators of Attack (IoAs) to maintain optimal performance.

When deactivated, it shows the  icon next to the IoA.



IoA Status Icons

First Row Icon Status

- Gray icon – Indicates that at least one IoA is temporarily deactivated.
- Green checkmark icon – Indicates that all configured IoAs are activated.

Other Row Icon Status

- Gray icon – Appears next to specific domains where IoAs are deactivated.

Tooltip Information

When hovering over the status icons, you'll see the following tooltips:

- Gray icon – "One or several IoAs are deactivated temporarily"
- Green checkmark icon – "All configured IoAs are activated"

- Gray icon  in other rows: "IoA temporarily deactivated (since yyyy-mm-dd hh:mm) to maintain performance."

Alert Message

When Tenable Identity Exposure deactivates IoAs, an alert message appears above the IoA table:

"To maintain performance, Tenable Identity Exposure deactivated some IoAs. They will be reactivated automatically once the situation stabilizes. Refer to the icon in your IoA configuration for more information."

Visibility Rules

The deactivated status is visible at both domain and forest levels.

- If you uncheck a domain with a deactivation icon and no other domains have this icon, it disappears for the linked domain.
- If all domains linked to a forest have no more deactivation icons, the icon disappears for the linked forest.

Automatic Reactivation

Tenable Identity Exposure automatically reactivates deactivated IoAs once the system performance stabilizes. No manual intervention is required.

The temporary deactivation of IoAs is a built-in feature designed to maintain system performance. Tenable Identity Exposure dynamically adjusts active IoAs to ensure optimal operation without compromising security monitoring capabilities.

Responding to the Gray "Deactivated" Icon

When you see the gray "deactivated" icon:

1. Wait for the situation to resolve: In most cases, all you need to do is wait. Tenable Identity Exposure automatically reactivates the IoAs once system performance stabilizes.
2. For on-premises deployments:

- If you notice this happening frequently, despite following the resource matrix recommendations, you may need to add more resources to the machine hosting the Cygni service.
- Consider upgrading CPU, RAM, or disk space as needed to improve overall system performance.

3. Monitor frequency: Keep track of how often you see this icon. If it appears regularly, it may indicate that your current resources are consistently under strain.
4. Review your IoA configuration: While waiting for reactivation, you may want to review your current IoA setup to ensure it aligns with your security needs and available resources.

Troubleshoot Indicators of Attack

- Advanced Audit Policy Configuration Precedence
- Antivirus Detection
- Tenable Identity Exposure Log Files
- Event Logs Listener Validation
- DFS Replication Issues Mitigation
- Windows Event Log Retention
- “Unknowns” in the Indicators of Attack Alerts
- Operational Indicators of Attack
- Indicator of Attack Detection Delays

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 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
```

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
```

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

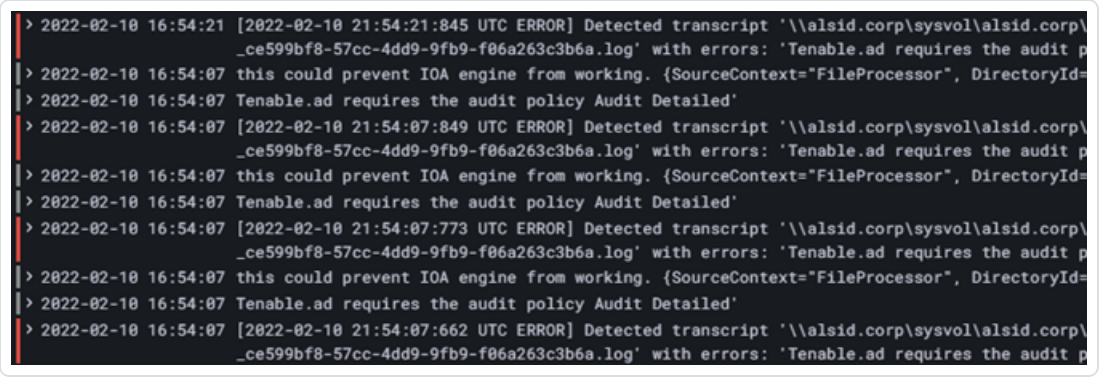
- Check for the following error message in the CETI Log:

```
[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

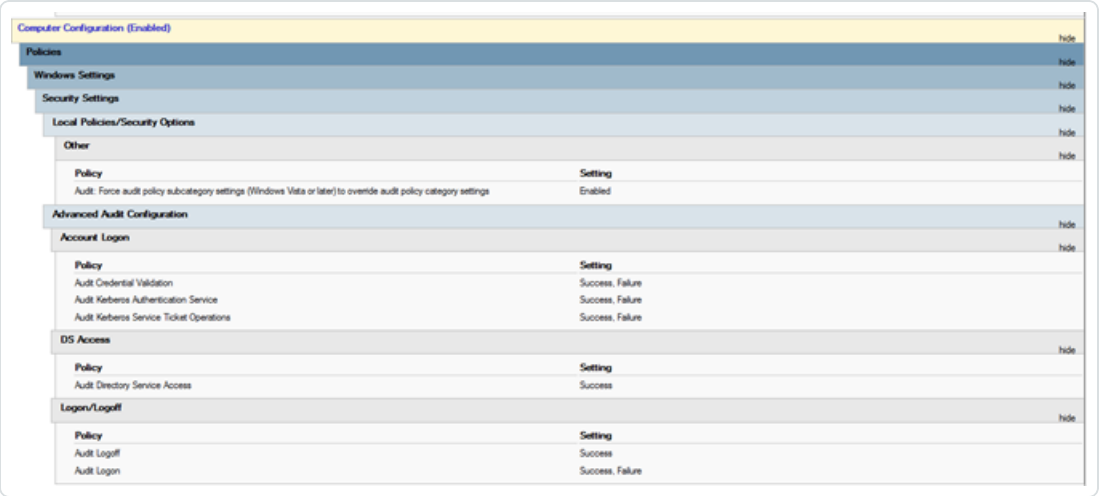
- If you see an error similar to the following one: "Tenable Identity Exposure requires the Audit Policy…", check your existing GPOs to ensure that you did not set the required audit policies to “No Auditing."



- If you get an error that states "RSOP...":



- Check the audit policies and look at the transcript file in the SYSVOL folder to see if you encountered any issues during the installation.



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

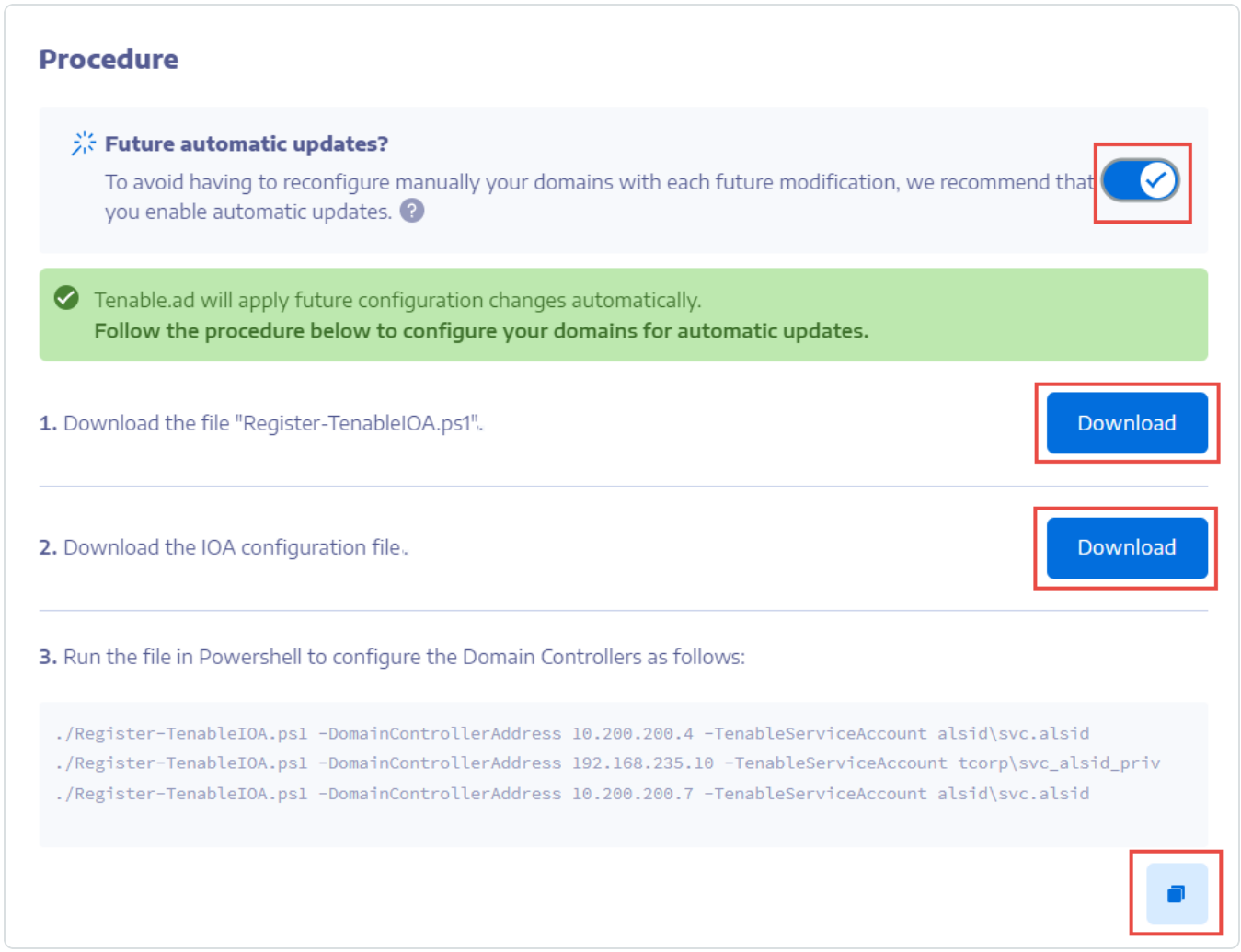
The value [X] of the parameter `-EventLogsFileWriteFrequency X` is the frequency at which the Tenable Identity Exposure listener generates an event logs file on non-PDCe domain controllers (DCs). The default and recommended value that the Tenable Identity Exposure listener uses is 15 seconds. However, 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](#).



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.

Windows Event Log Retention

While Tenable Identity Exposure strives to process as many Windows event logs as possible to support the security analysis within the Indicator of Attack feature, there are technical limitations, such as available memory on the machine running the services.

The **default global retention period** is 5 minutes. However, specific Windows event logs have extended retention periods to mitigate correlation issues that the security engine might encounter:

- `SYSMON 5722` and `5723`: Retained for 6 hours.
- `Microsoft-Windows-Security-Auditing/4624`: The retention period for this log is dynamic, as it is heavily used in Indicators of Attack for both detection and correlation. The system adjusts retention based on memory usage to balance event processing with system resources:
    - **First hour**: The security analysis service applies the default retention period of 5 minutes.
    - **After the first hour**, the system evaluates the remaining memory and adjusts retention as follows:
        - If available memory is **over 50%**: 1 day.
        - If available memory is **35%-50%**: 6 hours.
        - If available memory is **20%-35%**: 1 hour.
        - If available memory is **10%-20%**: 10 minutes.
        - If available memory is **below 10%**: The default 5 minutes.

This dynamic approach ensures that the system can manage incoming events efficiently while maintaining adequate memory for security analysis.

On-Premises Environments

For **on-premises environments**, you can customize the default retention period for event logs, as follows:

Set the environment variable: `ALSID_CASSIOPEIA_EVENT_LOGS_STORAGE_Application__DefaultRetentionInMinutes` on the machine hosting the `EventLogsStorage service`.

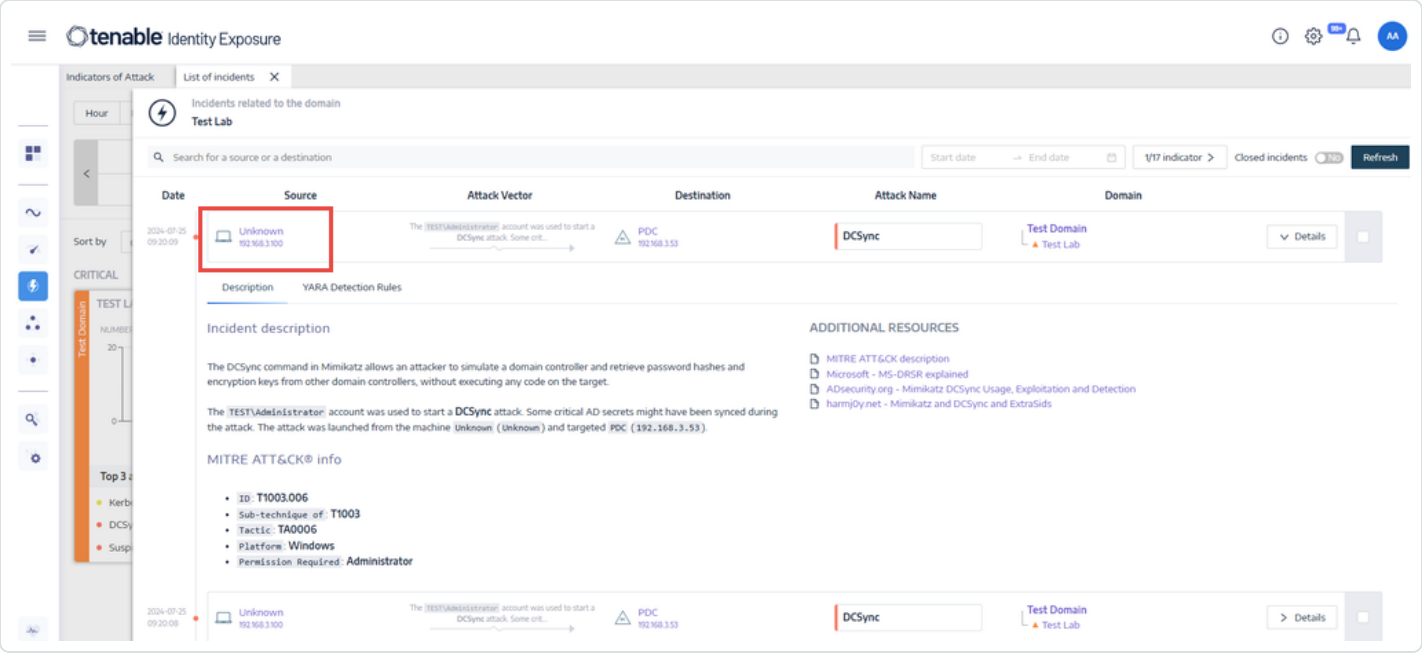
You can increase this value beyond the default 5 minutes. However, it's important to note that this change **will not affect** the specific retention rules for the three event logs mentioned earlier (`SYSMON 5722`, `5723`, and `Security-Auditing/4624`).

Additionally, the system reserves **4GB of memory** by default to maintain global stability. You can modify this threshold using the environment variable `ALSID_CASSIOPEIA_EVENT_LOGS_STORAGE_`

`Application__MinimumAvailableMemoryInMiB` on the machine hosting the `EventLogsStorage` service.

“Unknowns” in the Indicators of Attack Alerts

In some cases, you may encounter “unknown” entries in the Indicators of Attack (IoA) alerts, as shown in the following image:



These entries typically arise due to the following key scenarios:

1. **External DNS Outside Active Directory (AD)**

   If your organization uses DNS servers outside the Active Directory (AD) domain, it is important to note that the product does not support non-AD DNS environments. This means that when certain DNS queries or requests are routed through external DNS servers that are not part of AD, Tenable Identity Exposure cannot identify them, leading to “unknown” entries in the IoA alerts list.

   Such "unknowns" are expected in these cases and are not indicative of any malfunction or error within Tenable Identity Exposure. This is due to the nature of the integration with Active Directory, which requires DNS records to be managed within the AD environment for complete visibility and tracking.

   Solution

- To minimize these "unknown" entries, ensure that your DNS infrastructure is fully integrated into AD for domains and resources that are critical for identity exposure monitoring.
- If DNS queries must go outside of AD, understand that these “unknowns” will continue to appear, as Tenable Identity Exposure cannot resolve them.

2. **Insufficient Permissions for Tenable Identity Exposure Account**

   Another reason for "unknown" entries in the IoA alerts could be that the account Tenable Identity Exposure uses lacks sufficient permissions to read DNS entries. The Tenable Identity Exposure service requires read permissions to properly access and analyze DNS records within the Active Directory.

   Solutions

   To resolve this, ensure that the account Tenable Identity Exposure uses has read access to the necessary DNS entries within AD. Specifically, this account must have permission to query DNS servers and access the records it needs to perform identity exposure analysis.

   If the Tenable Identity Exposure account does not have proper read permissions, you can grant them using the following procedures.

   > Tip: In the script, you only need to change the name of the account Tenable Identity Exposure uses. Read permissions are included in the following attributes:
   >
   > - `distinguishedName`
   > - `dnsRecord (contains the IP)`
   > - `name`
   > - `ntSecurityDescriptor`
   > - `objectCategory`
   > - `objectClass`
   > - `objectGUID`

   You have the **two** following options using PowerShell scripts:

a. In your Active Directory manager, set the Read permissions on the container (dnsZone) and propagate it all children dnsNode (recommended solution if applicable):

```
Import-Module ActiveDirectory

$identity = New-Object System.Security.Principal.NTAccount('EXAMPLE\user2') # Service
account used by TIE for collect/listening
$dnsZonePartition = (Get-ADRootDSE).namingContexts | Where-Object { $_ -match
"DomainDnsZones" }

# dnsRecord attribute GUID
# and Public-Information property set GUID
$guids = @('e0fa1e69-9b45-11d0-afdd-00c04fd930c9', 'e48d0154-bcf8-11d1-8702-
00c04fb96050')

$dnsZones = Get-ADObject -LDAPFilter "(objectClass=dnsZone)" -SearchBase
$dnsZonePartition

ForEach ($dnsZone in $dnsZones) {
    $acl = Get-Acl -Path "AD:\$dnsZone"

    ForEach ($guid in $guids) {
      $ace = New-Object System.DirectoryServices.ActiveDirectoryAccessRule(
        $identity,
        [System.DirectoryServices.ActiveDirectoryRights]::ReadProperty,
        [System.Security.AccessControl.AccessControlType]::Allow,
        [guid]$guid,
        [System.DirectoryServices.ActiveDirectorySecurityInheritance]::All,
        [guid]'e0fa1e8c-9b45-11d0-afdd-00c04fd930c9' # dnsZone GUID
        )

      $acl.AddAccessRule($ace)
    }

    # ntSecurityDescriptor
    $ace = New-Object System.DirectoryServices.ActiveDirectoryAccessRule(
        $identity,
        [System.DirectoryServices.ActiveDirectoryRights]::ReadControl,
        [System.Security.AccessControl.AccessControlType]::Allow,
        [System.DirectoryServices.ActiveDirectorySecurityInheritance]::All,
        [guid]'e0fa1e8c-9b45-11d0-afdd-00c04fd930c9' # dnsZone GUID
        )

    $acl.AddAccessRule($ace)
    Set-Acl -Path "AD:\$dnsZone" -AclObject $acl
}
```

b. Set the read permissions on all the existing dnsNode objects (on the dnsZone affecting all children dnsNode):

```
Import-Module ActiveDirectory
```

```
$identity = New-Object System.Security.Principal.NTAccount('EXAMPLE\user2') # Service
account used by TIE for collect/listening
$dnsZonePartition = (Get-ADRootDSE).namingContexts | Where-Object { $_ -match
"DomainDnsZones" }

# dnsRecord attribute GUID
# and Public-Information property set GUID
$guids = @('e0fa1e69-9b45-11d0-afdd-00c04fd930c9', 'e48d0154-bcf8-11d1-8702-
00c04fb96050')

$dnsNodes = Get-ADObject -LDAPFilter "(objectClass=dnsNode)" -SearchBase
$dnsZonePartition

ForEach ($dnsNode in $dnsNodes) {
    $acl = Get-Acl -Path "AD:\$dnsNode"

    ForEach ($guid in $guids) {
      $ace = New-Object System.DirectoryServices.ActiveDirectoryAccessRule(
        $identity,
        [System.DirectoryServices.ActiveDirectoryRights]::ReadProperty,
        [System.Security.AccessControl.AccessControlType]::Allow,
        [guid]$guid
        )

      $acl.AddAccessRule($ace)
    }

    # ntSecurityDescriptor
    $ace = New-Object System.DirectoryServices.ActiveDirectoryAccessRule(
        $identity,
        [System.DirectoryServices.ActiveDirectoryRights]::ReadControl,
        [System.Security.AccessControl.AccessControlType]::Allow
        )

    $acl.AddAccessRule($ace)
    Set-Acl -Path "AD:\$dnsNode" -AclObject $acl
}
```

3. **Supported DNS partitions**

   Tenable Identity Exposure does not perform active DNS resolution. Instead, it relies on DNS entries extracted from the `ForestDnsZones` and `DomainDnsZones` partitions. If you use custom DNS partitions, Tenable Identity Exposure will not crawl them or store their DNS entries.

Operational Indicators of Attack

Ensuring that Indicators of Attack processes are functioning properly is essential for accurate detection and response. This section provides step-by-step instructions to verify that IoA components are operational, troubleshoot common issues, and resolve problems efficiently. Follow the steps below to confirm everything is working as expected.

- Ensure that the Indicators of Attack (IoA) monitoring is operational across your Domain Controllers.
    - Check connectivity to the domain – Ensure that the Domain connectivity is functional by verifying the configuration. For more information, see Domains.
- Verify IoA GPO folder in SYSVOL:
    - Check the IoA GPO folder in the SYSVOL directory to confirm that each Domain Controller is producing an up-to-date `.gz` file.
    - If any Domain Controller is not generating this `.gz` file, proceed to the next steps.
- Confirm that the IoA Event Listener process is running:
    - Verify that the process `Register-TenableADEventsListener.exe` is running.
    - In the latest versions, this process is listed as "Tenable - IOA Events Listener" in Task Manager in addition to `Register-TenableADEventsListener.exe`.

      For more information, see Event Logs Listener Validation.
- If the process is not running:
    - Ensure any EDR/Antivirus software on the Domain Controllers is not blocking the `Register-TenableADEventsListener.exe` process.

      For more information, see Antivirus Detection.
- Start the process manually:
    - Edit the associated task (`TenableADTask_*`) in the Task Scheduler and click **OK** to restart the process.
- Escalate if issues persist – If the above steps do not resolve the issue, raise a Support Case with Tenable. There may be an underlying issue preventing the `Register-TenableADEventsListener.exe` process from running.

Indicator of Attack Detection Delays

Tenable Identity Exposure automatically adjusts the analysis window when it detects lost or delayed events–such as those caused by long GZ file replication times or a high volume of generated data.

While it typically analyzes data in 5-minute windows, it can extend the window up to one hour to account for late-arriving events. This adjustment may delay attack detection by up to one hour after the attack occurs.

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. Use this procedure 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**.

Important Consideration for Windows Server 2025:

There is a limitation in **Windows Server 2025** where LDAP configuration with SASL bindings disabled **only works if LDAPS is enabled.**

To ensure proper functionality:

- If using **UPN** or **DN** for the Tenable service account, you can **enable SASL bindings** in the LDAP configuration, and it will work correctly.
- If you prefer to **keep SASL bindings disabled**, you must **enable LDAPS** for LDAP to function properly.

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.

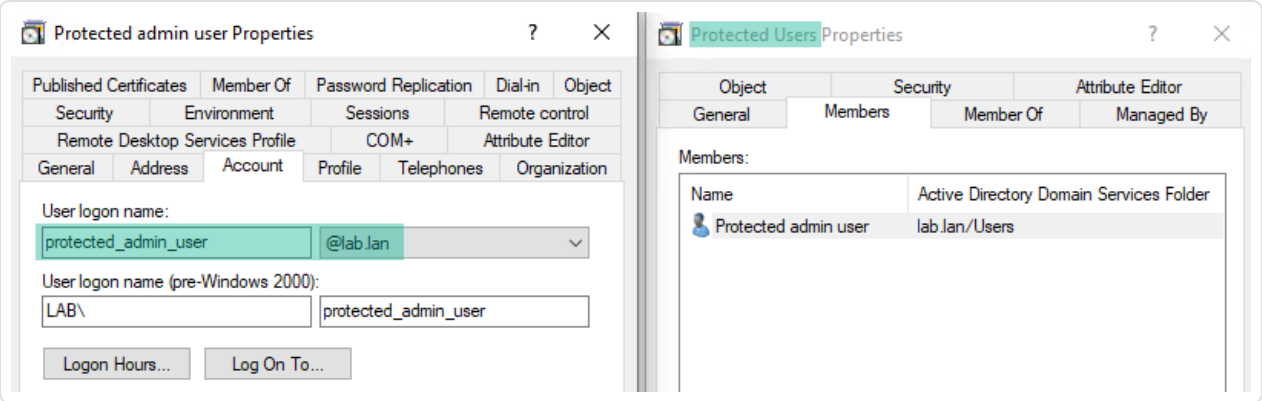
   - In the **LDAP group name** box, type the distinguished name of the group (example: `CN=TAD_User,OU=Groups,DC=Tenable,DC=ad`)
   - In the **Default profile** drop-down box, select the profile for the allowed group.
   - In the **Default roles** box, select the roles for the allowed group.

7. If necessary, click on **+** to add a new allowed group.
8. Click **Save**.

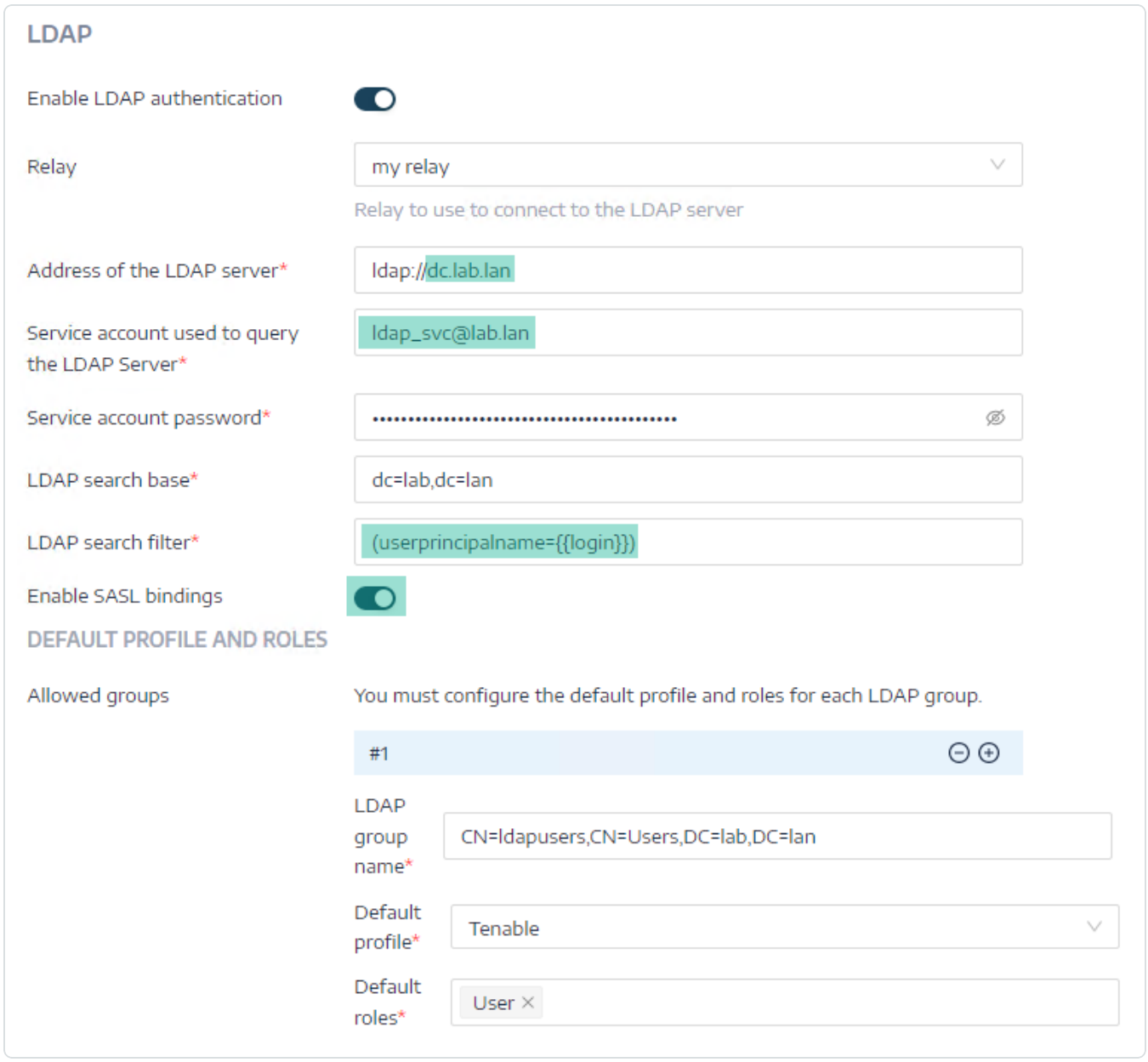
To use LDAP with members of the "Protected Users" group in AD:

Since members of the Protected Users group cannot use NTLM, you must ensure that you configure LDAP authentication correctly to use Kerberos instead.

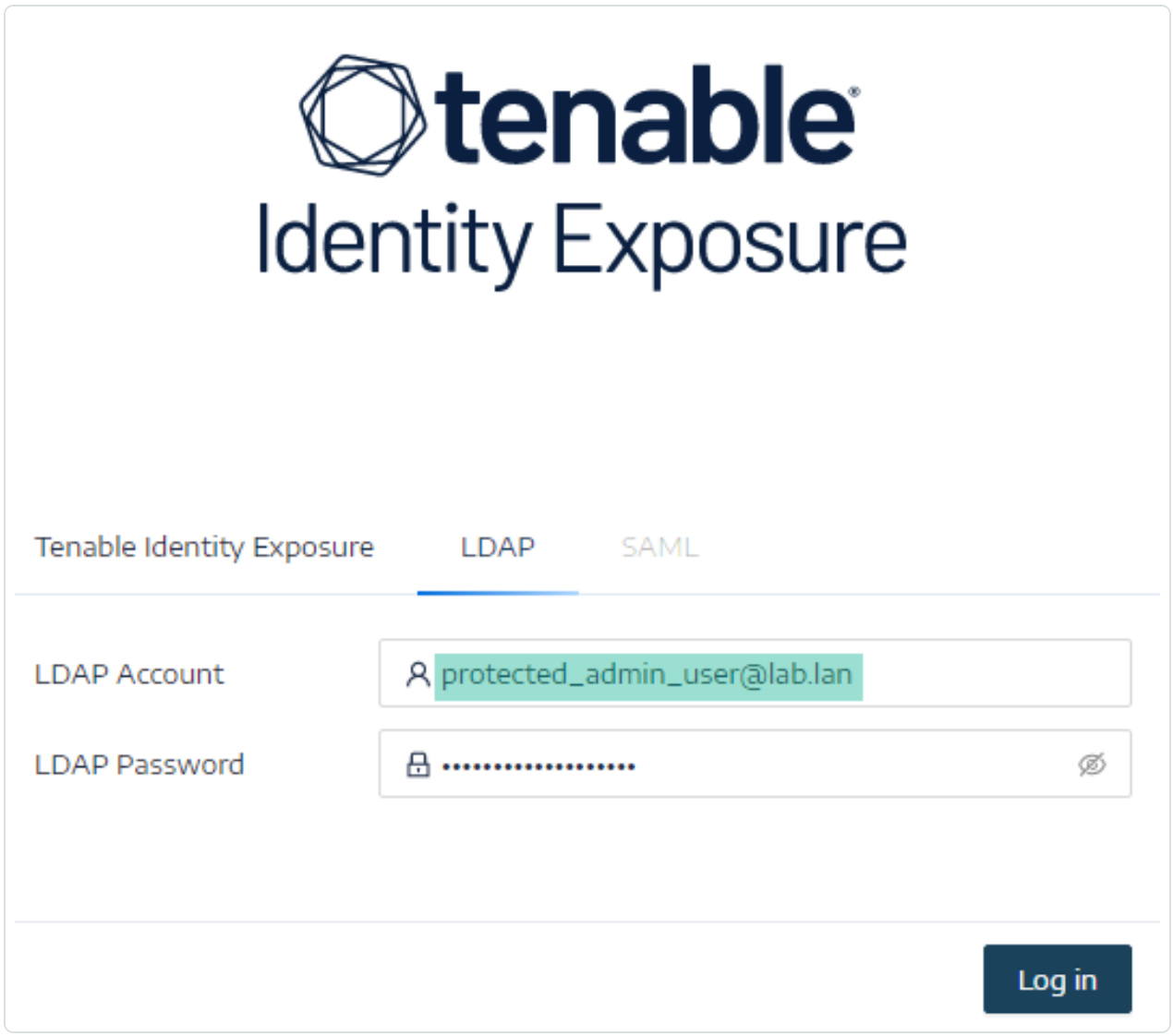
1. **Prerequisites**: You must have already configured a User Principal Name (UPN) in Microsoft Active Directory. This is a username format used similar to an email address. It typically follows the format username@domain.com, where "username" is the user's account name and "domain.com" is the domain where the account is located.



2. Log in to Tenable Identity Exposure with your credentials.
3. Configure the following LDAP options:
    - Use FQDN for the address of the LDAP server (ensure Secure Relay can resolve it).
    - Use a service account in UPN format (e.g. login@domain.com).
    - Set the LDAP search filter to "`(userprincipalname={{login}})`"
    - Set SASL bindings to "on."



4. Log in to Tenable Identity Exposure using LDAP credentials as a member of the 'Protected Users' group with the User Principal Name syntax.



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**.

LDAP Authentication Issues

After you complete and save the configuration, the LDAP option should appear on the login page. To confirm that the configuration is valid, you must be able to login using an LDAP account.

Error Messages

Two error messages can happen at this point:

- An error has occurred during the authentication process. Please try again.
    - In this case there is a problem with the configuration.
    - Double check the complete configuration.
    - Check that the server hosting Tenable Identity Exposure is able to reach the LDAP server.
    - Check that the account used for the search is able to bind on the LDAP server.
    - For more details, check the application logs.
- Your login or password is incorrect.
    - Verify that CAPS LOCK is not on and then retype your tested login and password.
    - This can be due to a problem with the group filter, the search filter or the search base fields.
    - Try to remove any group filtering temporarily. For more details, check the application logs.

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 -----`.

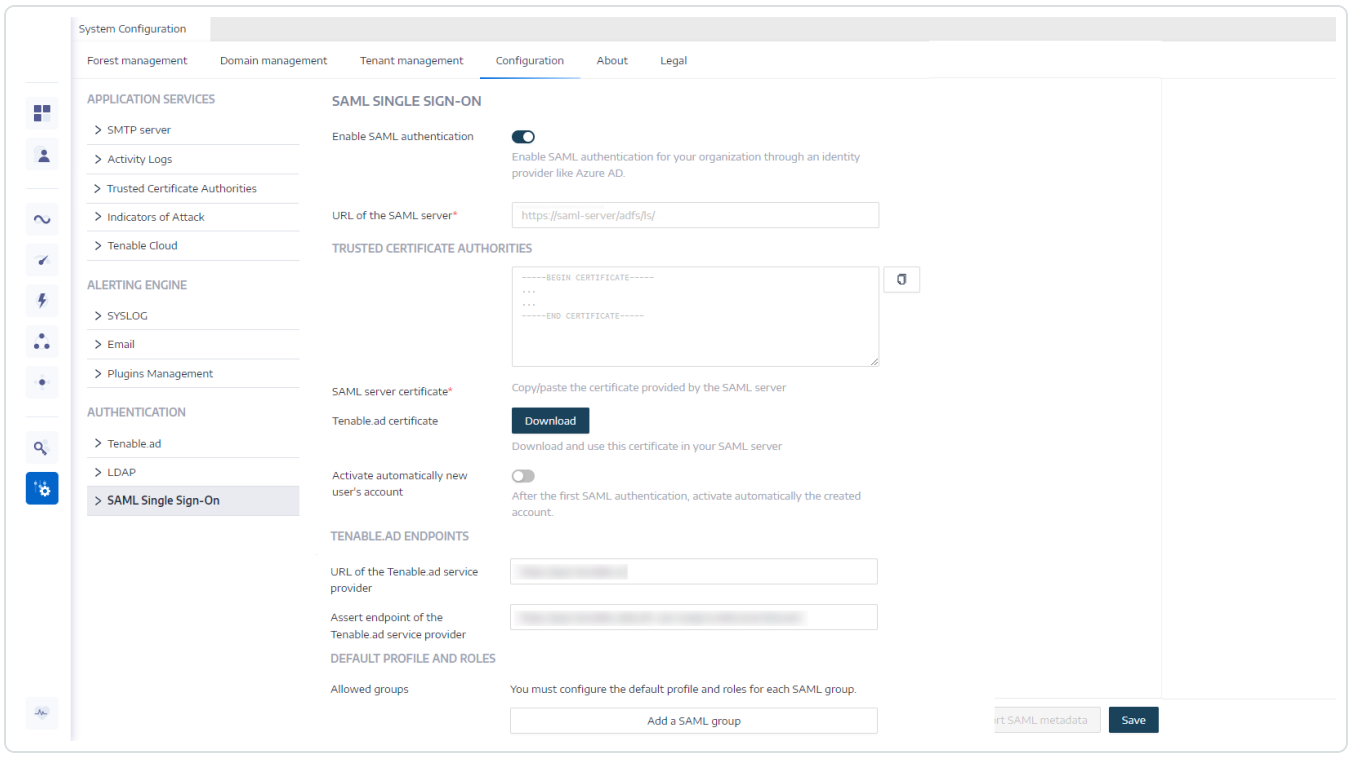
To configure SAML authentication:

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.



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 **+** 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.

Caution

If you have a **standalone Tenable Identity Exposure license**, you can opt to send data to the Tenable Platform through your settings. By doing this, you activate the Identity 360 and Security Engine features of Tenable Identity Exposure.

To facilitate communication with the Tenable Platform and track user actions, Tenable Identity Exposure automatically creates the following objects in the Tenable platform, visible in the Tenable Vulnerability Management container settings:

- A group named with the pattern `TIE - Autogenerated users - {random_string}`
- A Permission named `TIE - Autogenerated - Can view all assets - {random_string}` applied to the Group `TIE - Autogenerated users - {random_string}`. It allows the users to see the assets that Tenable Identity Exposure exported to the Tenable platform.
- For each Tenable Identity Exposure user, a user named according to the pattern `tie-{username}-{random_string}` who is a member of the Group `TIE - Autogenerated users - {random_string}`. This user has a strong random password and you should **not** use it to authenticate in the Tenable Vulnerability Management container. It has `Basic` read-only rights in the Tenable Vulnerability Management container.

An administrator can see these objects but **must not alter** them, as changes could disrupt the Indentity 360 and Security Engine features.

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.

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.

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.

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.

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.

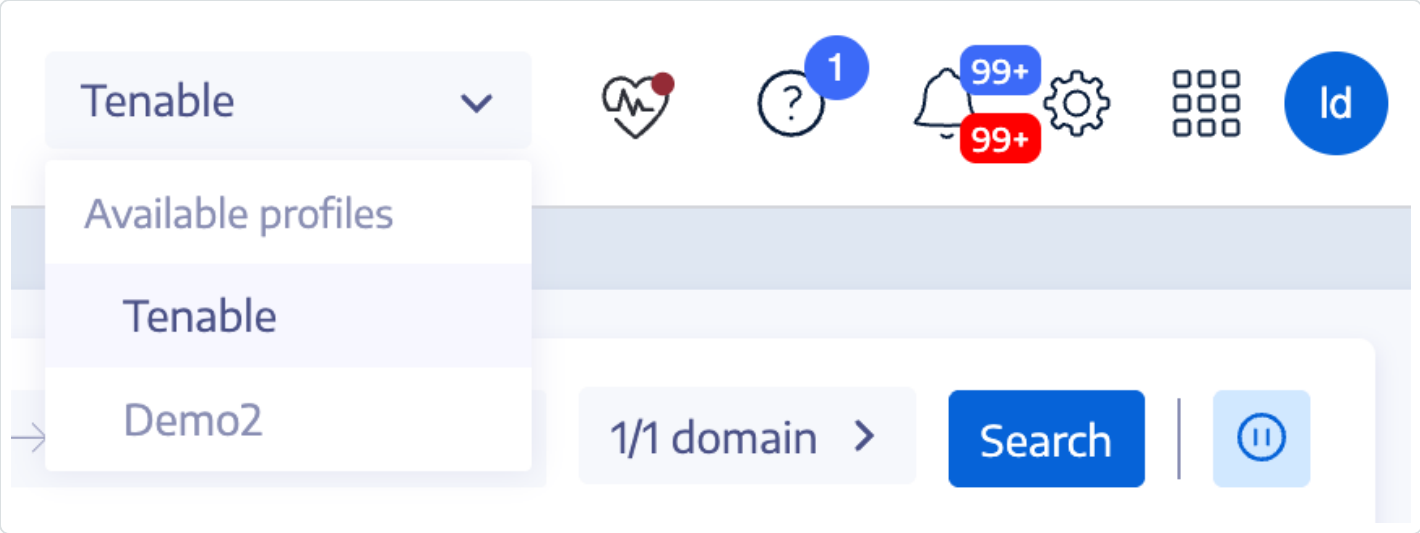
Applying a security profile allows different types of users to review the data analysis from different reporting angles, as defined by the indicators for that security profile.

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.

Note: If a security profile setting is configured with the same option in both the **global** and **domain-specific** customizations, the domain-specific customization takes precedence.

The top right corner of the Tenable Identity Exposure header shows your active security profile with a drop-down menu that lets you switch to another profile (similar to the selection in user preferences).



Note: For features such as Insights, Identity 360, and Exposure Center, Tenable Identity Exposure applies the default Tenable security profile. The profile selection is read-only.

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 an indicator to customize.

   The **Indicator Customization** pane appears.

6. Select the options from the Options table.

   Tip: To enable the **aggressive mode** for Indicators of Attack, click the toggle button for the option "Aggressive mode" to "Yes."

Tip: Certain indicator options require the use of regular expressions (regex). Regex are a 'contain' match instead of an 'equal' match.
- 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.

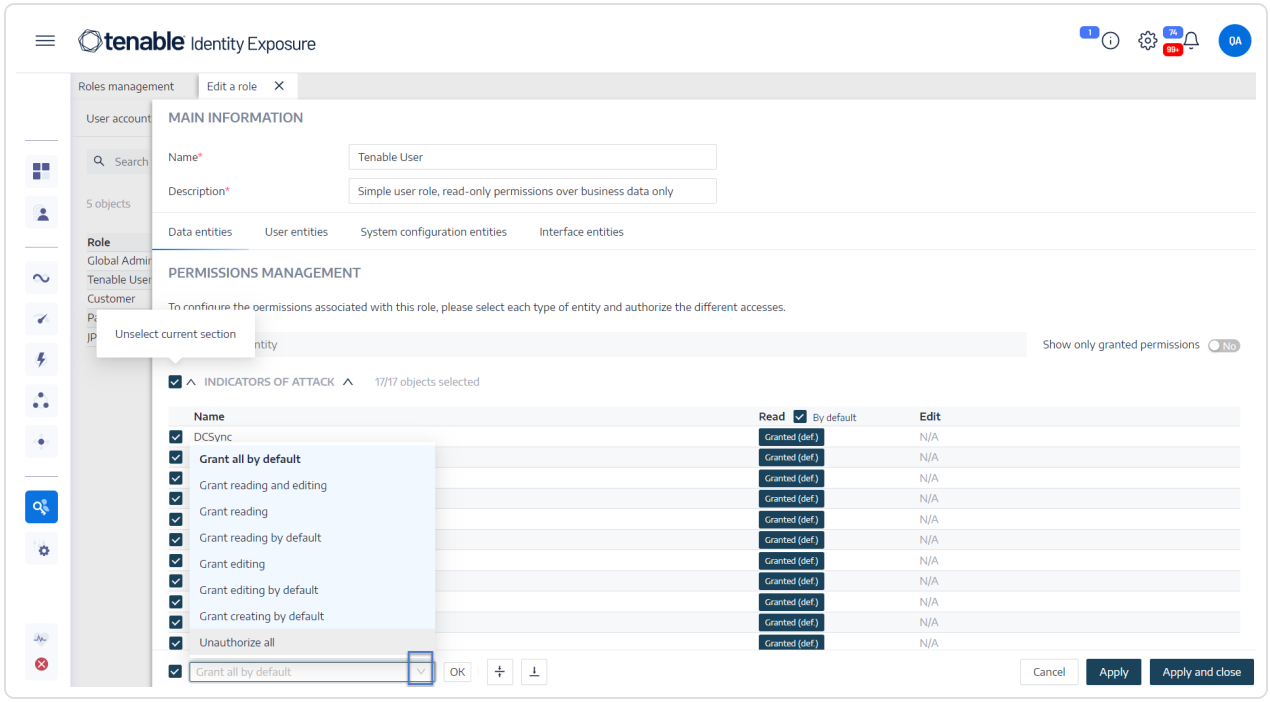
To set permissions in bulk for a role:

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.



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 analysis and to modify personal information and preferences.	• Preferences • Dashboards • Widgets • API key • Personal information	Edit, Create
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,	Read, Edit

	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) • Configuring Microsoft Entra ID as an Identity Provider • Health Checks • Display only user's own traces	
Interface Entities		
This entity defines the permissions to access specific parts of the Tenable	Access paths to specific Tenable Identity Exposure	Granted, Unauthorized

Identity Exposure user interface and features.	features. For more information, see Set Permissions on User Interface Entities (Example)	

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:

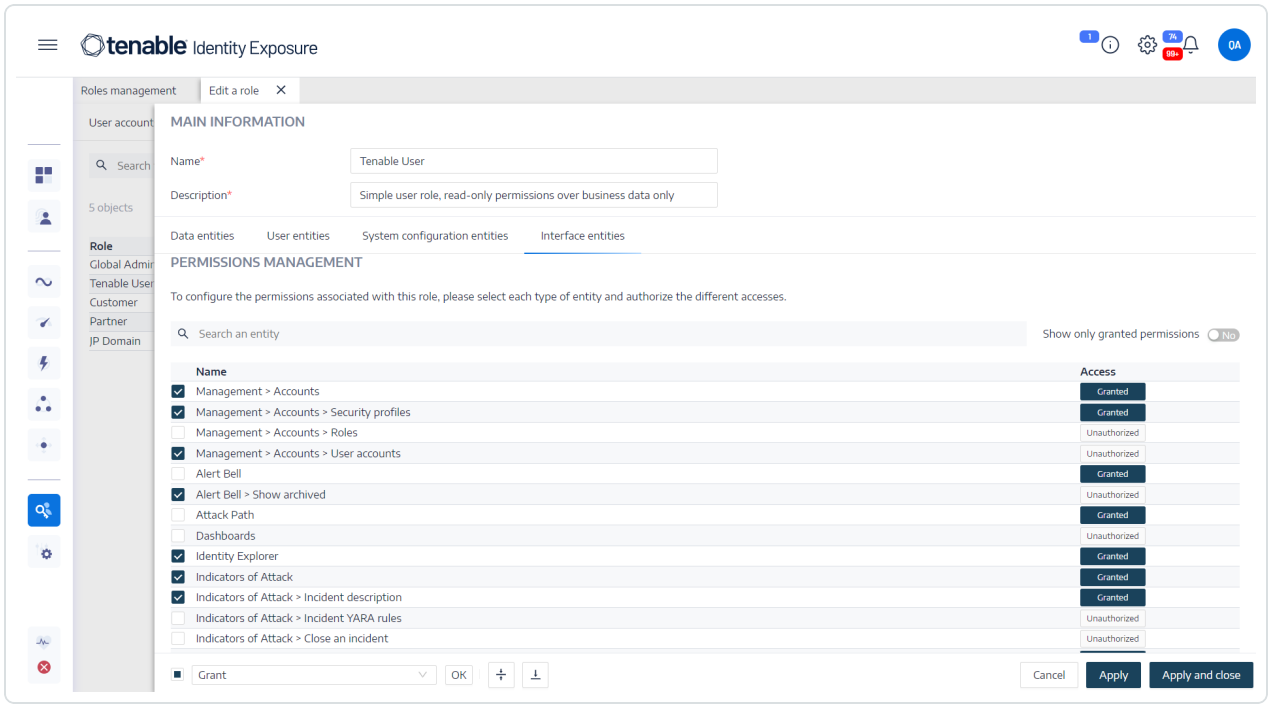
1. In Tenable Identity Exposure, click **Accounts** > **Roles management**.
2. Hover over the role for which you want to set permissions and click the  icon on the right.

   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.

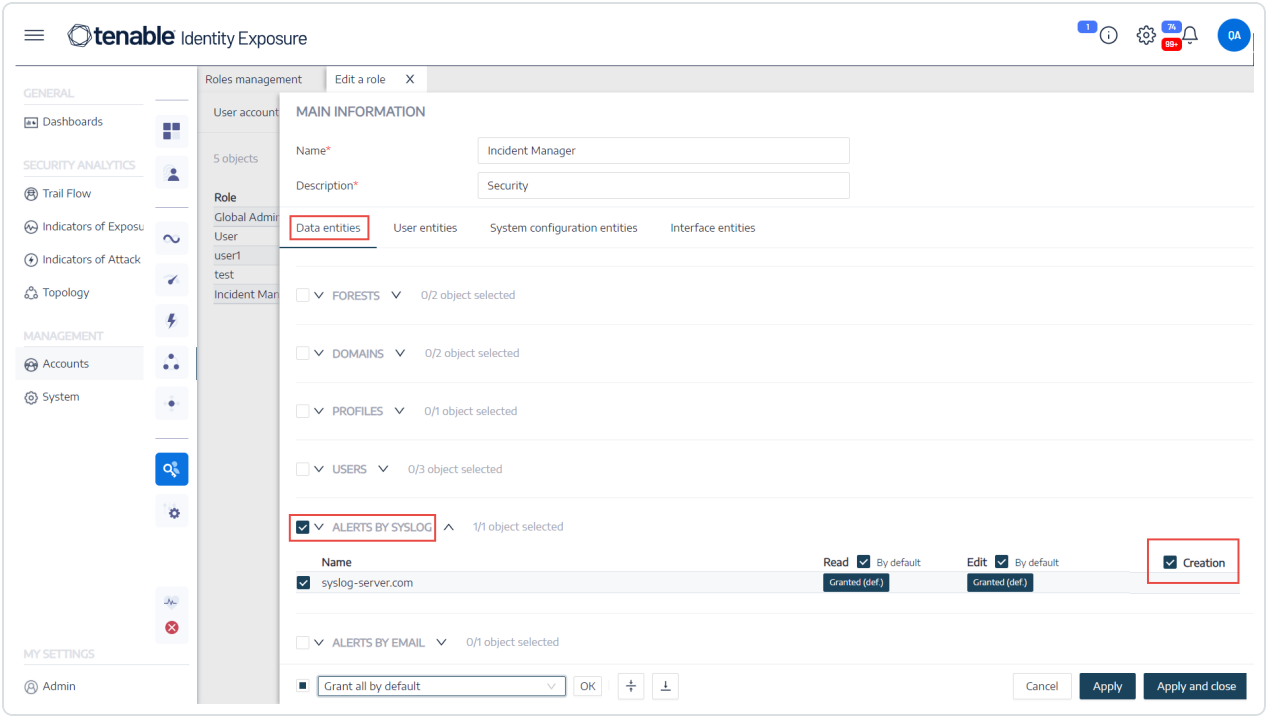


6. Under **Permissions Management**, select **Data Entities**.
7. In the list of entity sections, select **Alerts by Syslog**.
8. Select the **Creation** permission.

   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.



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.

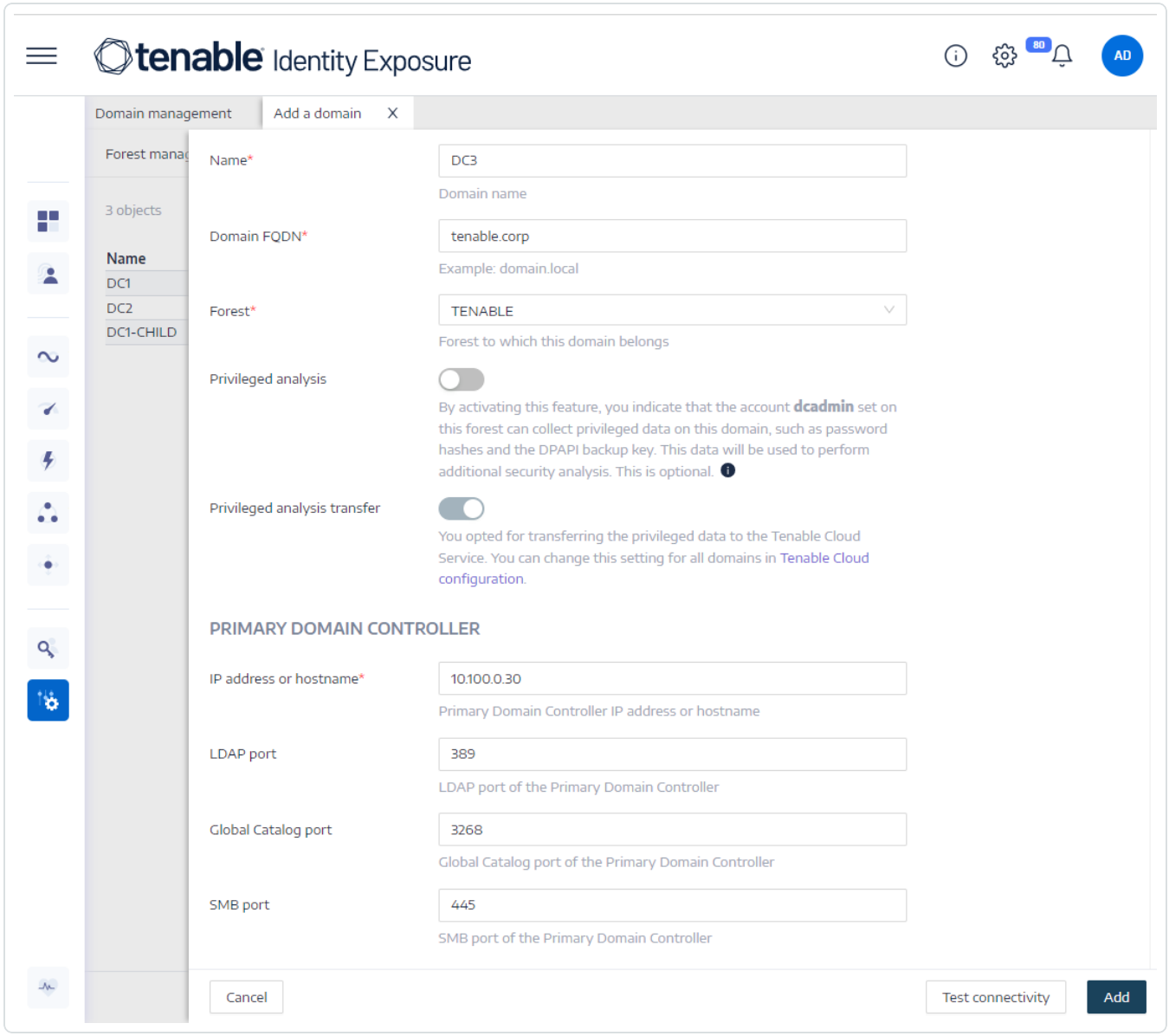
To add a domain:

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.



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 and historical data:

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 of the "domain_name" domain.
5. Click **Delete**.

   A message appears to confirm that Tenable Identity Exposure deleted the domain.
6. Wait for the system to clean up any historical Active Directory data associated with the deleted 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.

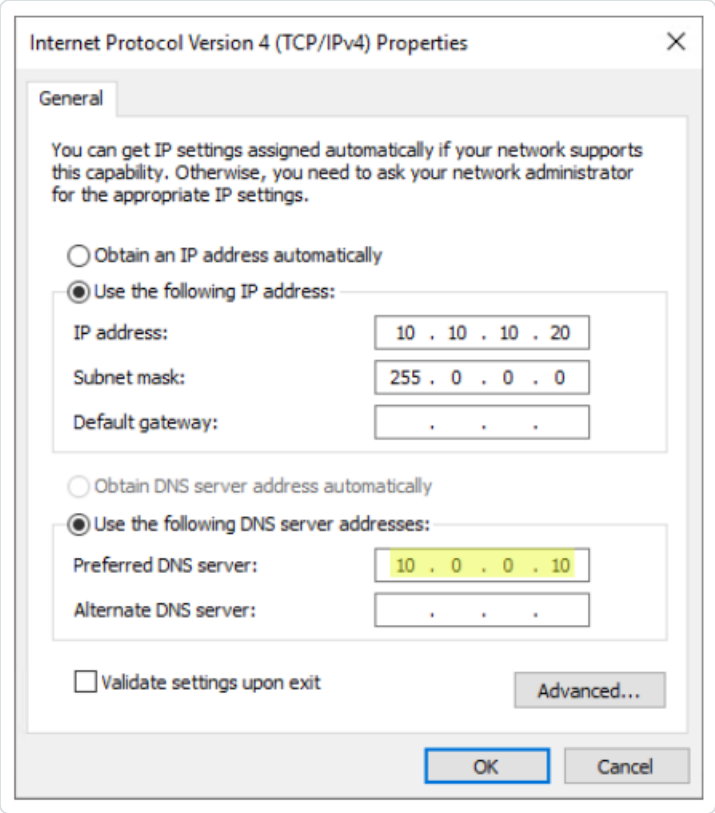
Compatibility with Tenable Identity Exposure Deployment Modes

Deployment Mode	Kerberos Support
On-Premises	Yes
SaaS-TLS (legacy)	Yes
SaaS with Secure Relay for Tenable Identity Exposure 3.59	Yes

SaaS with VPN	No – You must switch your installation to the Secure Relay for Tenable Identity Exposure 3.59 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:



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.

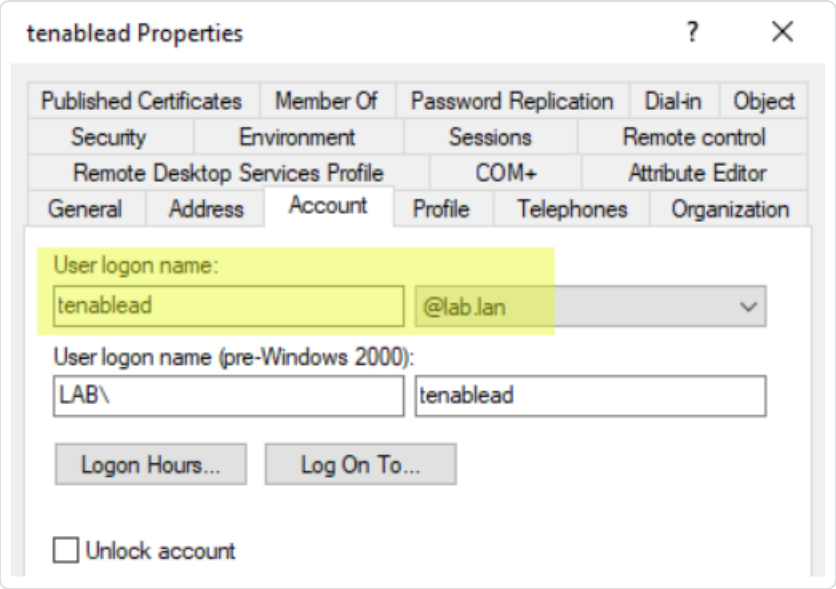
  > **Note**: The Directory Listener or Relay machine does not need to be domain-joined to use Kerberos.

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`".

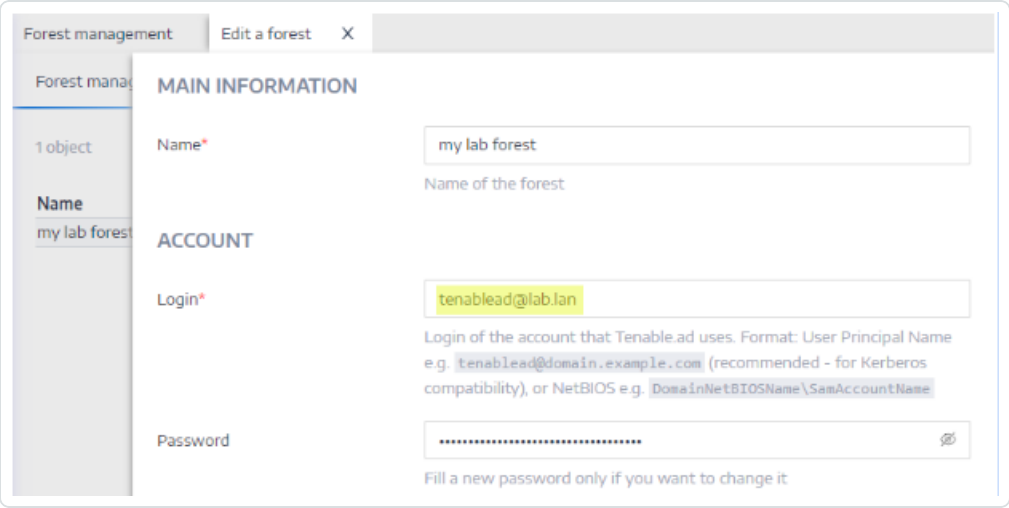
   a. Locate the UPN attribute in the domain of the forest that contains the service account as follows:



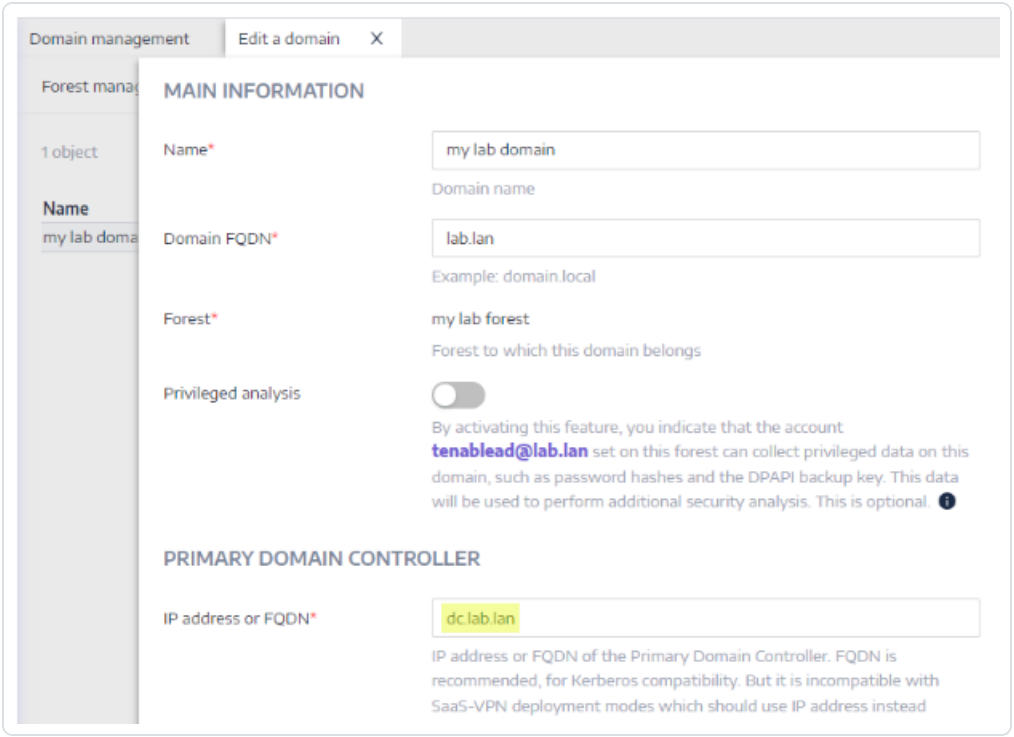

```
PS C:\Users\admin> Get-ADUser tenablead


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:



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.

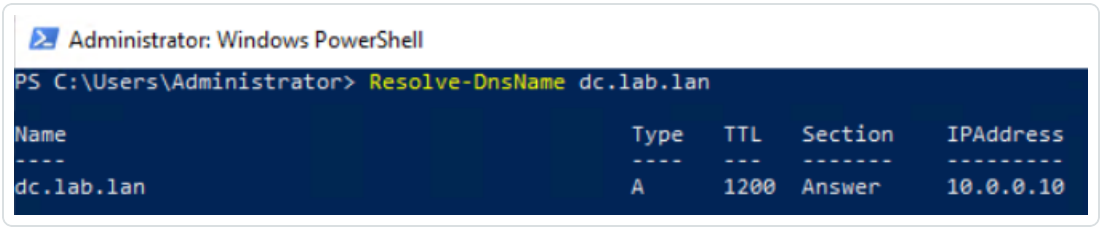


Troubleshooting

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:



Kerberos

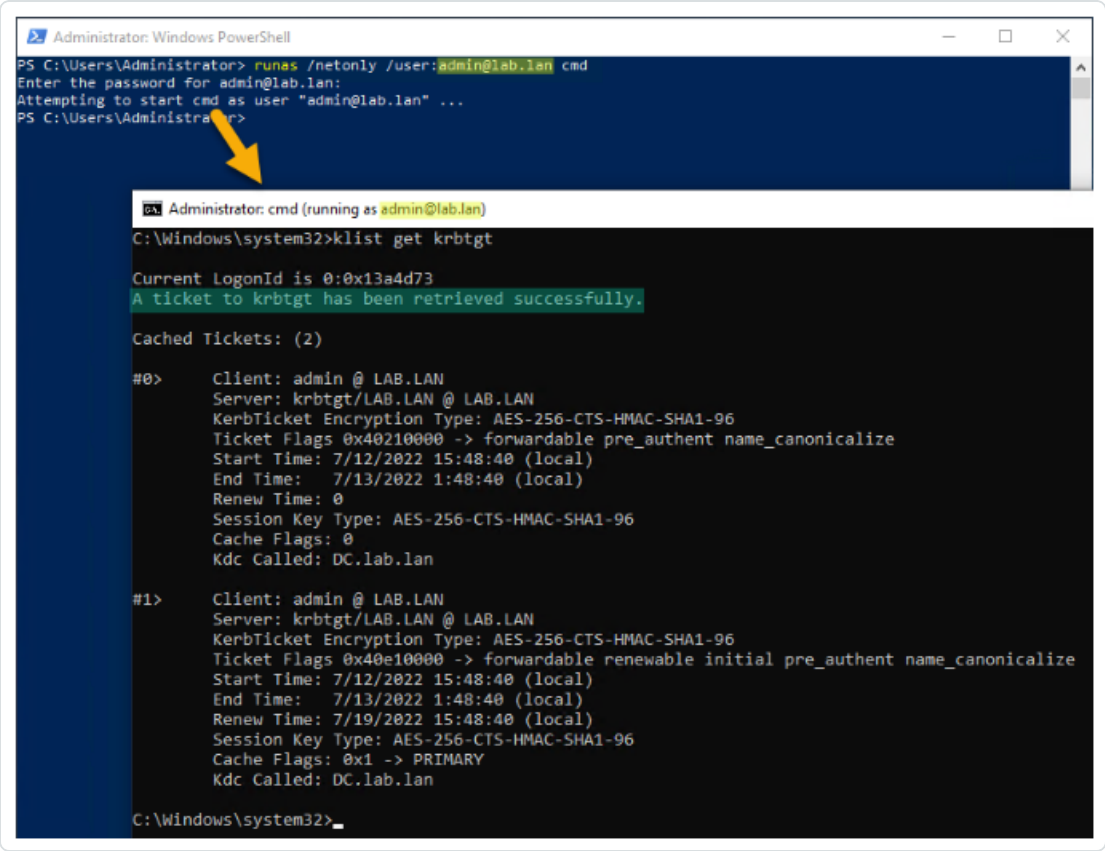
To verify that Kerberos works with the commands you run on the Directory Listener or Relay machine:

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:

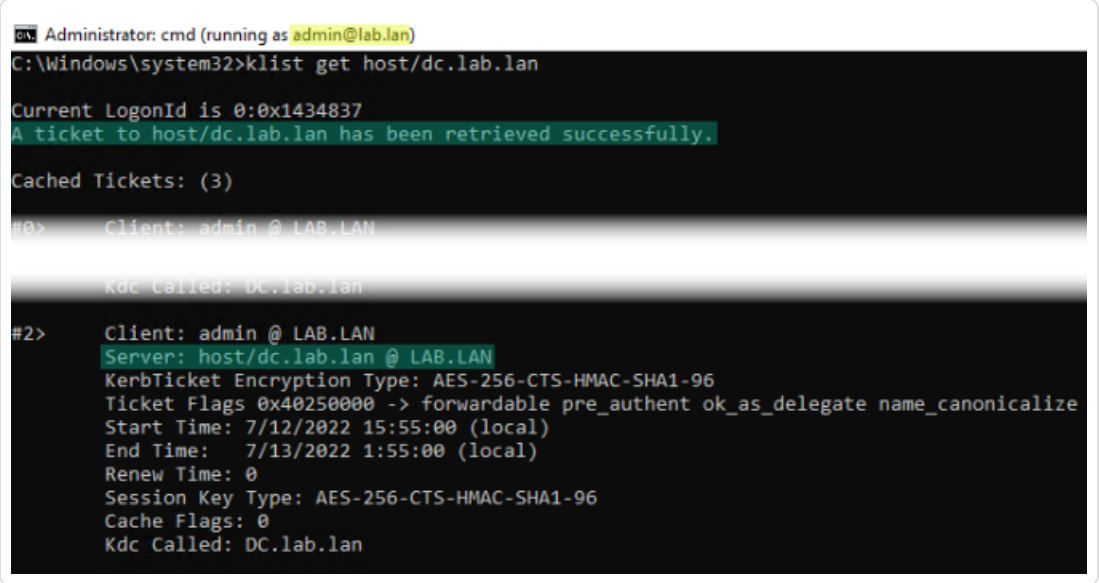


The following are potential error codes:

- `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:



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.

- Microsoft 365 SMTP OAuth Configuration
- 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.

Differences in Deployment Architecture

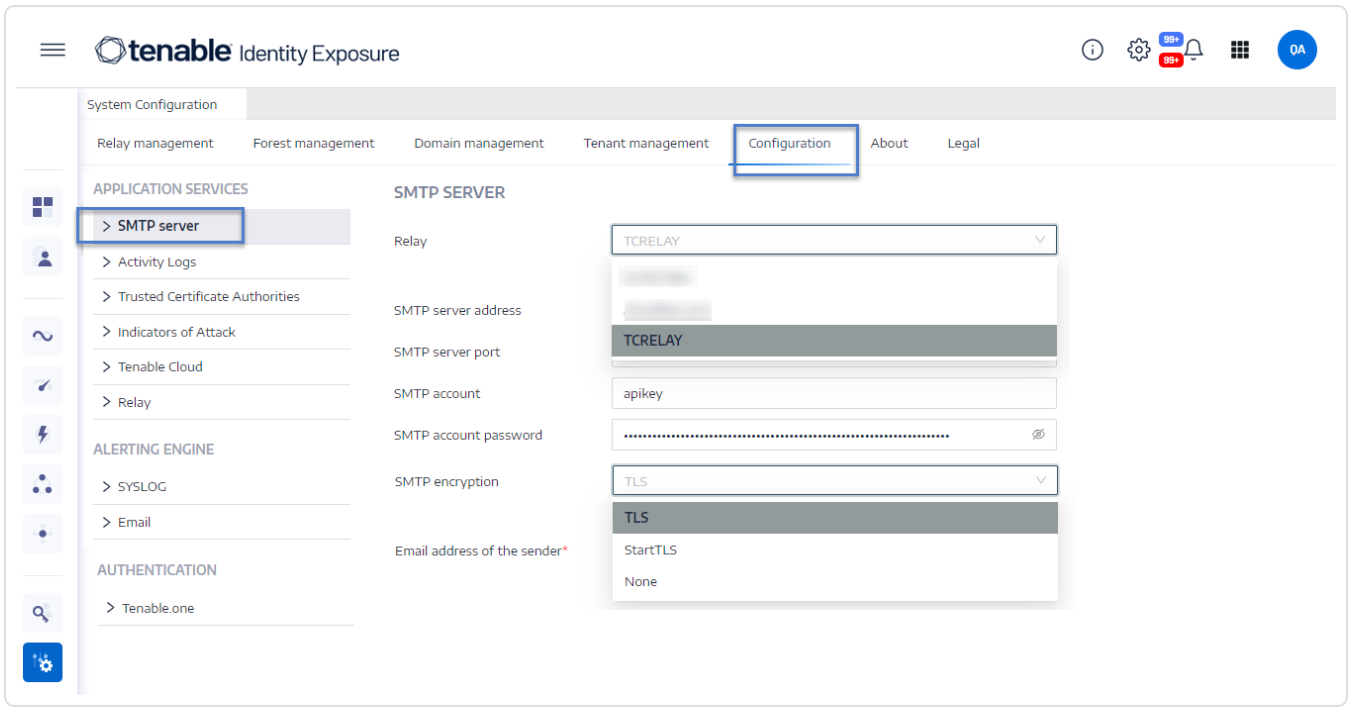
- For **Secure Relay** Architecture:
  - The Secure Relay is **installed in the customer's environment**.
  - You manage communication between the Secure Relay and the SMTP/SYSLOG server.
- For **VPN** Architecture:
  - The Secure Relay service is **hosted on Tenable's Cloud**.
  - You open a support case with Tenable to manage communication for alerting.

SMTP Server Configuration for Secure Relay Environments

To configure the SMTP server **for Secure Relay**:

1. In Tenable Identity Exposure, click **System** > **Configuration**.
2. Under **Application Services**, select **SMTP Server**.

   The **SMTP Server** pane opens.



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.

SMTP Server Configuration for VPN Environments

To configure the SMTP server **for VPN**:

1. Identify whether the SMTP server is hosted:
    - **Inside** the customer network (**private**).
    - **Outside** the customer network (**public**).
2. Depending on your network setup:
    - For an SMTP server Hosted **inside** the customer network:
        - Provide the private IP address of the SMTP server to Tenable by opening a Support Case. Include the request to whitelist this IP for communication within the VPN tunnel.
        - Wait for Tenable's development team to complete the configuration.

- Test the VPN tunnel to confirm connectivity between Tenable Cloud and the internal SMTP server.

- For an SMTP server hosted **outside** the customer network:
  - Confirm whether the external SMTP server filters inbound connections:
    - If **filtering** inbound traffic based on source IP:
      - Open a support case with Tenable to request the alerting IP address for the VPN tunnel.
      - Work with the external SMTP provider to whitelist Tenable's alerting IP address.
    - If **not filtering** inbound traffic: Ensure the SMTP server's public IP is reachable over the VPN tunnel.

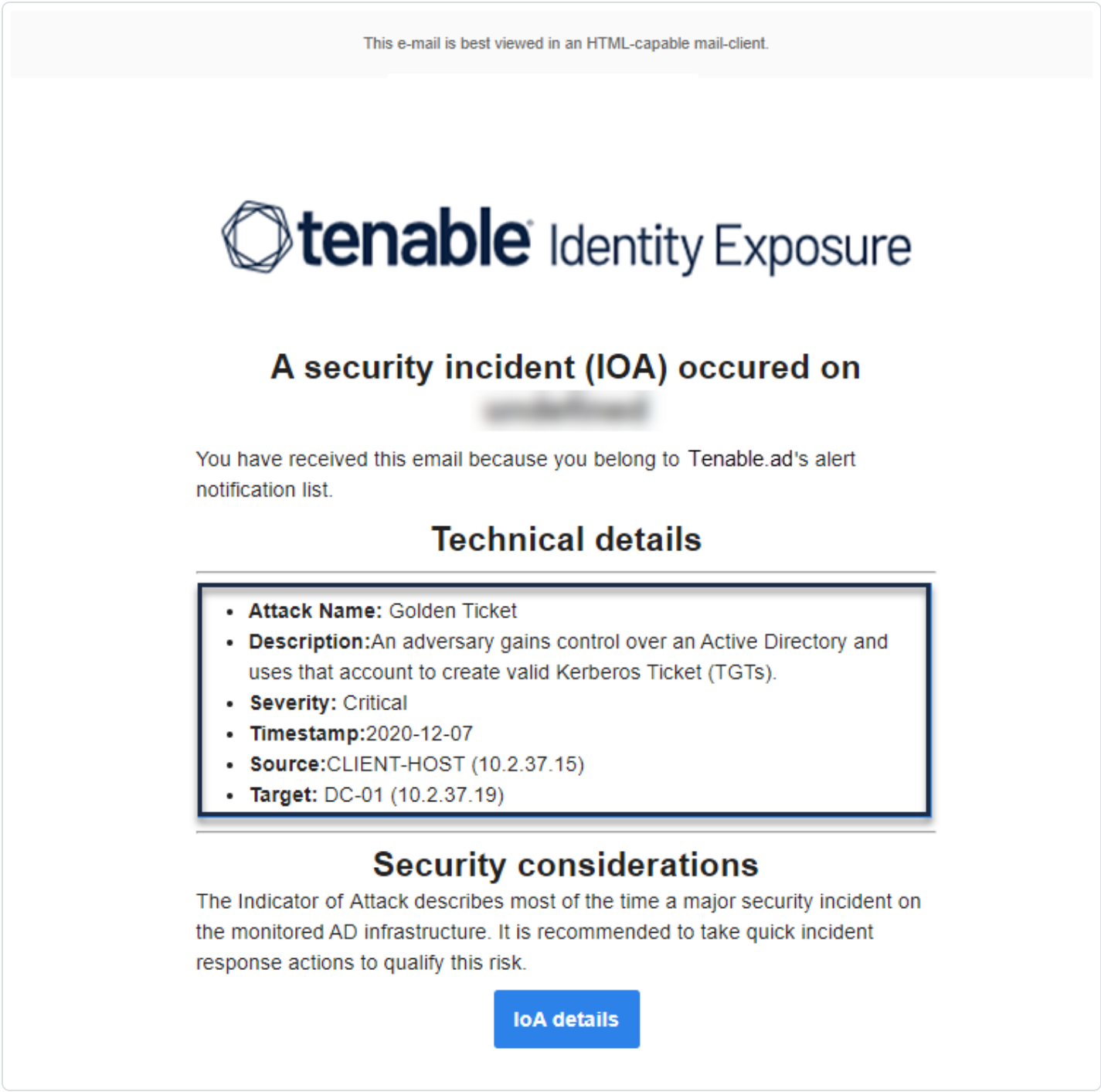
3. **Ongoing maintenance**: Notify Tenable of any changes to the SMTP server's private or public IP address to maintain VPN tunnel functionality.

Troubleshooting Common Issues

- **Unable to send alerts** (SMTP/SYSLOG):
  - Verify that the SMTP server (private or public) is reachable within the VPN tunnel.
  - Confirm that the IP address is whitelisted on both ends (Tenable Cloud and the SMTP server).
- **Connection timeout**:
  - Check VPN tunnel activity and routing configuration.

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:



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 previous 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

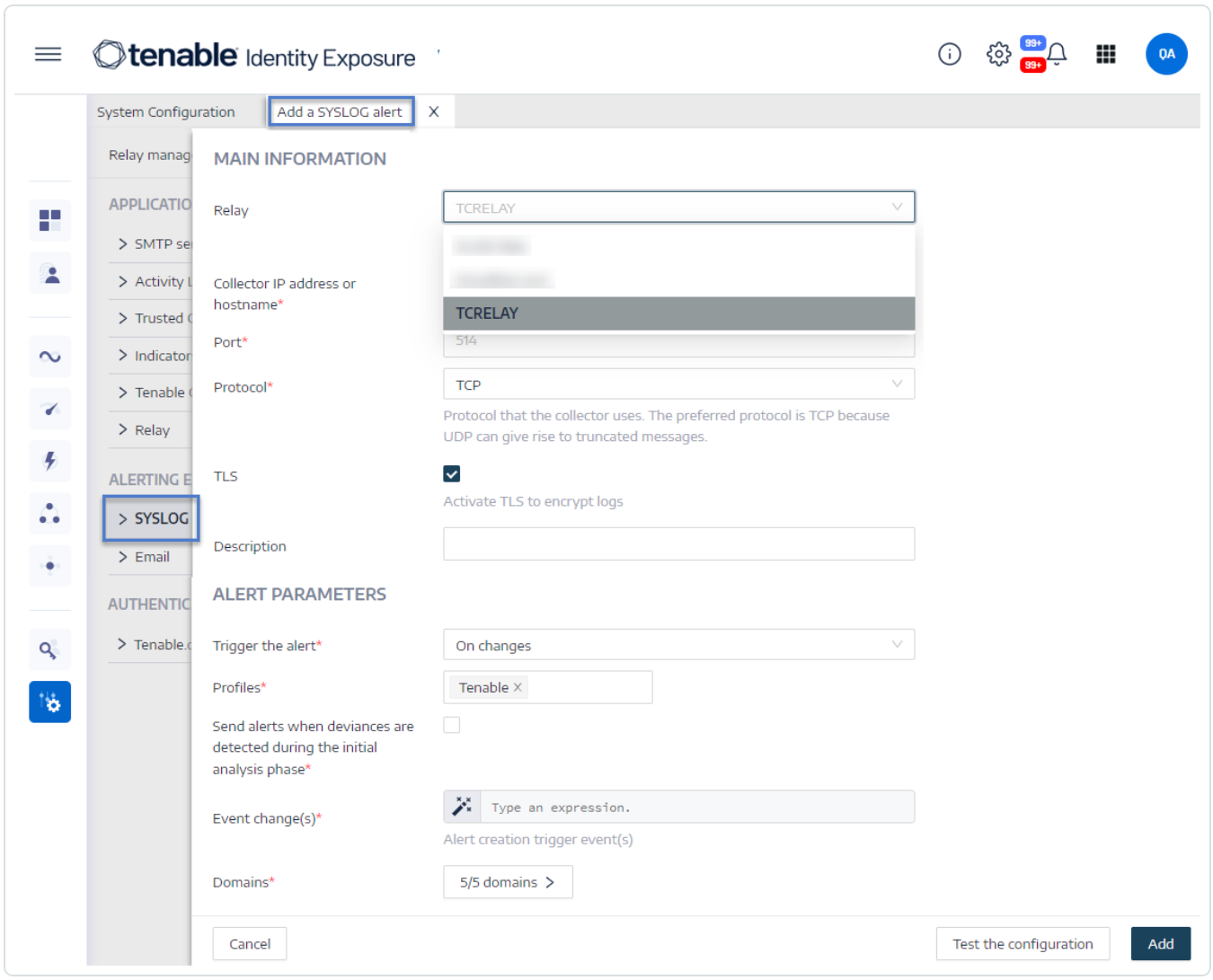
Syslog Alerts

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.



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 Syslog messages when a system reboot triggers alerts.
    - Unselect the checkbox: Tenable Identity Exposure does not send out Syslog messages 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.

> **Note**: Tenable Identity Exposure applies this filter as soon as it receives events to forward them to Syslog before performing any additional security analysis. As a result, filters that rely on enriched or post-processed data will not work at this stage.

- **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 previous 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.

> **Note**: There is an ingestion time to consider before you receive IoA alerts. This delay is different from the timing observed during the "test the configuration" phase when you configure Syslog and email alerts. Hence, do not use the duration from the test configuration as a baseline to compare with the timing of alerts triggered by an actual attack.

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"
```

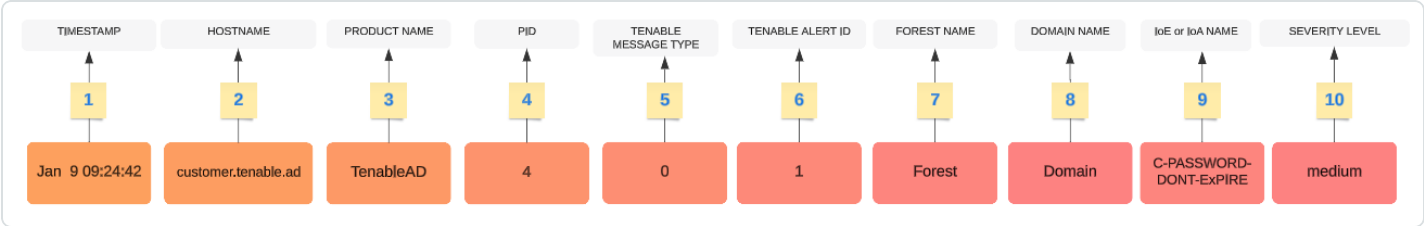
Example of an alert for an Indicator of Attack (IoA)

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

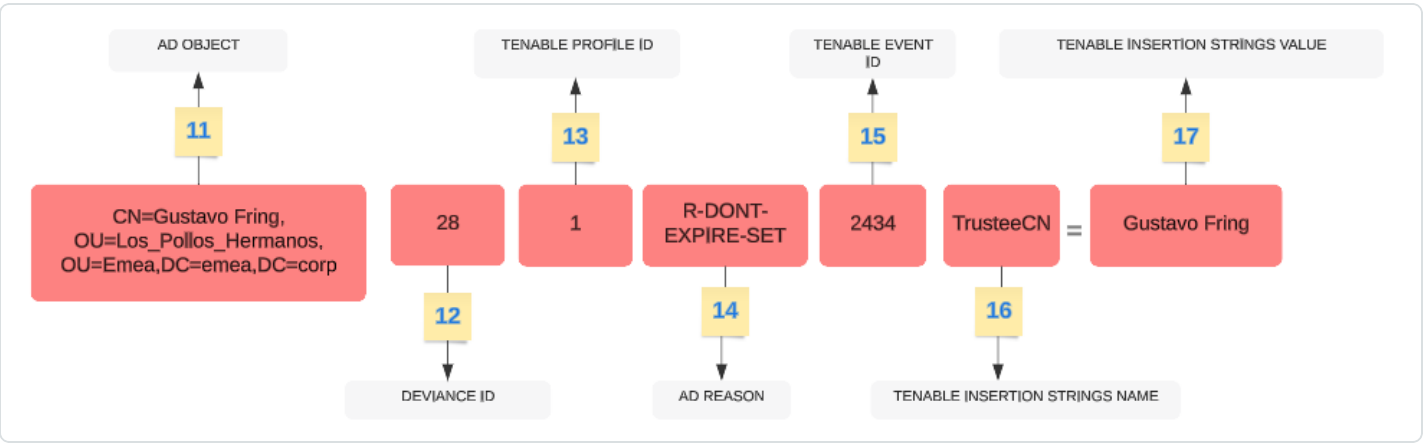


The header structure includes the following parts, as described in the table.

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), "3" (=On health check status change)
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"

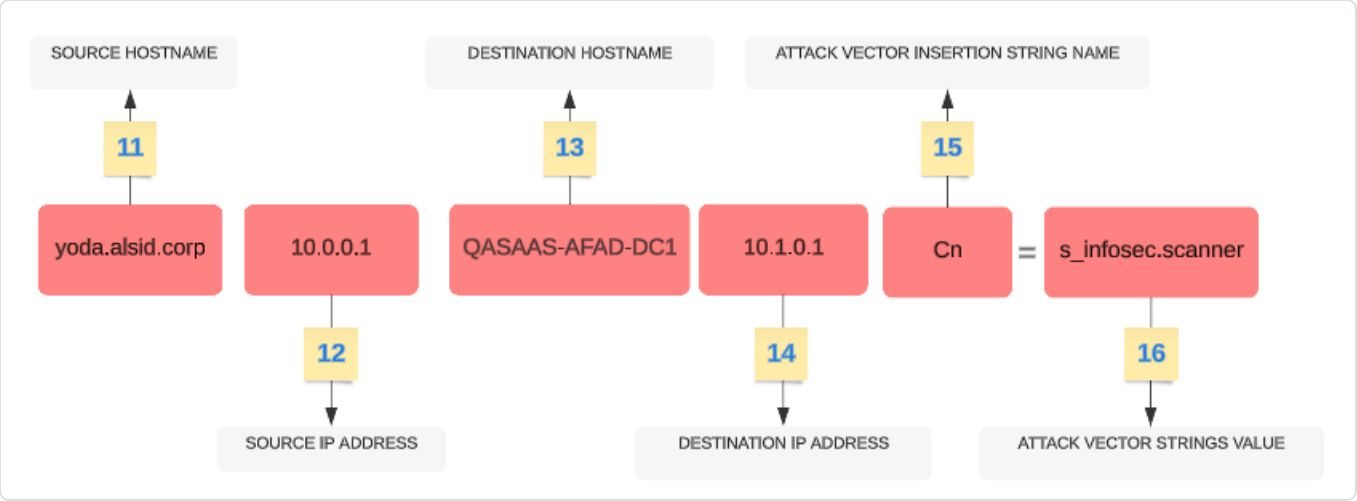
IoE Specific Elements



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.

Syslog Message Framing

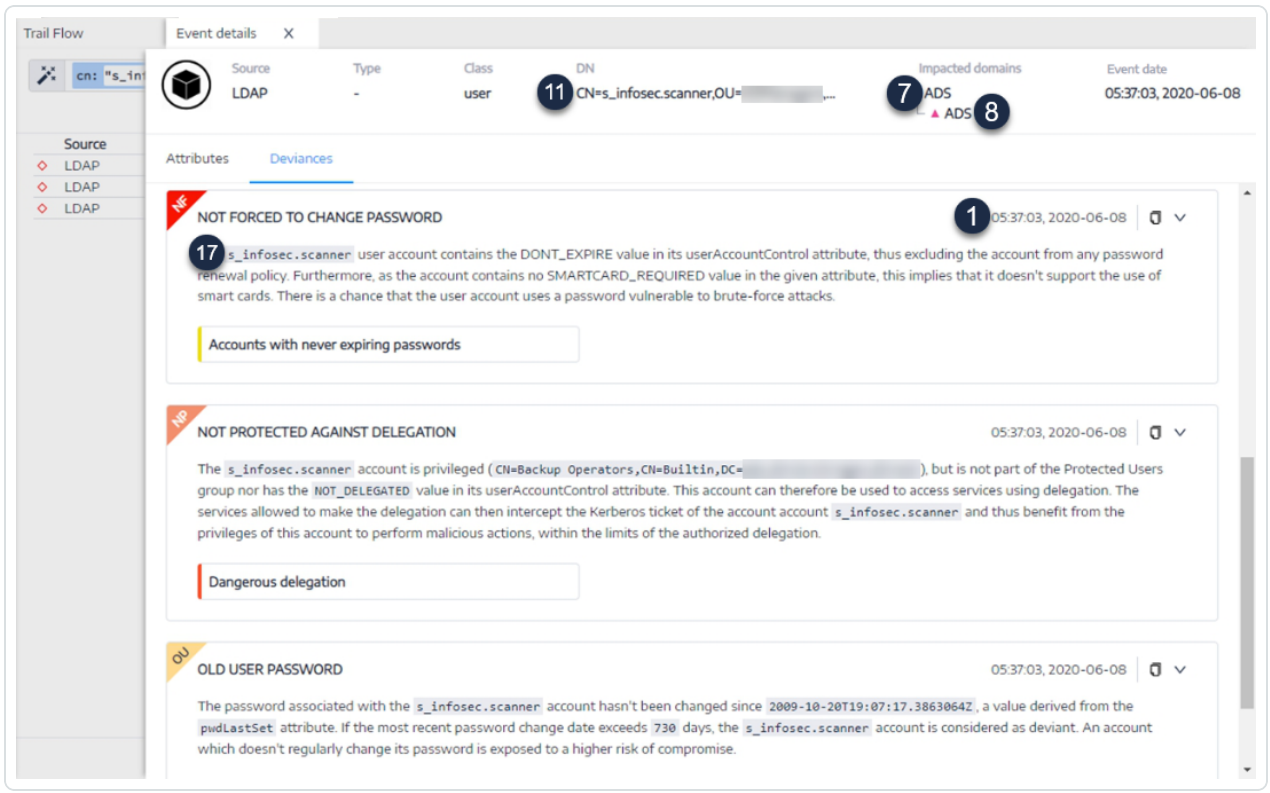
- For UDP and TCP syslog configuration, Tenable Identity Exposure uses Non-Transparent-Framing method as per RFC-6587#3.4.2 to delimit messages. The framing character is LF (\n).
- For TCP with TLS, Tenable Identity Exposure uses Octet Counting method as described in RFC-6587#3.4.1.

Examples

Trail Flow Event Details

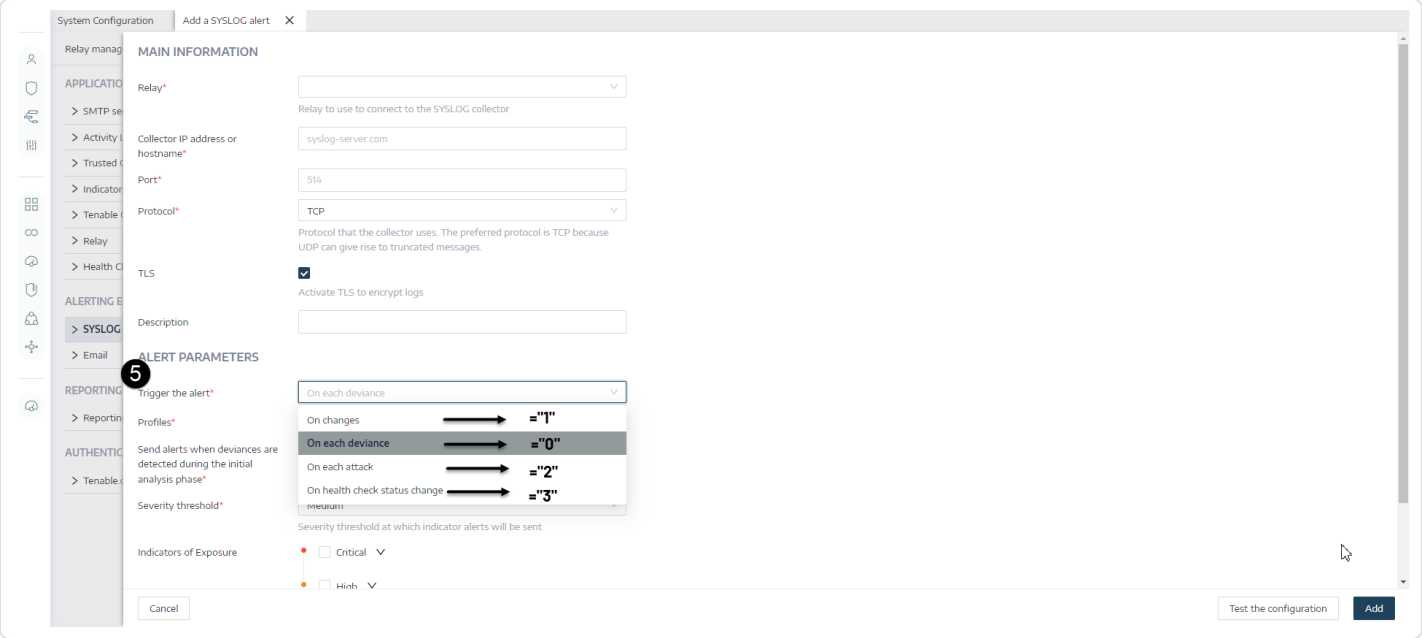
The following example shows details of an event in the Trail Flow containing the following:

- 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)



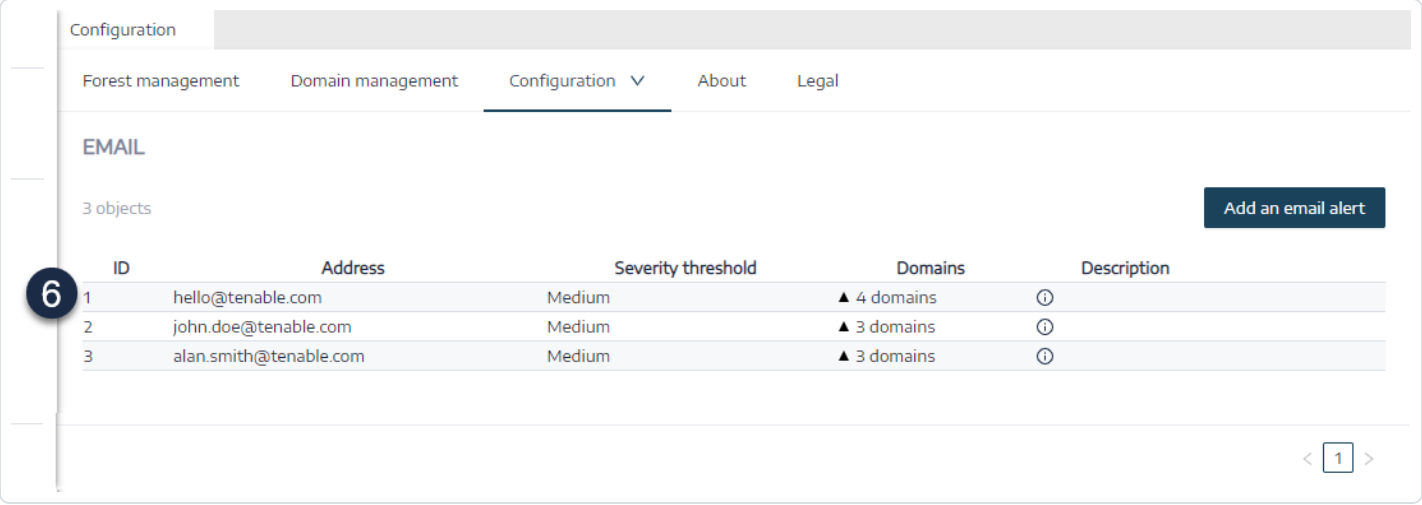
Event Source

This example shows the source for the event (5). You set this parameter in the Syslog configuration page. For more information, see Syslog Alerts.



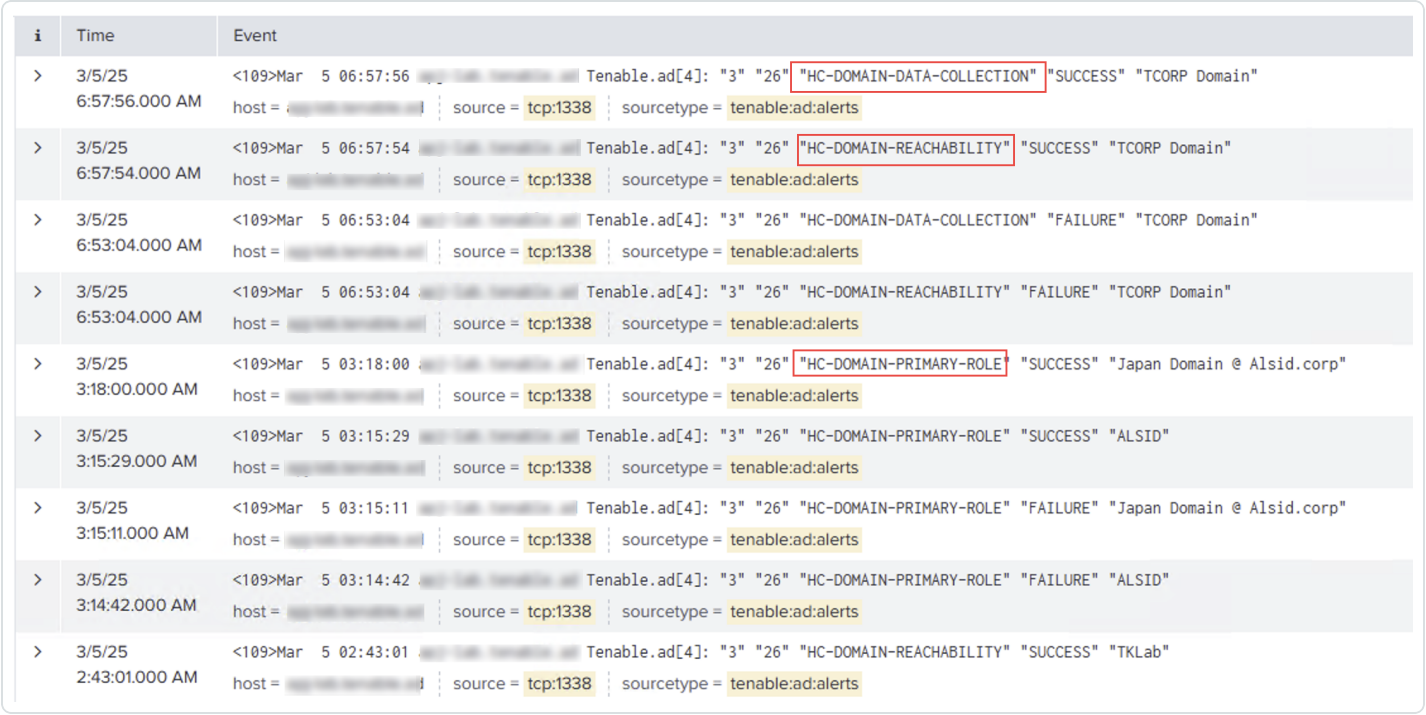
Alert ID

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**.

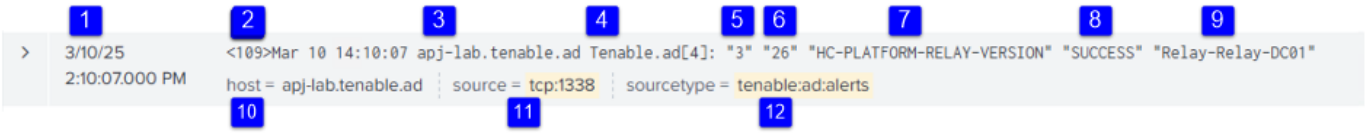


Health Checks

This example shows the results for the health checks that Tenable Identity Exposure carried out in your environment. For more information, see Health Checks.



i	Time	Event
>	3/5/25 6:57:56.000 AM	<109>Mar 5 06:57:56 [redacted] Tenable.ad[4]: "3" "26" "HC-DOMAIN-DATA-COLLECTION" "SUCCESS" "TCORP Domain" host = [redacted] source = tcp:1338 sourcetype = tenable:ad:alerts
>	3/5/25 6:57:54.000 AM	<109>Mar 5 06:57:54 [redacted] Tenable.ad[4]: "3" "26" "HC-DOMAIN-REACHABILITY" "SUCCESS" "TCORP Domain" host = [redacted] source = tcp:1338 sourcetype = tenable:ad:alerts
>	3/5/25 6:53:04.000 AM	<109>Mar 5 06:53:04 [redacted] Tenable.ad[4]: "3" "26" "HC-DOMAIN-DATA-COLLECTION" "FAILURE" "TCORP Domain" host = [redacted] source = tcp:1338 sourcetype = tenable:ad:alerts
>	3/5/25 6:53:04.000 AM	<109>Mar 5 06:53:04 [redacted] Tenable.ad[4]: "3" "26" "HC-DOMAIN-REACHABILITY" "FAILURE" "TCORP Domain" host = [redacted] source = tcp:1338 sourcetype = tenable:ad:alerts
>	3/5/25 3:18:00.000 AM	<109>Mar 5 03:18:00 [redacted] Tenable.ad[4]: "3" "26" "HC-DOMAIN-PRIMARY-ROLE" "SUCCESS" "Japan Domain @ Alsid.corp" host = [redacted] source = tcp:1338 sourcetype = tenable:ad:alerts
>	3/5/25 3:15:29.000 AM	<109>Mar 5 03:15:29 [redacted] Tenable.ad[4]: "3" "26" "HC-DOMAIN-PRIMARY-ROLE" "SUCCESS" "ALSID" host = [redacted] source = tcp:1338 sourcetype = tenable:ad:alerts
>	3/5/25 3:15:11.000 AM	<109>Mar 5 03:15:11 [redacted] Tenable.ad[4]: "3" "26" "HC-DOMAIN-PRIMARY-ROLE" "FAILURE" "Japan Domain @ Alsid.corp" host = [redacted] source = tcp:1338 sourcetype = tenable:ad:alerts
>	3/5/25 3:14:42.000 AM	<109>Mar 5 03:14:42 [redacted] Tenable.ad[4]: "3" "26" "HC-DOMAIN-PRIMARY-ROLE" "FAILURE" "ALSID" host = [redacted] source = tcp:1338 sourcetype = tenable:ad:alerts
>	3/5/25 2:43:01.000 AM	<109>Mar 5 02:43:01 [redacted] Tenable.ad[4]: "3" "26" "HC-DOMAIN-REACHABILITY" "SUCCESS" "TKLab" host = [redacted] source = tcp:1338 sourcetype = tenable:ad:alerts



The header structure includes the following parts, as described in the table.

Part	Description
1	**Time Stamp**– Indicates the date and time when the event was detected.
2	**Syslog Priority** – This is the syslog priority value, combining the facility and severity levels (RFC-3164)
3	**Hostname** – The hostname of the application or device that generated the alert.
4	**Product Name and PID** – Specifies the product name and its process ID.
5	**Tenable Msg Type** – The identifier of event sources. Example: "0" (= On each deviance), "1" (= On changes), "2" (= On each attack), "3" (=On health check status

	change)
6	**Tenable Alert ID** – The unique ID of the alert. Example: "0", "132"
7	**Health Check Codename** – Denotes the specific health check performed. For more information, see Health Checks.
8	**Health Check Status** – Indicates the outcome of the health check.
9	**Relay Name or Domain Name** – Identifies the relay or domain controller associated with this health check.
10-12	**Metadata Fields**: • Host (10): Reiterates the hostname for indexing and search purposes. • Source (11): Specifies the source of the log. • Sourcetype (12): Categorizes the log format for parsing and analysis.

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.

Health 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.
- Indicators of Attack: Domain Controller activity – Tenable Identity Exposure receives Windows event logs from all Domain Controllers.
- Indicators of Attack: Domain installation – Ensure Tenable IoA GPO configuration is correct.

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. For more information, see List of Health Checks below.

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**.

List of Health Checks

Health Check Name	Type	Description of Check	Details
Domain Reachability (HC-DOMAIN-REACHABILITY)	Domain	Ability to establish a connection with the AD domain.	• Reachable Domain Controller IP Address or FQDN • Reachable Global Catalog LDAP Server • Reachable LDAP Server • Reachable SMB Server • Working Connection to the Dynamic RPC Port • Working Connection to RPC Port
Authentication to the AD Domain (HC-DOMAIN-AUTHENTICATION)	Domain	Ability to authenticate to the AD domain.	• Valid Credentials • Idle LDAP Server

			• Available LDAP Server • LDAP Access Granted • SMB Access Granted
Permissions to Collect the AD Domain Data (HC-DOMAIN-DATA-COLLECTION)	Domain	Ability to collect the AD domain data.	• Granted Permissions to Collect Privileged Data
Permissions to Access the AD Containers (HC-DOMAIN-CONTAINER-ACCESS)	Domain	Ability to can access the AD containers.	• Granted Permissions to Access Deleted Objects Container • Granted Permissions to Access Password Settings Container
Domain Linked to Relay (HC-DOMAIN-LINKED-TO-RELAY)	Domain	The domain is linked to a Relay.	• Domain Linked to a Relay
IoAs - Domain Controller Activity (HC-DOMAIN-EVENT-LOGS-COLLECTION-DOMAIN-CONTROLLER-ACTIVITY)	Domain	Tenable Identity Exposure receives Windows event logs from all Domain	• Inactive Domain Controllers

		Controllers.	
Monitored Domain Controller has the PDCe role (HC-DOMAIN-PRIMARY-ROLE)	Domain	The monitored Domain Controller holds the PDC Emulator (PDCe) role, which is essential for certain security features.	• Ensures the optimal functioning of Indicators of Exposure (IoE) and Indicators of Attack (IoA)
IoAs - SMB Share Setup (HC-DOMAIN-EVENT-LOGS-COLLECTION-SMB-SHARE-CONFIGURATION)	Domain	The Tenable Identity Exposure Windows event log collection is correctly configured for SMB share mode (will not show if SMB mode is disabled).	
IoAs - SMB Share Reachable (HC-DOMAIN-EVENT-LOGS-COLLECTION-SMB-SHARE-REACHABILITY)	Domain	The Tenable Identity Exposure event log collection SMB share is reachable (will not show if SMB mode is disabled).	
IoAs - Domain Installation (HC-DOMAIN-IOA-CONFIGURATION)	Domain	Ensure Tenable IoA GPO configuration is	• Tenable IoA GPO exists in the LDAP

		correct.	• Tenable IoA GPO folder exists in the SYSVOL • Tenable IoA GPO IoA folder exists in the SYSVOL • Tenable IoA GPO EVT Subscribe listener file exists in the SYSVOL • Tenable IoA GPO configuration file exists in the SYSVOL • Tenable IoA GPO `audit.csv` file exists in the SYSVOL
Email Alerting (HC-PLATFORM-ALERTING)	Platform	The email alerting using MS 365/Office SMTP servers via OAuth 2 functions correctly.	• Correct SMTP server configuration for OAuth 2
Relay Service Up	Platform	The Relay is	• Running Relay

(HC-PLATFORM-RELAY-UP)		working as expected.	Service
Relay Service Version (HC-PLATFORM-RELAY-VERSION)	Platform	The Relay version is aligned with the product.	• Relay Version Consistency
AD Data Collector Up (HC-PLATFORM-AD-DATA-COLLECTOR-UP)	Platform	The AD data collector is working as expected.	• Running AD Data Collector Bridge • Running AD Data Collector Service • Running Broker
Synchronization between Tenable Cloud & Tenable Identity Exposure services (HC-PLATFORM-TENABLE-CLOUD-SYNC)	Platform	Created Tenable Cloud group, permissions, and users are synchronized with Tenable Identity Exposure database.	• Tenable Cloud availability

Reporting Center

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

It offers the following functions:

- **Granular filtering**: Refine reports using granular filters based on date range, domain, Indicator of Attack (IoA), Indicator of Exposure (IoE), and more, ensuring laser-focused insights.

- **Automated delivery**: Schedule reports for automatic generation and delivery at desired intervals, streamlining security monitoring and reporting processes.
- **Flexible exporting**: Export reports in various formats like CSV for further analysis, sharing using reports access key, or integration with existing reporting workflows.

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

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

To access the reporting center:

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

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

See also

- Reporting Center
- Set Permissions for a Role

Configuring Microsoft Entra ID as an Identity Provider

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

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

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

Prerequisites

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

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

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

Permissions

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

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

Network Flows

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

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

License Count

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

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

Configure Microsoft Entra ID settings

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

1. **Create an application:**

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

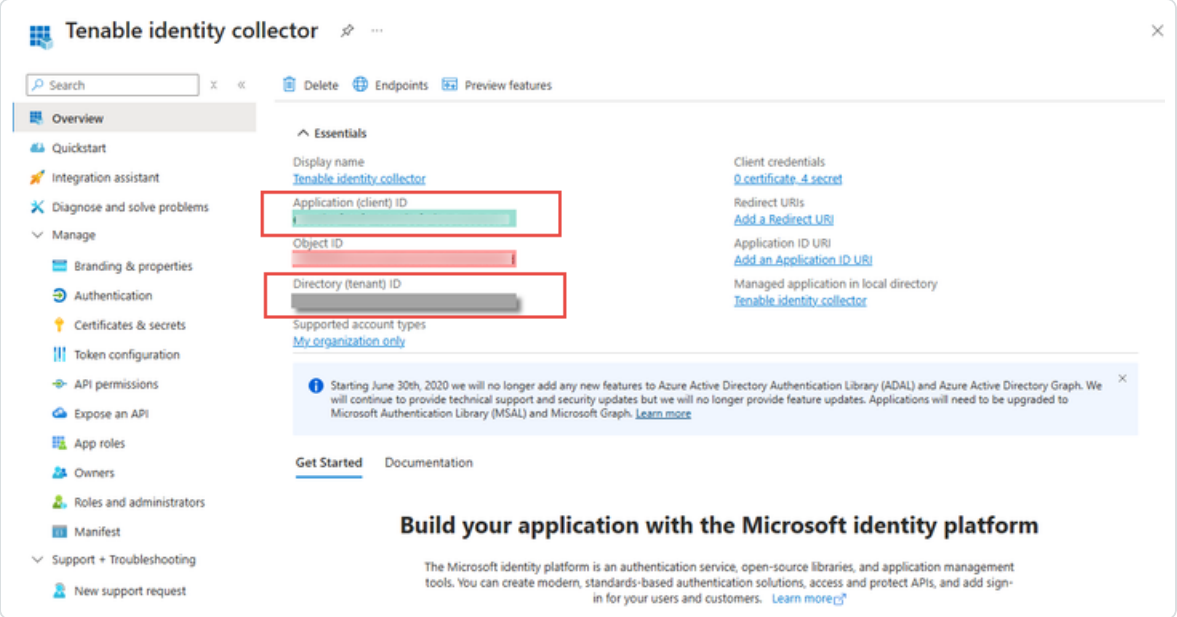
   b. Click **+ New registration**.

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

   d. Click **Register**.

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

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



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.

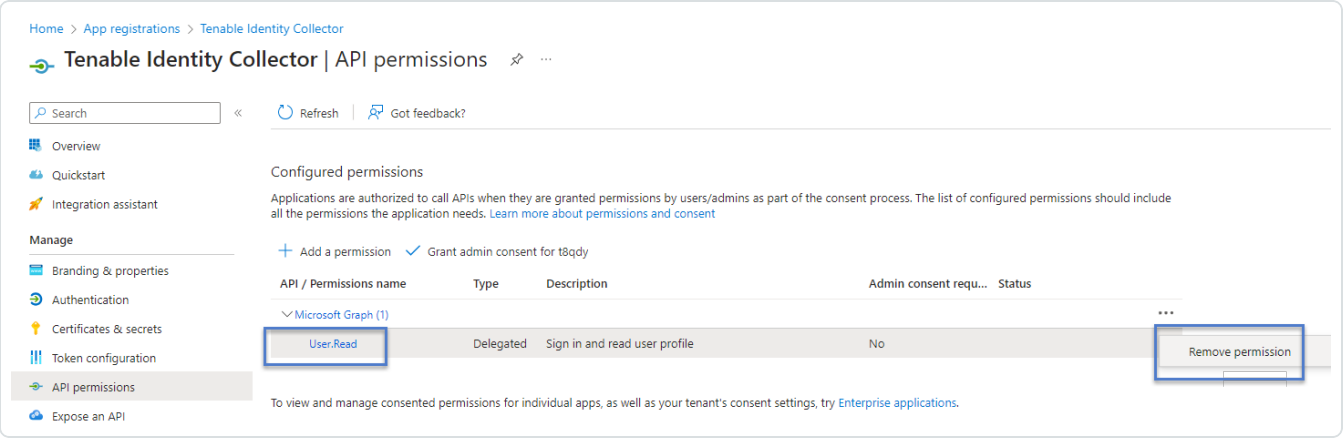
3. **Assign permissions to the application:**

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

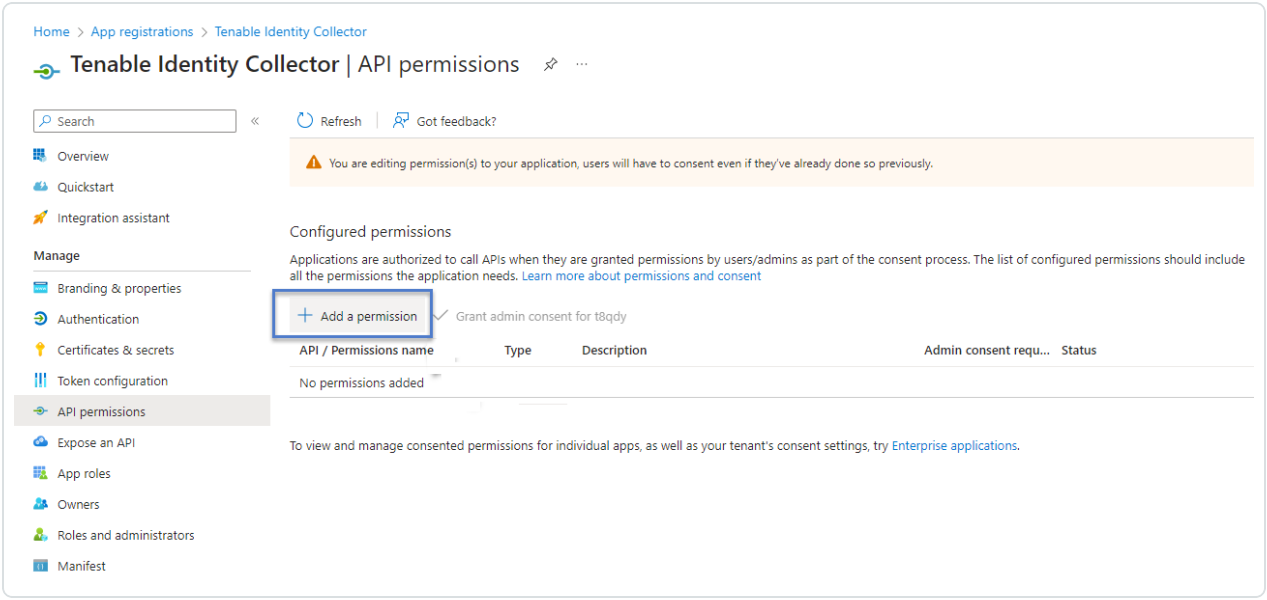
b. Click on the application you created.

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

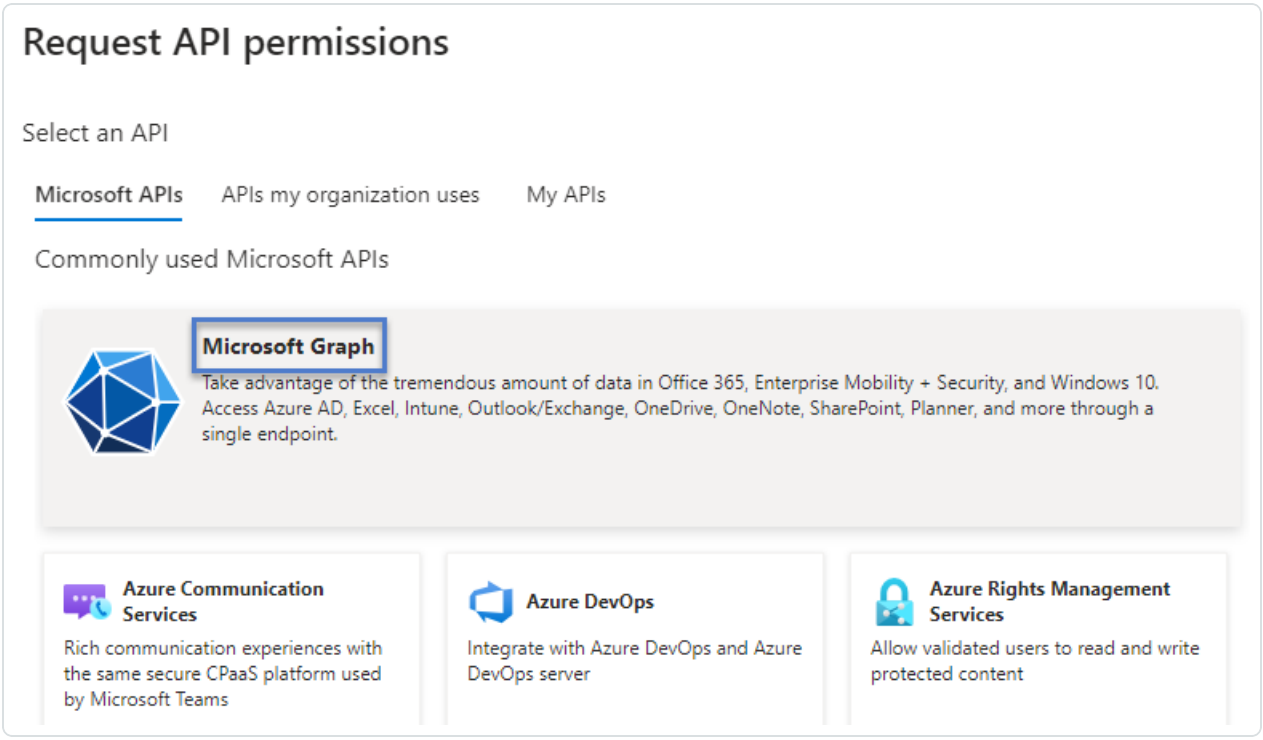
d. Remove the existing `User.Read` permission:



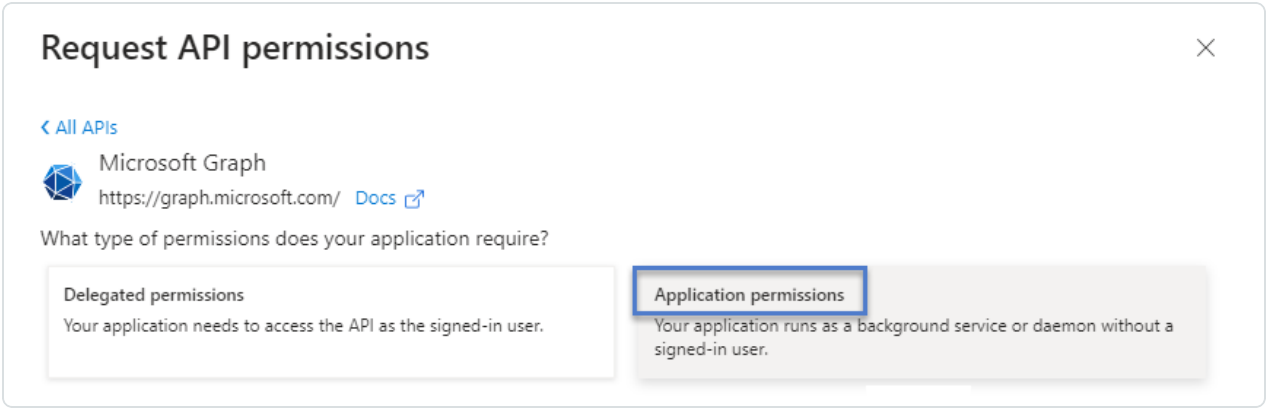
e. Click **+ Add a permission**:



f. Select **Microsoft Graph**:



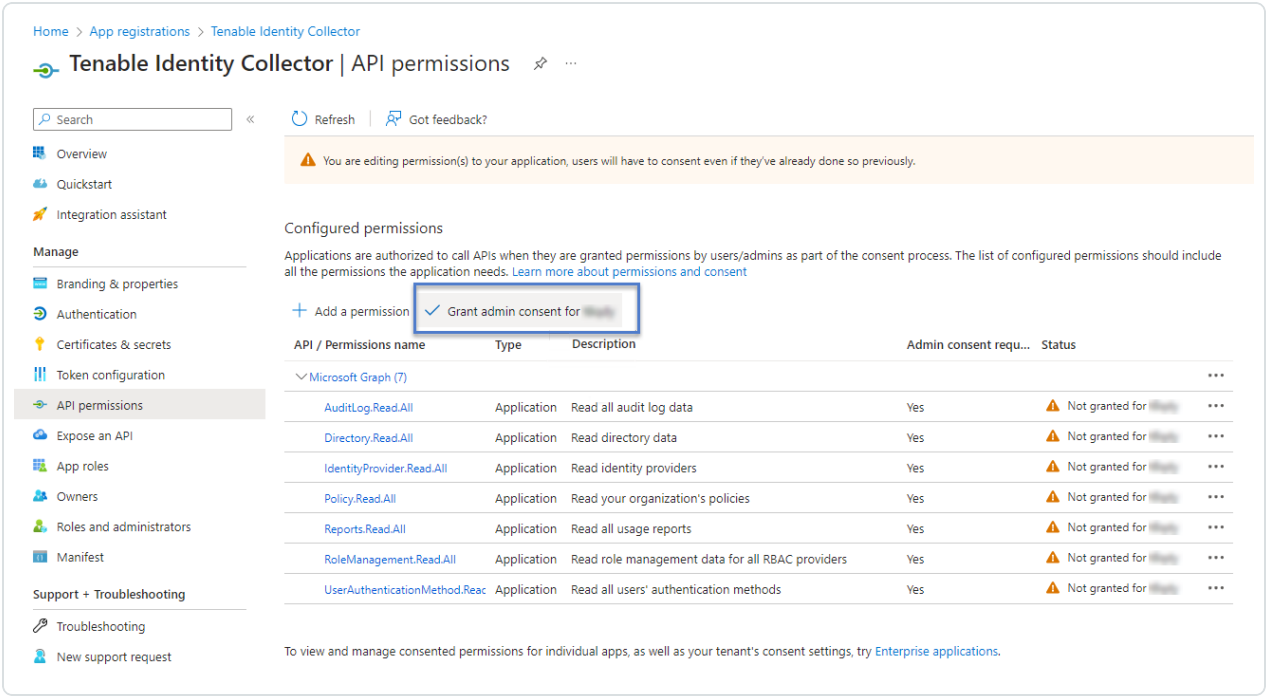
g. Select **Application permissions** (not "Delegated permissions").

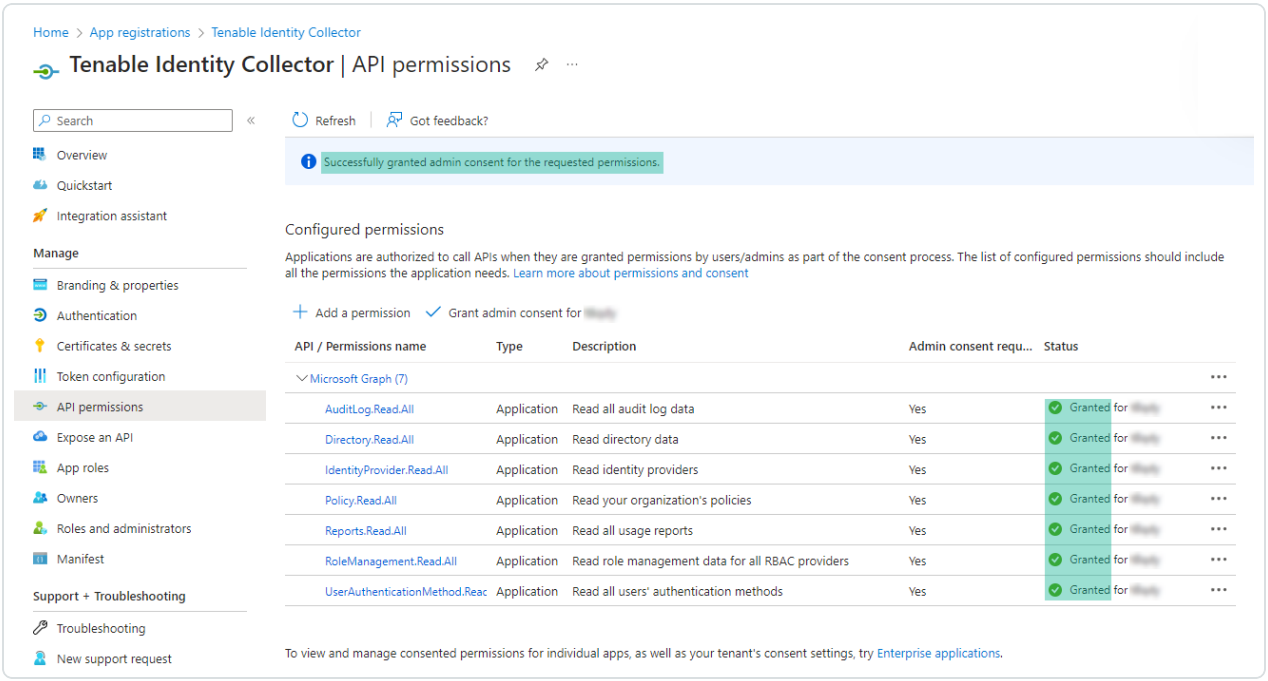


h. Use the list or the search bar to find and select all the following permissions:
   - `AuditLog.Read.All`
   - `Directory.Read.All`
   - `IdentityProvider.Read.All`
   - `Policy.Read.All`
   - `Reports.Read.All`
   - `RoleManagement.Read.All`
   - `UserAuthenticationMethod.Read.All`

i. Click **Add permissions**.

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





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

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

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

Activate Microsoft Entra ID support

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

Enable tenant scans

To add a new Microsoft Entra ID tenant:

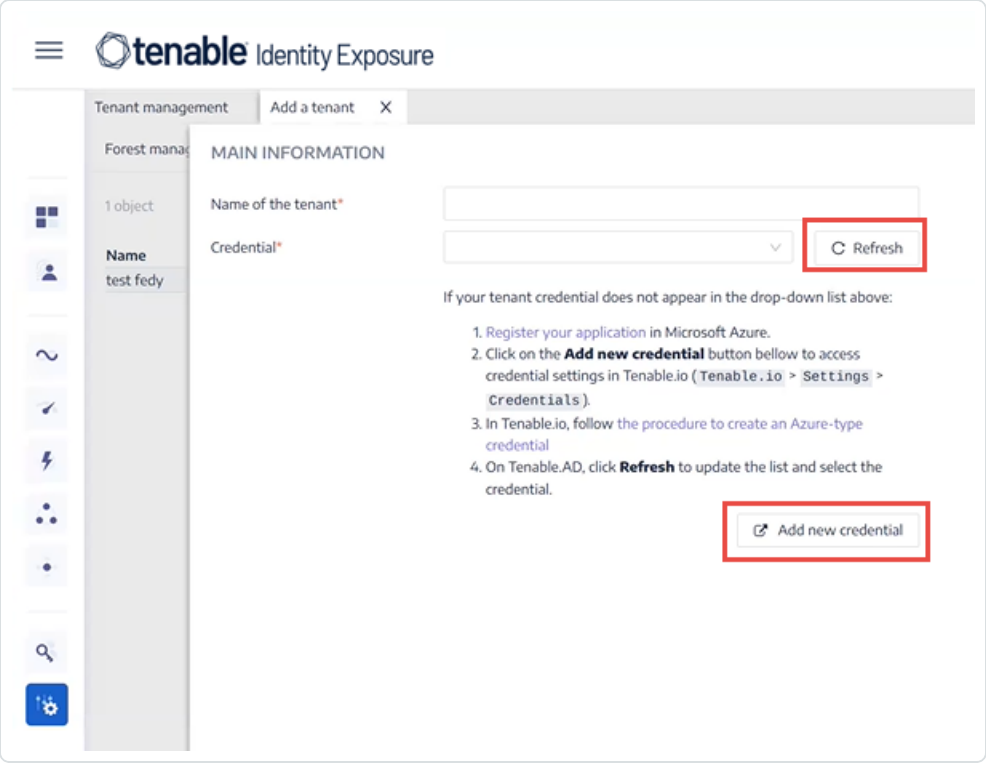
Adding a tenant links Tenable Identity Exposure with the Microsoft Entra ID tenant to perform scans on that tenant.

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

   The **Tenant Management** page opens.

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

   The **Add a tenant** page opens.



3. In the **Name of the tenant** box, type a name.
4. In the **Credentials** box, click the drop-down list to select a credential.

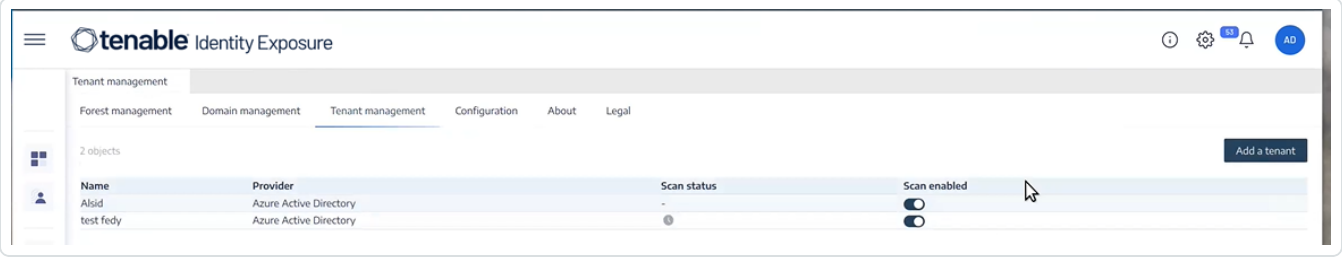
5. If your credential does not appear in the list, you can either:
    - Create one in Tenable Vulnerability Management (Tenable Vulnerability Management > **Settings** > **Credentials**). For more information, see the procedure to create an Azure-type credential in Tenable Vulnerability Management.
    - Check that you have the "Can use" or "Can edit" permission for the credential in Tenable Vulnerability Management. Unless you have these permissions, Tenable Identity Exposure does not show the credential in the drop-down list.
6. Click **Refresh** to update the drop-down list of credentials.
7. Select the credential you created.
8. Click **Add**.

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

To enable scans for the tenant:

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

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



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

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

Refresh Entra ID Credentials

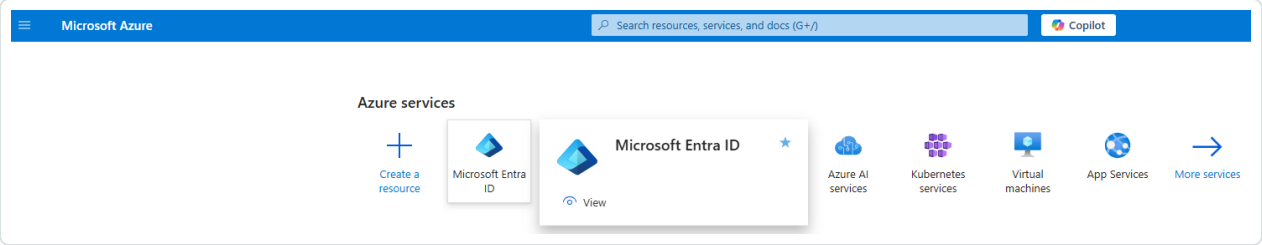
In Microsoft Entra ID (formerly Azure Active Directory), credential expiration varies depending on the type of credential and your organization's configuration.

When your Entra ID credentials expire, Tenable Vulnerability Management stops syncing assets and vulnerabilities from Entra ID. You see a warning message indicating that the connector is no longer working.

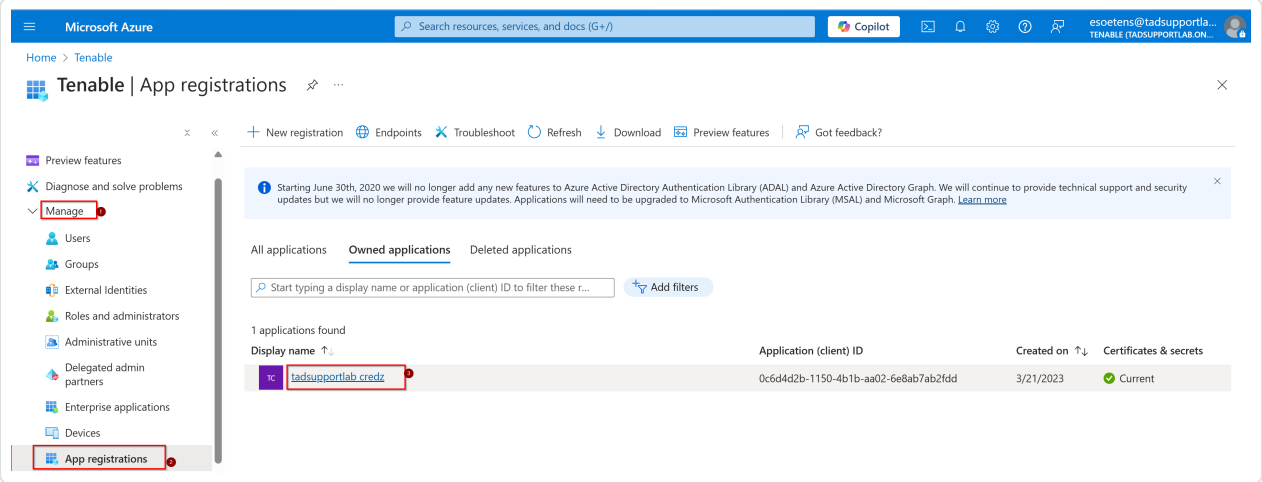
To refresh your credentials and restore synchronization:

1. Access **Microsoft Entra ID**:

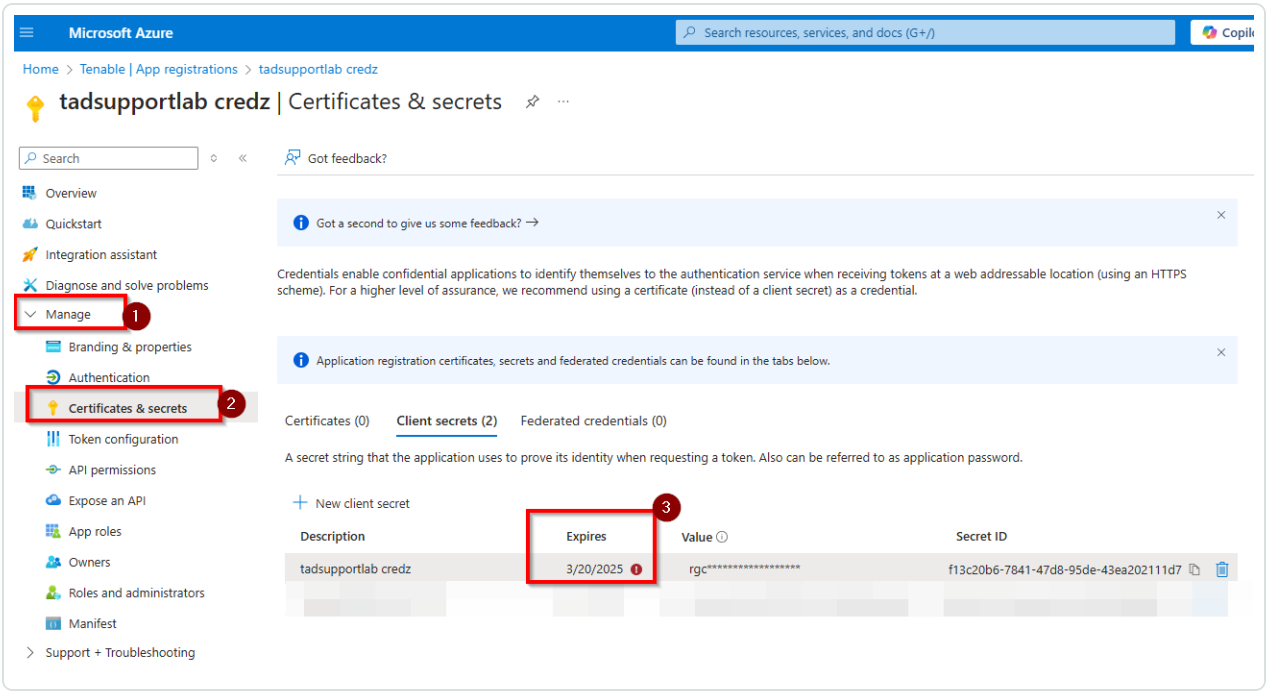
    a. Log in to your Microsoft Entra ID tenant.



    b. Go to **Manage → App registrations.**



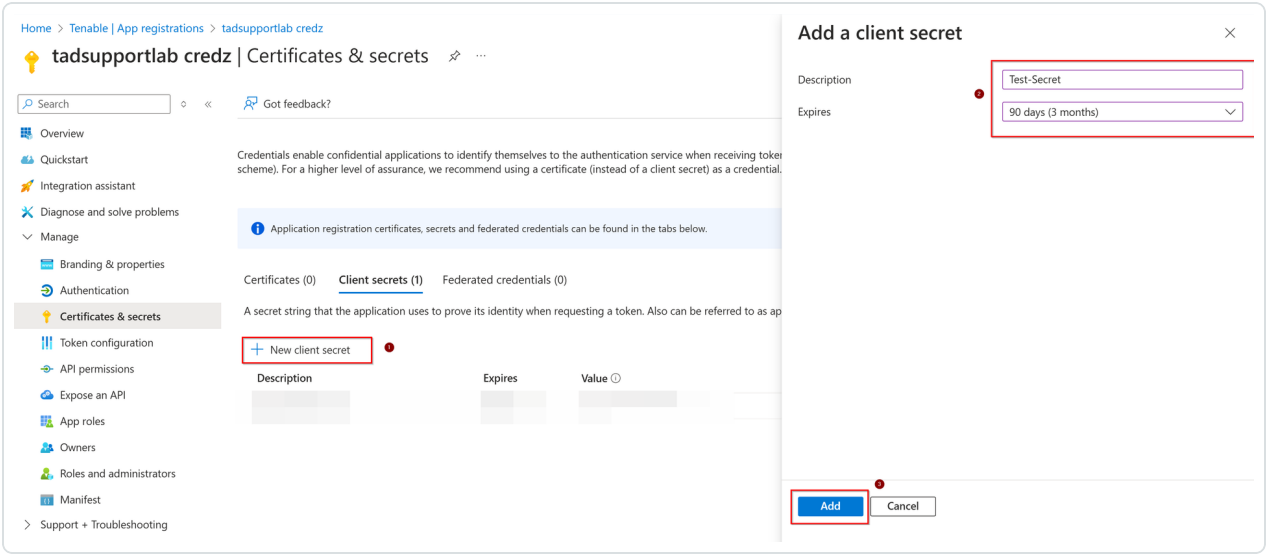
c. Select the app you previously created for Tenable Identity Exposure.



2. Create a new client secret:

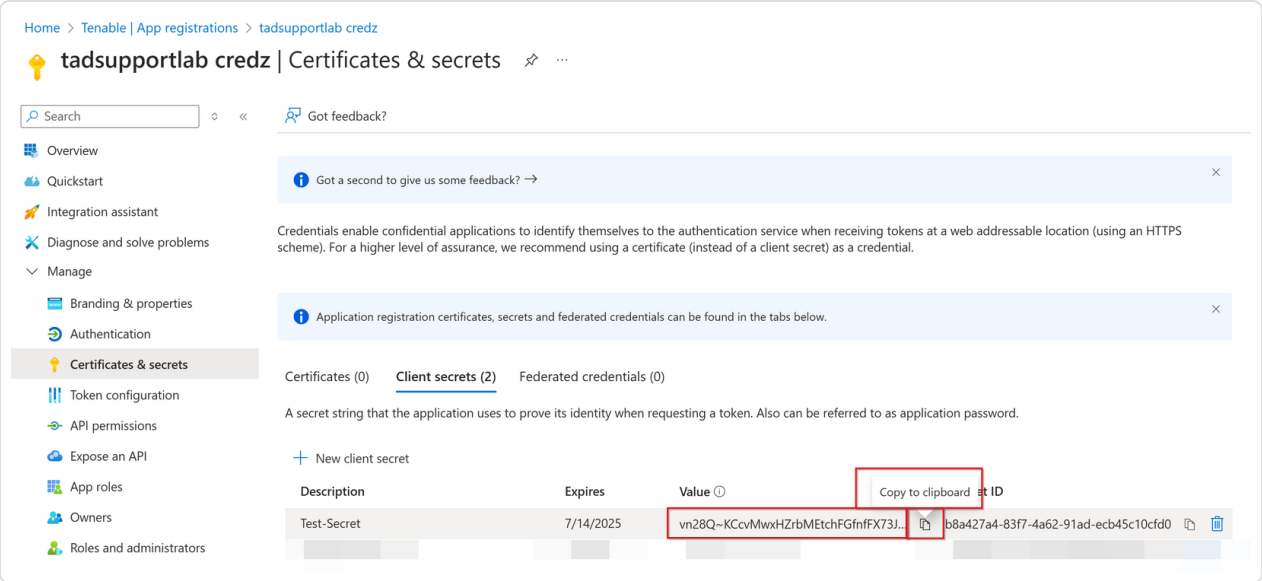
a. Under **Manage**, click **Certificates & secrets**.

b. Click **+ New client secret**.



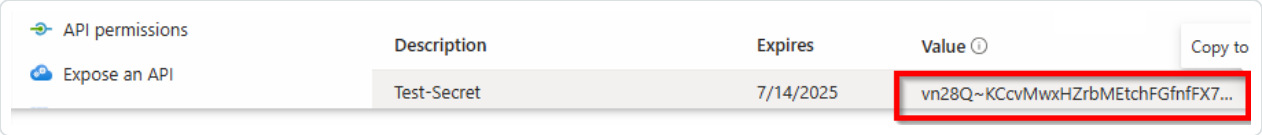
c. Enter a description, set an expiration period (e.g., 6 or 12 months), and click **Add**.

d. **Important**: Immediately copy the **value of the client secret** (not the Secret ID), and securely store it in a password vault.



> **Note**: This step is critical because the client secret's value is displayed **only once** at the time of creation. It's a common mistake to copy the Secret ID (which remains visible) instead of the actual secret value.

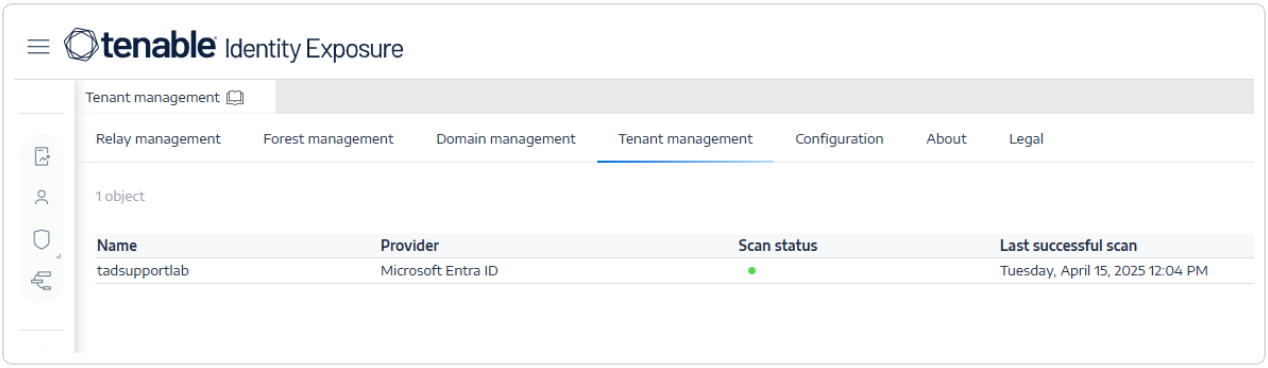
3. Update credentials in Tenable Vulnerability Management:
   a. Log in to **Tenable Vulnerability Management**.
   b. Navigate to **Settings** → **Credentials**.
   c. Locate the expired credential to edit it.



   d. Replace the value of your client secret with the new value from EntraID.
   e. Save the new value.

4. Confirm status:

    - After saving the new credentials, check your scan status.



        - A Green status indicates success.
        - If the status is Orange, ensure you did not mix up the Secret Value with the Secret ID. If necessary, repeat from Step 2.

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.

Prerequisites

To use Privileged Analysis, you must open the dynamic RPC ports **TCP/49152-65535** and **UDP/49152-65535**. For additional information, see Network Flow Matrix.

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, password hashes never leave the client's infrastructure, as only the Relay handles them. The Relay does not store passwords nor passwords hashes but retrieves the user's password hash 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.

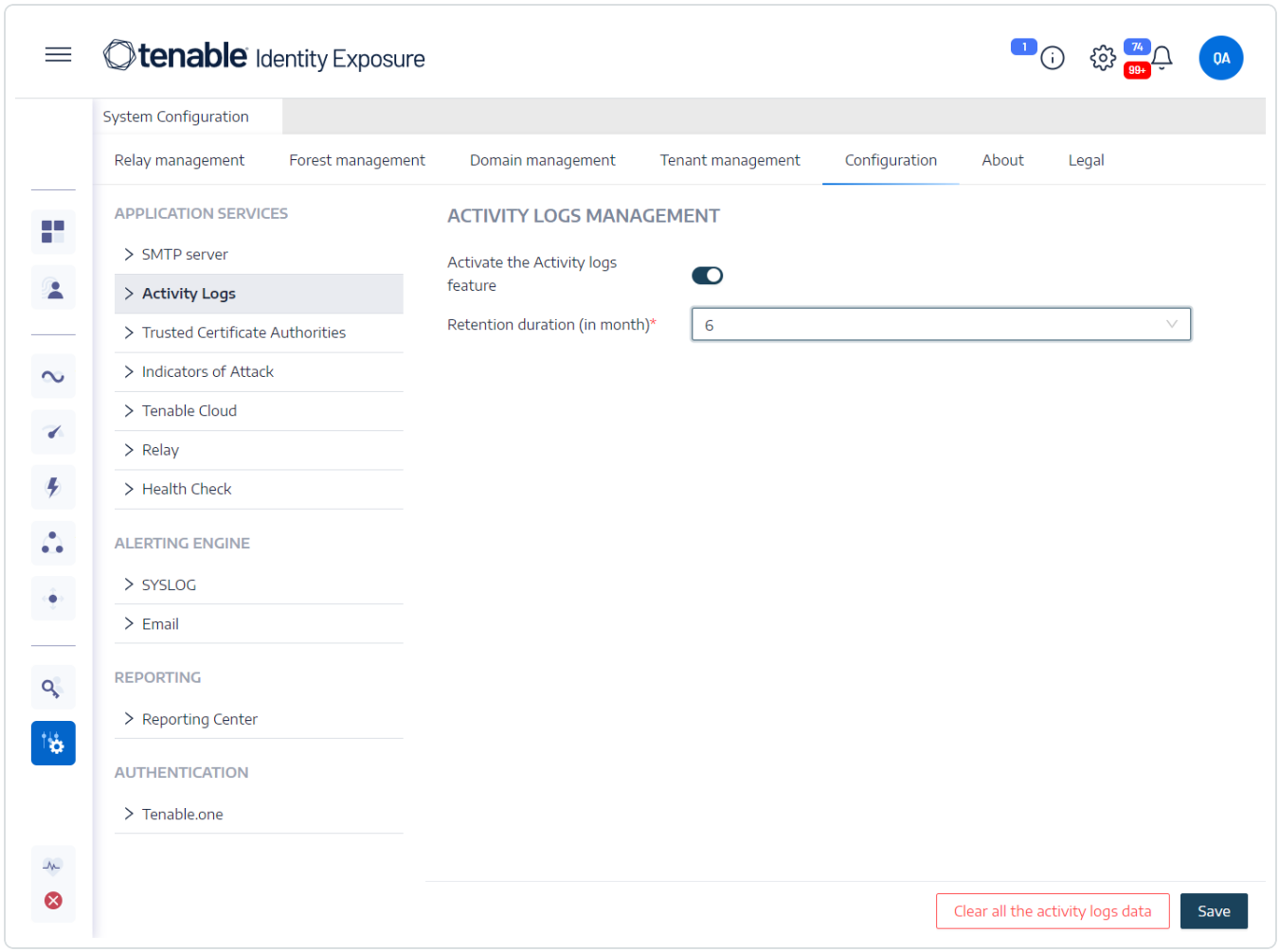
2. Under the **Application Services** section, click **Activity Logs**.

   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.



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.

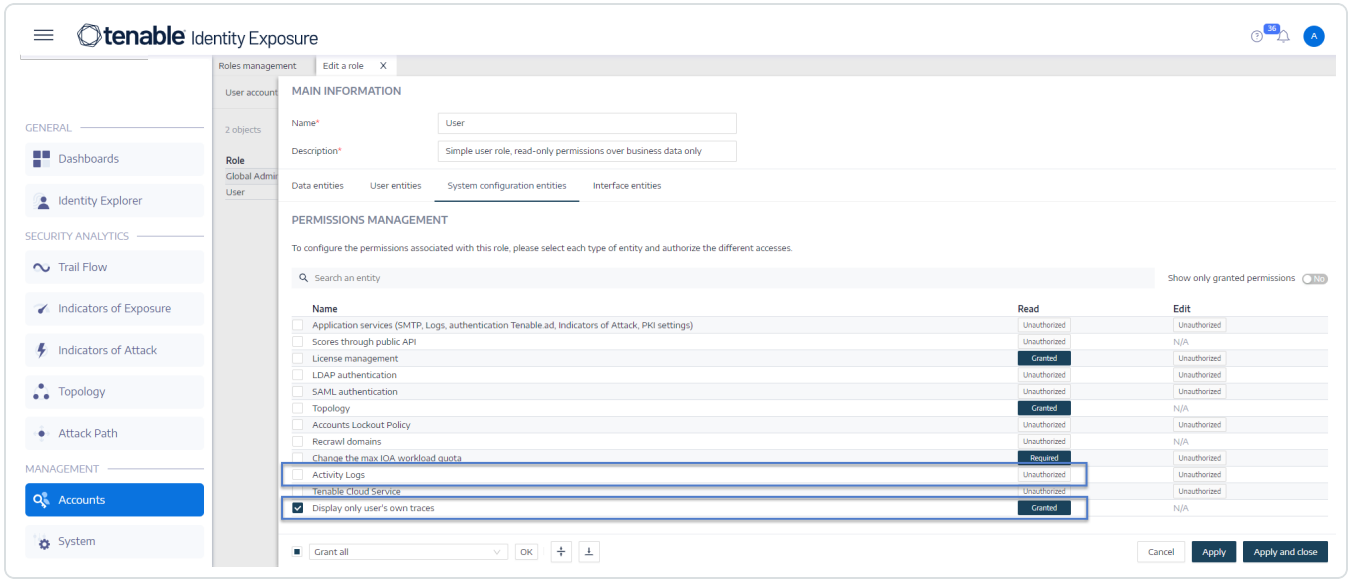
4. Under the **Main Information** section, select the **System Configuration Entities** tab.

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.



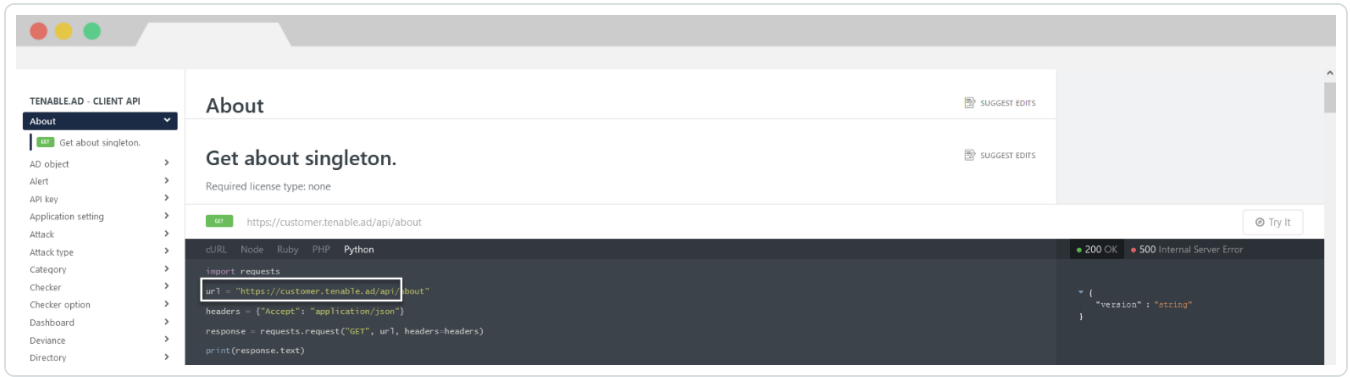
Tenable Identity Exposure Public API

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.

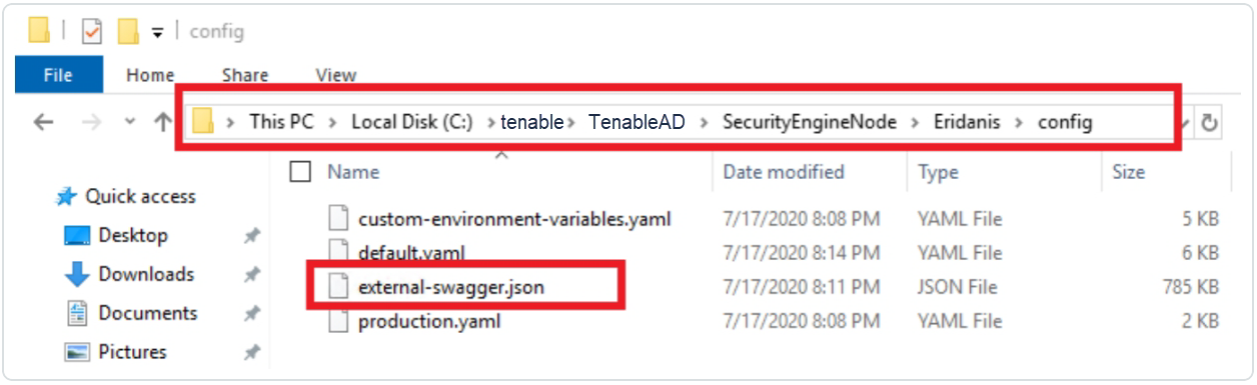
To access the API for your Tenable Identity Exposure instance:

- In your browser, open this URL:



To download the OpenAPI file:

- For On-Premises installations, follow this path to the Security Engine Node:



- 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 .

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 from Microsoft Entra ID and Active Directory for up to 15 months.

Capability	Retention Period
Attack Path	6 months
Topology	
Trail Flow	
Dashboards and Reporting	12 months
Exposure Center	Up to 15 months
Identity 360	
Indicators of Exposure (Entra ID)	
Indicators of Exposure (Active Directory)	• Active issues: Retained indefinitely • Addressed issues: Retained for 6 months
Indicators of Attack (Active Directory)	

For more information, see Tenable Cloud Platform Data.

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.

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.

Use this PowerShell script to trace enabled user accounts in AD:

```
(Get-ADuser -Filter 'enabled -eq $true').count
```

Use this PowerShell script to trace enabled user accounts in Entra ID:

```
(Get-MgUser -All -Filter "accountEnabled eq true" -Property onPremisesSyncEnabled | where {
$_.onPremisesSyncEnabled -ne $true }).Count
```

Tenable Identity Exposure Components

Both versions of Tenable Identity Exposure come with the following components:

- Trail Flow
- Topology
- Indicators of Exposure
- Indicators of Attacks
- Attack Paths
- Exposure Center
- 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. You can temporarily exceed your licensed identity count. However, when you scan more identities than you have licensed, Tenable clearly communicates the overage and then reduces functionality in three stages.

Note: For on-premises environments using Tenable Identity Exposure 3.77 or later, the license enforcement is immediate.

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 30+ days	A message appears in Tenable Identity Exposure and you cannot use the Indicator of Exposure feature in the user interface or API.

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.

Tip: The license file is located in the Tenable Community Portal under "My Products" (you must be an administrator in the Tenable Community to view the license file.)

Tip: To download the license file from Tenable One, see this video for step-by-step instructions.

Caution: If you do not apply a valid license to your SaaS platform, Tenable decommissions it after a certain period.

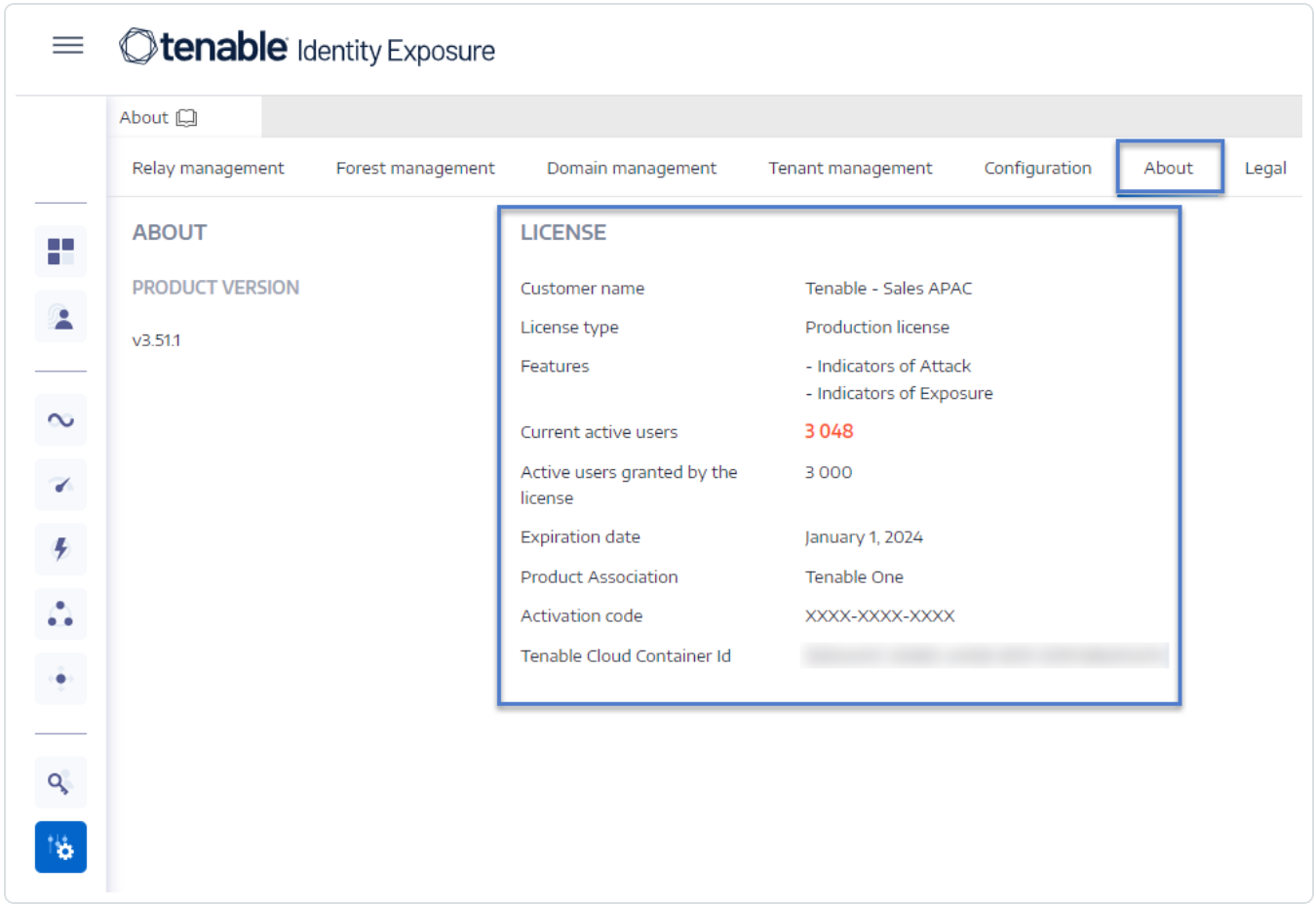
The Tenable Identity Exposure licenses can include:

- 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.



License Consumption

For on-premises installations, Tenable Identity Exposure tracks the license consumption if there is an internet connection available.

Prevention of Container UUID Mismatches

In Tenable Identity Exposure, each license includes a unique Container UUID, linking the application to a specific Tenable Cloud container. This container UUID must remain consistent to ensure seamless integration and avoid operational issues.

In order to prevent container UUID inconsistency (for example when upload a new license on after renewal) Tenable Identity Exposure can detect container UUID “mismatches”.

If you attempt to upload a license with a different Container UUID, the message "Cannot change Tenable Cloud container" appears. You may be in one of the following scenarios:

- Migration from Tenable Identity Exposure standalone to a Tenable One license.
- Migration of your container from one Tenable AWS site to another.
- Expiration of the former container and creation of a new one.

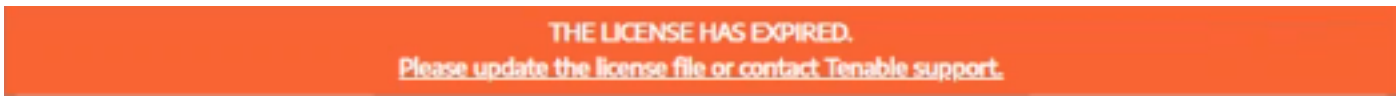
If you are in one of these cases, please contact Tenable to discuss changing your Tenable Cloud container for this Tenable Identity Exposure platform.

License Validity

The Tenable Identity Exposure license remains valid as long as you meet the following criteria:

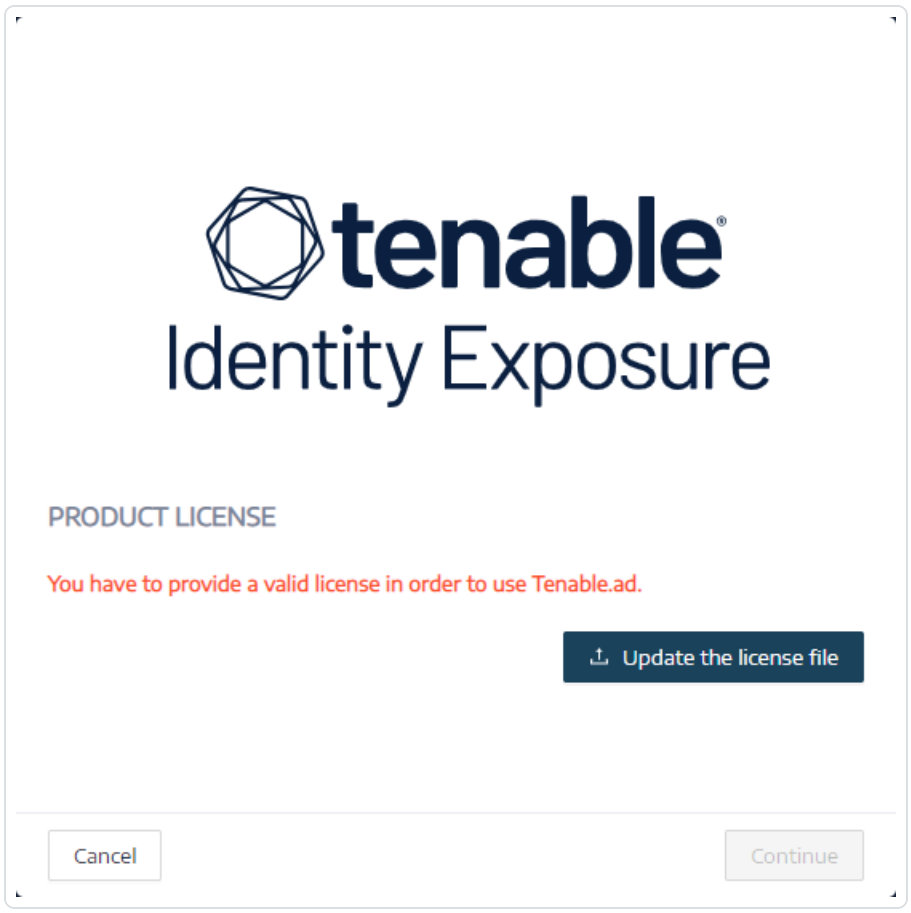
- The number of active users does not exceed the number granted on the license. Tenable Identity Exposure shows three types warning messages depending on your case.
    - The number of active users **is near the limit** of the license conditions: you must update your license.
    - The number of active users **exceeds** the license conditions: you must update your license.
    - The number of active users **exceeds the license conditions (by 10%)**: you no longer have access to the Indicator of Exposure page and must update your 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:



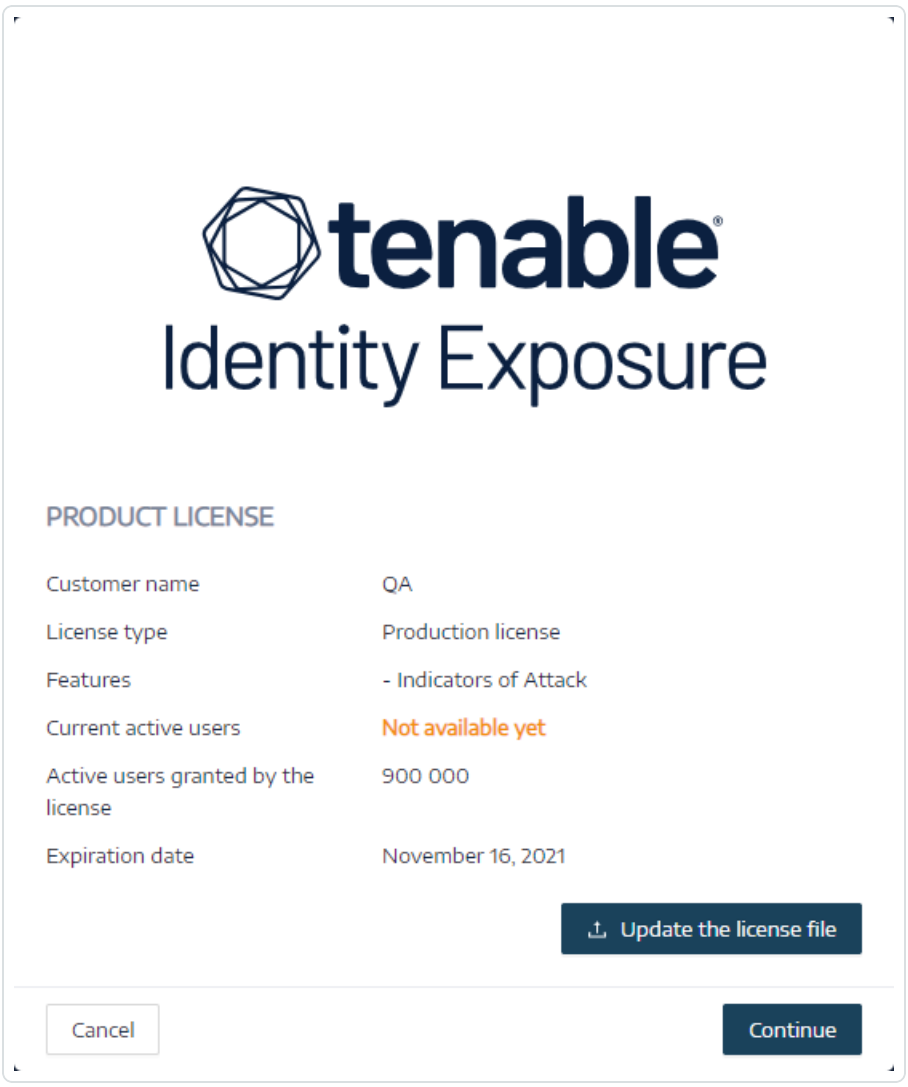
To upload a license file:

1. From the login window, click **Update the license file**.



2. Browse to the location of your license file and click **Open**.

   The following example shows a successfully applied license file:



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.

Long-Term Support (LTS) vs. Interim Versions: Key Differences and Benefits

What is LTS?

LTS (Long-Term Support) versions are software releases that we maintain for an extended period—18 months. During this time, we provide regular updates, such as security patches and critical bug fixes, without introducing new features that might disrupt existing functionality.

LTS versions are designed for customers who prioritize stability, reliability, and long-term maintenance over having the latest features. These versions are ideal for environments where frequent updates or changes could lead to downtime or additional testing and deployment costs.

What are Interim Versions?

Interim versions are our standard software releases, which include new features, improvements, and updates. These versions are more dynamic and updated frequently—every 6 months—but receive support for a shorter period compared to LTS releases.

Interim versions are ideal for customers who want to stay on the cutting edge of technology and regularly adopt new features and updates, even if this requires more frequent upgrades.

Key Differences Between LTS and Interim Versions:

- **Support Duration** – LTS versions receive support for 18 months, while interim versions are supported for 6 months.
- **Stability vs. Innovation** – LTS focuses on stability and security with minimal feature changes, whereas regular versions emphasize innovation, introducing new features more frequently.
- **Upgrade Frequency** – Customers using LTS versions upgrade less often, while those on regular versions may need to upgrade more frequently to stay up to date.

Why Choose LTS?

LTS versions are perfect for mission-critical systems or environments where downtime is costly. They offer peace of mind by ensuring the version remains stable and supported for the long term.

Why Choose Interim Versions?

If you value having the latest features and improvements, regular versions are more suitable. While they might require more frequent updates, they provide access to the newest capabilities.

Troubleshooting Tenable Identity Exposure

The following topics assist you with issues that may arise when using Tenable Identity Exposure (formerly known as Tenable.ad):

- SYSVOL Hardening Interference with Tenable Identity Exposure
- System Utility (handle.exe)

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.

Requirements to use the diagnostics tool

- The target must accept WMI requests.
- The target must allow execution of the `Invoke-Command` cmdlet.
- The target must recognize the currently connected user (the one launching the script) as an elevated user.
- The Diagnostic Tool must run on all nodes of the Tenable Identity Exposure architecture.

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:

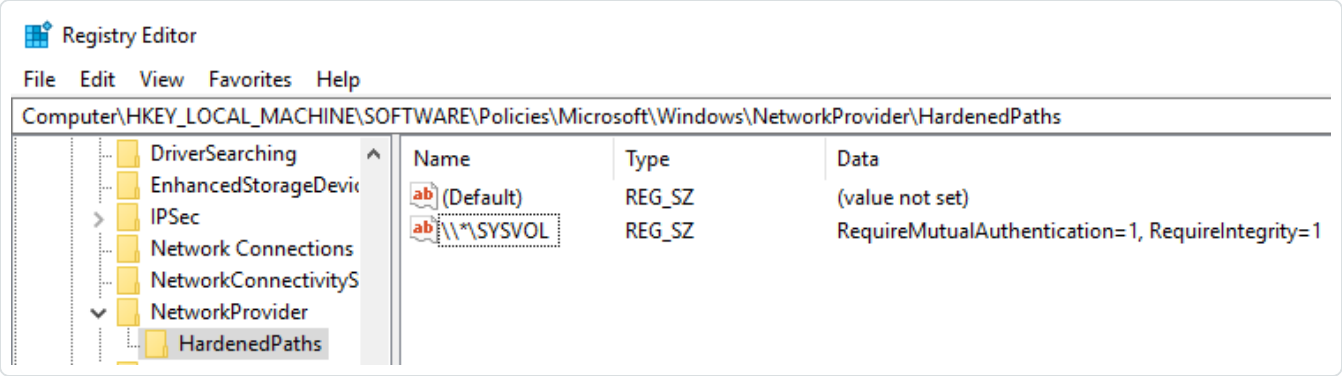
- SaaS with VPN

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.

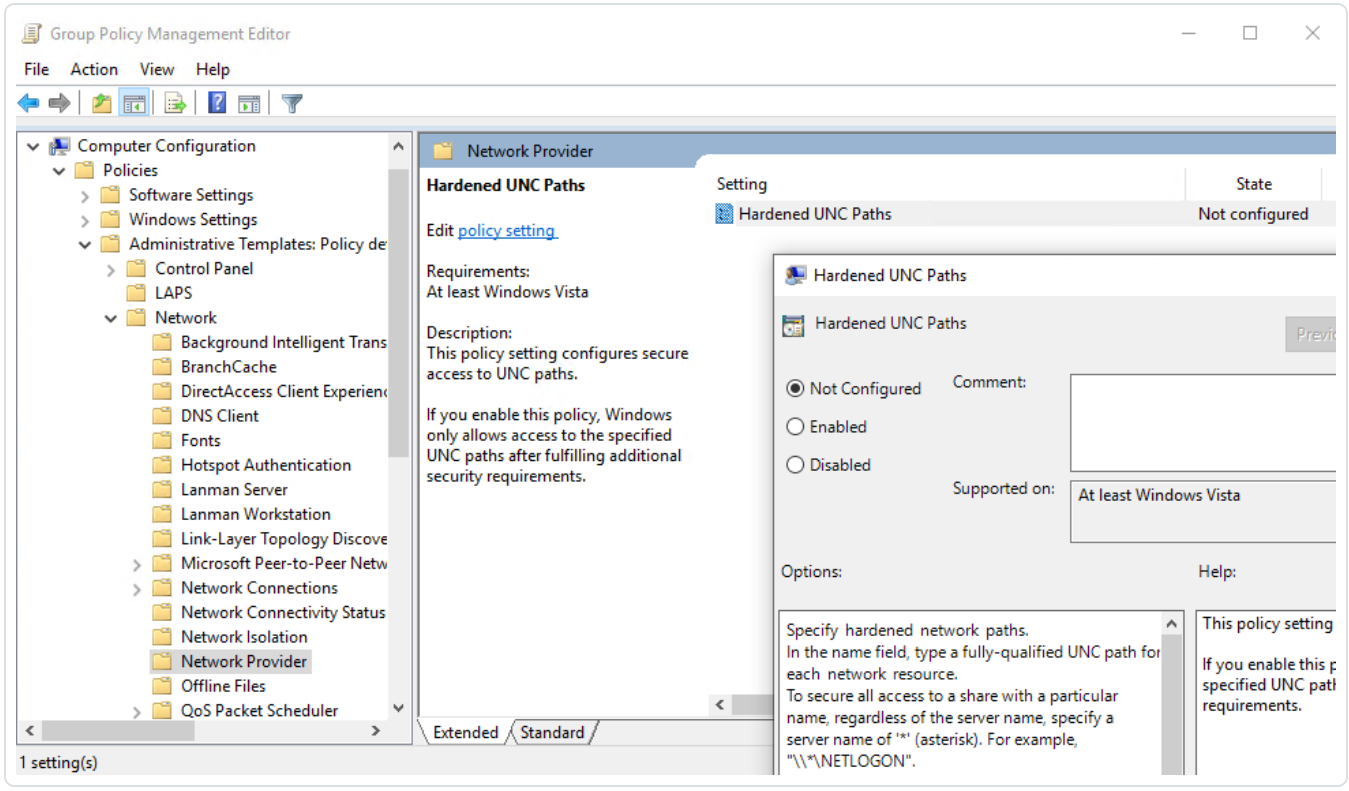
Some organizations also want to ensure the activation of this parameter and enforce it by using the related GPO setting or by setting the corresponding registry key directly.

- You can find the registry keys related to UNC hardened paths under "`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetworkProvider\HardenedPaths`":



- You can find the corresponding GPO setting under "`Computer Configuration/Administrative Templates/Network/Network Provider/Hardened`

`UNC paths`":



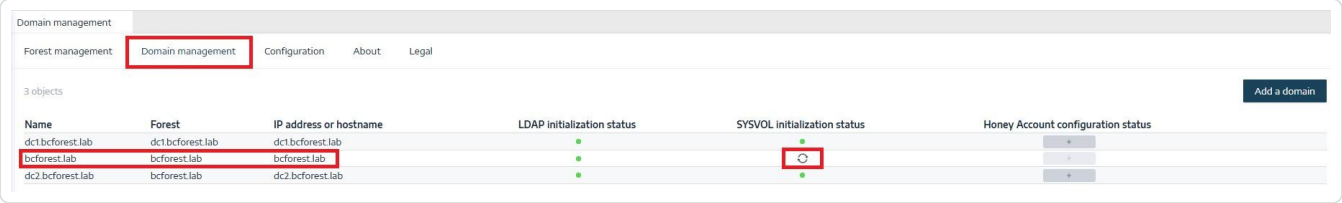
SYSVOL hardening enforcement occurs when a UNC path referring to SYSVOL - for example "`\\*\SYSVOL`" - has the parameters "`RequireMutualAuthentication`" and "`RequireIntegrity`" set to the value "`1`".

Signs of SYSVOL Hardening Issues

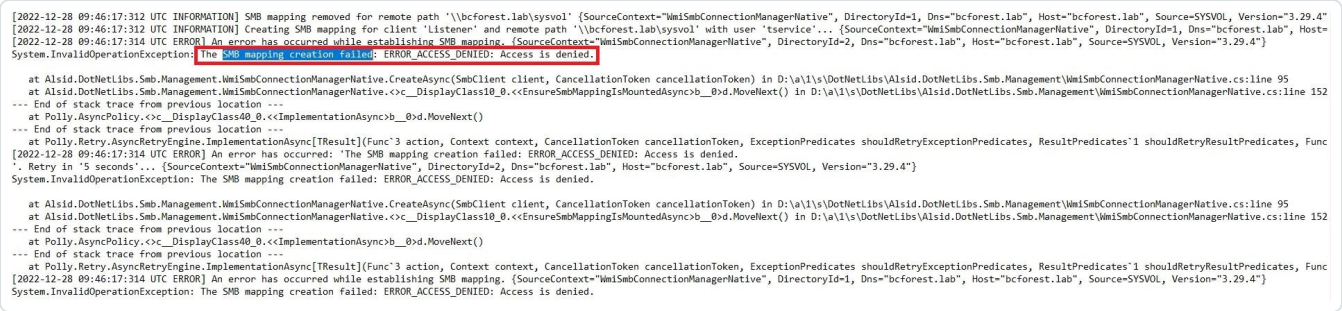
When you suspect that SYSVOL hardening interferes with Tenable Identity Exposure, check for the following:

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.



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.



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:

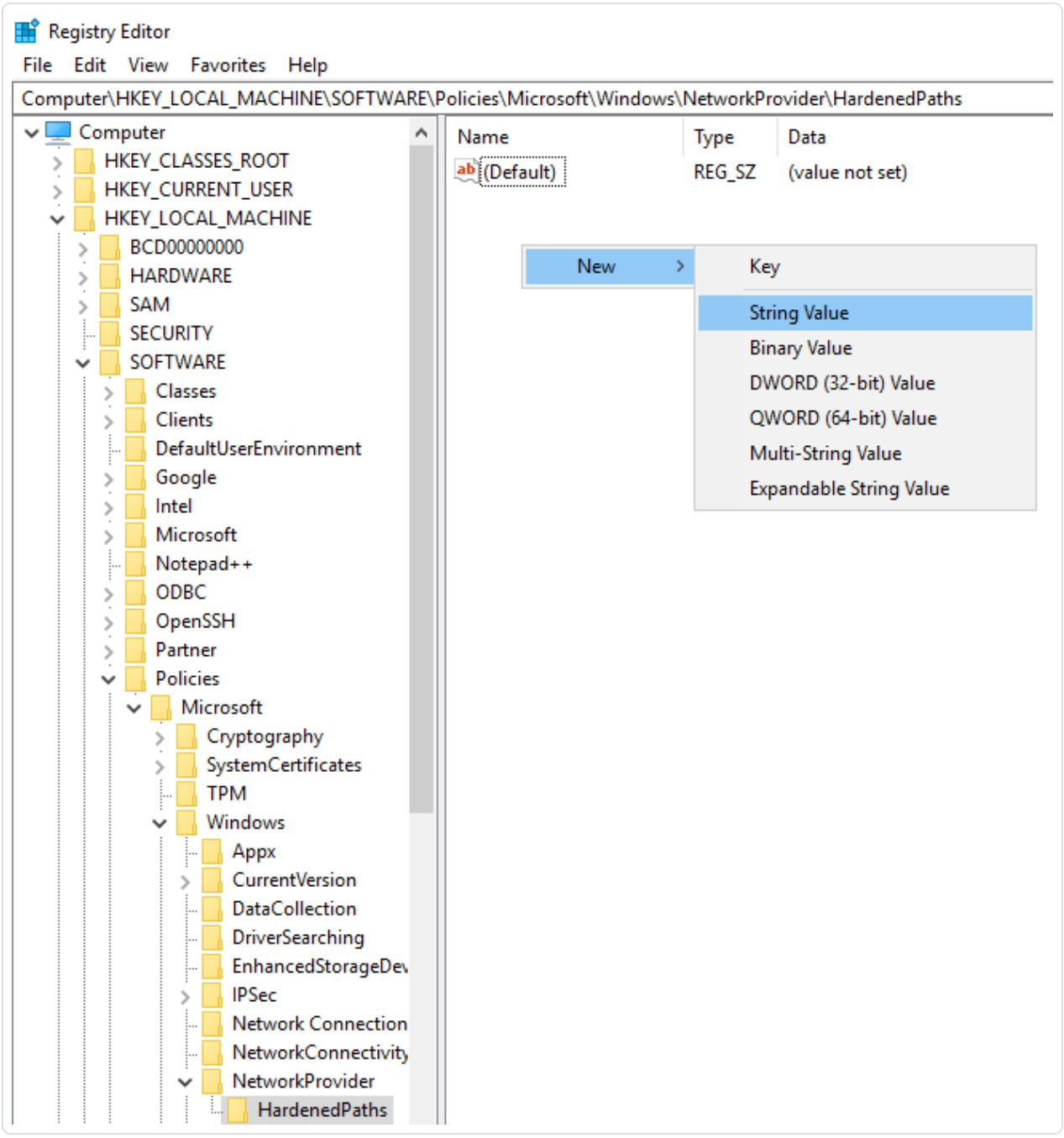


Registry – GUI

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**.

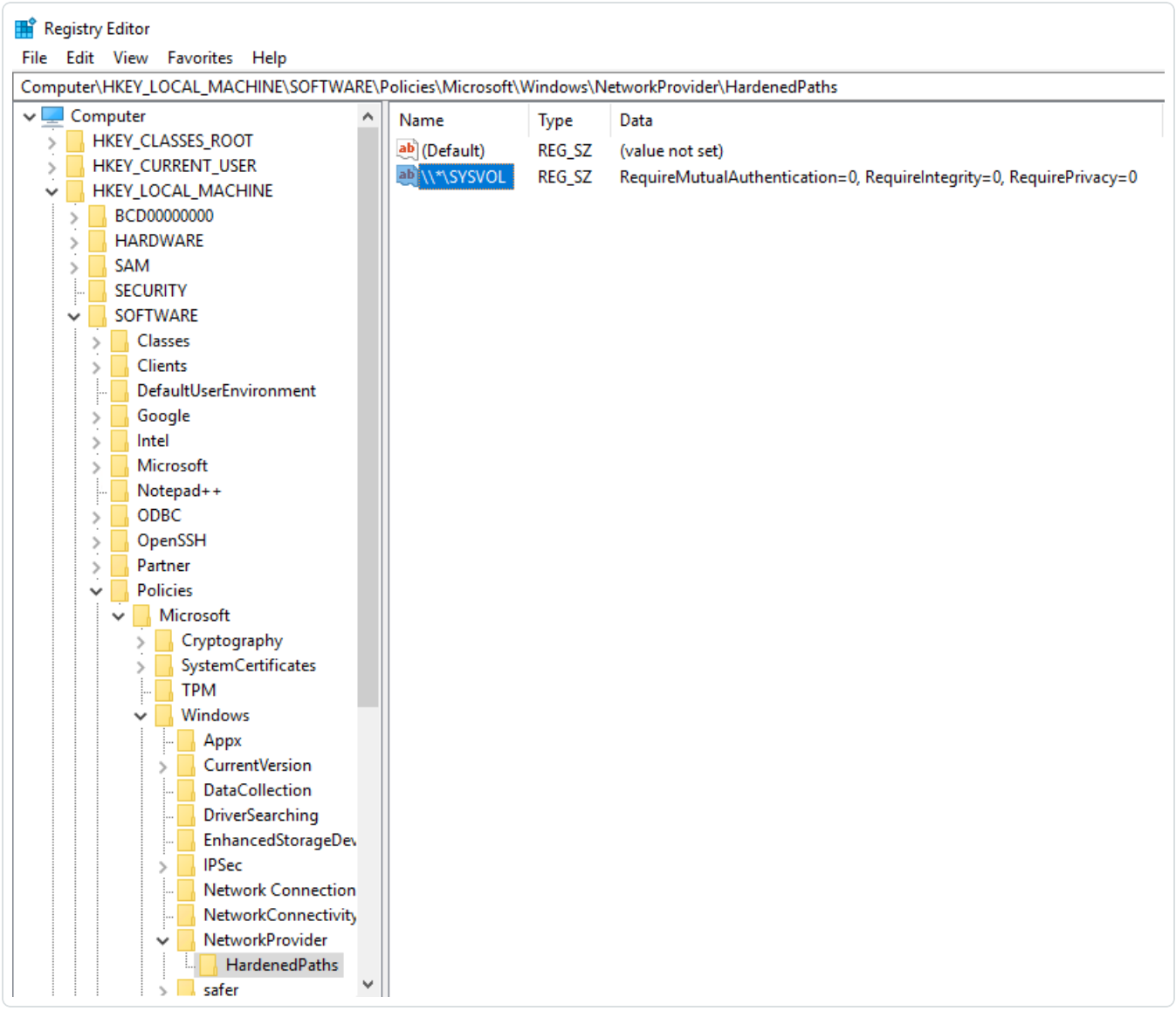


b. In the Name field, enter `\\*\SYSVOL`.

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:



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.

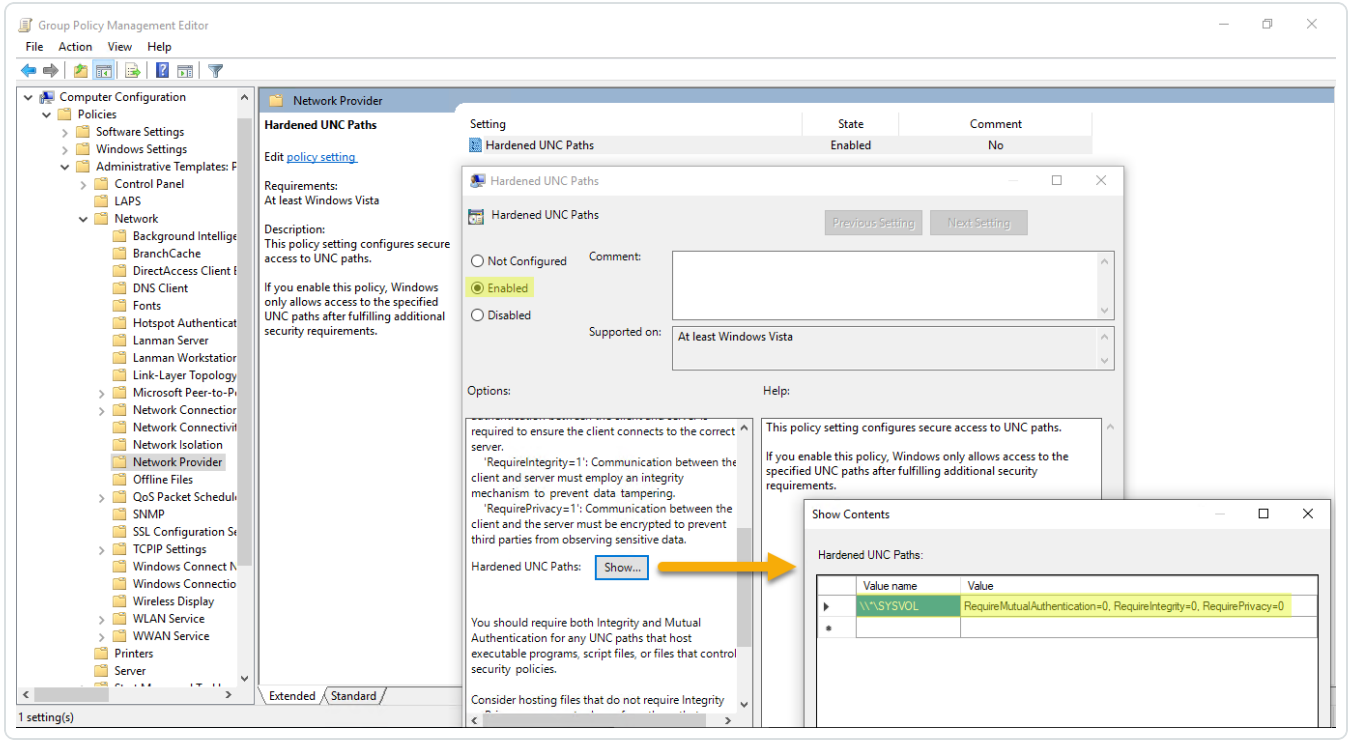
GPO

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:

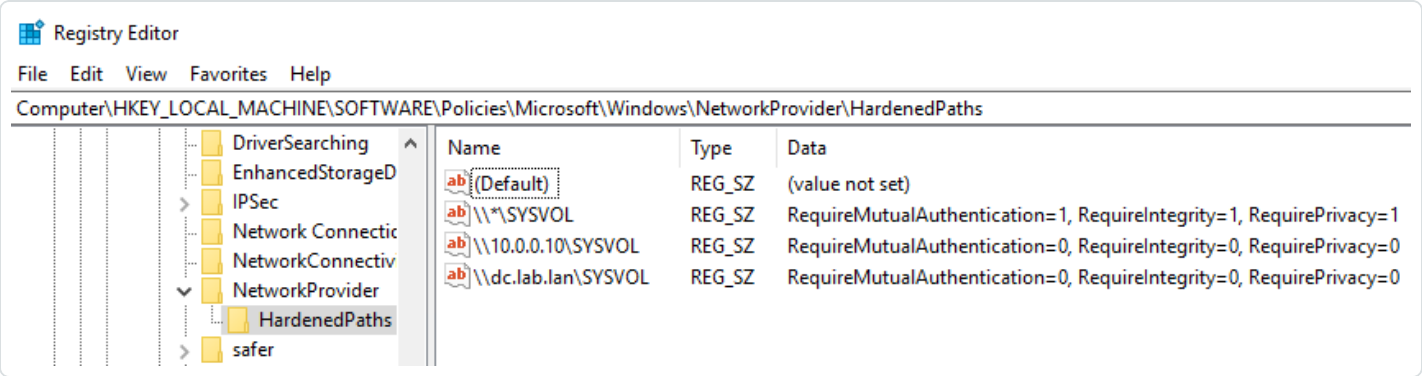


5. Click **OK** to confirm.
6. Link this GPO to the Organizational Unit that contains theTenable Identity Exposure Directory Listener or Relay machine. You can also use the security group filters GPO feature to ensure that this GPO applies only to this machine.

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:



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 Exposuredoes 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.

System Utility (handle.exe)

`Handle.exe` is a legitimate Windows process that Tenable Identity Exposure uses for detailed information about system resource usage, specifically open handles for any sytem processes. For more information, see the Microsoft documentation.

Make sure your antivirus software does not block it.

Manage Tenable Identity Exposure

Using its web portal, Tenable Identity Exposure allows you to review, manage, and receive relevant information about the security state of the monitored infrastructure. The web portal displays the following:

- Live Active Directory security flows to allow security teams to perform security compliance tasks, threat hunting, or incident response tasks.
- Administrative panes to manage the monitoring of new infrastructures.
- Access rights of each user or service connected to the platform.

Tenable Identity Exposure can also forward its security monitoring flows to other services such as internal application logs for further correlation.

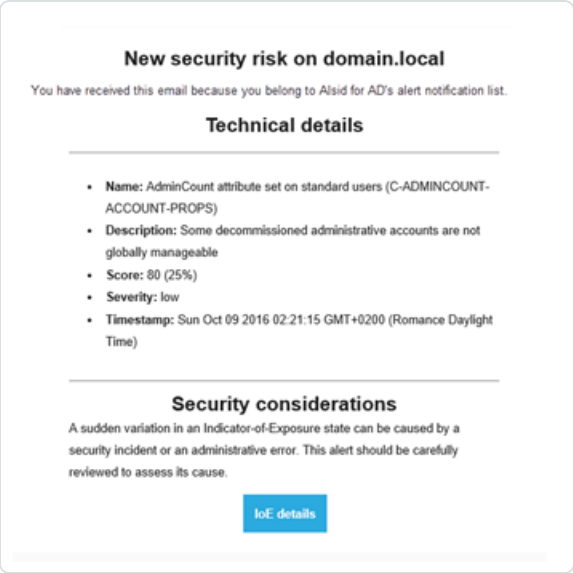
Alerts and Notifications

Tenable Identity Exposure includes notifications and alerts that you can connect to third-party services, such as an event log collector (for example, a Security Information and Event Management), an email service provider using SMTP, or a ticketing system. When a new security incident appears, Tenable Identity Exposure raises notifications to inform security teams to take immediate action.

Tenable Identity Exposure uses email notifications to send general purpose information to users, such as password recovery information, as well as notifications about security incidents.

To enable alerts, provide Tenable Identity Exposure with credentials for a user account with permissions to send emails to the selected SMTP server. This can be the same user account as the one you use to connect to your Active Directory.

The following is a generic email template for a security incident detected by Tenable:



Tenable REST v3 API

You can integrate Tenable Identity Exposure into a security ecosystem using its RESTv3 (Representational State Transfer) API to enable management, logging. or notification capabilities.

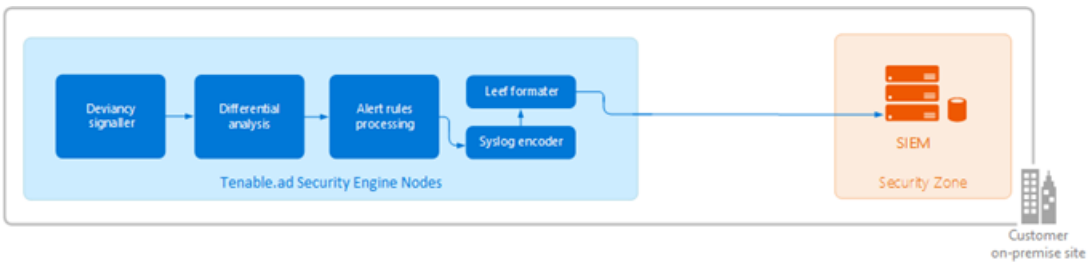
Tenable Identity Exposure provides a public API that you can use to connect the platform to third-party services. This API supports the REST v3 standard which you access using HTTP.

For more information, see the Tenable Identity Exposure API Reference Portal.

Connect to an Event Log Collector

You can configure Tenable Identity Exposure to send notifications, such as alerts or security offenses, to an event log collector. Tenable Identity Exposure also allows you to redirect a subset of the traffic flows to a collector for further correlation.

The following illustration shows an integrated process managing Security Information and Event Management (SIEM) events.



Tenable Identity Exposure uses the Syslog protocol to carry messages in LEEF format.

Tenable Identity Exposure supports most SIEMs or event log collectors. Tenable Identity Exposure supports the following event collectors:

- IBM QRadar
- Splunk
- RSA Netwitness
- LogRhythm
- Micro Focus ArcSight
- Tibco Loglogic
- McAfee Enterprise Security Manager

Scale Tenable Identity Exposure Services

Required User Role: Administrator on the local machine

To improve data processing performance, you can scale up or down these Tenable Identity Exposure services.

Cancri

Cancri is the service in charge of translating and decoding the raw data it receives.

Cancri's scaling up mechanism goes through its reconfiguration using an environment variable.

To scale Cancri:

1. Open a PowerShell (x64) terminal.
2. Define the environment variable `TENABLE_CASSIOPEIA_CANCRI_Application__MaxConcurrentPublishToEridanis`:

Note: The default value is 100.

```
[Environment]::SetEnvironmentVariable("ALSID_CASSIOPEIA_CANCRI_Application__
MaxConcurrentPublishToEridanis", "IntegerValue", "Machine")
```

3. Restart Cancri:

```
Restart-Service -Name Alsid_Cancri
```

Example:

```
[[Environment]::SetEnvironmentVariable("ALSID_CASSIOPEIA_CANCRI_Application__
MaxConcurrentPublishToEridanis", "200", "Machine")
Restart-Service -Name Alsid_Cancri
```

Cygni

The Cygni service analyzes changes in AD objects to identify potential risks. If these changes collectively meet deviance criteria, it transmits the deviance to the database and it becomes visible in Tenable Identity Exposure.

If your security requirements do not align with the default settings of the Tenable security profile, you can deactivate it to enhance performance by circumventing the computation associated with this profile. Alternatively, you can create a new profile by duplicating the Tenable security profile and customizing it to your specific needs. This allows you to create a personalized profile aligned with your own security standards based on Tenable recommendations. You can then deactivate the default Tenable profile, ensuring that your system adheres to your security requirements.

Note: Disabling analysis on this profile pauses the results.

To disable IoE analysis on the Tenable security profile:

1. On the Security Engine Node machine, open a PowerShell (x64) terminal.
2. Run the following command:

```
[Environment]::SetEnvironmentVariable("ALSID_CASSIOPEIA_CYGNI_Application__IOE__
IgnoreDefaultProfile", "true", [System.EnvironmentVariableTarget]::Machine)
```

3. Restart the Cygni service:

```
Restart-Service -Name 'alsid_Cygni'
```

Eridanis

Eridanis is the API service that stores the business data (configuration and AD objects, deviances, etc.) in the MSSQL Server and forwards it to other services.

To scale up the total number of Eridanis instances, you must update the `ERIDANIS_WORKER_COUNT` environment variable.

To scale Eridanis:

1. Open a PowerShell (x64) terminal.
2. Run the following command (replace the value in brackets with the real expected value):

```
[System.Environment]::SetEnvironmentVariable('ERIDANIS_WORKER_COUNT', <number of Eridanis
instances>, 'Machine')
```

3. Restart Eridanis:

```
Restart-Service -Name 'alsid_Eridanis'
```

Example: For 3 Instances of Eridanis

```
[System.Environment]::SetEnvironmentVariable('ERIDANIS_WORKER_COUNT', 3, 'Machine')
Restart-Service -Name 'alsid_Eridanis' -Force
```

EventLogsDecoder

The `EventLogsDecoder` component needs to process data at a high speed. It's possible that a single instance of `EventLogsDecoder` may not suffice, so consider running multiple instances of this component concurrently.

To determine when to initiate additional instances, you monitor a specific metric, which is the number of messages queued in the RabbitMQ queue named `event-logs-decoder-ioa-input-queue`. When this metric reaches a threshold of 8000 messages, it's imperative to launch a new instance of the EventLogsDecoder component.

To scale a new instance of EventLogsDecoder on a new machine, launch the installation program on this machine and follow the same procedure as the one you used for the first instance:

- Default TLS
- Default TLS in "Expert Mode"
- TLS without Peer Verification
- TLS with Peer Verification
- No TLS

You do not need to restart any service because Tenable Identity Exposure automatically takes in account this new instance.

> **Note**: It is not possible to add several instances of `EventLogsDecoder` on the same machine.

Change IP Addresses or FQDNs for Tenable Identity Exposure Nodes

Changing the IP addresses or fully qualified domain names (FQDNs) of machines running the Storage Manager (SM), Security Engine Nodes (SEN), and Directory Listener (DL) is a required task in certain situations, such as disaster recovery testing. Using scripts to modify environment variables with the new IPs or FQDNs and to restart services is the most efficient way to perform this operation which also minimizes downtime.

To change the IP addresses or FQDN for Tenable Identity Exposure nodes:

1. If your Tenable Identity Exposure installation type uses:
    - **Default TLS**: Generate and replace all self-signed TLS certificates with the new IP addresses or FQDNs.
    - **Custom TLS**: Generate and replace all custom TLS certificates with the new IP addresses or FQDNs.
    - **No TLS**: Proceed to the next step.
2. In PowerShell, list all the IP/FQDN-related environment variables with the new IPs or FQDNs, such as in the following example:

    Note: The following scripts only show the environment variables that you would need to update in a conventional setup of Tenable Identity Exposure. It excludes any setup using split SENs or multiple DLs.

    - Security Engine Node (SEN):

    Update environment variables with new IPs or FQDNs for SEN

```
# Script to run on the Security Engine Node Server
$vars = @{
    ERIDANIS_MSSQL_HOST = ""  # Storage Manager Server IP Address
    ALSID_CASSIOPEIA_EVENT_LOGS_DECODER_Service__EventLogsStorage__Host = ""  #
Storage Manager Server IP Address
    ALSID_CASSIOPEIA_CYGNI_Service__EventLogsStorage__Host = ""  # Storage Manager
Server IP Address
    HEALTHCHECK_MSSQL_HOST = ""  # Storage Manager Server IP Address
}

# Prompt the user once for the value to set all environment variables to
$value = Read-Host "Please enter the value for Storage Manager IP Address"
Write-Output "You have entered: $value"

# Use a temporary hashtable to store updated values
$tempVars = @{}

# Populate the temporary hashtable with the same value for all keys
ForEach ($key in $vars.Keys) {
    $tempVars[$key] = $value
}

# Update the original hashtable with values from the temporary hashtable
ForEach ($key in $tempVars.Keys) {
    $vars[$key] = $tempVars[$key]
}


# Set environment variables
```

```
ForEach ($var in $vars.GetEnumerator()) {
    [System.Environment]::SetEnvironmentVariable($var.Name, $var.Value, 'Machine')
    Write-Output "Environment variable set: $($var.Name) = $($var.Value)"
}

# Restart all services
Get-Service alsid* | Restart-Service
Get-Service tenable* | Restart-Service
```

- Directory Listener (DL):

Update environment variables with new IPs or FQDNs for DL

```
# To run on the Directory Listener Server
$vars = @{
    ALSID_CASSIOPEIA_CETI_Service__Broker__Host = ""  # Directory Listener Server
IP Address
}

# Prompt the user once for the value to set all environment variables to
$value = Read-Host "Please enter the value for Security Engine Node Server IP
Address"
Write-Output "You have entered: $value"

# Use a temporary hashtable to store updated values
$tempVars = @{}

# Populate the temporary hashtable with the same value for all keys
ForEach ($key in $vars.Keys) {
    $tempVars[$key] = $value
}

# Update the original hashtable with values from the temporary hashtable
ForEach ($key in $tempVars.Keys) {
    $vars[$key] = $tempVars[$key]
}

# Set environment variables
ForEach ($var in $vars.GetEnumerator()) {
    [System.Environment]::SetEnvironmentVariable($var.Name, $var.Value, 'Machine')
    Write-Output "Environment variable set: $($var.Name) = $($var.Value)"
}

# Restart all services
Get-Service alsid* | Restart-Service
Get-Service tenable* | Restart-Service
```

HTTPS for Tenable Identity Exposure Web Application

When the Tenable Identity Exposure installation process installs the Security Engine Node (SEN), it creates a self-signed certificate and binds it to the Tenable Identity Exposure web application to let you access Tenable Identity Exposure via HTTPS.

For example, if the SEN server's IP address is `10.0.48.55`, you can log in to the Tenable Identity Exposure web application at `https://10.0.48.55` after installation.

Tenable Identity Exposure provides a default self-signed certificate for your convenience. But to secure fully the web application, you must change this IIS certificate for a valid one, such as a signed certificate from the organization's PKI/internal Certificate Authority.

Moreover, the SSL/TLS protocols versions and their enabled cipher suites have globally configured settings in the underlying Windows operating system (OS). Tenable Identity Exposure does not modify these settings, so you must configure them to obtain the desired level of security in line with your organization's requirements.

In the absence of specific requirements and within a modern environment, Tenable recommends that you enable TLS 1.2. You can enable TLS 1.3 if you use Windows Server 2022 with the compatible Tenable Identity Exposure version. You should also disable weak cipher suites (DES, 3DES, RC2, RC4, AES 128, etc.)

Refer to the Microsoft documentation to Restrict the use of certain cryptographic algorithms and protocols in Schannel.dll. Use the configuration method that your organization recommends to deploy those settings (for example local configuration, GPO, third-party tool, etc.) However, Tenable does not offer support around this.

For more information, see:

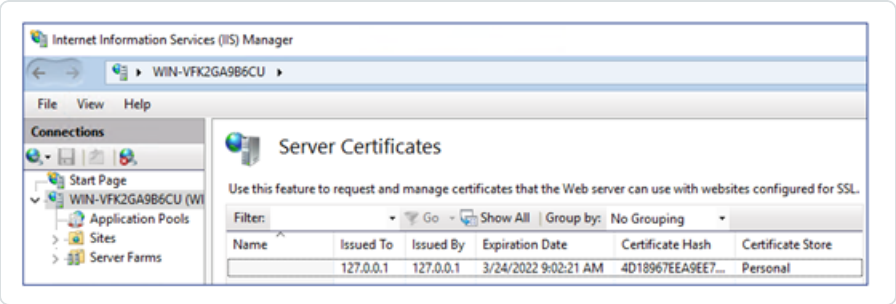
- View the IIS Certificate
- Change the IIS Certificate

View the IIS Certificate

The Tenable Identity Exposure installation process creates and places a self-signed certificate in Internet Information Services (IIS) Manager.

To view the IIS certificate:

1. Go to **Windows Start** > **Windows Administrative Tools** > **Internet Information Services (IIS) Manager**.
2. In the **Connections** panel on the left, click on the server name.
3. Double-click on **Server Certificates** to display certificates in the IIS Manager.

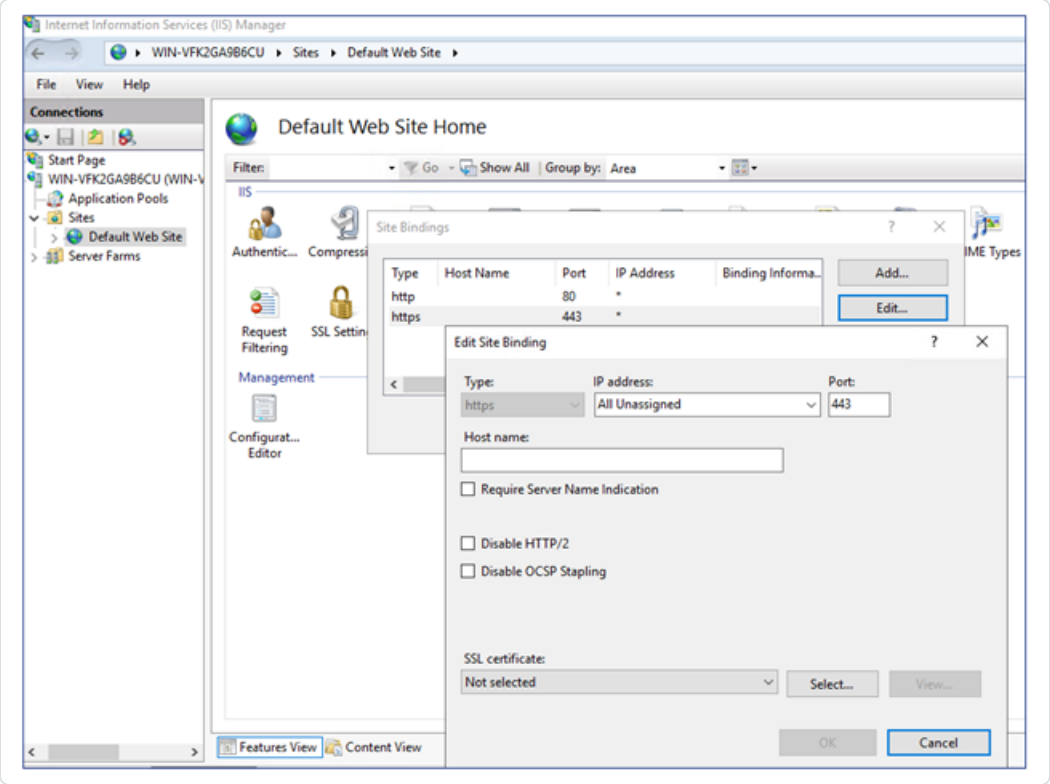


> **Note**: By default, the installation process creates the self-signed certificate and the IIS site binding by using HTTPS port 443.

4. To explore the binding, expand **Sites** on the left panel.
5. Right-click your website and choose **Edit Bindings**.

   The **Site Bindings** window appears.
6. Select the **https** binding.
7. Click **Edit**.

   The **Edit Site Binding** window appears.



8. Under SSL Certificates, click on the drop-down menu to view installed certificates.

Change the IIS Certificate

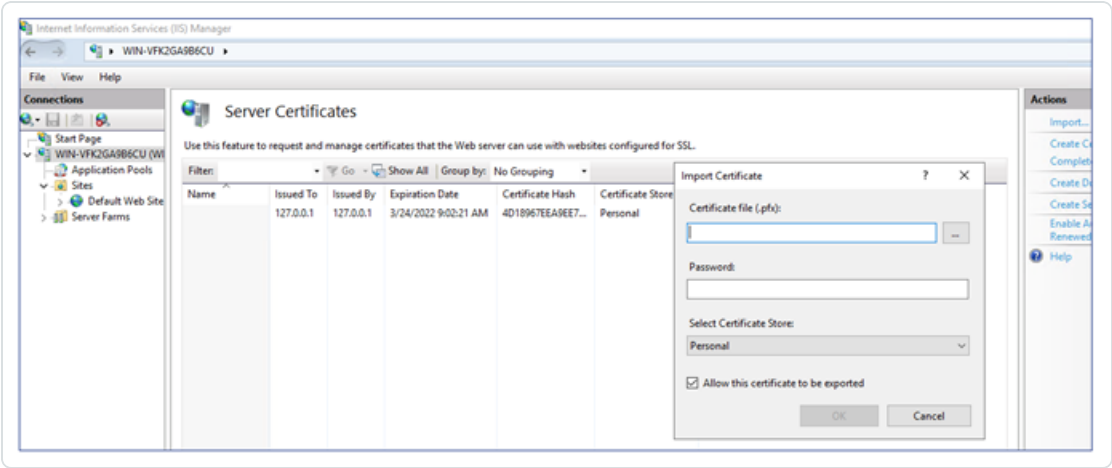
To use your certificate for the Tenable Identity Exposure web application, you must:

1. Install your certificate in IIS.
2. Edit site binding to use your installed certificate.

To install the IIS certificate:

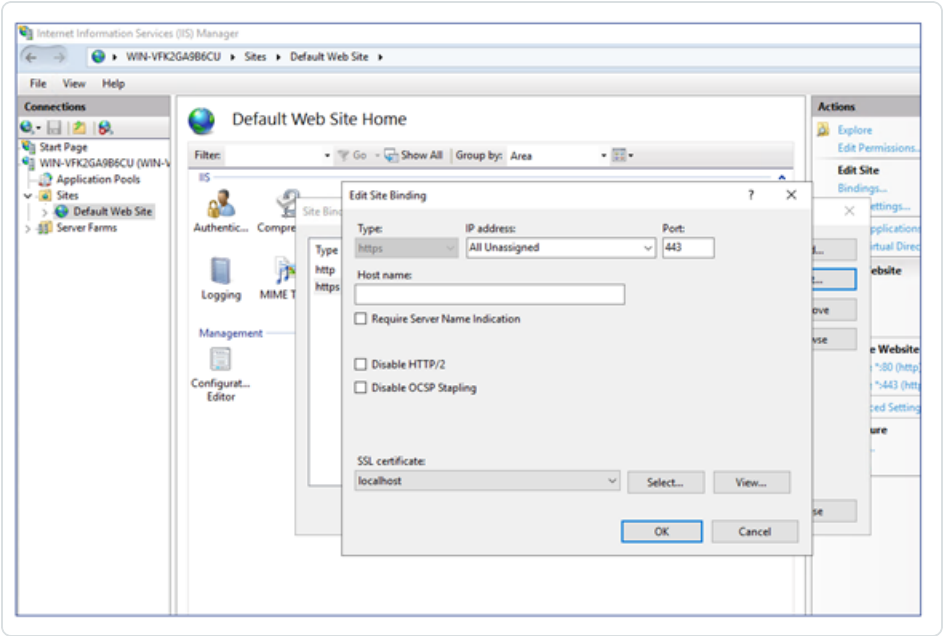
1. Go to **Windows Start** > **Windows Administrative Tools** > **Internet Information Services (IIS) Manager**.
2. In the **Connections** panel on the left, click on the server name.
3. Double-click on **Server Certificates** to display certificates in the IIS Manager.

4. In the right panel, click **Import** to import your certificate.



To change the IIS certificate:

1. View the IIS Certificate.
2. From the drop-down list of SSL certificates, select the certificate you just installed.
3. Click **OK**.



4. Right-click on the website in the **Connections** panel and select **Manage Website** > **Restart** for

the new certificate to take effect.



Upgrade and Maintenance

As part of its upgrade program, Tenable frequently publishes updates to provide new detection capabilities and new features.

- These upgrades include security patches for the underlying operating system. See the latest Tenable Identity Exposure Release Notes for more information.
- You can access them on Tenable Downloads site.

To upgrade Tenable Identity Exposure, deploy the installation packages on each Windows Server machine. For more information about the upgrade process, see Upgrade Tenable Identity Exposure.

Maintenance and Support Services

To keep servers in good security conditions the Tenable Identity Exposure platform requires access to the following support services.

During maintenance operations, Tenable Support requires administrative access to the operating systems that host Tenable Identity Exposure.

Service Name	Description
Update management	Your company's update management infrastructure (e.g., WSUS or SCCM) or Microsoft update servers on the Internet. This service applies security

infrastructure	patches on the underlying operating system.
Time Server	Your company's time server (e.g., NTP server). This service synchronizes Tenable Identity Exposure's platform internal clock to your reference time. Time synchronization offers consistent security monitoring.
Identity provider	Your identity and access provider. This service activates SAML, LDAP, or OAUTH authentication to Tenable Identity Exposure's web services (portal, API, etc.).

Uninstall Tenable Identity Exposure

Required User Role: Administrator on the local machine

The uninstallation process removes all Tenable Identity Exposure components.

To uninstall Tenable Identity Exposure:

1. In Windows, go to **Control Panel** > **Programs** > **Programs and Features**.
2. Select Tenable Identity Exposure.
3. Click **Uninstall**. A dialog box asks for confirmation:
4. Click **Yes**.
    - The confirmation dialog box disappears after the uninstallation completes.
    - An icon in the system tray indicates that a second uninstallation phase is in progress and disappears when this phase has fully completed.
    - A PowerShell pop up tray indicates that a final uninstallation phase is in progress and disappears when this phase has fully completed.