Tenable Identity Exposure Best Practices Guide

Last Revised: September 26, 2025

Table of Contents

Welcome to Tenable Identity Exposure Best Practices Guide

Last updated: September 26, 2025

Tenable Identity Exposure provides real-time security monitoring for Microsoft Active Directory (AD) infrastructures. By leveraging a non-intrusive approach based on the AD replication process, Tenable empowers security teams in their audit, threat hunting, detection, and incident response tasks.

About this Guide

This guide serves as a comprehensive guide to best practices, designed to elevate user experience through tailored guidance, recommendations, and proven methodologies. It covers a range of topics, including pre- and post-deployment considerations, pre- and post-upgrade strategies, and optimal practices for enhancing user experience.

It is based on the **Tenable Identity Exposure On-Premises User Guide** and gives the following information:

- The technical requirements to deploy and operate Tenable Identity Exposure as an on-premises platform that is disconnected from the Internet.
- The environment specifications from a network and application perspective.
- The tasks to perform before enabling security monitoring.

For a successful deployment of your platform, follow the Get Started with Tenable Identity Exposure 3.77 On-Premises.

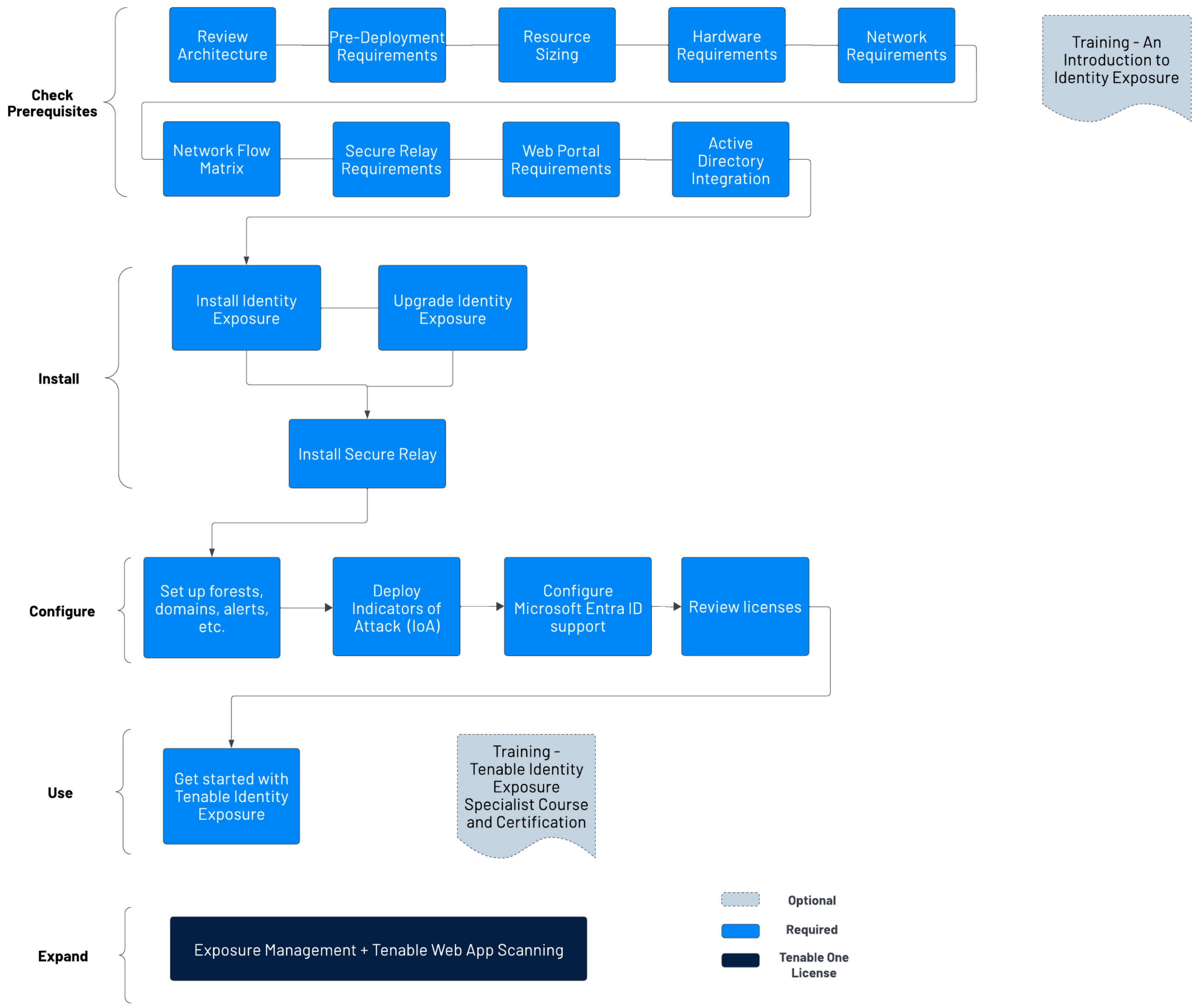
For complete information about installation and upgrade, see the Tenable Identity Exposure On-Premises Installation Guide for 3.59.

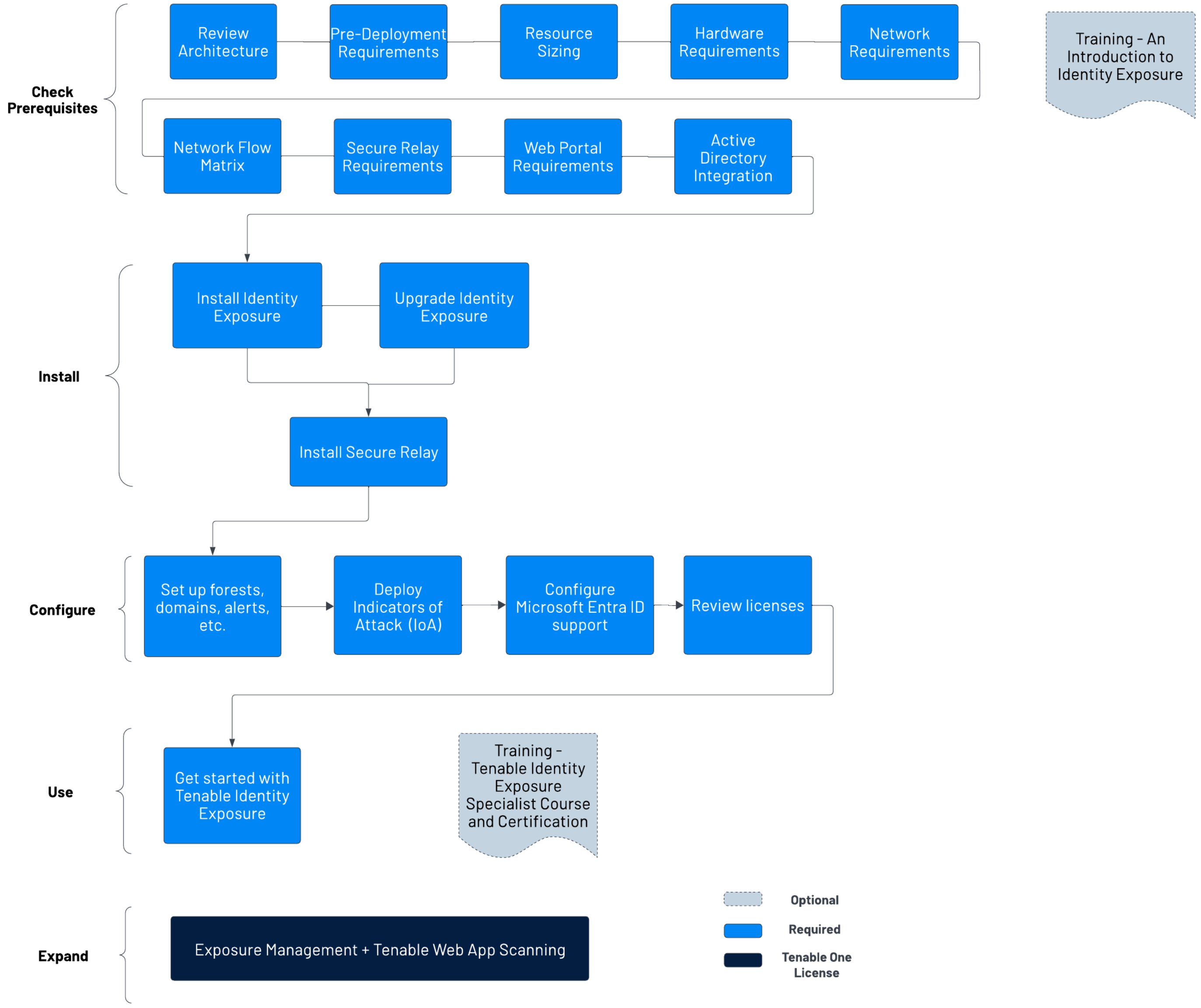
Migration

Chart a smooth course to success with **Tenable's Professional Services** by your side. We'll meticulously map your needs to the perfect solution and ensure a stress-free journey from start to finish. Trust in our friendly guidance and experience the power of seamless migration. Ready to navigate with expert guidance? Get a free scoping call and quote today from Tenable.

Get Started with Tenable Identity Exposure 3.77 On-Premises

Use the following workflow to perform your deployment of Tenable Identity Exposure 3.77.


Check Prerequisites
Review Architecture
Pre-Deployment Requirements
Resource Sizing
Hardware Requirements
Network Requirements
Training - An Introduction to Identity Exposure
Network Flow Matrix
Secure Relay Requirements
Web Portal Requirements
Active Directory Integration
Install
Install Identity Exposure
Upgrade Identity Exposure
Install Secure Relay
Configure
Set up forests, domains, alerts, etc.
Deploy Indicators of Attack (IoA)
Configure Microsoft Entra ID support
Review licenses
Use
Get started with Tenable Identity Exposure
Training - Tenable Identity Exposure Specialist Course and Certification
Expand
Exposure Management + Tenable Web App Scanning
Optional
Required
Tenable One License



Check Prerequisites

Review Architecture

Pre-Deployment Requirements

Resource Sizing

Hardware Requirements

Network Requirements

Network Flow Matrix

Secure Relay Requirements

Web Portal Requirements

Active Directory Integration

Training - An Introduction to Identity Exposure

Install

Install Identity Exposure

Upgrade Identity Exposure

Install Secure Relay

Configure

Set up forests, domains, alerts, etc.

Deploy Indicators of Attack (IoA)

Configure Microsoft Entra ID support

Review licenses

Use

Get started with Tenable Identity Exposure

Training - Tenable Identity Exposure Specialist Course and Certification

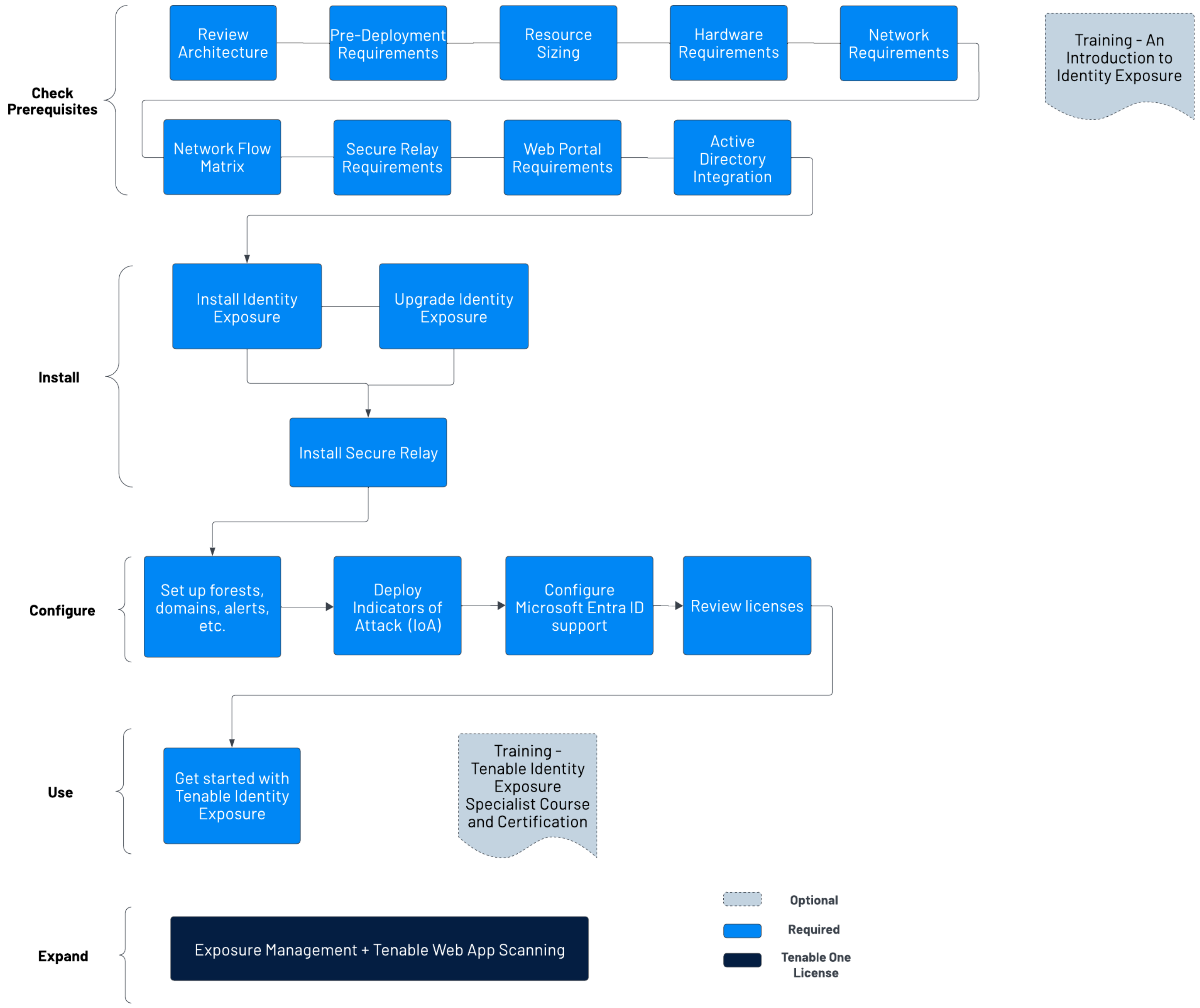
Expand

Exposure Management + Tenable Web App Scanning

▨ Optional

🟦 Required

■ Tenable One License


Check Prerequisites
Review Architecture
Pre-Deployment Requirements
Resource Sizing
Hardware Requirements
Network Requirements
Training - An Introduction to Identity Exposure
Network Flow Matrix
Secure Relay Requirements
Web Portal Requirements
Active Directory Integration
Install
Install Identity Exposure
Upgrade Identity Exposure
Install Secure Relay
Configure
Set up forests, domains, alerts, etc.
Deploy Indicators of Attack (IoA)
Configure Microsoft Entra ID support
Review licenses
Use
Get started with Tenable Identity Exposure
Training - Tenable Identity Exposure Specialist Course and Certification
Expand
Exposure Management + Tenable Web App Scanning
Optional
Required
Tenable One License

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 **3.77**, 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 3.77.

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.

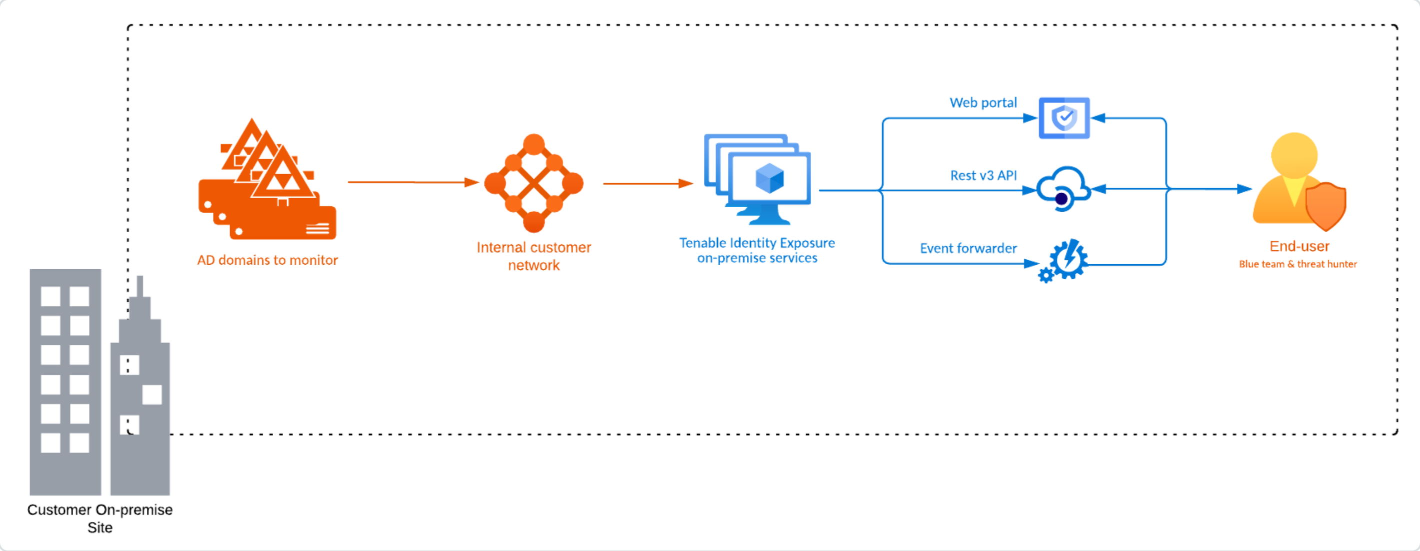
    You can adjust these if needed to ensure you’re viewing the most critical attack path data.

    - 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:


AD domains to monitor
Internal customer network
Tenable Identity Exposure on-premise services
Web portal
Rest v3 API
Event forwarder
End-user
Blue team & threat hunter
Customer On-premise Site

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.

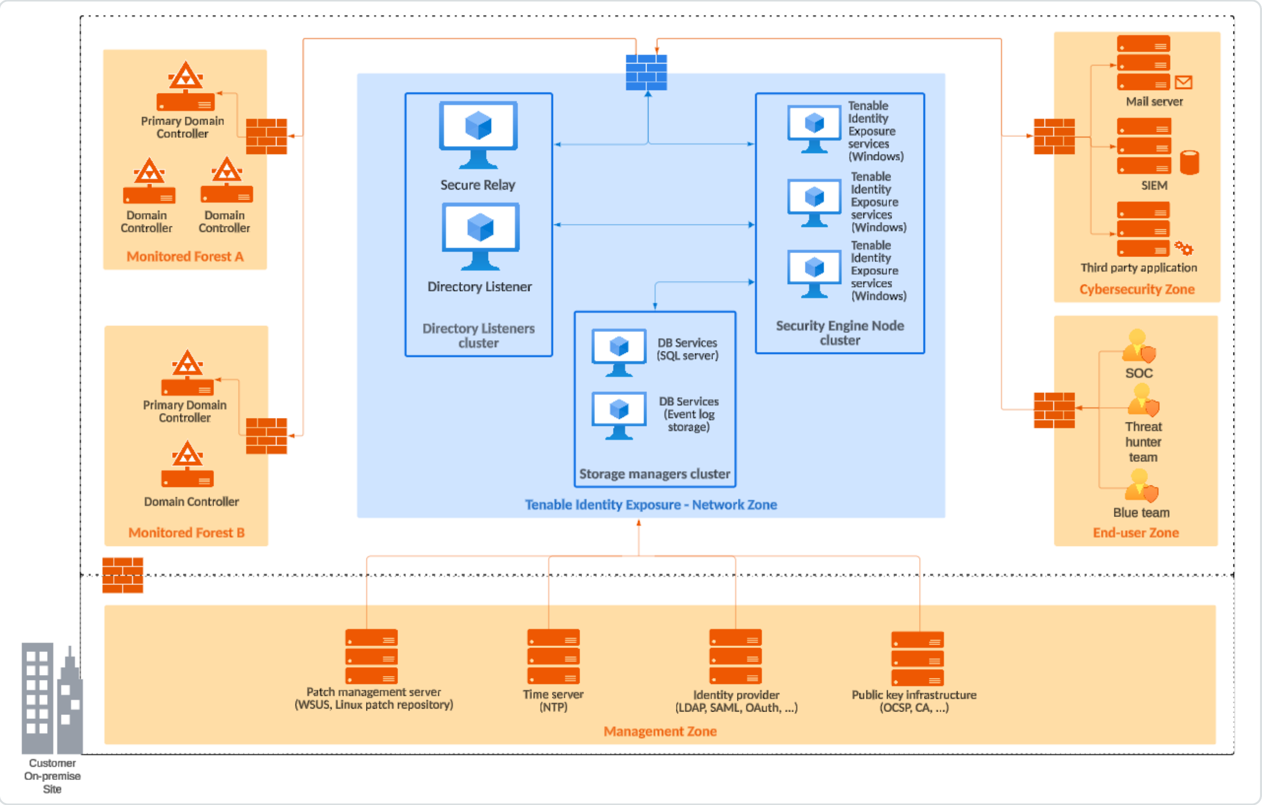
Architectures

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.


Primary Domain Controller
Domain Controller
Domain Controller
Monitored Forest A
Primary Domain Controller
Domain Controller
Monitored Forest B
Secure Relay
Directory Listener
Directory Listeners cluster
Tenable Identity Exposure services (Windows)
Tenable Identity Exposure services (Windows)
Tenable Identity Exposure services (Windows)
Security Engine Node cluster
DB Services (SQL server)
DB Services (Event log storage)
Storage managers cluster
Tenable Identity Exposure - Network Zone
Mail server
SIEM
Third party application
Cybersecurity Zone
SOC
Threat hunter team
Blue team
End-user Zone
Patch management server (WSUS, Linux patch repository)
Time server (NTP)
Identity provider (LDAP, SAML, OAuth, ...)
Public key infrastructure (OCSP, CA, ...)
Management Zone
Customer On-premise Site

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

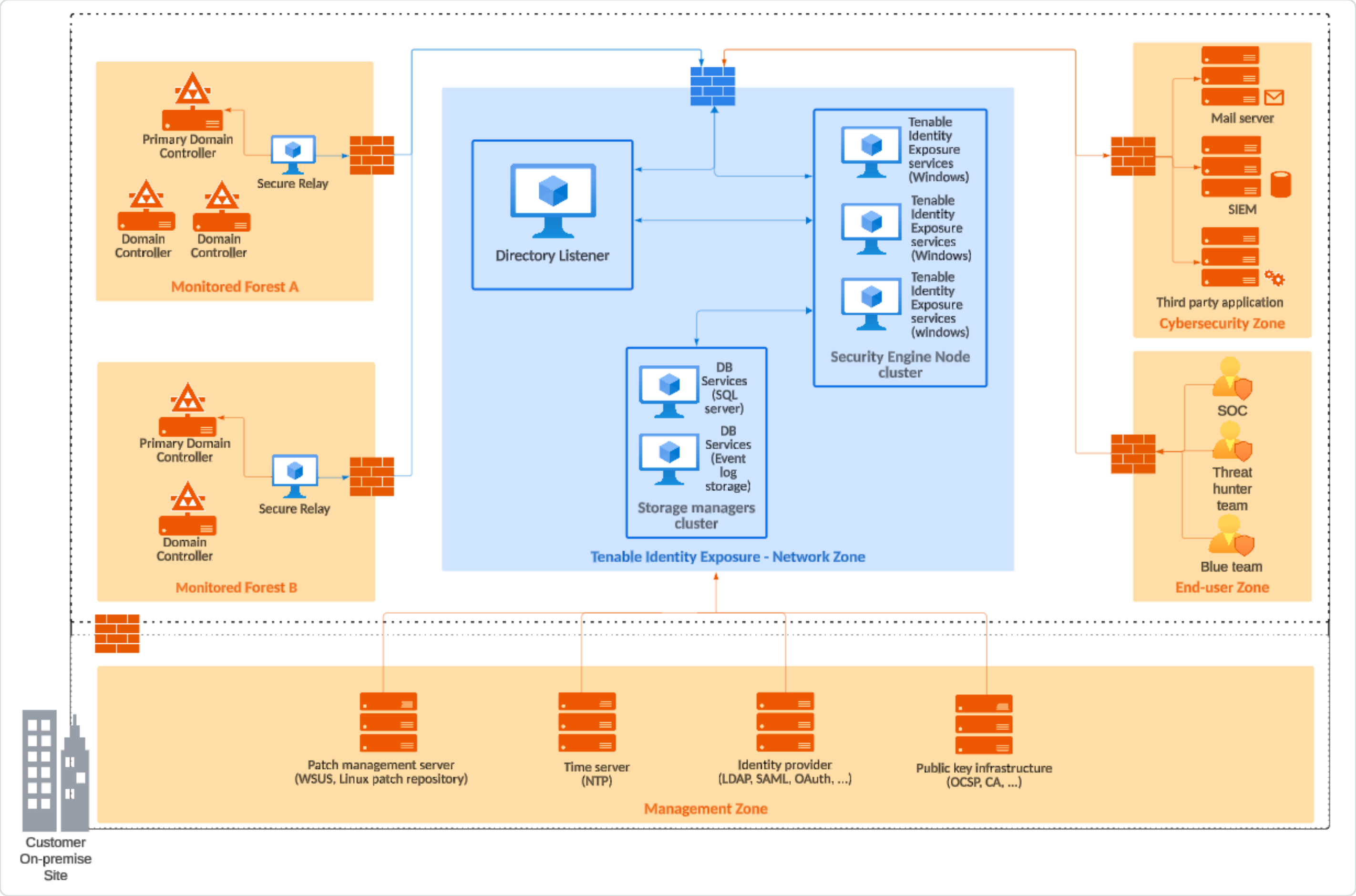
- Each Tenable Identity Exposure service is at the same logical place behind a unique firewall.
- Each service flow (Active Directory, end-users, alerts, etc.) goes through the same network equipment.
- This architecture links new Active Directory domains easily because it does not need service or extra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


Primary Domain Controller
Secure Relay
Domain Controller
Domain Controller
Monitored Forest A
Primary Domain Controller
Secure Relay
Domain Controller
Monitored Forest B
Directory Listener
Tenable Identity Exposure services (Windows)
Tenable Identity Exposure services (Windows)
Tenable Identity Exposure services (windows)
Security Engine Node cluster
DB Services (SQL server)
DB Services (Event log storage)
Storage managers cluster
Tenable Identity Exposure - Network Zone
Mail server
SIEM
Third party application
Cybersecurity Zone
SOC
Threat hunter team
Blue team
End-user Zone
Patch management server (WSUS, Linux patch repository)
Time server (NTP)
Identity provider (LDAP, SAML, OAuth, ...)
Public key infrastructure (OCSP, CA, ...)
Management Zone
Customer On-premise Site

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

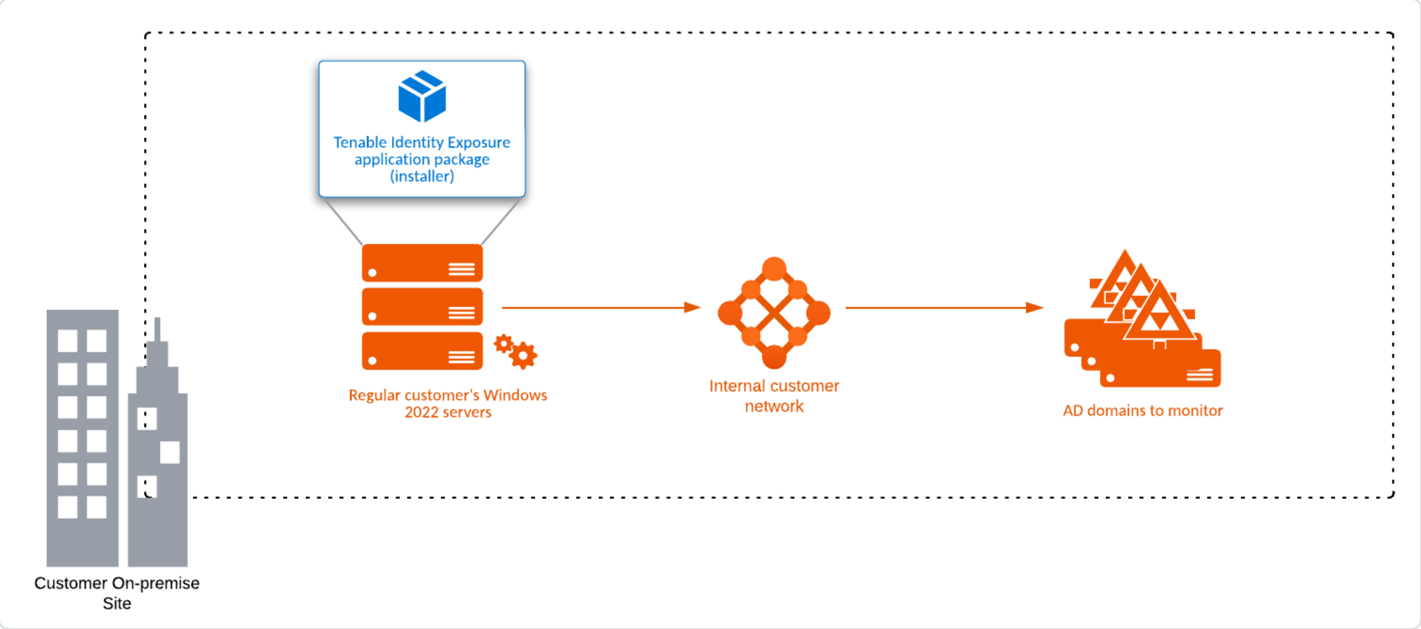
Before you begin, check that you meet the following prerequisites to ensure a smooth installation process.

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.

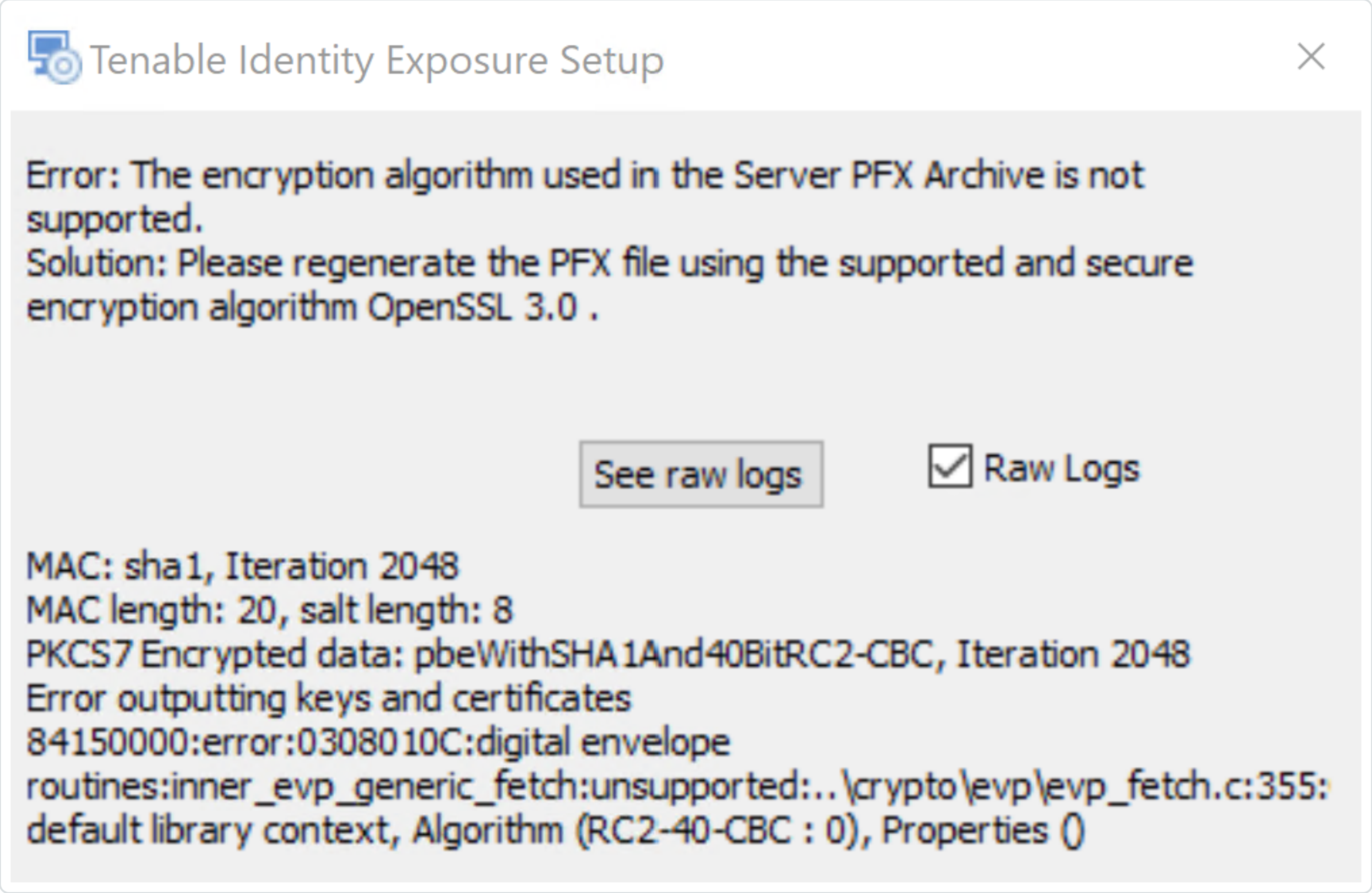

Tenable Identity Exposure application package (installer)
Regular customer's Windows 2022 servers
Internal customer network
AD domains to monitor
Customer On-premise Site

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.

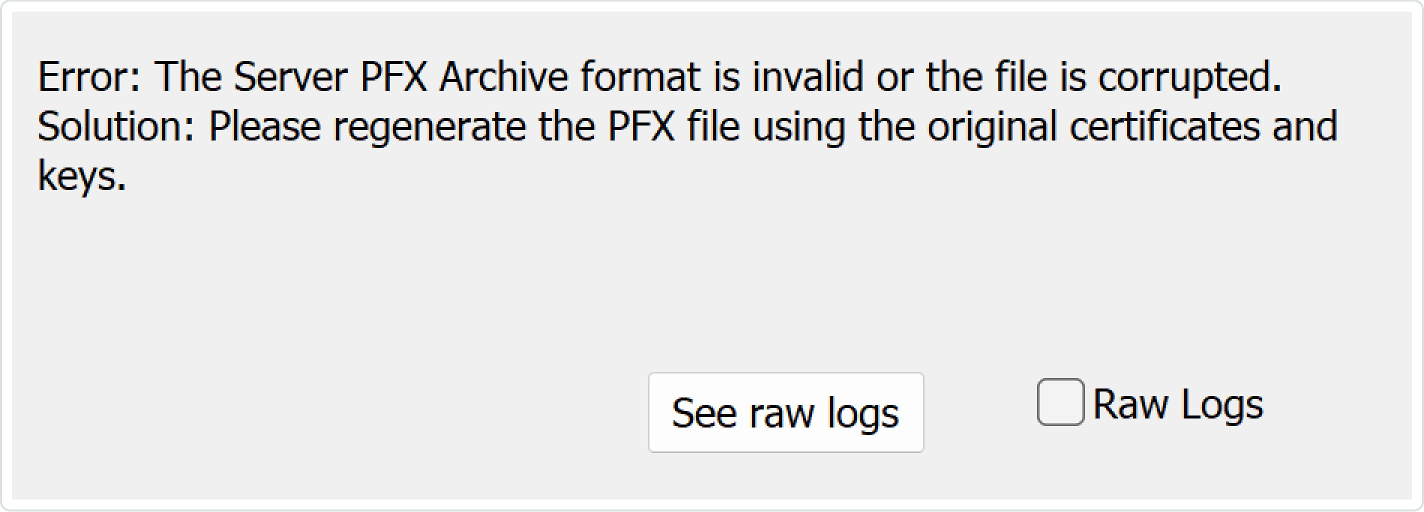
You must upgrade your certificates in response to this change. If you continue the installation without updating your certificates to use OpenSSL 3.0, the Tenable Identity Exposure installer returns the following error messages with recommended fixes:



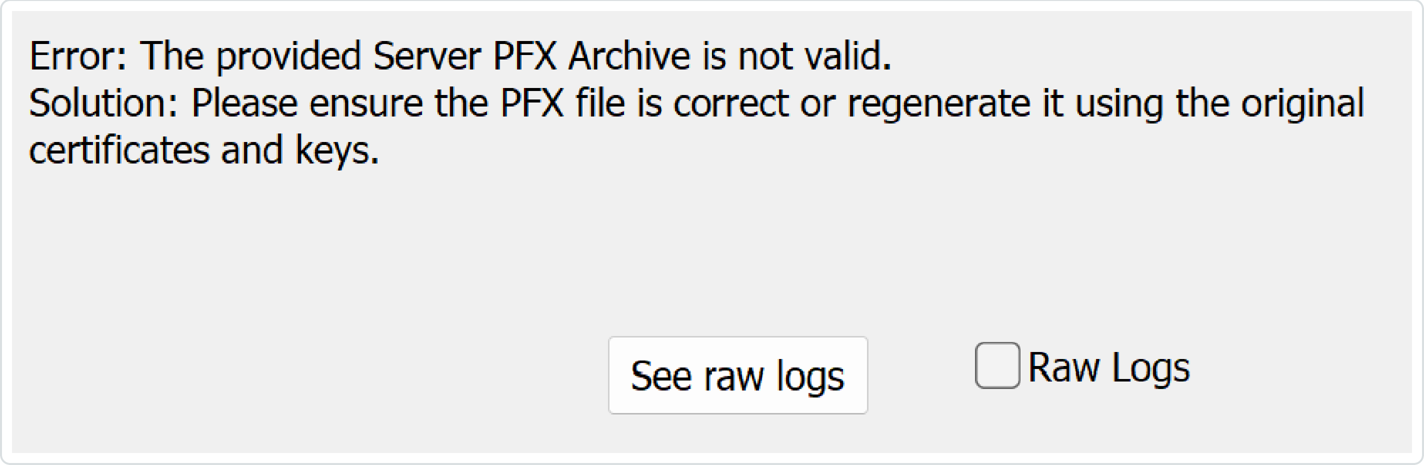
Tenable Identity Exposure Setup

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 .

```
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.



Error: The provided Server PFX Archive is not valid.
Solution: Please ensure the PFX file is correct or regenerate it using the original certificates and keys.

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	4 cores on 2	32 GB of	30 GB

	machine	sockets	RAM	(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 – 500,001+	1 virtual machine	16 cores on 4 sockets	128 GB of RAM	8 TB

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 – 150,000	4 TB	1.6 TB	3 TB	300 GB	800 GB	100 GB	200 GB
150,001 – 300,000	6 TB	2.45 TB	4.7 TB	400 GB	1 TB	150 GB	300 GB
	8 TB	3.3 TB	6.4 TB	500 GB	1.2 TB	200 GB	400 GB

300,001 – 500,001+							

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 – 150,000	250	7,500	500	15,000
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.

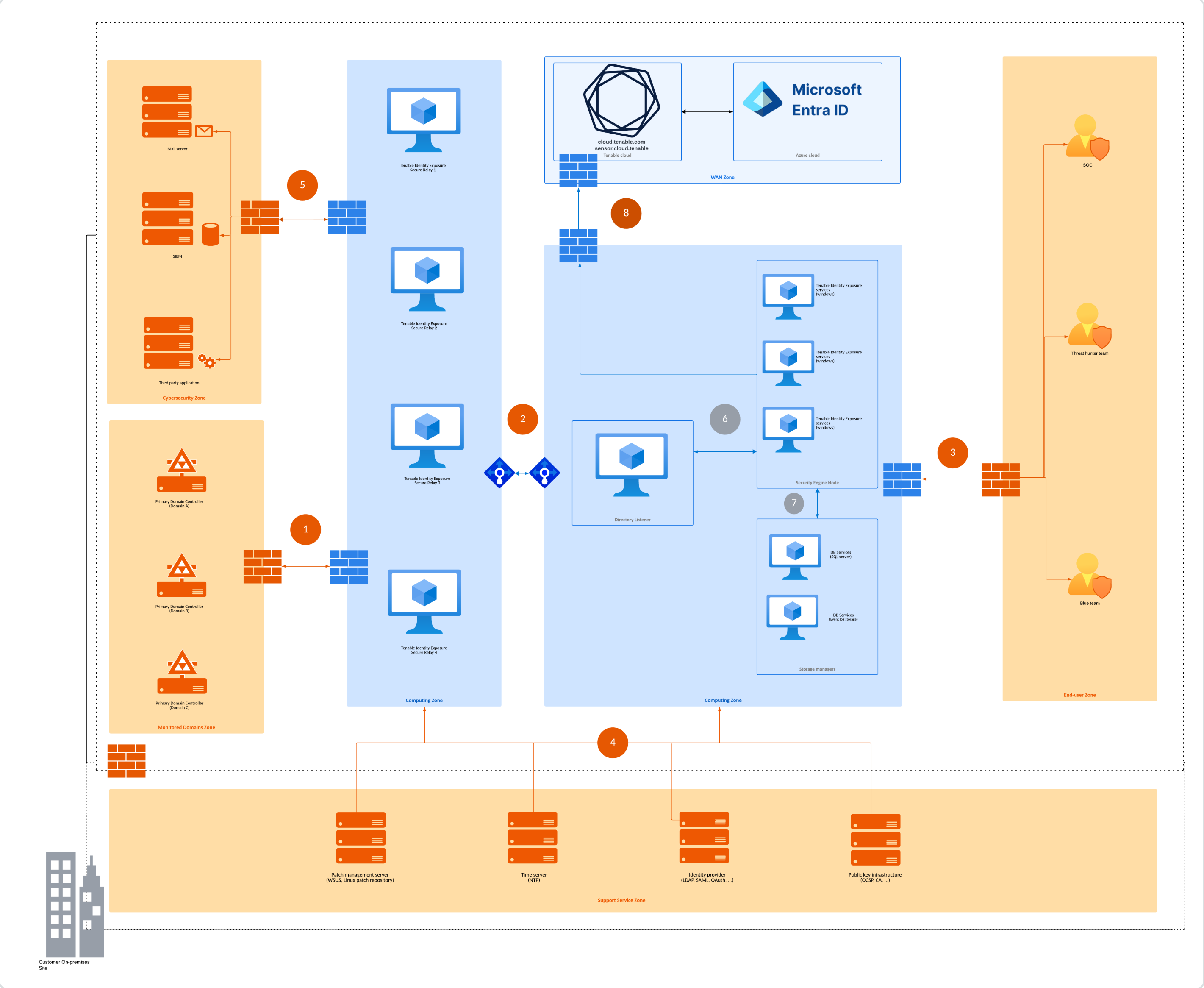
Network Flow Matrix

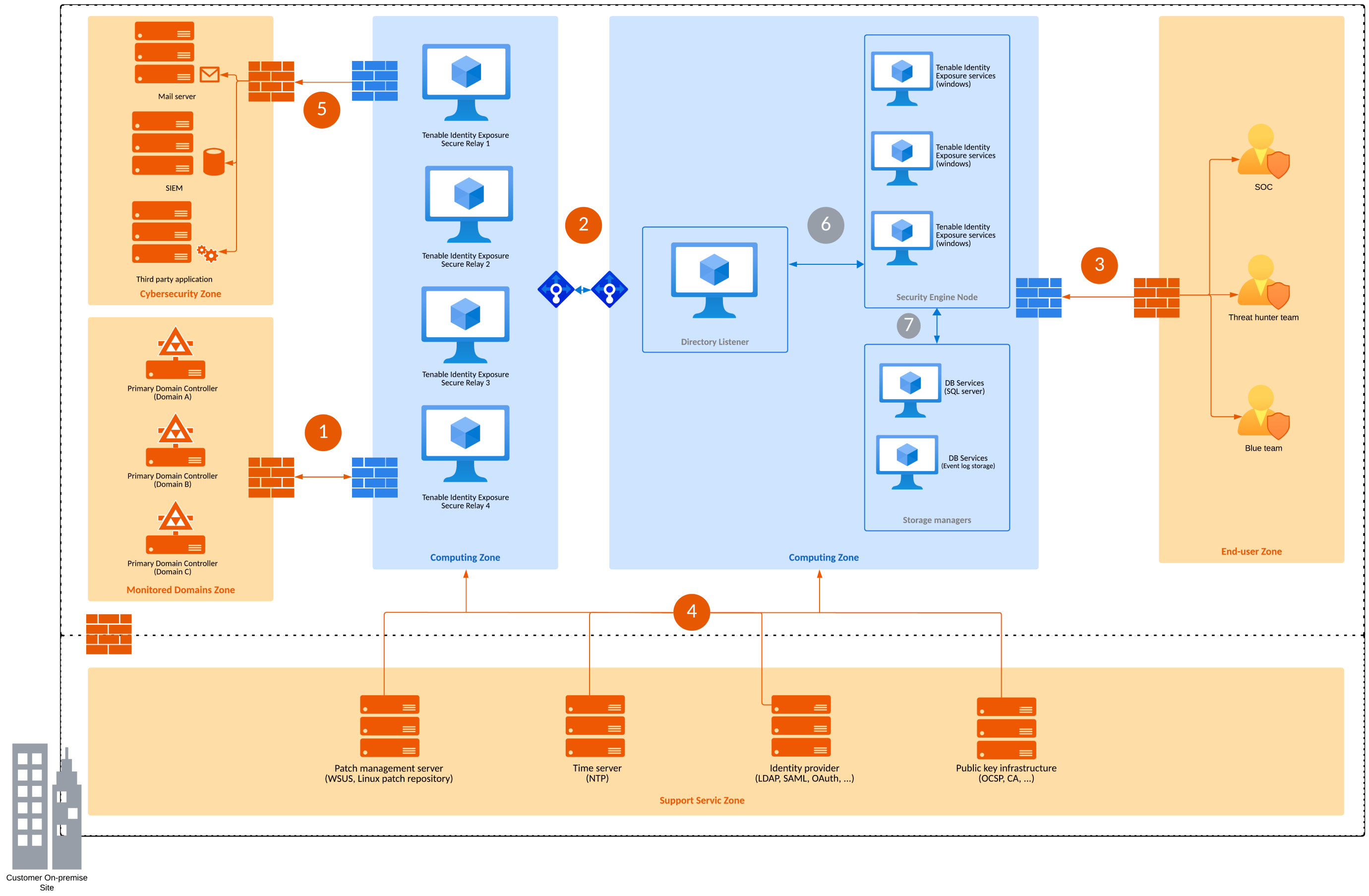
To do security monitoring, Tenable Identity Exposure must communicate with the Primary Domain Controller emulator (PDCe) of each domain. You must open network ports and transport protocols on each PDCe to ensure efficient monitoring.

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.


Mail server
SIEM
Third party application
Cybersecurity Zone
5
Tenable Identity Exposure Secure Relay 1
Tenable Identity Exposure Secure Relay 2
Tenable Identity Exposure Secure Relay 3
Tenable Identity Exposure Secure Relay 4
Computing Zone
2
1
Primary Domain Controller (Domain A)
Primary Domain Controller (Domain B)
Primary Domain Controller (Domain C)
Monitored Domains Zone
cloud.tenable.com
sensor.cloud.tenable
Tenable cloud
Microsoft Entra ID
Azure cloud
WAN Zone
8
Tenable Identity Exposure services (windows)
Tenable Identity Exposure services (windows)
Tenable Identity Exposure services (windows)
Security Engine Node
6
Directory Listener
7
DB Services (SQL server)
DB Services (Event log storage)
Storage managers
Computing Zone
3
SOC
Threat hunter team
Blue team
End-user Zone
4
Patch management server (WSUS, Linux patch repository)
Time server (NTP)
Identity provider (LDAP, SAML, OAuth, ...)
Public key infrastructure (OCSP, CA, ...)
Support Service Zone
Customer On-premises Site


Mail server
SIEM
Third party application
Cybersecurity Zone
Primary Domain Controller (Domain A)
Primary Domain Controller (Domain B)
Primary Domain Controller (Domain C)
Monitored Domains Zone
5
1
Tenable Identity Exposure Secure Relay 1
Tenable Identity Exposure Secure Relay 2
Tenable Identity Exposure Secure Relay 3
Tenable Identity Exposure Secure Relay 4
Computing Zone
2
Directory Listener
6
Tenable Identity Exposure services (windows)
Tenable Identity Exposure services (windows)
Tenable Identity Exposure services (windows)
Security Engine Node
7
DB Services (SQL server)
DB Services (Event log storage)
Storage managers
Computing Zone
3
SOC
Threat hunter team
Blue team
End-user Zone
4
Patch management server (WSUS, Linux patch repository)
Time server (NTP)
Identity provider (LDAP, SAML, OAuth, ...)
Public key infrastructure (OCSP, CA, ...)
Support Servic Zone
Customer On-premise Site

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, Group Policy,	LDAP/LDAPS	TCP/389 and TCP/636 ICMP/echo-request ICMP/echo-

			Trusts		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 Identity Exposure's	Tenable Identity Exposure's end-user services	HTTPS	TCP/443

		Security engine nodes	(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	Type of Traffic	Protocol and Port

			Exposure’s Usage (optional)		
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.

	From	To	Tenable	Type of	Protoco

Network flows			Identity Exposure’s Usage	Traffic	l 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
8.	Tenable Identity Exposure’s Security Engine Nodes	Tenable Cloud • cloud.tenable.com • sensor.cloud.tenable.com	Tenable Identity Exposure Cloud service	HTTPS	TCP/443

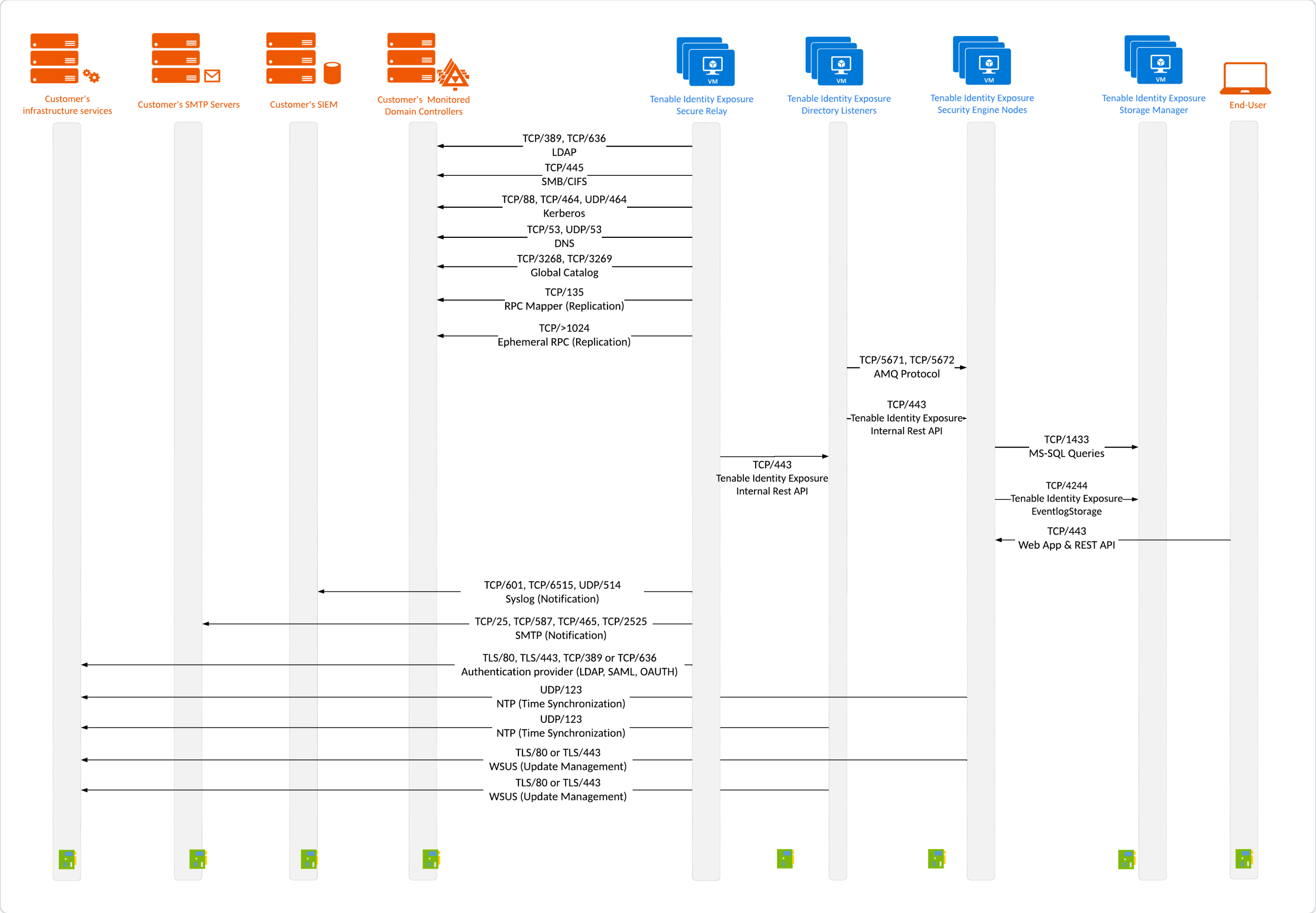
Support Services

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.

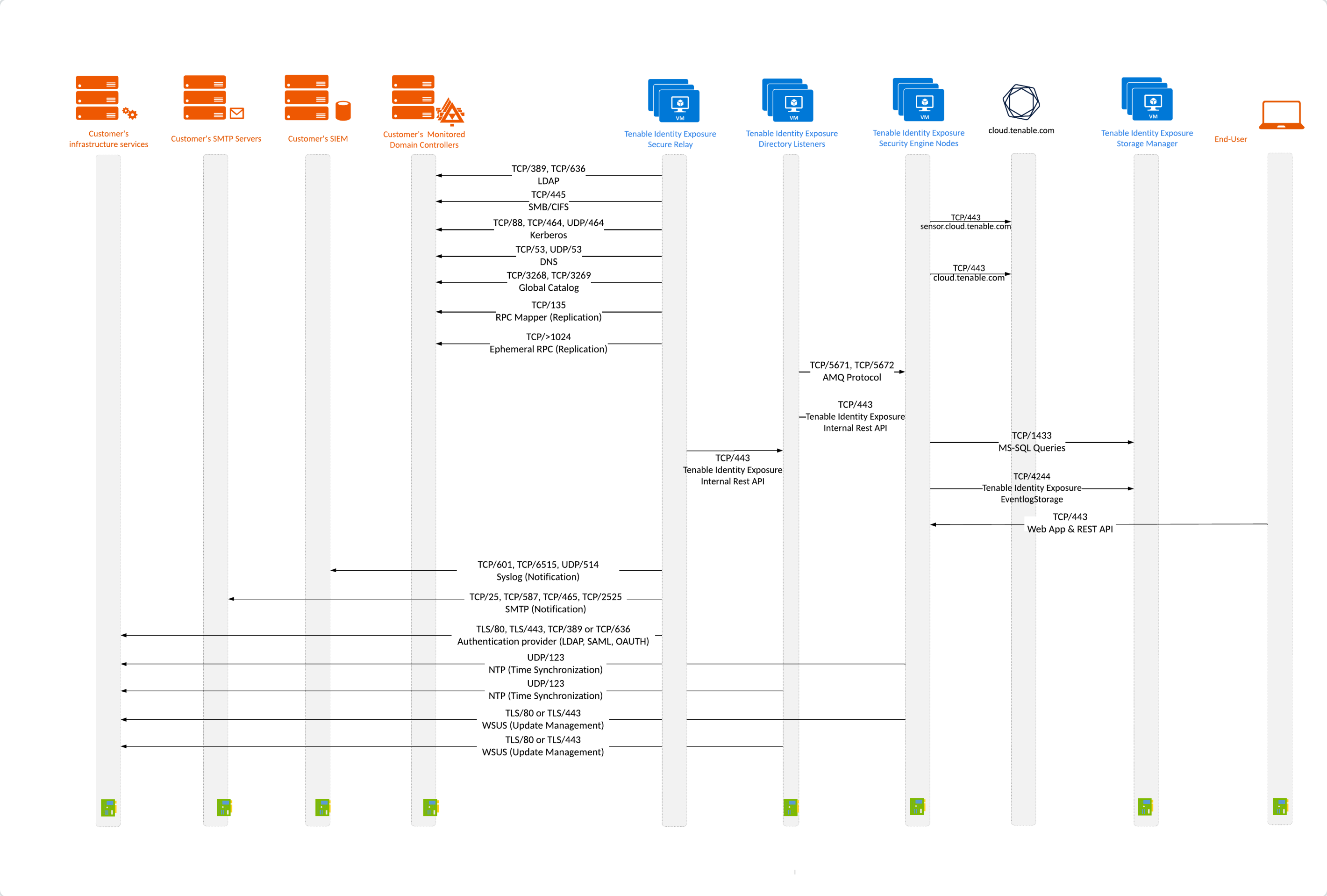
Network Address Translation (NAT) support

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


Customer's infrastructure services
Customer's SMTP Servers
Customer's SIEM
Customer's Monitored Domain Controllers
Tenable Identity Exposure Secure Relay
Tenable Identity Exposure Directory Listeners
Tenable Identity Exposure Security Engine Nodes
Tenable Identity Exposure Storage Manager
End-User
VM
TCP/389, TCP/636
LDAP
TCP/445
SMB/CIFS
TCP/88, TCP/464, UDP/464
Kerberos
TCP/53, UDP/53
DNS
TCP/3268, TCP/3269
Global Catalog
TCP/135
RPC Mapper (Replication)
TCP/>1024
Ephemeral RPC (Replication)
TCP/5671, TCP/5672
AMQ Protocol
TCP/443
Tenable Identity Exposure
Internal Rest API
TCP/1433
MS-SQL Queries
TCP/443
Tenable Identity Exposure
Internal Rest API
TCP/4244
Tenable Identity Exposure
EventlogStorage
TCP/443
Web App & REST API
TCP/601, TCP/6515, UDP/514
Syslog (Notification)
TCP/25, TCP/587, TCP/465, TCP/2525
SMTP (Notification)
TLS/80, TLS/443, TCP/389 or TCP/636
Authentication provider (LDAP, SAML, OAUTH)
UDP/123
NTP (Time Synchronization)
UDP/123
NTP (Time Synchronization)
TLS/80 or TLS/443
WSUS (Update Management)
TLS/80 or TLS/443
WSUS (Update Management)

On-Premises platform using Secure Relay with Proxy



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:

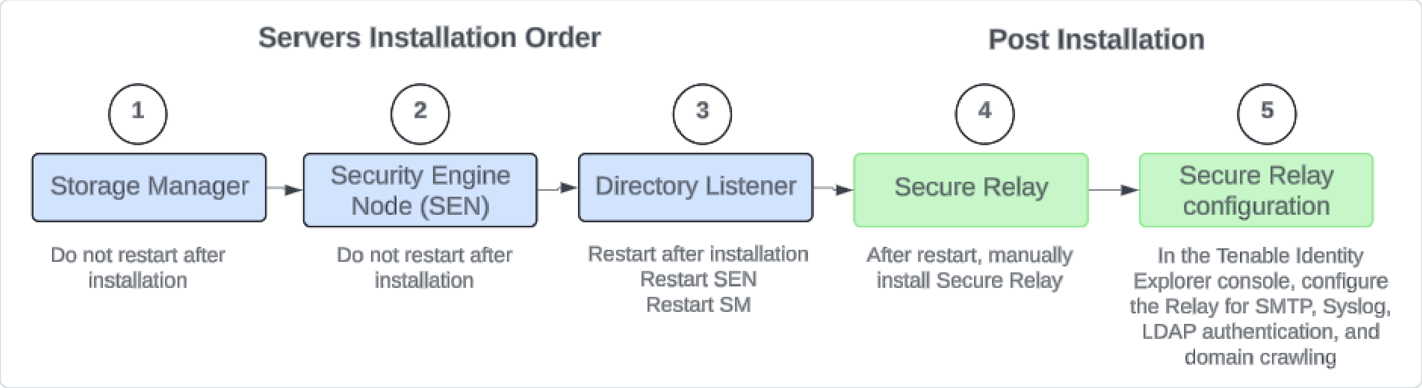
- A **Storage Manager** (SM) to host all data based on MSSQL.
- A **Directory Listener** (DL) to target audited domains.
- A **Security Engine Node** (SEN) to perform security analysis and serve the user interface.

  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** 3.77, proceed in the following order:


Servers Installation Order
Post Installation
1
Storage Manager
Do not restart after installation
2
Security Engine Node (SEN)
Do not restart after installation
3
Directory Listener
Restart after installation
Restart SEN
Restart SM
4
Secure Relay
After restart, manually install Secure Relay
5
Secure Relay configuration
In the Tenable Identity Explorer console, configure the Relay for SMTP, Syslog, LDAP authentication, and domain crawling

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:

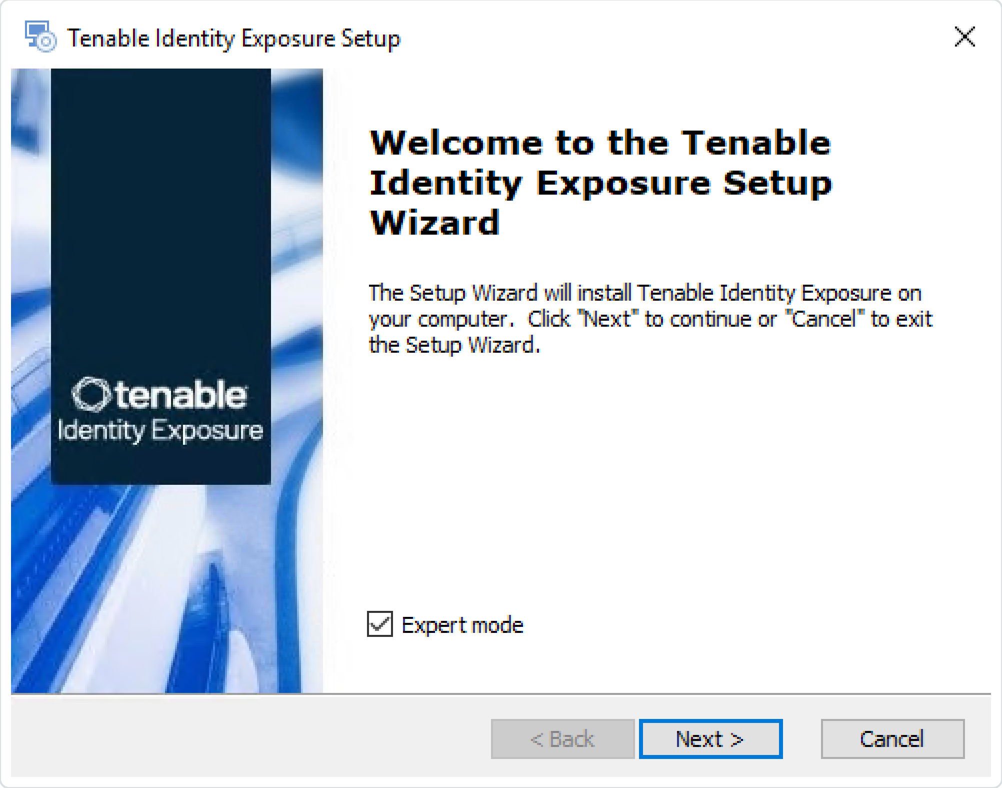
1. On the local machine, run the **Tenable Identity Exposure 3.77** On-Premises installer.

   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.



Tenable Identity Exposure Setup

Welcome to the Tenable Identity Exposure Setup Wizard

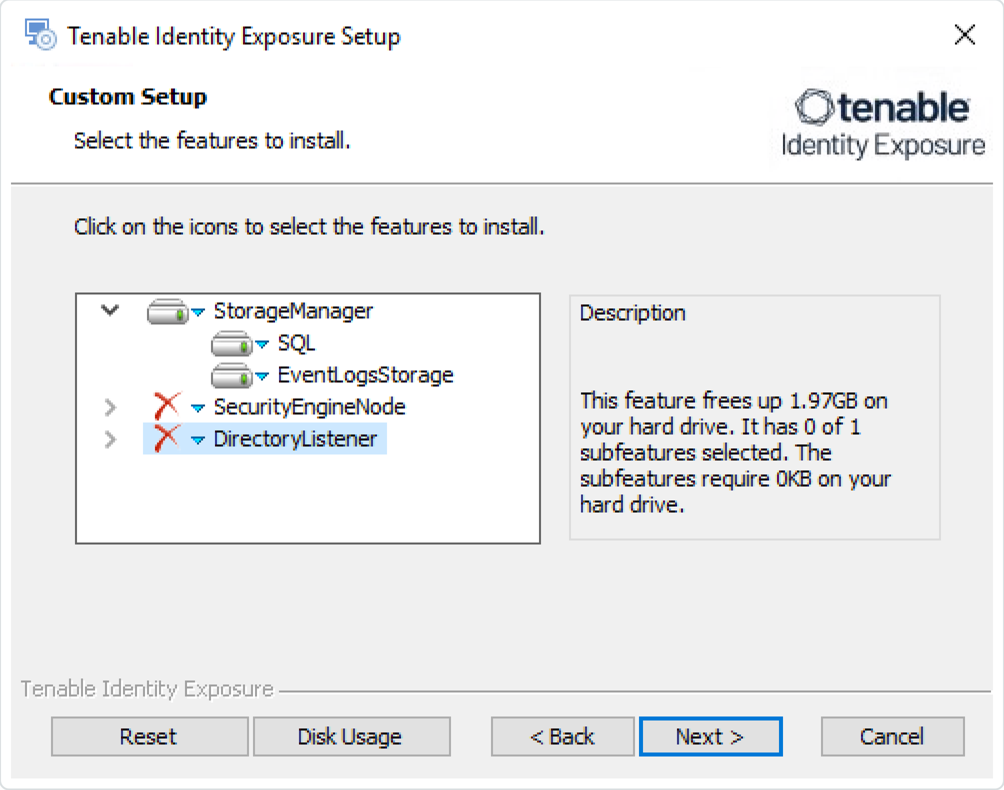
The Setup Wizard will install Tenable Identity Exposure on your computer. Click "Next" to continue or "Cancel" to exit the Setup Wizard.

☑ Expert mode

4. Click **Next**.

   The **Custom Setup** window appears.

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



Tenable Identity Exposure Setup

Custom Setup

Select the features to install.

Click on the icons to select the features to install.

- StorageManager
  - SQL
  - EventLogsStorage
- SecurityEngineNode
- DirectoryListener

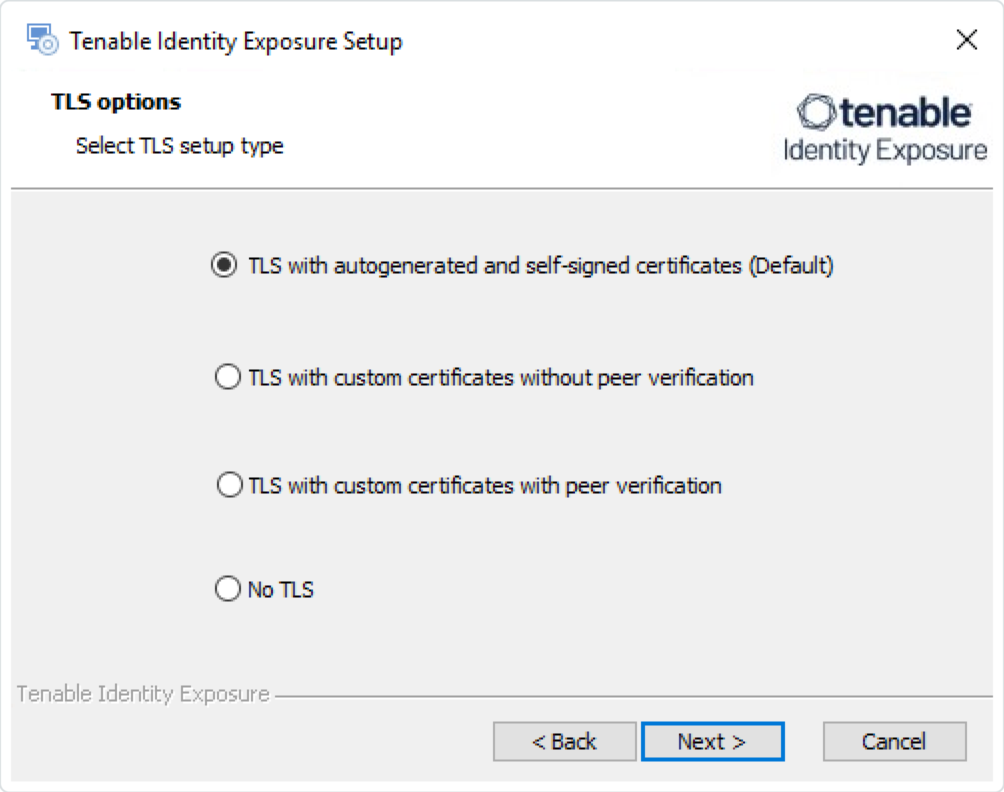
Description

This feature frees up 1.97GB on your hard drive. It has 0 of 1 subfeatures selected. The subfeatures require 0KB on your hard drive.

6. Click **Next**.

   The **TLS Options** window appears.

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



Tenable Identity Exposure Setup

TLS options

Select TLS setup type

● TLS with autogenerated and self-signed certificates (Default)

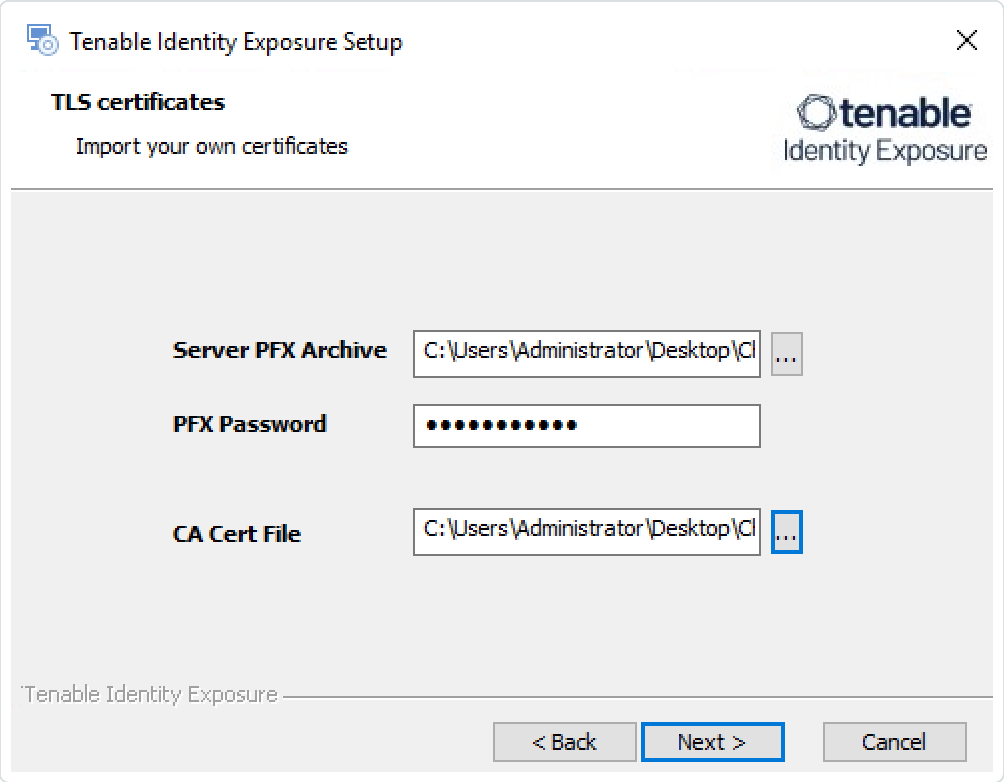
○ TLS with custom certificates without peer verification

○ TLS with custom certificates with peer verification

○ No TLS

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.


Tenable Identity Exposure Setup

TLS certificates

Import your own certificates

Server PFX Archive: C:\Users\Administrator\Desktop\Cl

PFX Password: ●●●●●●●●●●●

CA Cert File: C:\Users\Administrator\Desktop\Cl

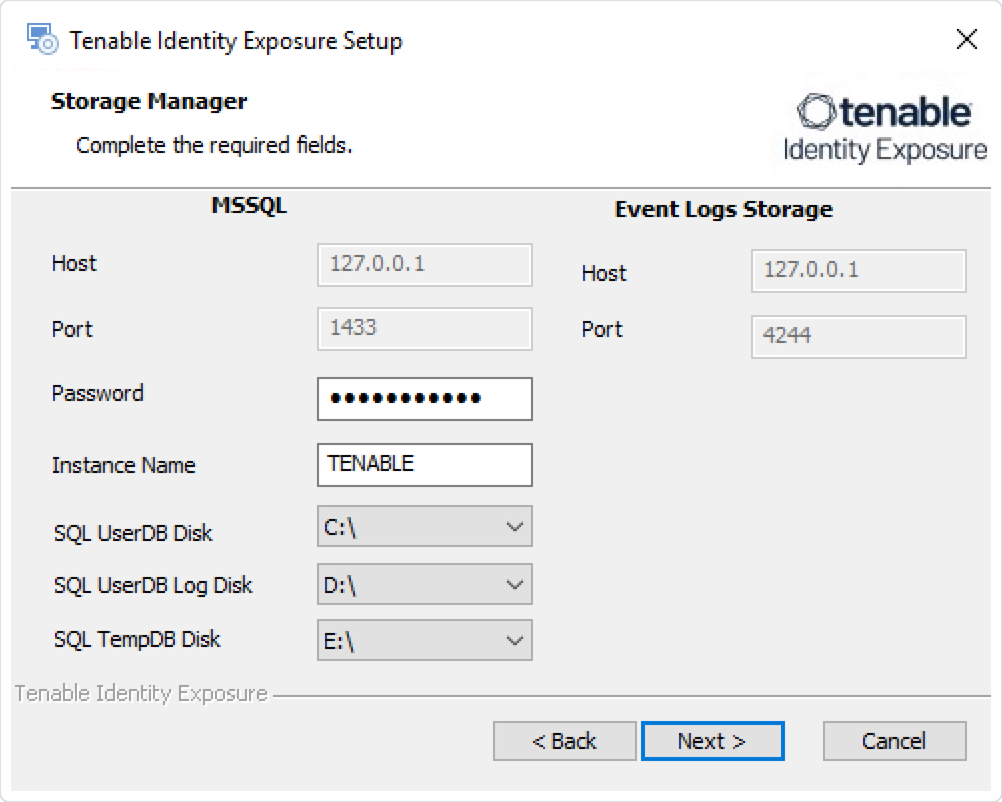
8. Click **Next**.

   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.



Tenable Identity Exposure Setup

Storage Manager

Complete the required fields.

MSSQL

Host: 127.0.0.1

Port: 1433

Password: ●●●●●●●●●●●●

Instance Name: TENABLE

SQL UserDB Disk: C:\

SQL UserDB Log Disk: D:\

SQL TempDB Disk: E:\

Event Logs Storage

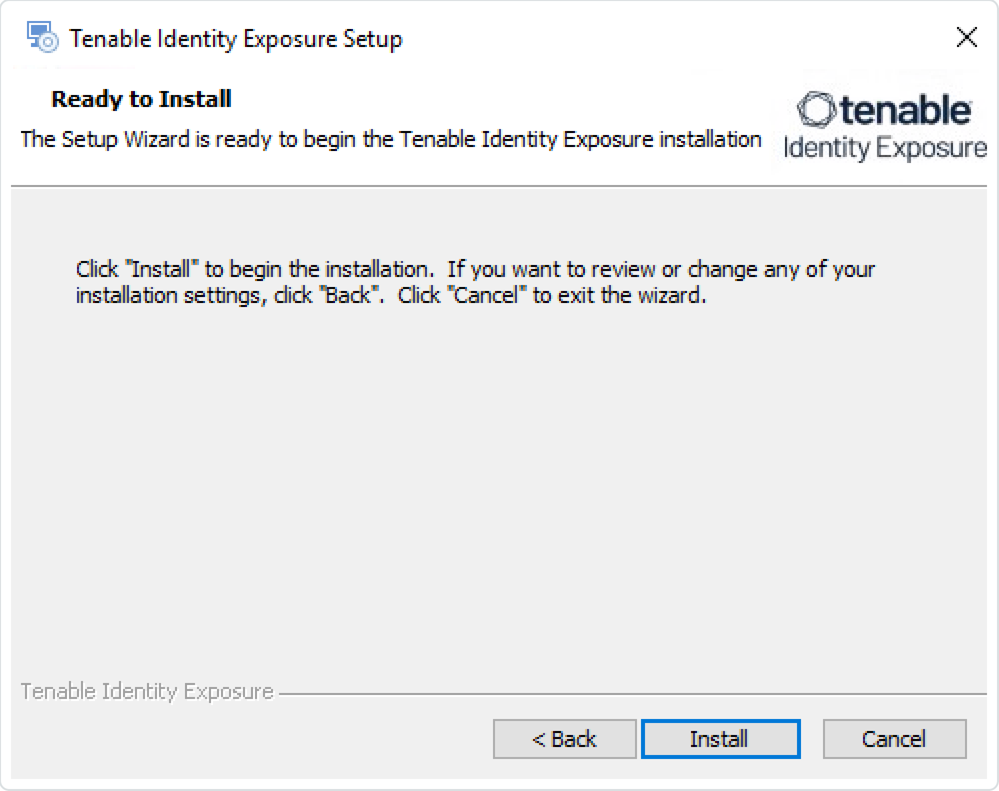
Host: 127.0.0.1

Port: 4244

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

10. Click **Next**.

    The **Ready to Install** window appears.



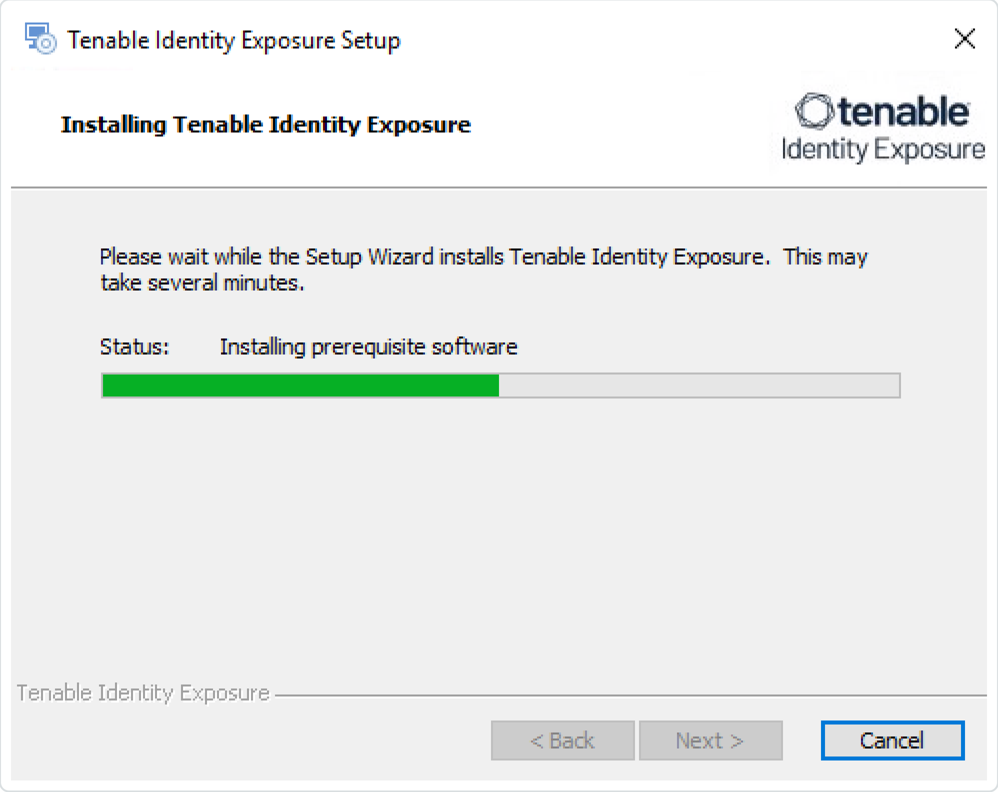
Tenable Identity Exposure Setup

Ready to Install

The Setup Wizard is ready to begin the Tenable Identity Exposure installation

Click "Install" to begin the installation. If you want to review or change any of your installation settings, click "Back". Click "Cancel" to exit the wizard.

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


Tenable Identity Exposure Setup

Installing Tenable Identity Exposure

Please wait while the Setup Wizard installs Tenable Identity Exposure. This may take several minutes.

Status: Installing prerequisite software

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:

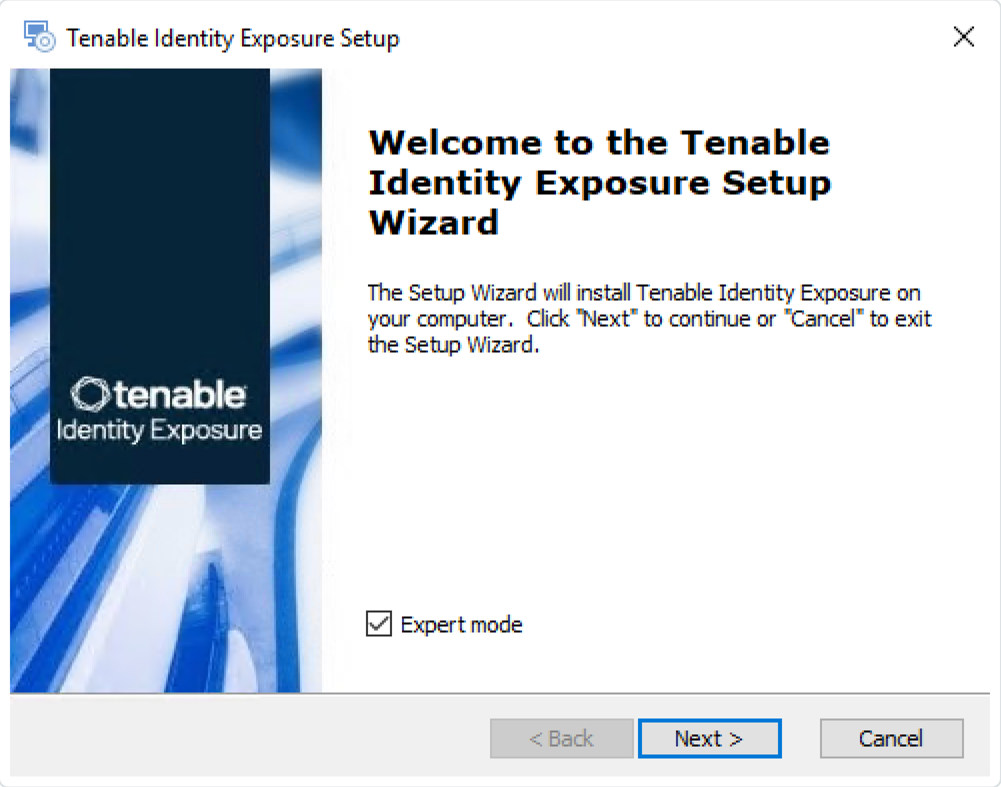
1. On the local machine, run the **Tenable Identity Exposure 3.77** On-Premises installer.

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.



Tenable Identity Exposure Setup

Welcome to the Tenable Identity Exposure Setup Wizard

The Setup Wizard will install Tenable Identity Exposure on your computer. Click "Next" to continue or "Cancel" to exit the Setup Wizard.

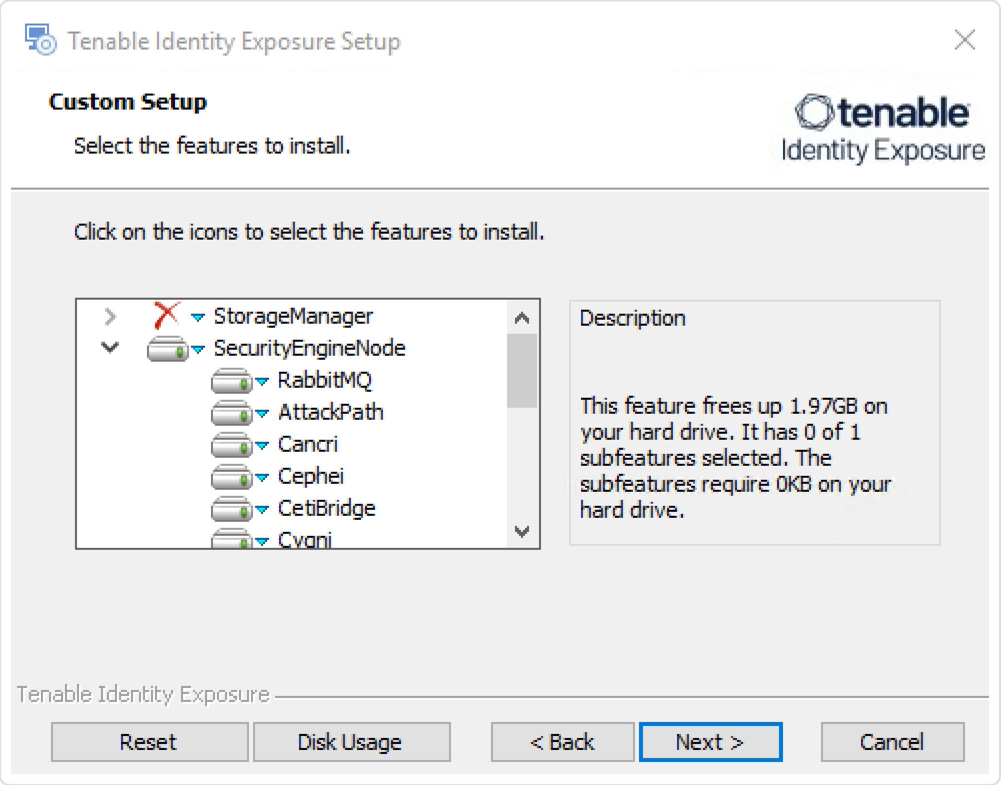
☑ Expert mode

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 Up SEN Services.

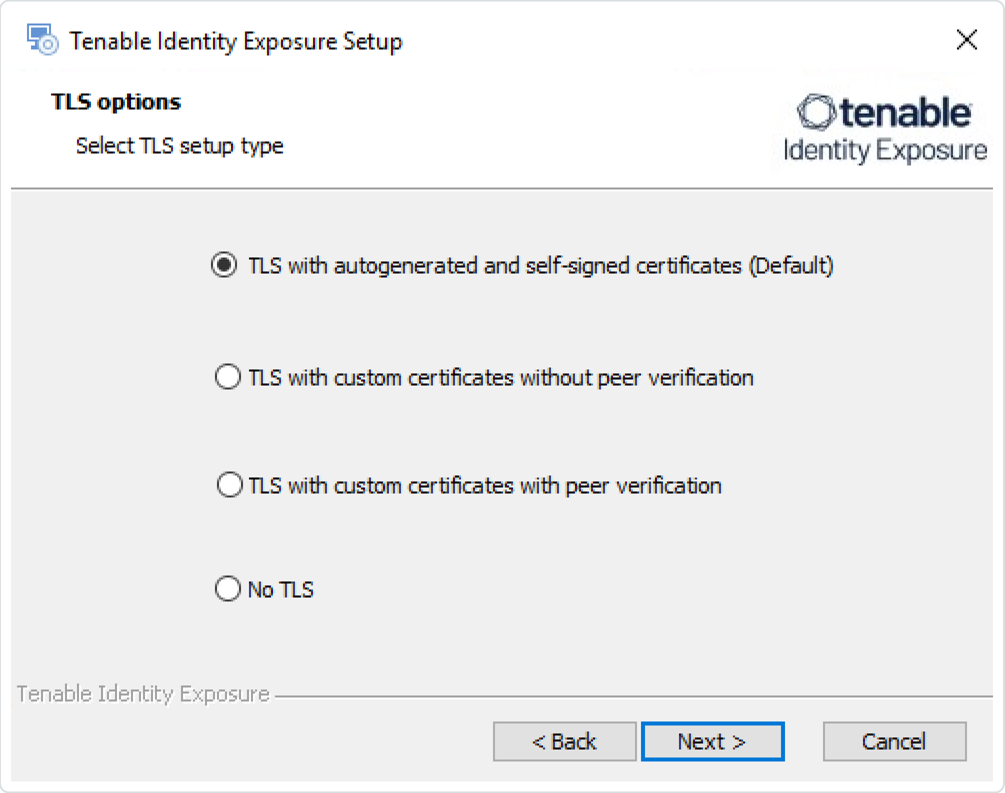


Tenable Identity Exposure Setup
Custom Setup
Select the features to install.
tenable
Identity Exposure
Click on the icons to select the features to install.
StorageManager
SecurityEngineNode
RabbitMQ
AttackPath
Cancri
Cephei
CetiBridge
Cygni
Description
This feature frees up 1.97GB on your hard drive. It has 0 of 1 subfeatures selected. The subfeatures require 0KB on your hard drive.
Tenable Identity Exposure
Reset
Disk Usage
< Back
Next >
Cancel

6. Click **Next**.

   The **TLS Options** window appears.

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



Tenable Identity Exposure Setup

TLS options

Select TLS setup type

● TLS with autogenerated and self-signed certificates (Default)

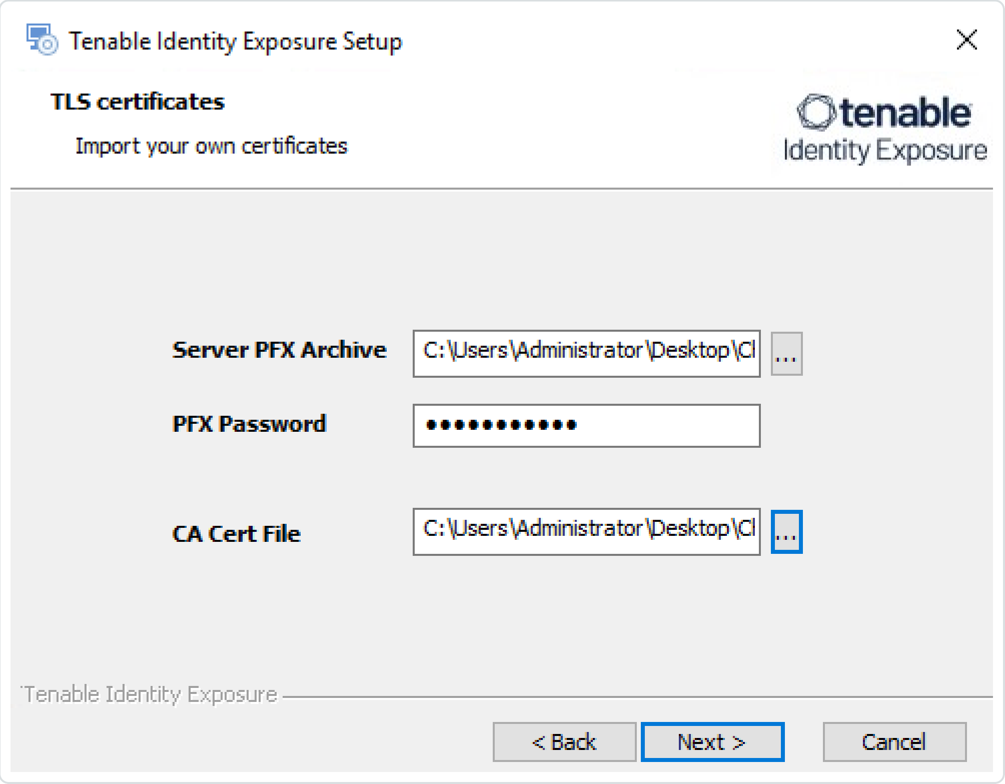
○ TLS with custom certificates without peer verification

○ TLS with custom certificates with peer verification

○ No TLS

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.


Tenable Identity Exposure Setup

TLS certificates

Import your own certificates

Server PFX Archive: C:\Users\Administrator\Desktop\Cl

PFX Password: ●●●●●●●●●●●

CA Cert File: C:\Users\Administrator\Desktop\Cl

8. Click **Next**.

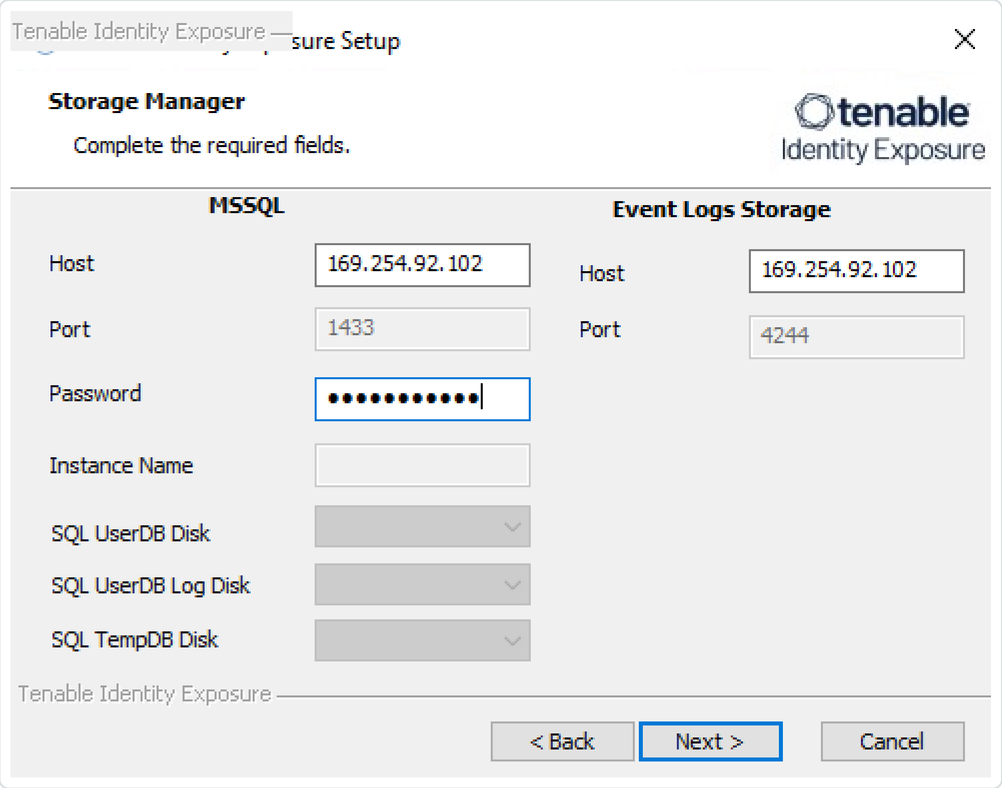
   The **Storage Manager** window appears.

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.


Tenable Identity Exposure —sure Setup
tenable Identity Exposure
Tenable Identity Exposure
< Back
Next >
Cancel

Storage Manager

Complete the required fields.

MSSQL

Host: 169.254.92.102

Port: 1433

Password: ●●●●●●●●●●●●

Instance Name:

SQL UserDB Disk:

SQL UserDB Log Disk:

SQL TempDB Disk:

Event Logs Storage

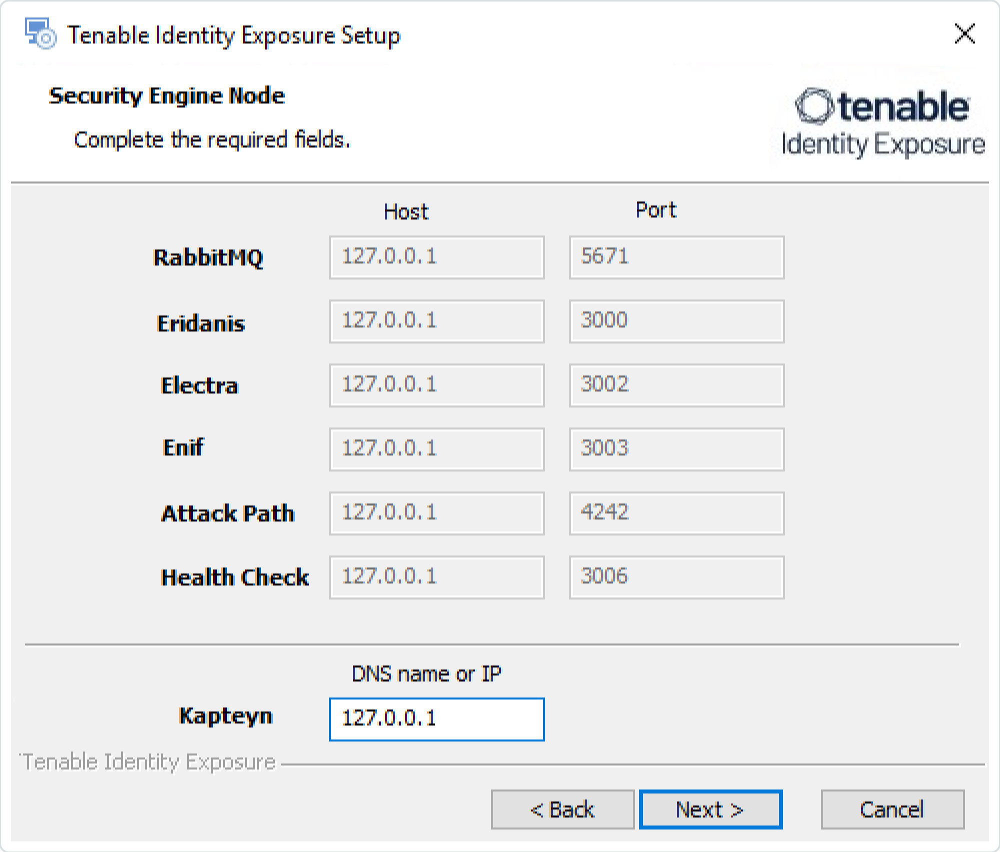
Host: 169.254.92.102

Port: 4244

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.


Tenable Identity Exposure Setup
tenable Identity Exposure
Tenable Identity Exposure
< Back
Next >
Cancel

Security Engine Node

Complete the required fields.

	Host	Port
RabbitMQ	127.0.0.1	5671
Eridanis	127.0.0.1	3000
Electra	127.0.0.1	3002
Enif	127.0.0.1	3003
Attack Path	127.0.0.1	4242
Health Check	127.0.0.1	3006

	DNS name or IP
Kapteyn	127.0.0.1

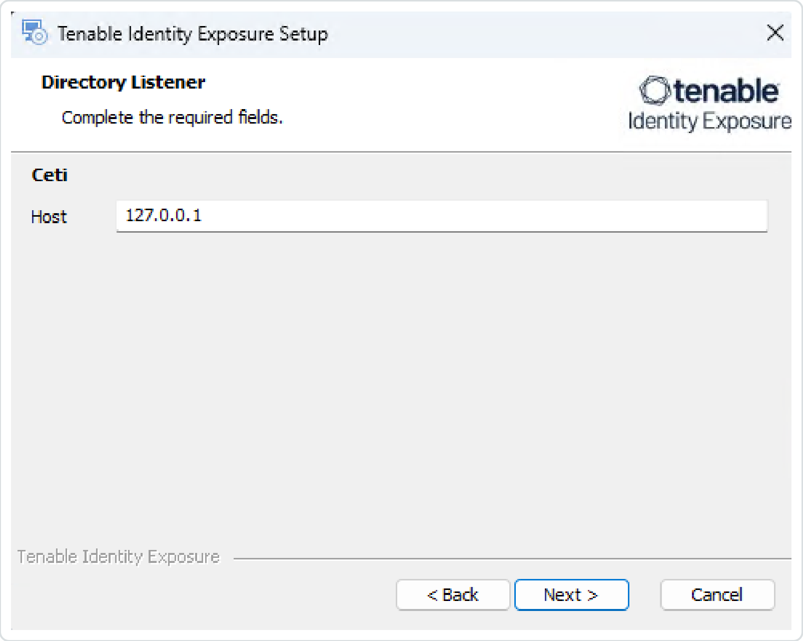
> **Note**: By default, the installation process creates a self-signed certificate with the DNS name or the IP address that you entered. For more information, see Change the IIS Certificate.

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.


Tenable Identity Exposure Setup
Directory Listener
Complete the required fields.
tenable
Identity Exposure
Tenable Identity Exposure
< Back
Next >
Cancel

Ceti

Host: 127.0.0.1

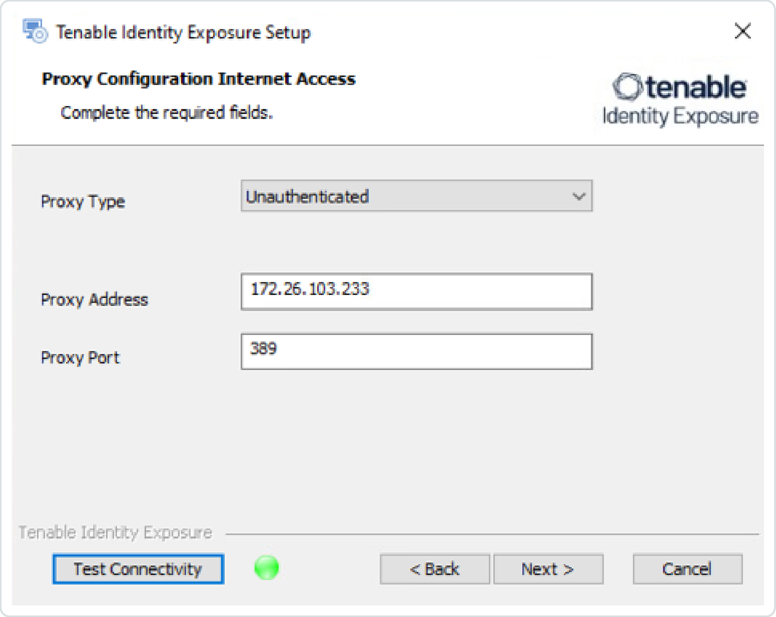
The **Proxy Configuration** window appears.

14. You have the following proxy types:

    - **None**: Select "None" from the drop-down list box and click **Next**.

    - **Unauthenticated:** Select "Unauthenticated" from the drop-down list box.

        - In the boxes **Proxy Address** and **Proxy Port,** enter the address and port of your proxy server.



Tenable Identity Exposure Setup

Proxy Configuration Internet Access

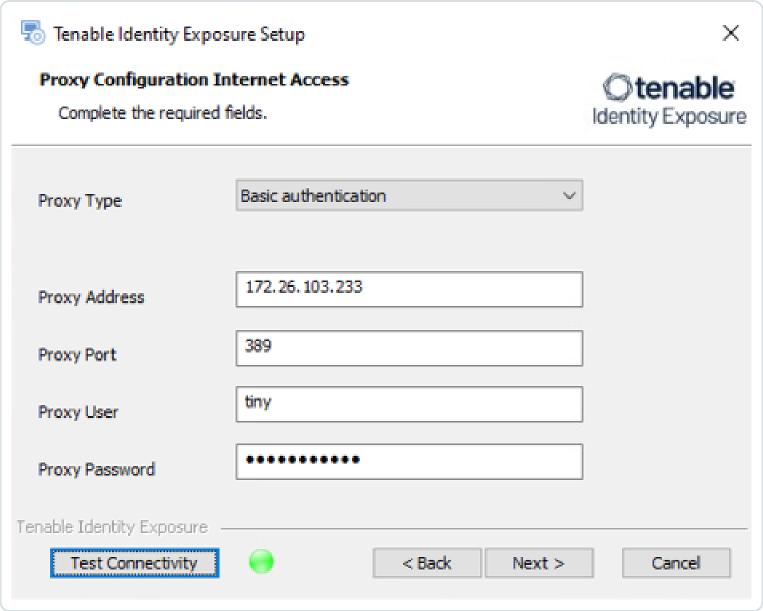
Complete the required fields.

Proxy Type: Unauthenticated

Proxy Address: 172.26.103.233

Proxy Port: 389

- ○ **Basic Authentication**: Select "Basic authentication" from the drop-down list box.
  - In the boxes **Proxy Address** and **Proxy Port,** type the address and port of your proxy server.
  - In the box **Proxy User** and **Proxy Password**, type the name of the specific user account authorized to access a proxy server and the associated credential to allow requests through the proxy server.



Tenable Identity Exposure Setup

Proxy Configuration Internet Access

Complete the required fields.

Proxy Type: Basic authentication

Proxy Address: 172.26.103.233

Proxy Port: 389

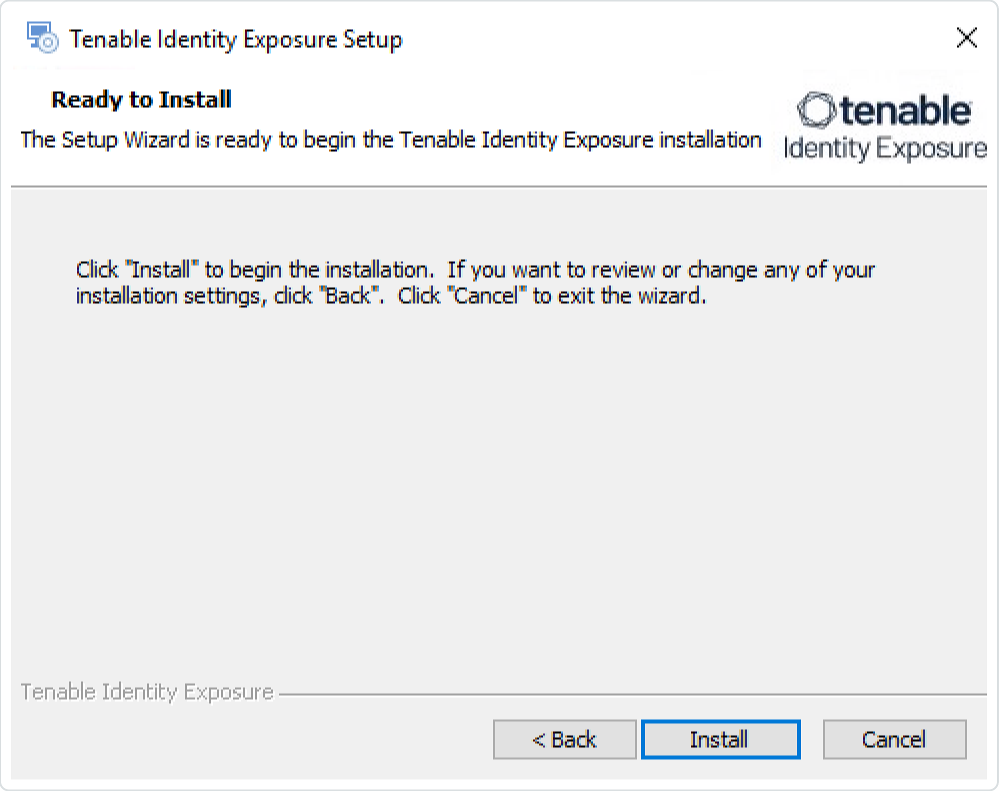
Proxy User: tiny

Proxy Password: ●●●●●●●●●●●●

15. Click **Test Connectivity**.

16. Click **Next**.

    The **Ready to Install** window appears.

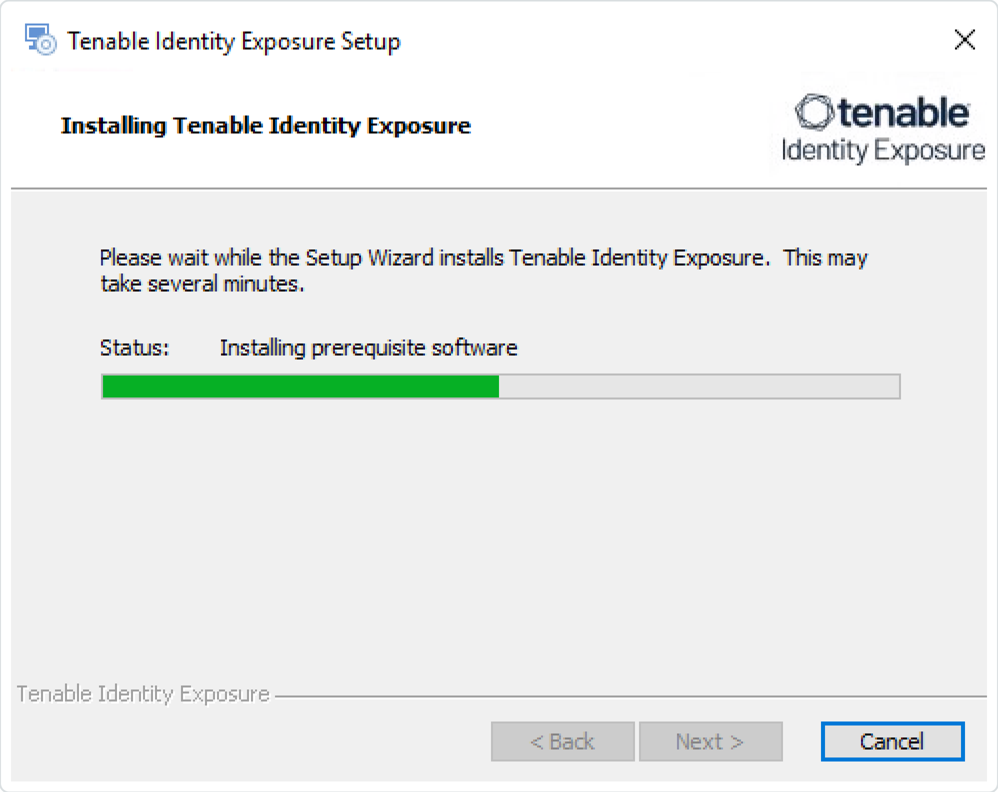
17. 

    Ready to Install

    The Setup Wizard is ready to begin the Tenable Identity Exposure installation

    Click "Install" to begin the installation. If you want to review or change any of your installation settings, click "Back". Click "Cancel" to exit the wizard.

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



Tenable Identity Exposure Setup

Installing Tenable Identity Exposure

Please wait while the Setup Wizard installs Tenable Identity Exposure. This may take several minutes.

Status: Installing prerequisite software

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

19. Click **Finish**.

    A dialog box asks you to restart your machine.

20. Click **No**.

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

21. Install the Directory Listener.

To install the Directory Listener:

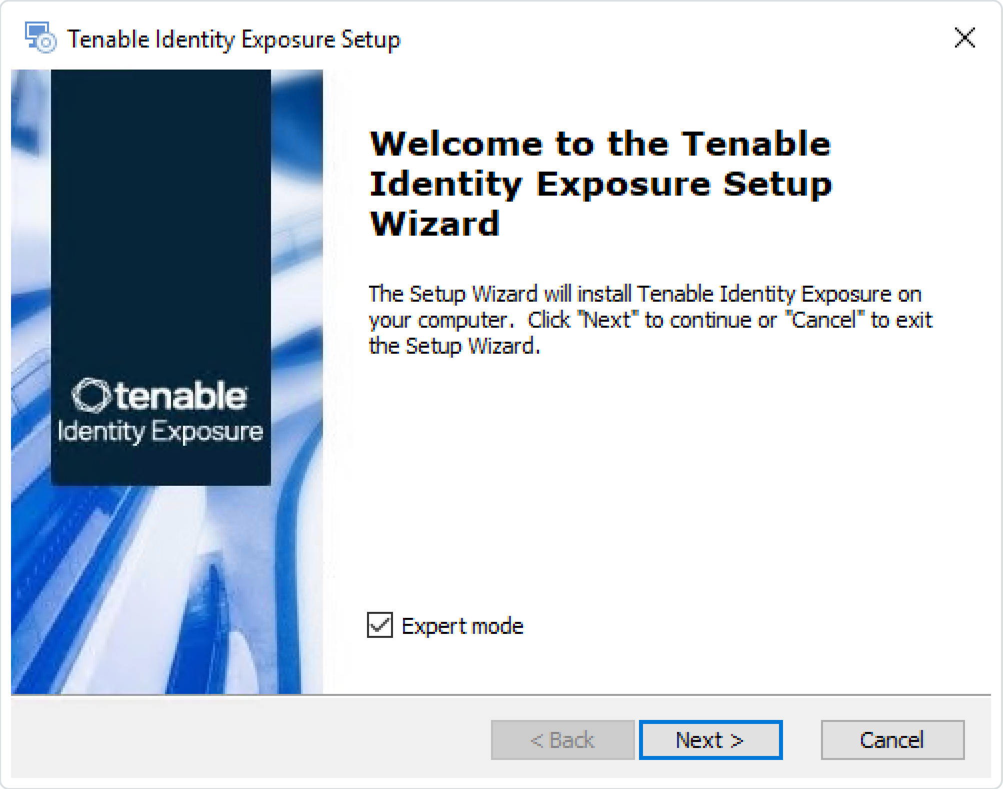
1. On the local machine, run the **Tenable Identity Exposure 3.77** On-Premises installer.

   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.



Welcome to the Tenable Identity Exposure Setup Wizard

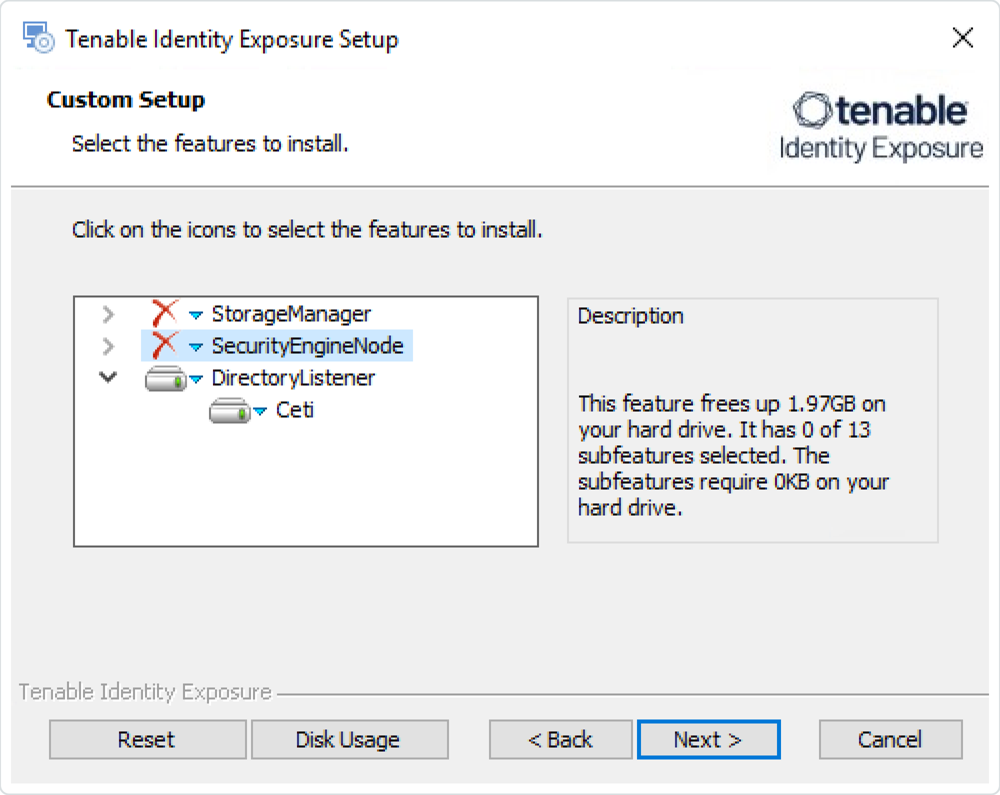
The Setup Wizard will install Tenable Identity Exposure on your computer. Click "Next" to continue or "Cancel" to exit the Setup Wizard.

☑ Expert mode

4. Click **Next**.

   The **Custom Setup** window appears.

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



Tenable Identity Exposure Setup

Custom Setup

Select the features to install.

Click on the icons to select the features to install.

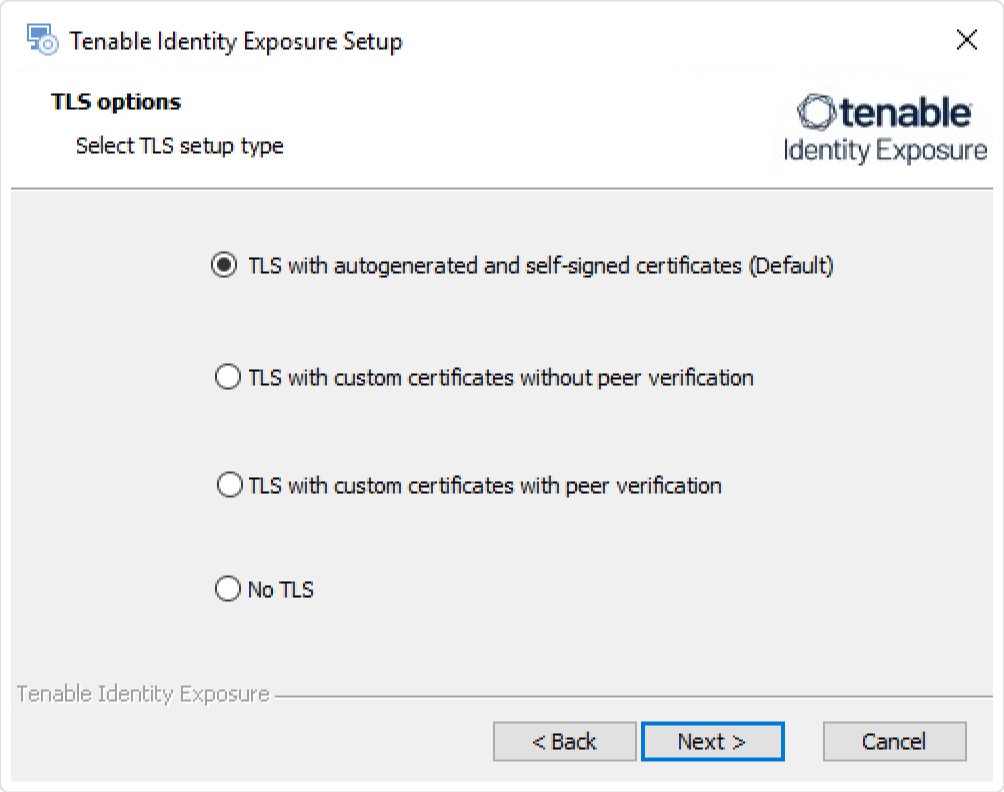
Description

This feature frees up 1.97GB on your hard drive. It has 0 of 13 subfeatures selected. The subfeatures require 0KB on your hard drive.

6. Click **Next**.

   The **TLS Options** window appears.

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



Tenable Identity Exposure Setup

TLS options

Select TLS setup type

● TLS with autogenerated and self-signed certificates (Default)

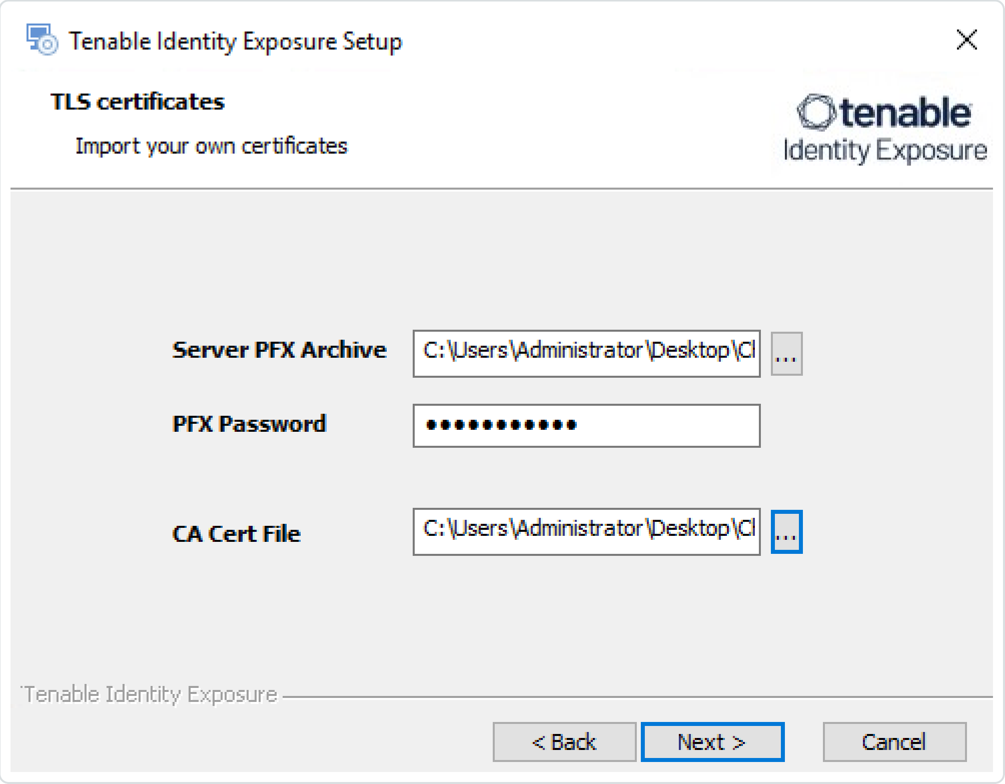
○ TLS with custom certificates without peer verification

○ TLS with custom certificates with peer verification

○ No TLS

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.



Tenable Identity Exposure Setup

TLS certificates

Import your own certificates

Server PFX Archive: C:\Users\Administrator\Desktop\Cl

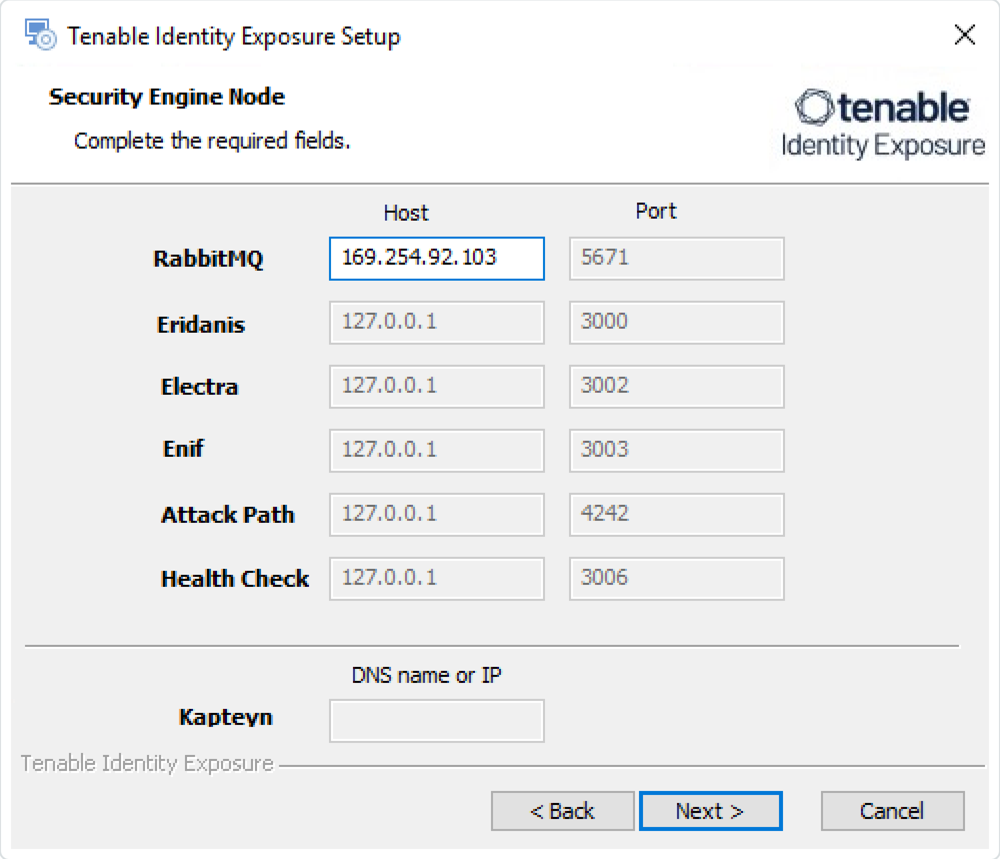
PFX Password: ●●●●●●●●●●●

CA Cert File: C:\Users\Administrator\Desktop\Cl

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.



Tenable Identity Exposure Setup

Security Engine Node

Complete the required fields.

	Host	Port
RabbitMQ	169.254.92.103	5671
Eridanis	127.0.0.1	3000
Electra	127.0.0.1	3002
Enif	127.0.0.1	3003
Attack Path	127.0.0.1	4242
Health Check	127.0.0.1	3006

	DNS name or IP
Kapteyn	

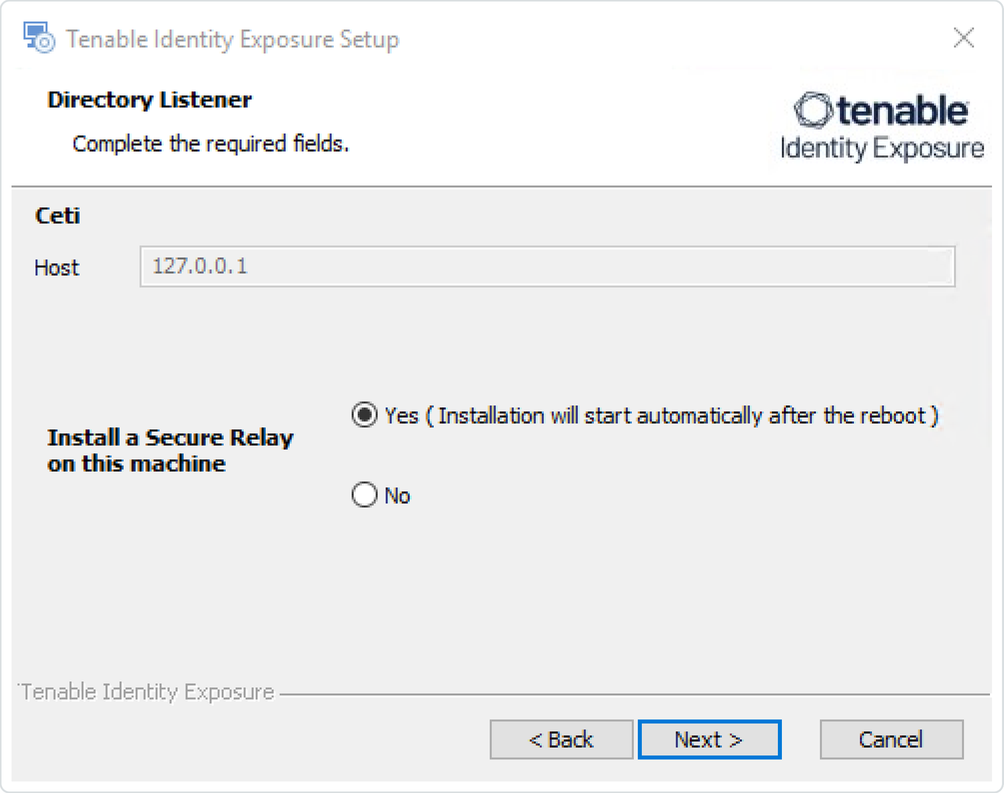
10. Click **Next**.

    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.


Tenable Identity Exposure Setup

Directory Listener

Complete the required fields.

Ceti

Host: 127.0.0.1

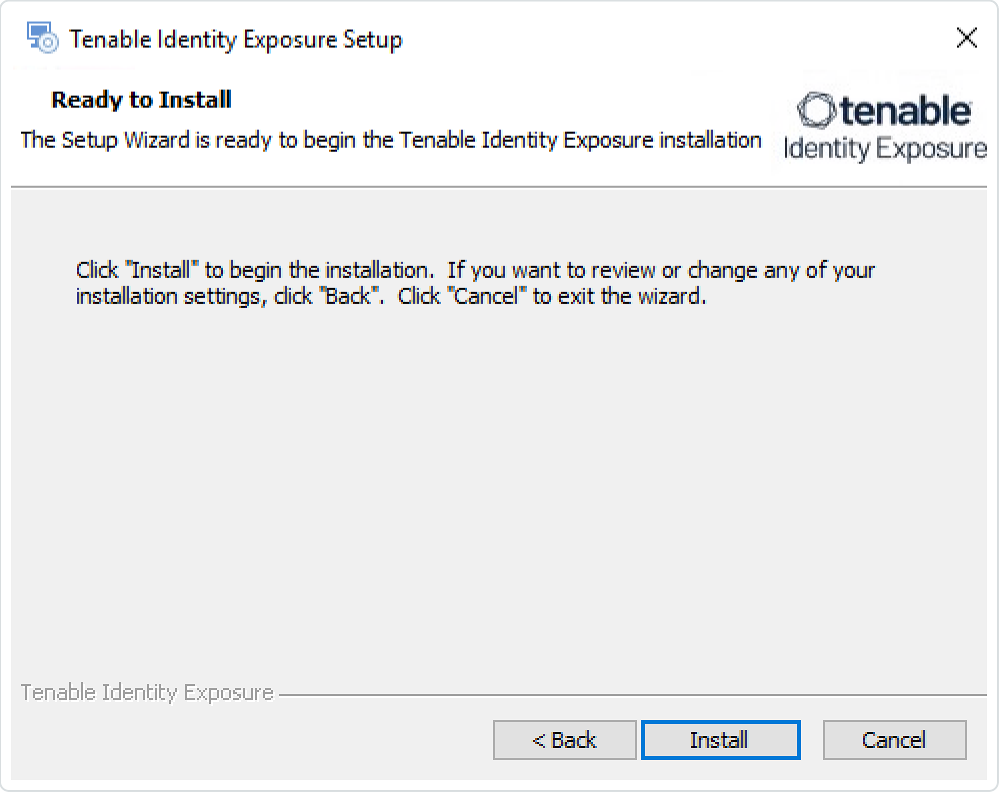
Install a Secure Relay on this machine

● Yes (Installation will start automatically after the reboot)

○ No

12. Click **Next**.

    The **Ready to Install** window appears.



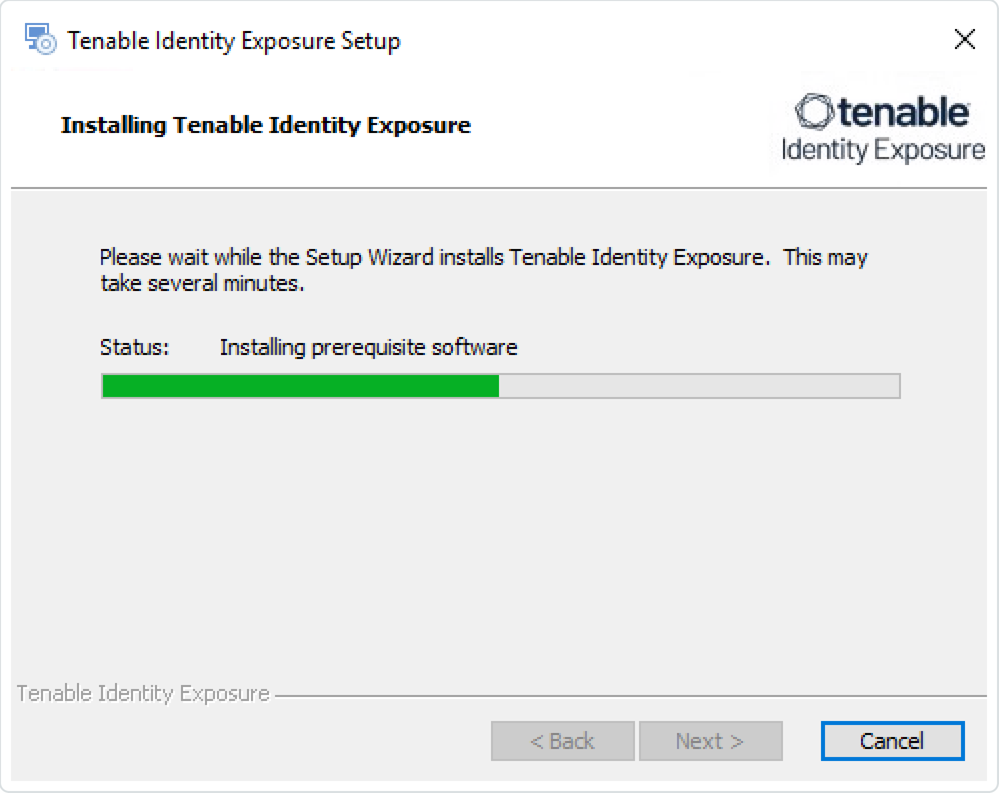
Tenable Identity Exposure Setup

Ready to Install

The Setup Wizard is ready to begin the Tenable Identity Exposure installation

Click "Install" to begin the installation. If you want to review or change any of your installation settings, click "Back". Click "Cancel" to exit the wizard.

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



Tenable Identity Exposure Setup

Installing Tenable Identity Exposure

Please wait while the Setup Wizard installs Tenable Identity Exposure. This may take several minutes.

Status: Installing prerequisite software

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 3.77 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 3.77.

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 **3.77** 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 3.77
- Manual installation of Secure Relay for Tenable Identity Exposure 3.77 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:

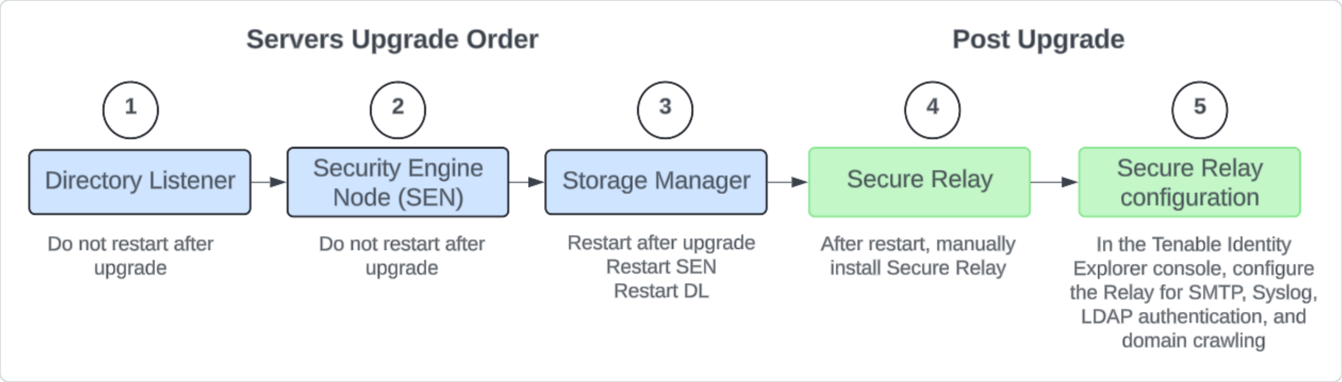
- 2.7 -> 3.1 -> 3.11 -> 3.19 -> 3.29 -> 3.42 -> 3.77.
- 3.x -> 3.59 -> 3.77.

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

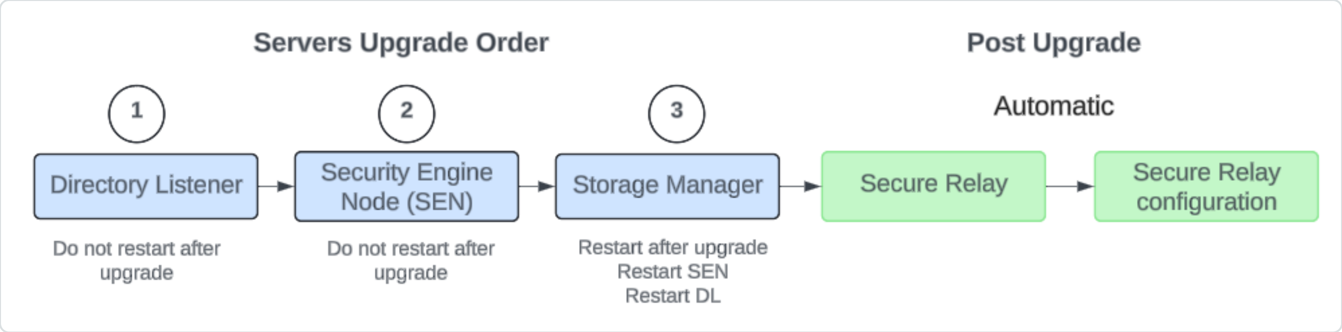
Note: You can upgrade to the next major release from any minor release.

Upgrade Order

- From **Tenable Identity Exposure 3.42** to **3.77**, proceed in the following order:


Servers Upgrade Order
Post Upgrade
1
Directory Listener
Do not restart after upgrade
2
Security Engine Node (SEN)
Do not restart after upgrade
3
Storage Manager
Restart after upgrade
Restart SEN
Restart DL
4
Secure Relay
After restart, manually install Secure Relay
5
Secure Relay configuration
In the Tenable Identity Explorer console, configure the Relay for SMTP, Syslog, LDAP authentication, and domain crawling

- From **Tenable Identity Exposure 3.59** to **3.77**, 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 an administrator on the local machine.

- **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.

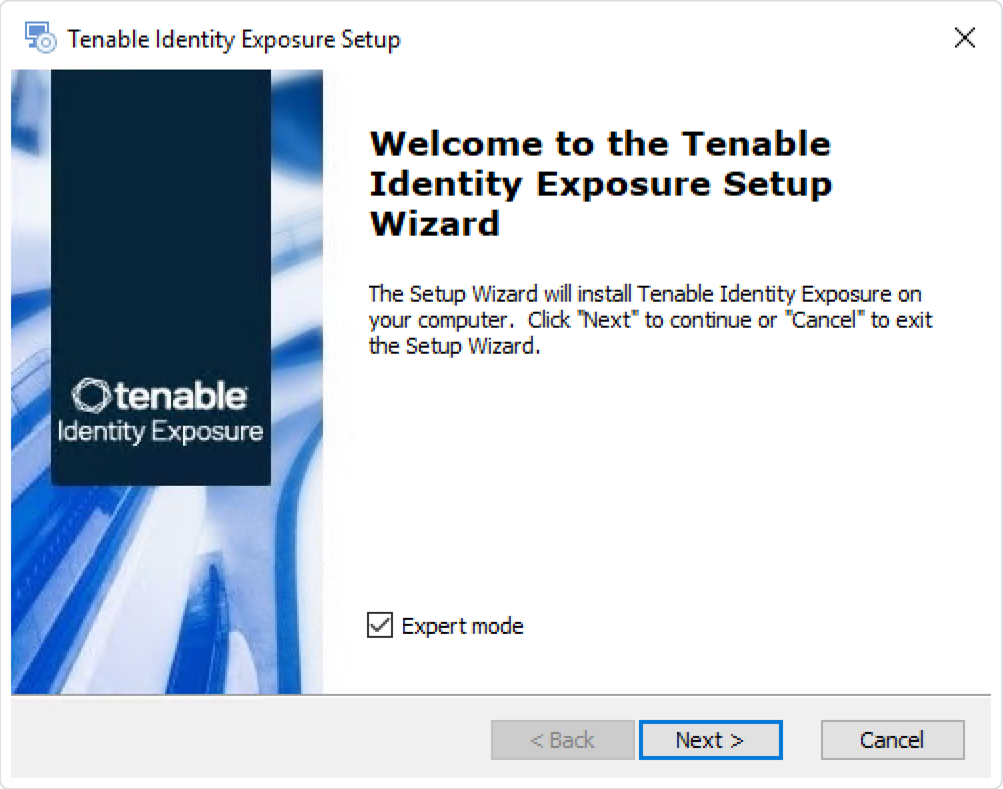
To upgrade the Directory Listener:

1. On the local machine, restart the server and run the **Tenable Identity Exposure 3.77** 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.



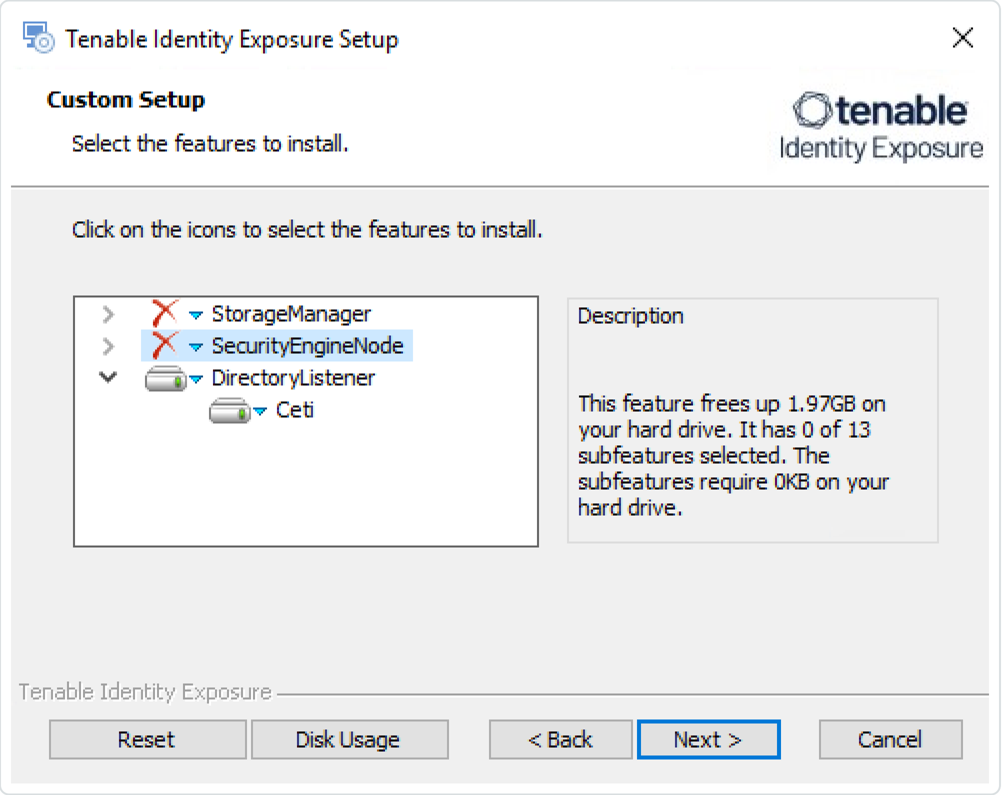
Welcome to the Tenable Identity Exposure Setup Wizard

The Setup Wizard will install Tenable Identity Exposure on your computer. Click "Next" to continue or "Cancel" to exit the Setup Wizard.

☑ Expert mode

3. Click **Next**.

   The **Custom Setup** window appears.



Tenable Identity Exposure Setup

Custom Setup

Select the features to install.

Click on the icons to select the features to install.

- StorageManager
- SecurityEngineNode
- DirectoryListener
  - Ceti

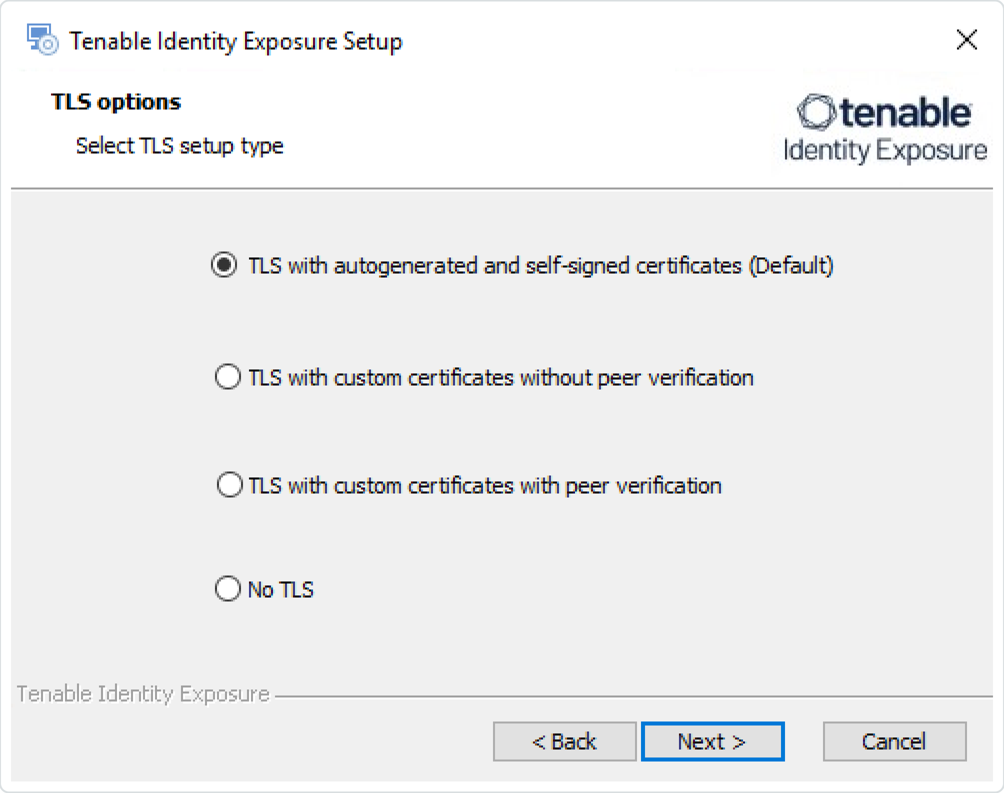
Description

This feature frees up 1.97GB on your hard drive. It has 0 of 13 subfeatures selected. The subfeatures require 0KB on your hard drive.

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.



Tenable Identity Exposure Setup

TLS options

Select TLS setup type

● TLS with autogenerated and self-signed certificates (Default)

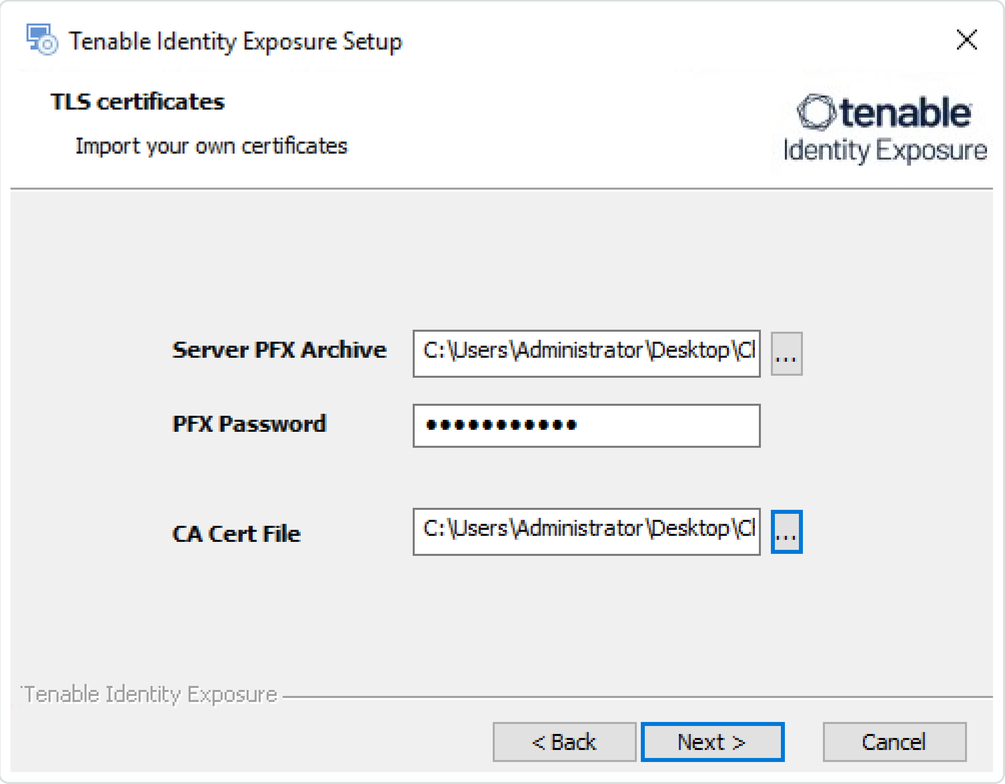
○ TLS with custom certificates without peer verification

○ TLS with custom certificates with peer verification

○ No TLS

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.



TLS certificates

Import your own certificates

Server PFX Archive: C:\Users\Administrator\Desktop\Cl

PFX Password: ●●●●●●●●●●●

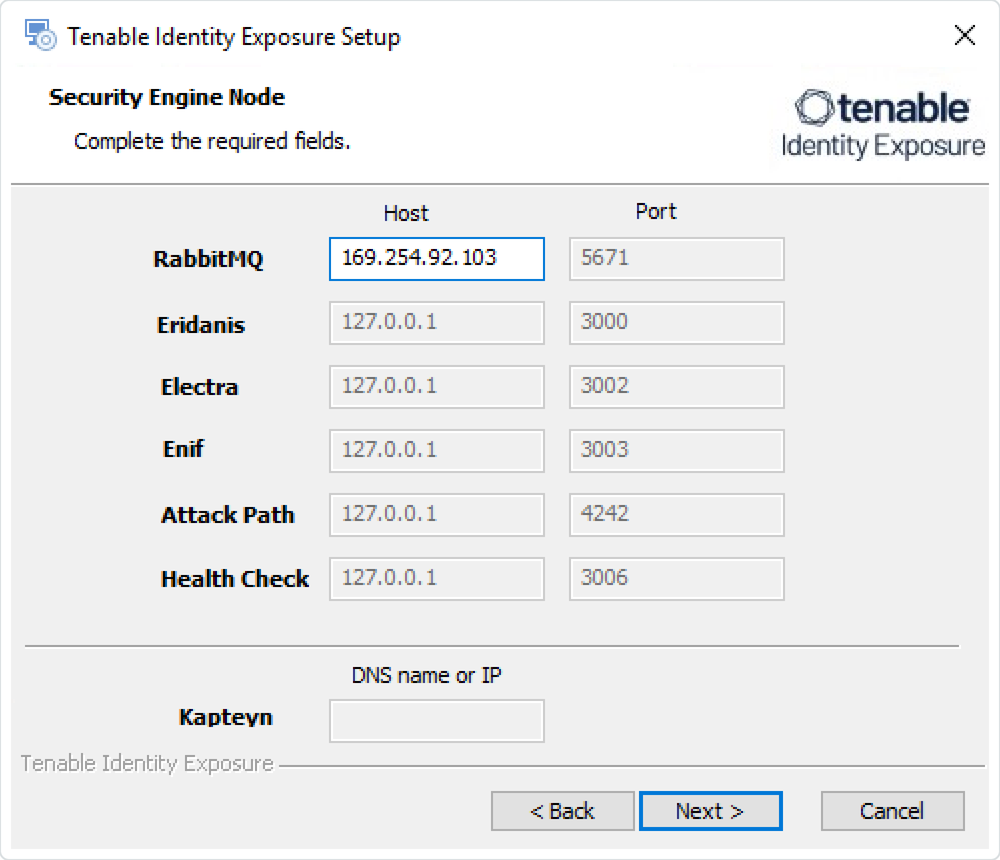
CA Cert File: C:\Users\Administrator\Desktop\Cl

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.



Tenable Identity Exposure Setup

Security Engine Node

Complete the required fields.

	Host	Port
RabbitMQ	169.254.92.103	5671
Eridanis	127.0.0.1	3000
Electra	127.0.0.1	3002
Enif	127.0.0.1	3003
Attack Path	127.0.0.1	4242
Health Check	127.0.0.1	3006

	DNS name or IP
Kapteyn	

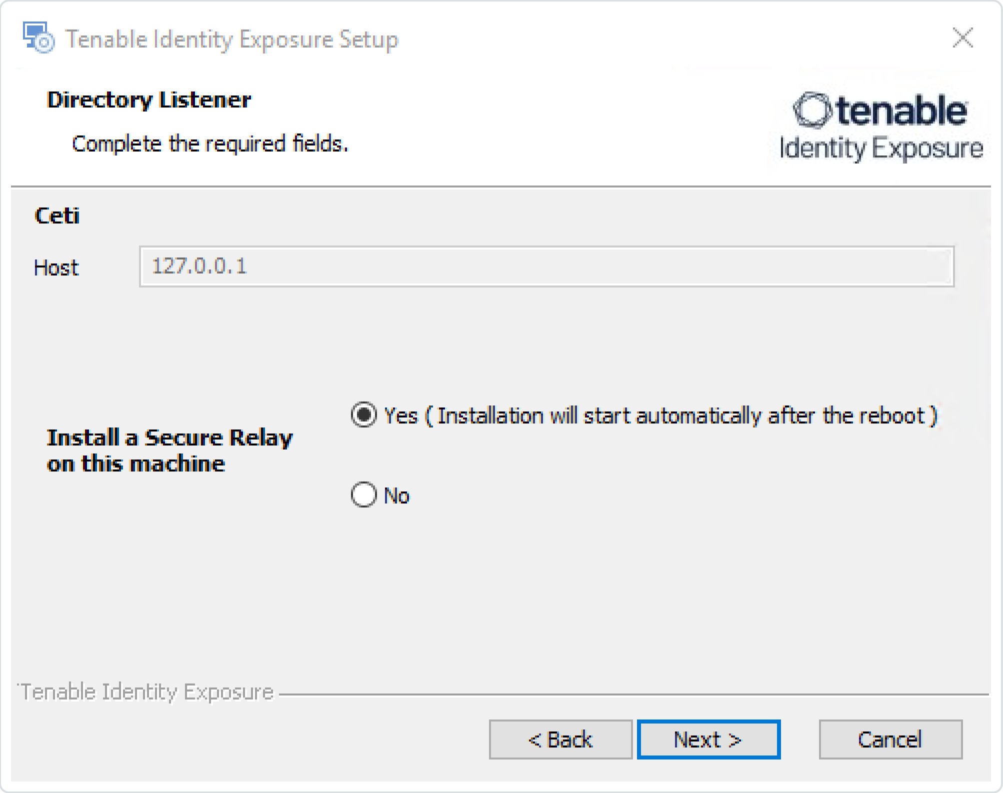
8. Click **Next**.

   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.



Tenable Identity Exposure Setup

Directory Listener

Complete the required fields.

Ceti

Host: 127.0.0.1

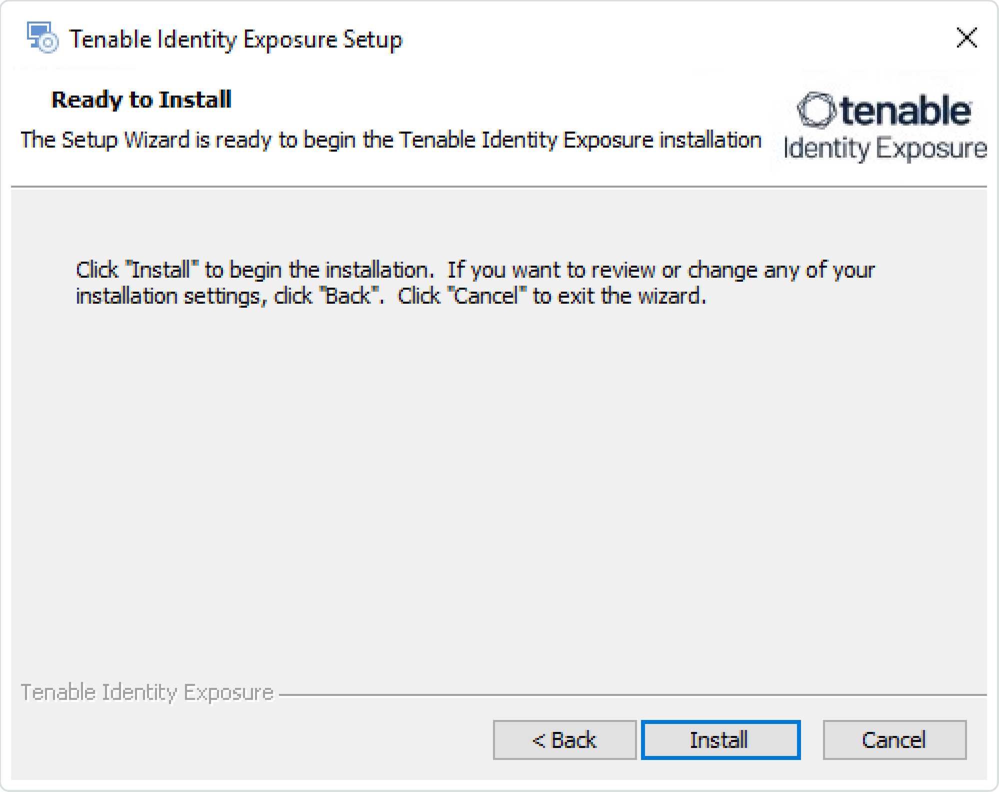
Install a Secure Relay on this machine

● Yes (Installation will start automatically after the reboot)

○ No

10. Click **Next**.

    The **Ready to Install** window appears.



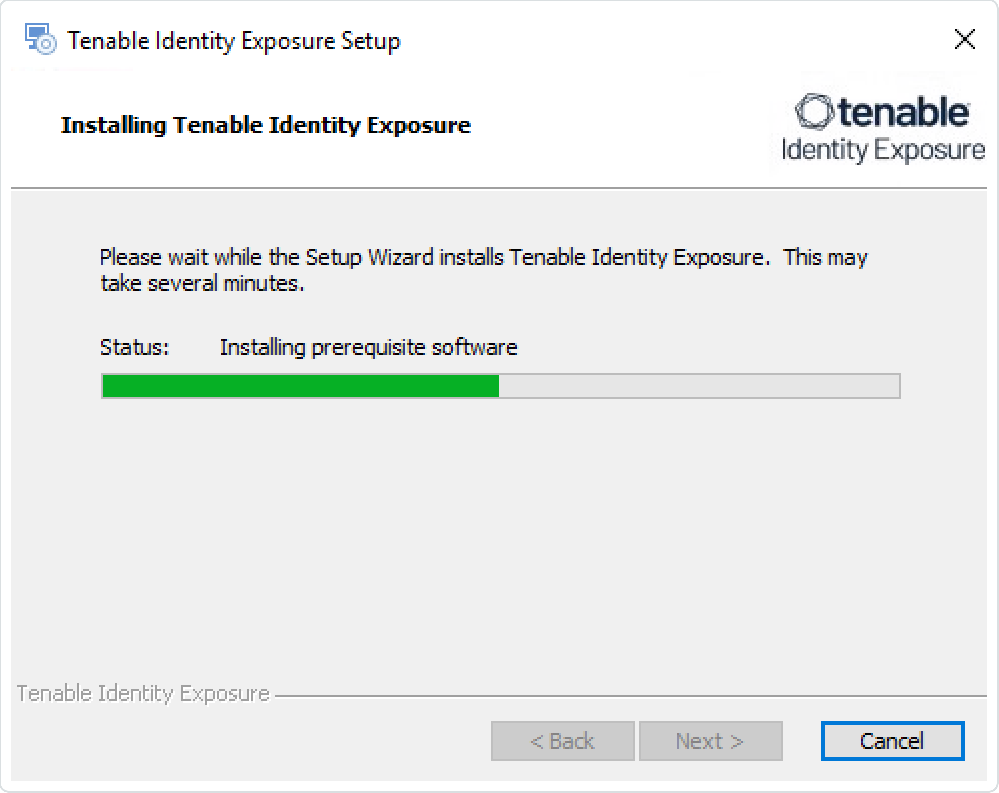
Tenable Identity Exposure Setup

Ready to Install

The Setup Wizard is ready to begin the Tenable Identity Exposure installation

Click "Install" to begin the installation. If you want to review or change any of your installation settings, click "Back". Click "Cancel" to exit the wizard.

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



Tenable Identity Exposure Setup

Installing Tenable Identity Exposure

Please wait while the Setup Wizard installs Tenable Identity Exposure. This may take several minutes.

Status: Installing prerequisite software

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).

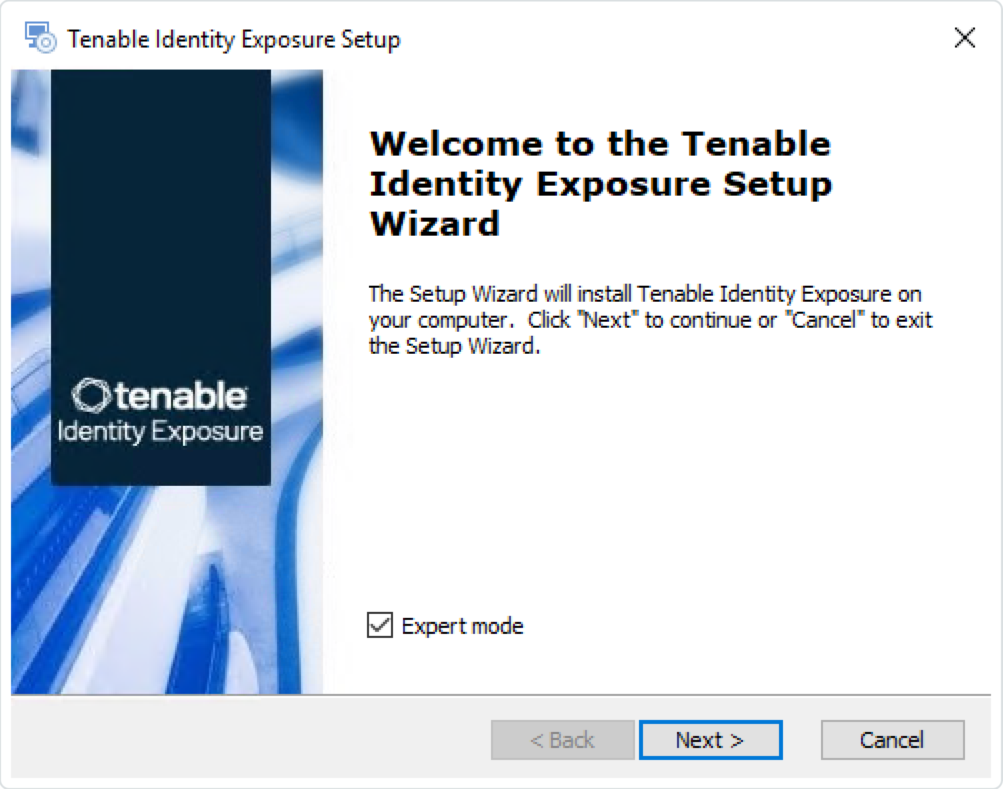
To upgrade the SEN:

1. On the local machine, restart the server and run the **Tenable Identity Exposure 3.77** 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.



Tenable Identity Exposure Setup

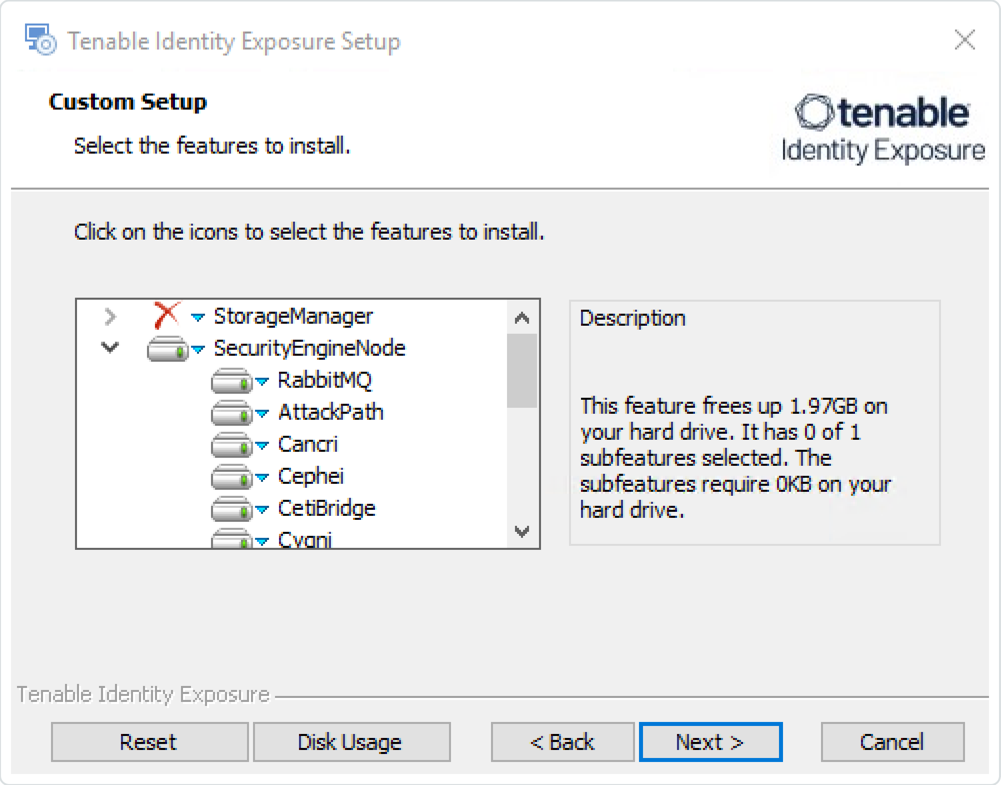
Welcome to the Tenable Identity Exposure Setup Wizard

The Setup Wizard will install Tenable Identity Exposure on your computer. Click "Next" to continue or "Cancel" to exit the Setup Wizard.

☑ Expert mode

3. Click **Next**.

   The **Custom Setup** window appears.



Custom Setup

Select the features to install.

Click on the icons to select the features to install.

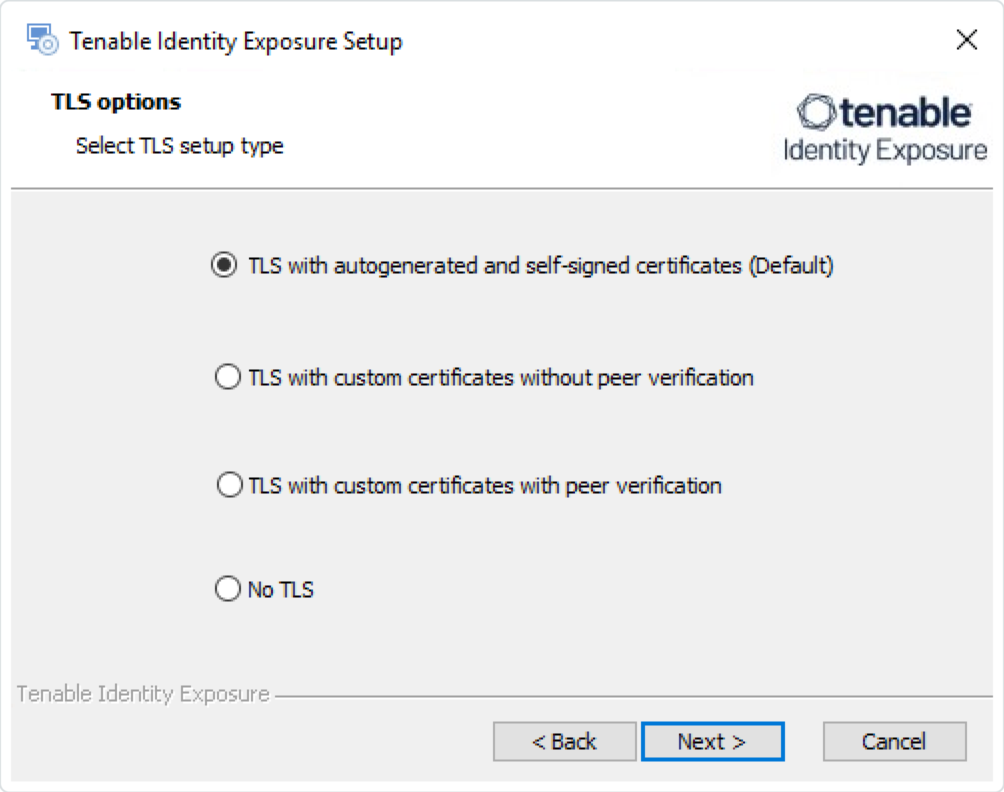
Description

This feature frees up 1.97GB on your hard drive. It has 0 of 1 subfeatures selected. The subfeatures require 0KB on your hard drive.

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.



TLS options

Select TLS setup type

● TLS with autogenerated and self-signed certificates (Default)

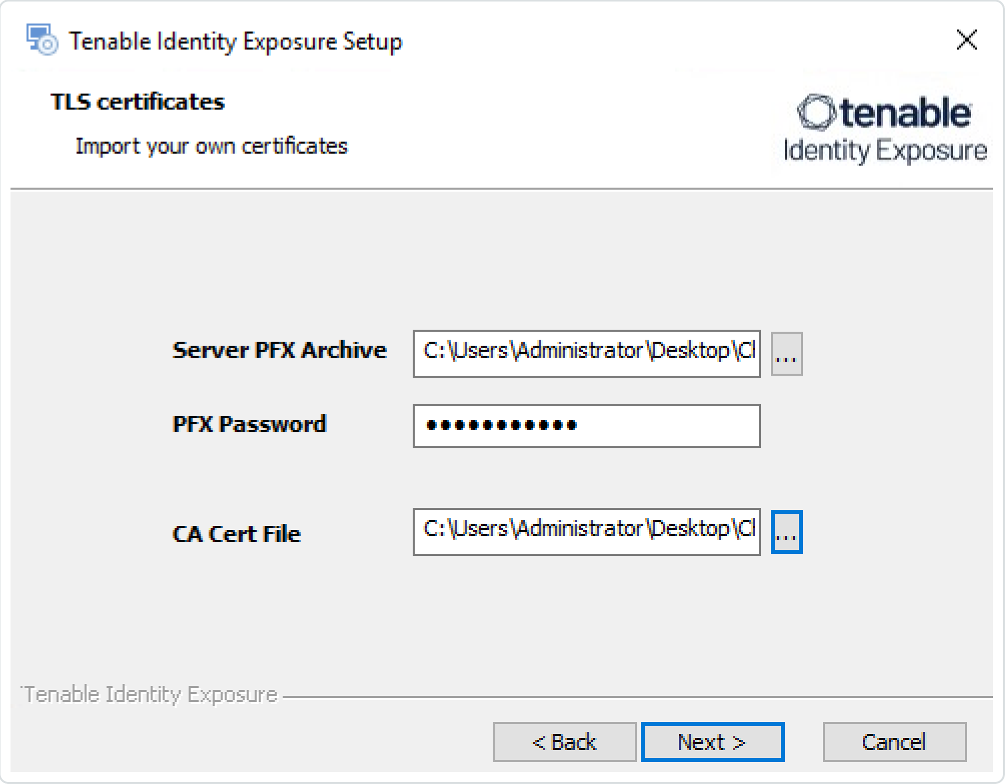
○ TLS with custom certificates without peer verification

○ TLS with custom certificates with peer verification

○ No TLS

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.



Tenable Identity Exposure Setup

TLS certificates

Import your own certificates

Server PFX Archive: C:\Users\Administrator\Desktop\Cl

PFX Password: ●●●●●●●●●●●

CA Cert File: C:\Users\Administrator\Desktop\Cl

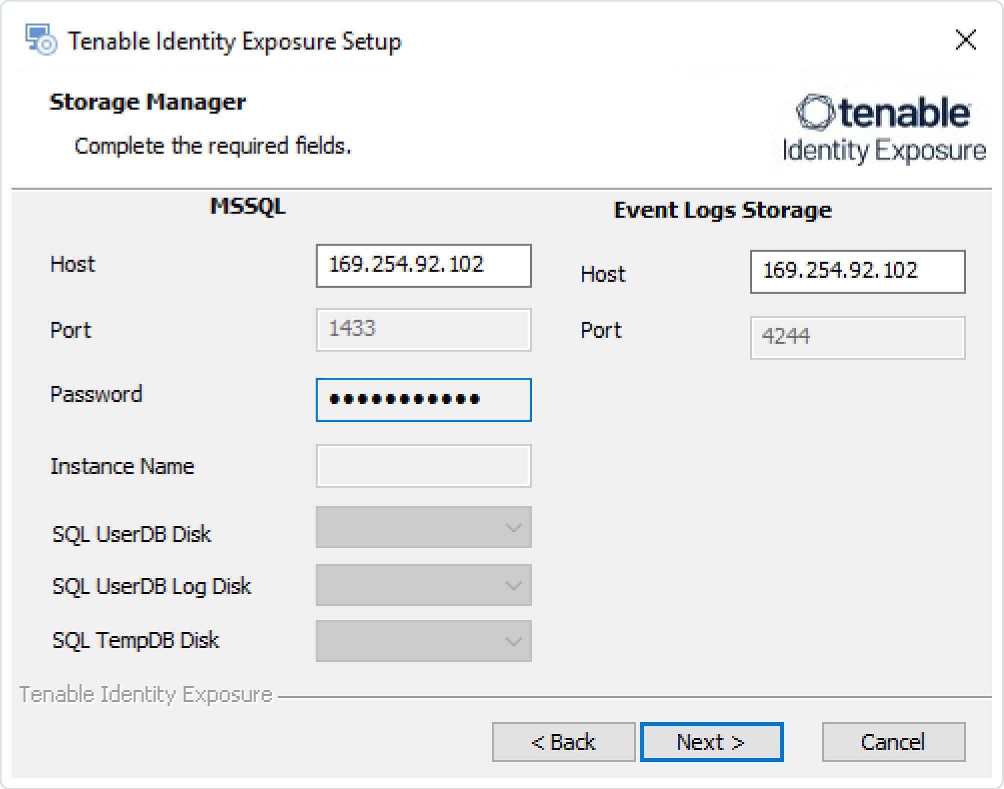
6. Click **Next**.

   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.



Tenable Identity Exposure Setup

Storage Manager

Complete the required fields.

MSSQL

Host: 169.254.92.102

Port: 1433

Password: ••••••••••••

Instance Name:

SQL UserDB Disk:

SQL UserDB Log Disk:

SQL TempDB Disk:

Event Logs Storage

Host: 169.254.92.102

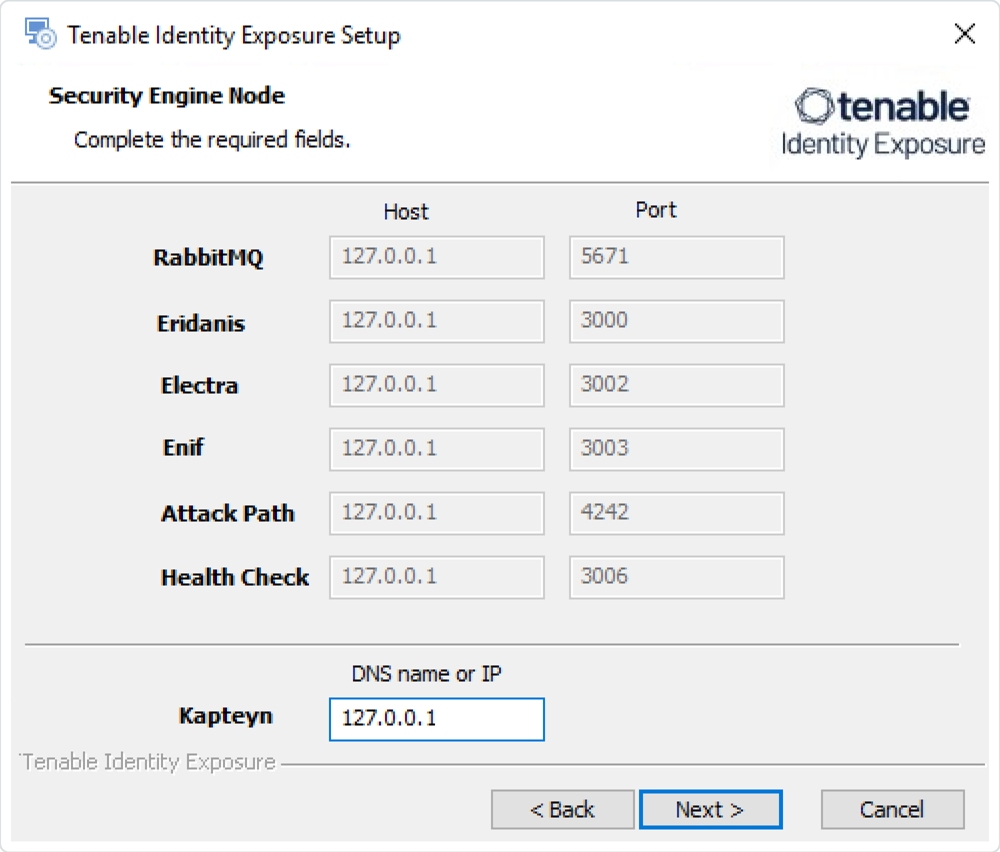
Port: 4244

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.



Security Engine Node

Complete the required fields.

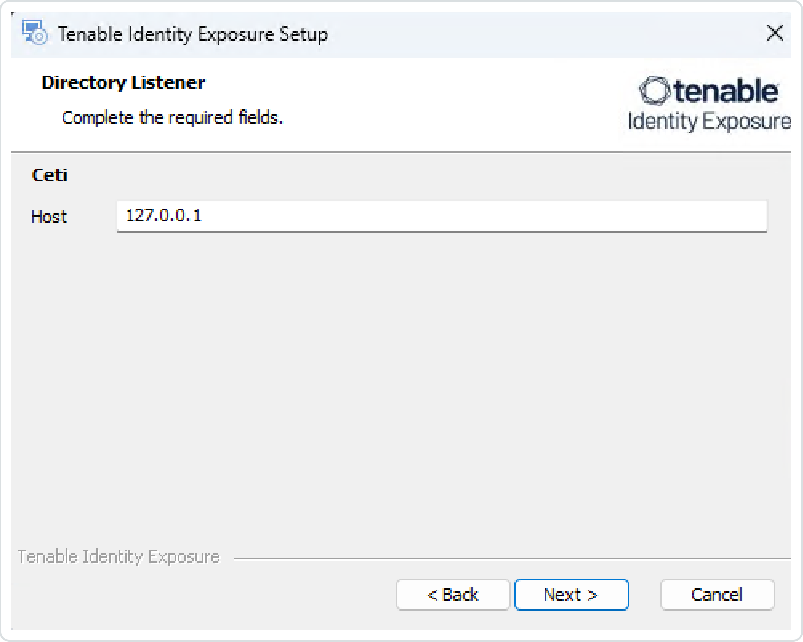
	Host	Port
RabbitMQ	127.0.0.1	5671
Eridanis	127.0.0.1	3000
Electra	127.0.0.1	3002
Enif	127.0.0.1	3003
Attack Path	127.0.0.1	4242
Health Check	127.0.0.1	3006

	DNS name or IP
Kapteyn	127.0.0.1

10. Click **Next**.

    The **Directory Listener** window appears.

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



Directory Listener

Complete the required fields.

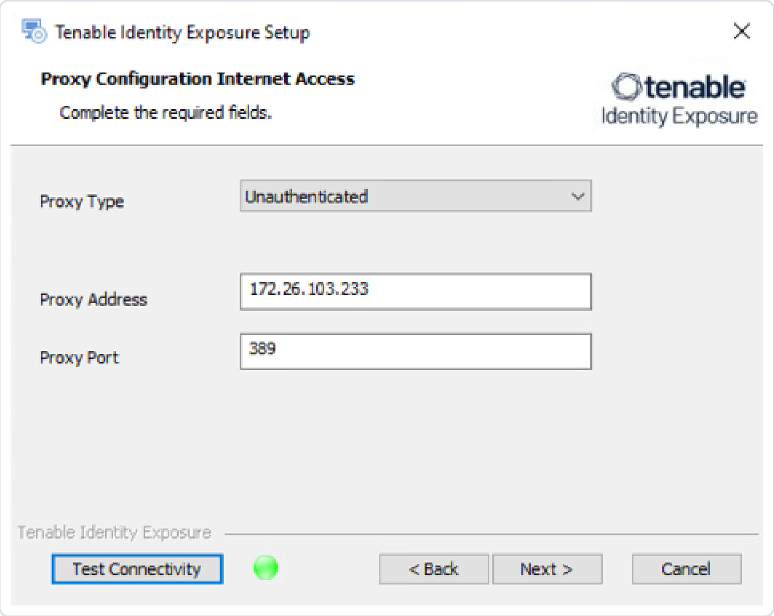
Ceti

Host 127.0.0.1

The **Proxy Configuration** window appears.

12. You have the following proxy types:

   - **None**: Select "None" from the drop-down list box and click **Next**.
   - **Unauthenticated:** Select "Unauthenticated" from the drop-down list box.
     - In the boxes **Proxy Address** and **Proxy Port,** enter the address and port of your proxy server.

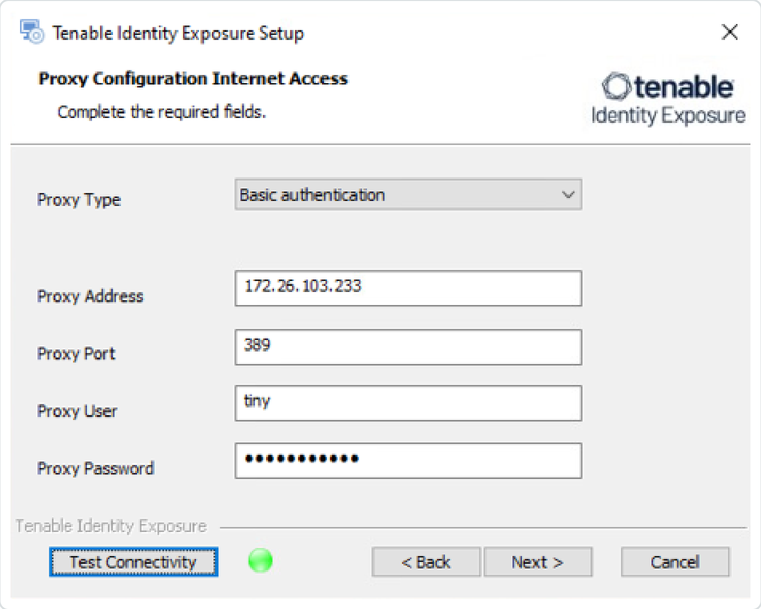

Tenable Identity Exposure Setup
Proxy Configuration Internet Access
Complete the required fields.
tenable Identity Exposure
Tenable Identity Exposure
Test Connectivity
< Back
Next >
Cancel

Proxy Type: Unauthenticated

Proxy Address: 172.26.103.233

Proxy Port: 389

- ○ **Basic Authentication**: Select "Basic authentication" from the drop-down list box.
  - In the boxes **Proxy Address** and **Proxy Port,** type the address and port of your proxy server.
  - In the box **Proxy User** and **Proxy Password**, type the name of the specific user account authorized to access a proxy server and the associated credential to allow requests through the proxy server.


Tenable Identity Exposure Setup
Proxy Configuration Internet Access
Complete the required fields.
tenable Identity Exposure
Tenable Identity Exposure
Test Connectivity
< Back
Next >
Cancel

Proxy Type: Basic authentication

Proxy Address: 172.26.103.233

Proxy Port: 389

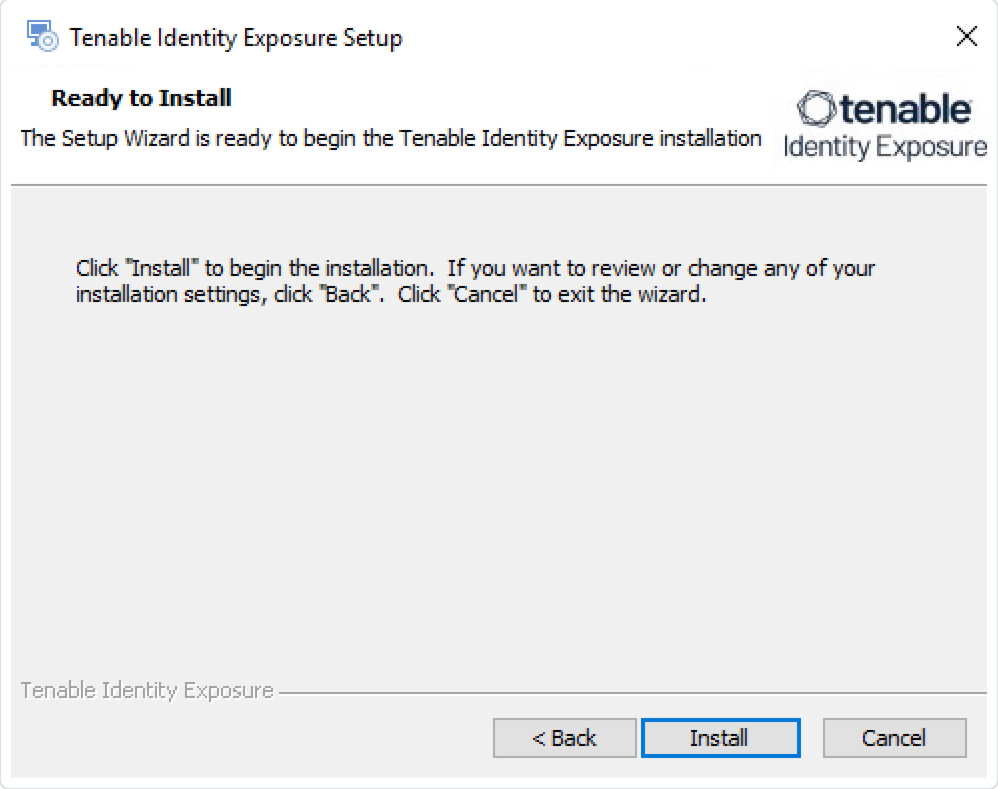
Proxy User: tiny

Proxy Password: ●●●●●●●●●●●●

13. Click **Test Connectivity**.

14. Click **Next**.

    The **Ready to Install** window appears.

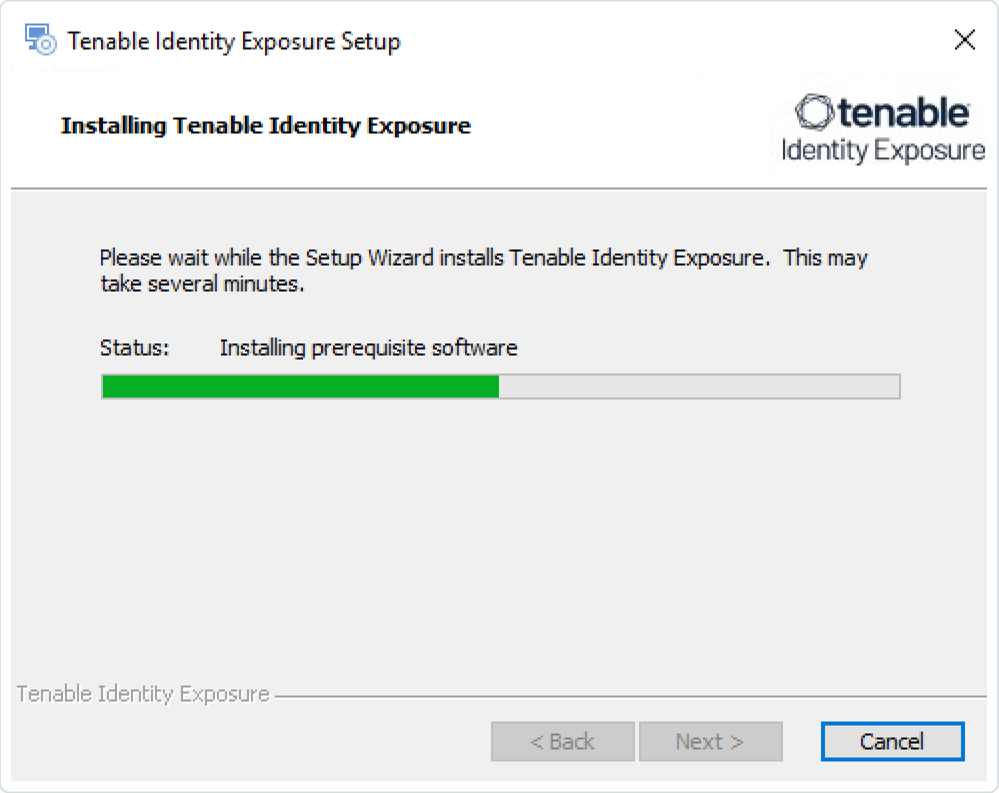
    Tenable Identity Exposure Setup

    Ready to Install

    The Setup Wizard is ready to begin the Tenable Identity Exposure installation

    Click "Install" to begin the installation. If you want to review or change any of your installation settings, click "Back". Click "Cancel" to exit the wizard.

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



Tenable Identity Exposure Setup

Installing Tenable Identity Exposure

Please wait while the Setup Wizard installs Tenable Identity Exposure. This may take several minutes.

Status: Installing prerequisite software

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

16. Click **Finish**.

    A dialog box asks you to restart your machine.

17. Click **No**.

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

18. Upgrade the Storage Manager.

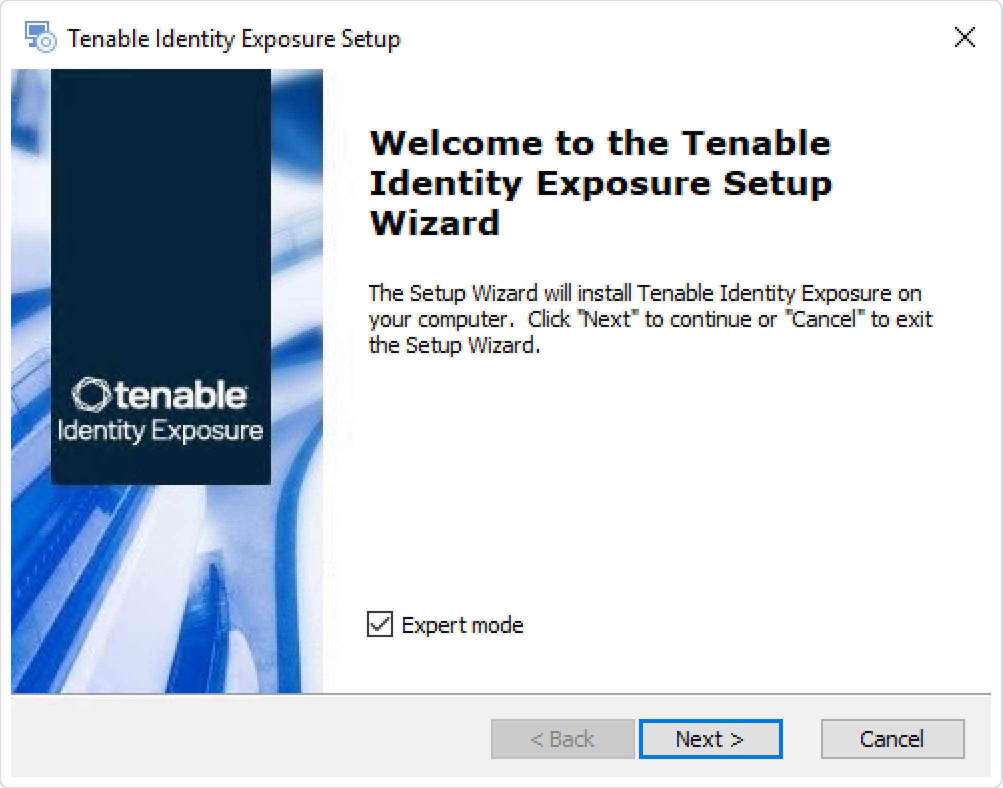
To upgrade the Storage Manager:

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.



Tenable Identity Exposure Setup

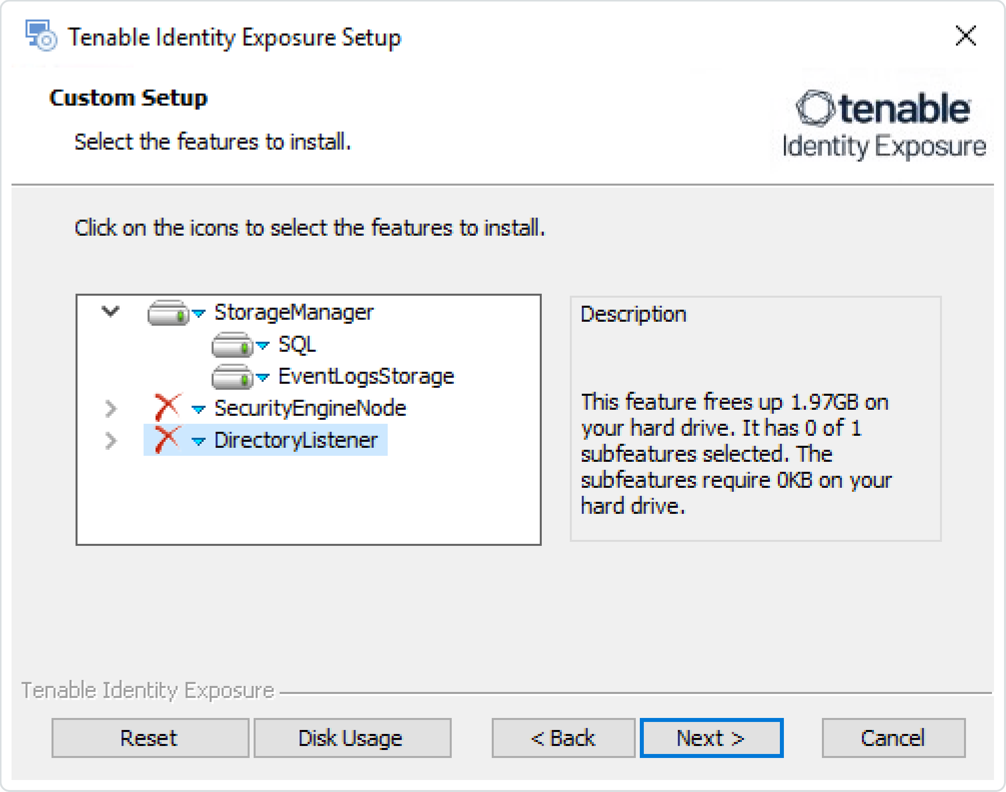
Welcome to the Tenable Identity Exposure Setup Wizard

The Setup Wizard will install Tenable Identity Exposure on your computer. Click "Next" to continue or "Cancel" to exit the Setup Wizard.

☑ Expert mode

3. Click **Next**.

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



Tenable Identity Exposure Setup

Custom Setup

Select the features to install.

Click on the icons to select the features to install.

Description

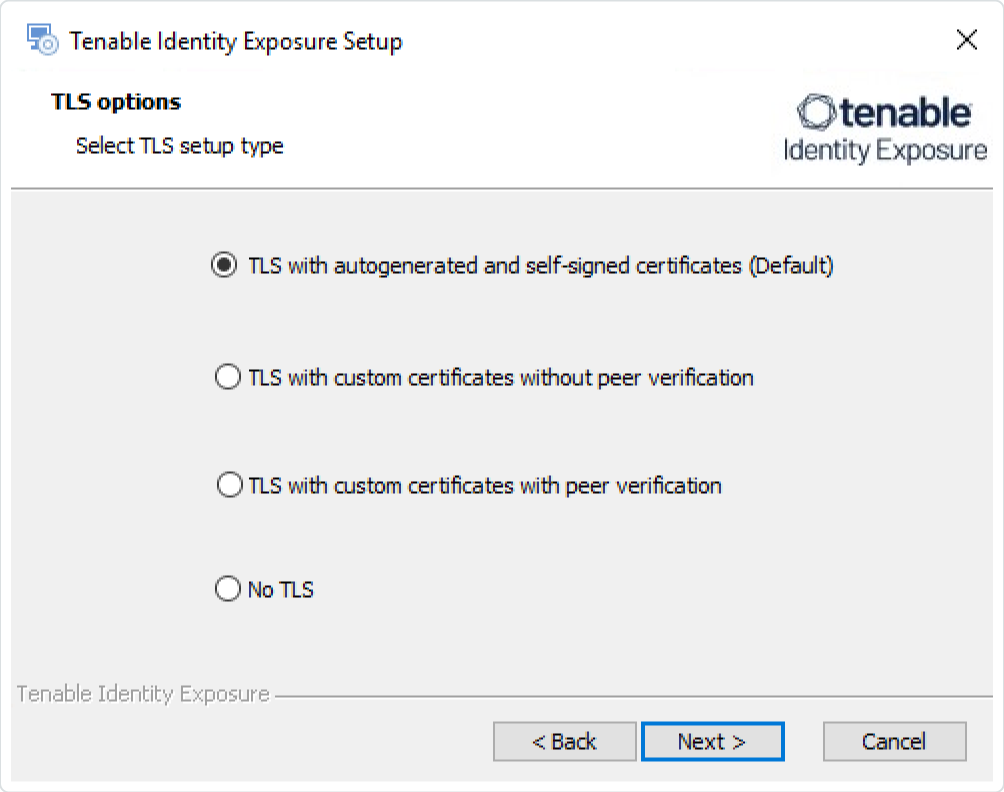
This feature frees up 1.97GB on your hard drive. It has 0 of 1 subfeatures selected. The subfeatures require 0KB on your hard drive.

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.



TLS options

Select TLS setup type

● TLS with autogenerated and self-signed certificates (Default)

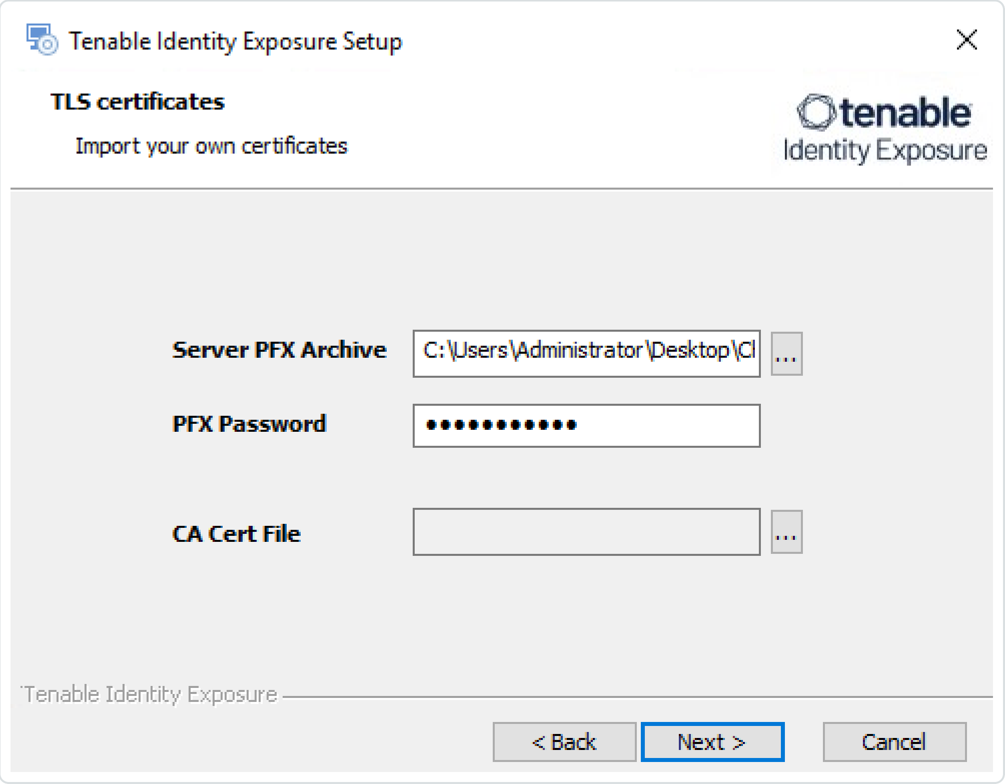
○ TLS with custom certificates without peer verification

○ TLS with custom certificates with peer verification

○ No TLS

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.



Tenable Identity Exposure Setup

TLS certificates

Import your own certificates

Server PFX Archive: C:\Users\Administrator\Desktop\Cl

PFX Password: ●●●●●●●●●●●

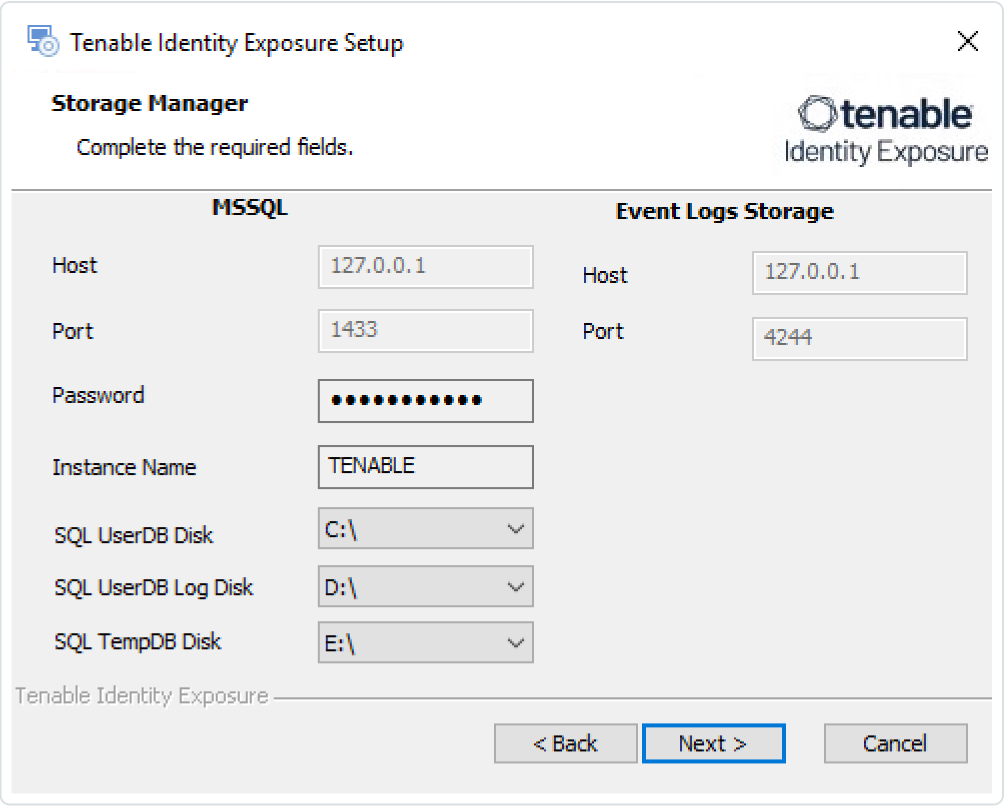
CA Cert File:

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

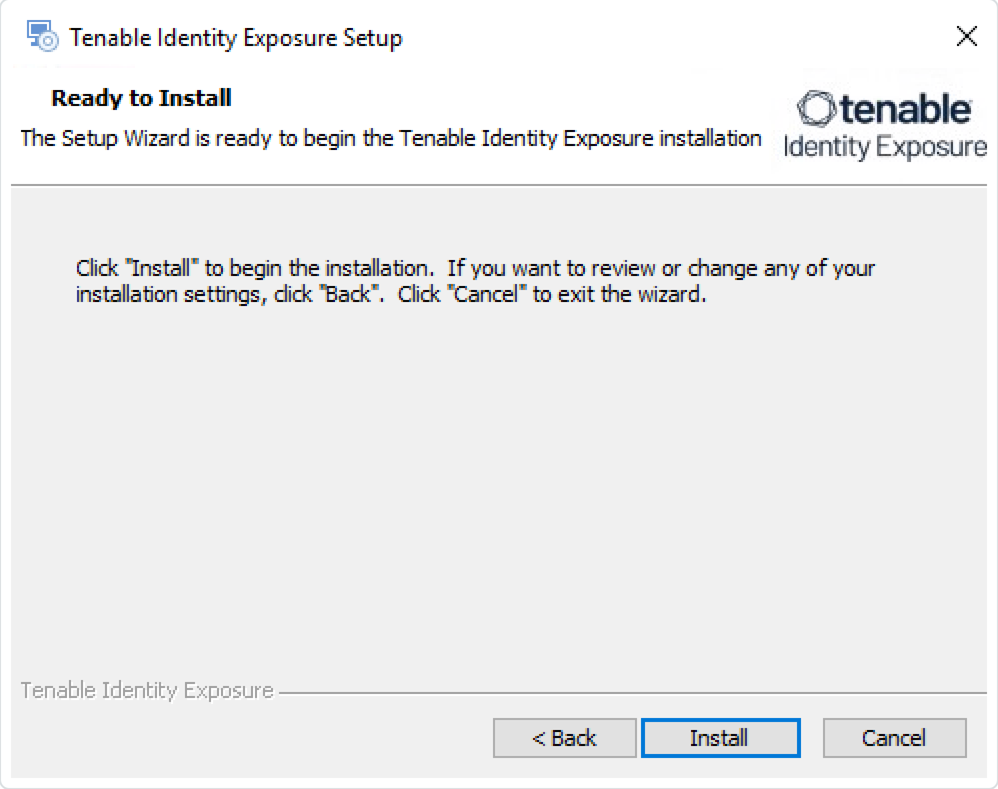
Complete the required fields.

MSSQL	
Host	127.0.0.1
Port	1433
Password	••••••••••••
Instance Name	TENABLE
SQL UserDB Disk	C:\
SQL UserDB Log Disk	D:\
SQL TempDB Disk	E:\

Event Logs Storage	
Host	127.0.0.1
Port	4244

9. Click **Next**.

   The **Ready to Install** window appears.



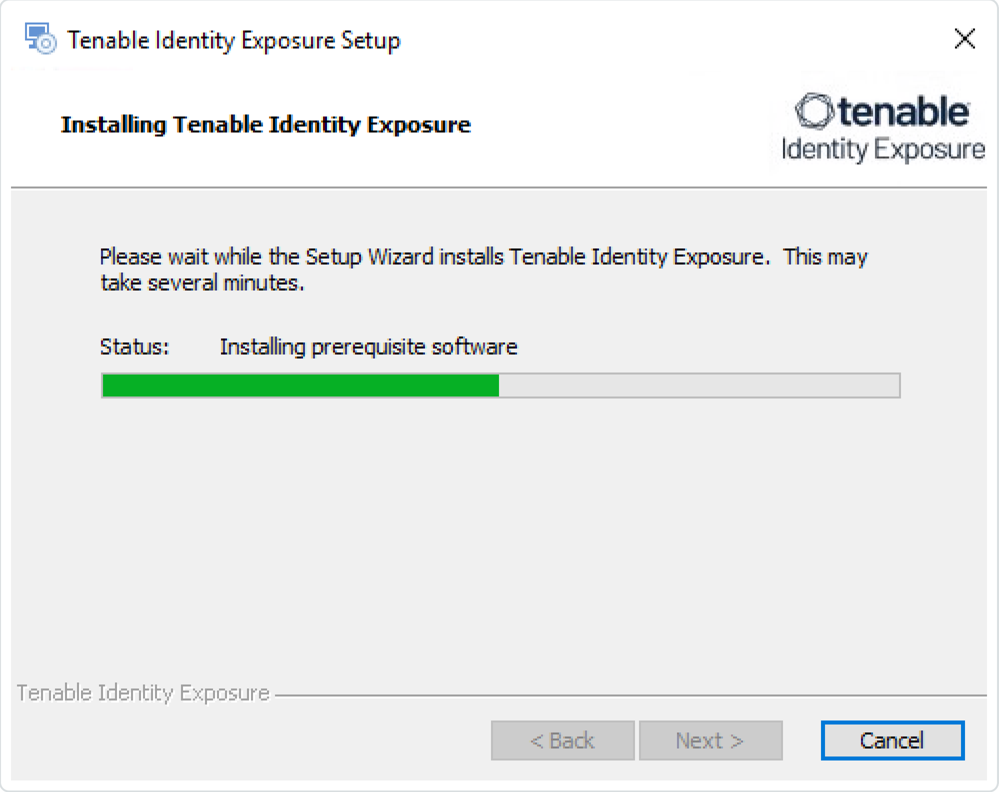
Tenable Identity Exposure Setup

Ready to Install

The Setup Wizard is ready to begin the Tenable Identity Exposure installation

Click "Install" to begin the installation. If you want to review or change any of your installation settings, click "Back". Click "Cancel" to exit the wizard.

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



Tenable Identity Exposure Setup

Installing Tenable Identity Exposure

Please wait while the Setup Wizard installs Tenable Identity Exposure. This may take several minutes.

Status: Installing prerequisite software

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 3.77 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 3.77.

Backups

Regular and dependable backups are crucial for ensuring the availability and integrity of data within the Tenable Identity Exposure application.

Purposes

- **Mitigate Data Loss**: Perform backups in the specified scenarios to mitigate the risk of data loss during upgrades, updates, or system changes.
- **Ensure a smooth recovery process**: Having backups ensures a smooth recovery process in case of unexpected issues during system modifications.

> **Tip**: Regularly monitor the backup process to ensure its effectiveness & perform a periodic test of the restoration process to confirm the integrity of the backup data and its ability to facilitate a successful system recovery.

> **Tip**: It is not required to stop application services when performing a backup.

Backup Type

The following approach ensures a secure and efficient backup strategy aligned with organizational policies.

- Use an image backup (snapshot) as the preferred method in your environment.
- Ensure that the backup captures the entire system state, including application configurations, databases, and associated files.

MSSQL Backup

Refer to Microsoft's documentation.

Backup Frequency

Perform regular backups at least once a month to capture the latest data changes and configurations.

Schedule backups during non-peak hours to minimize impact on system performance and user experience.

For MSSQL, perform regular backups at least once a week to capture the latest data.

Note: Backup of the SQL logs is not required.

Backup Scenarios

- **Tenable Identity Exposure version upgrades** — Before initiating any version upgrades for the Identity Exposure application, conduct reliable backups.
- **OS upgrades or significant updates** — Prior to performing any operating system upgrades or applying significant updates to the host system, ensure dependable backups are in place.
- **Hardware/OS changes to the Tenable Identity Exposure host** — Before making any modifications to the hardware or operating system configurations of the Identity Exposure host, conduct thorough backups.
- **Modifications recommended by Tenable Support** — Execute backups as required before implementing any changes or modifications suggested by Tenable Support for optimal system performance.

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:

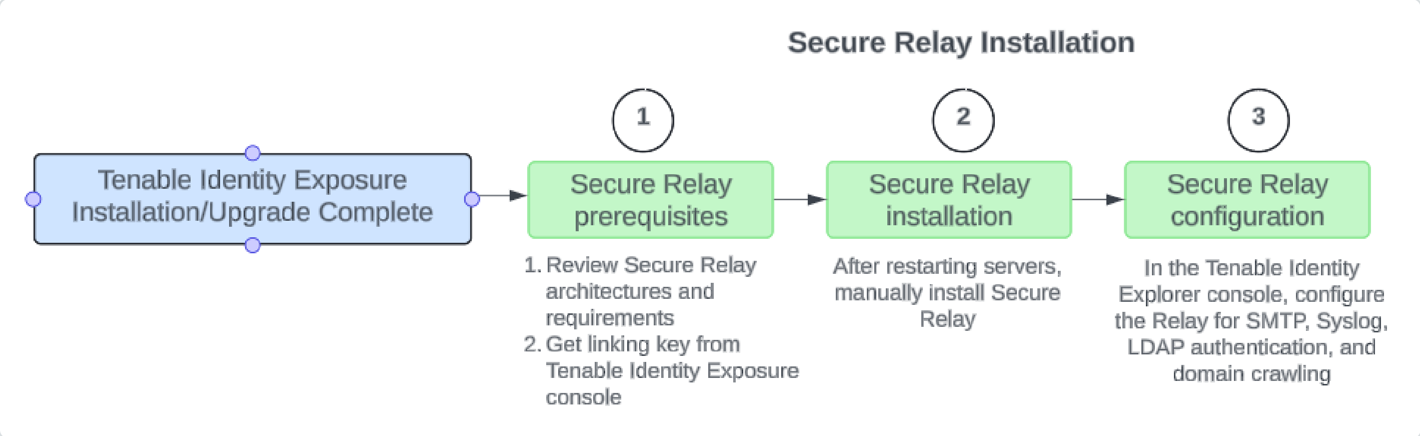
- `Tenable_ceti`
- `tenable_envoy_server`
- `tenable_envoy`
- `tenable_relay`

Secure Relay for Tenable Identity Exposure 3.77

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.


Secure Relay Installation
Tenable Identity Exposure Installation/Upgrade Complete
1
Secure Relay prerequisites
1. Review Secure Relay architectures and requirements
2. Get linking key from Tenable Identity Exposure console
2
Secure Relay installation
After restarting servers, manually install Secure Relay
3
Secure Relay configuration
In the Tenable Identity Explorer console, configure the Relay for SMTP, Syslog, LDAP authentication, and domain crawling

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**:

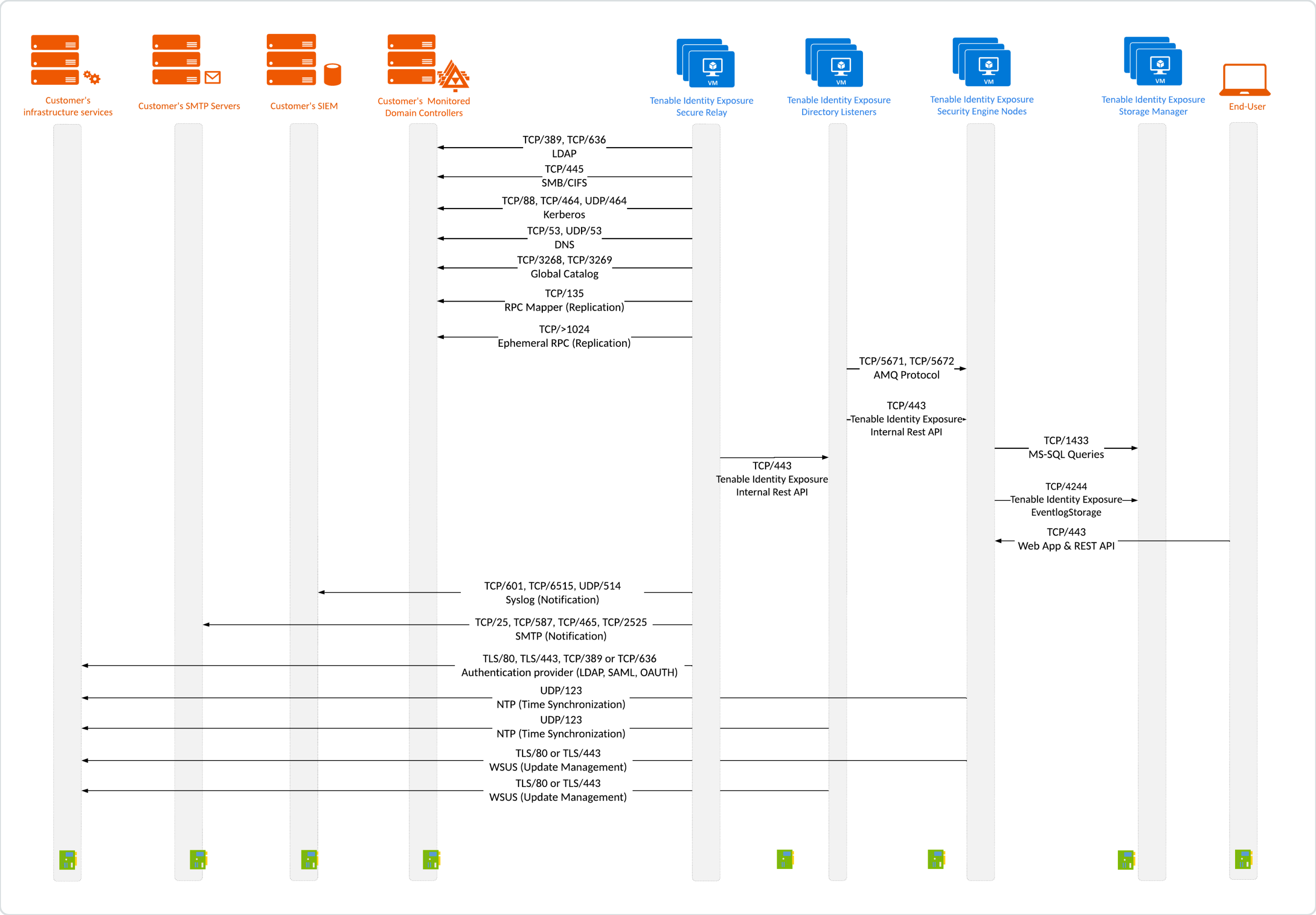
   - In previous and current versions, the DL communicated to the SEN directly, using the AMQP(S) protocol.

   - 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

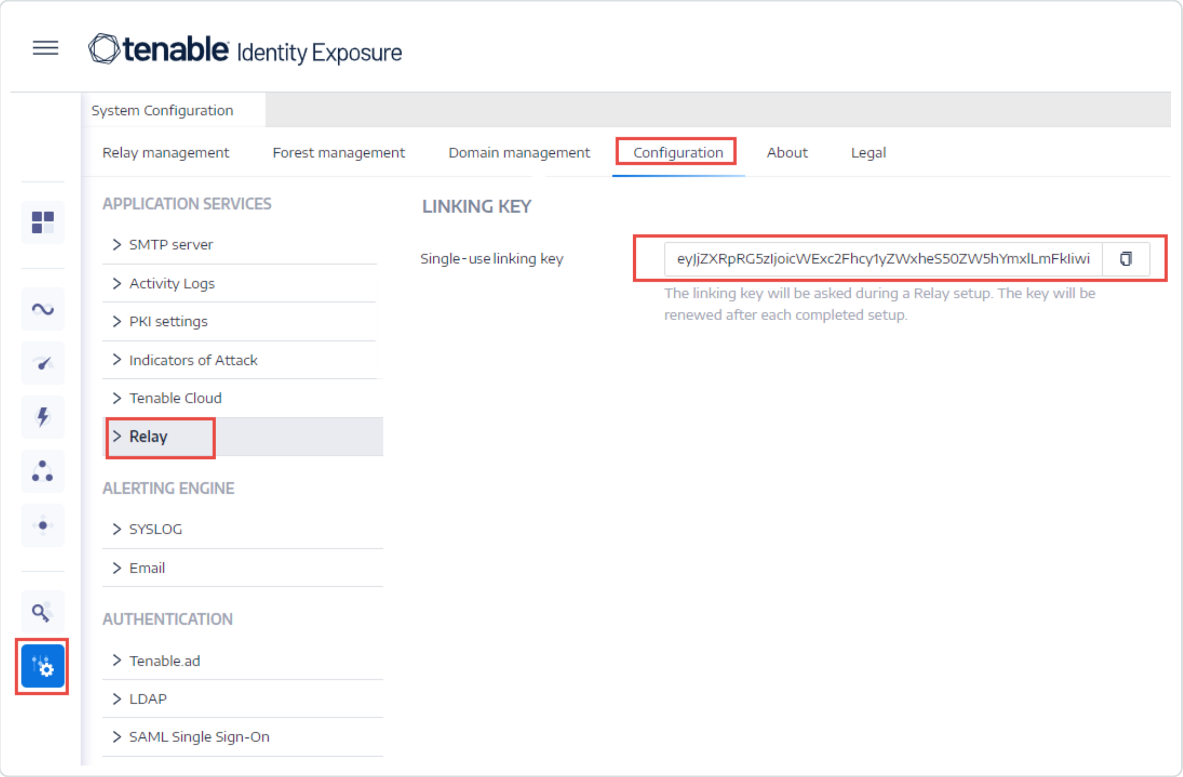
The following are network flows for an On-Premises platform using Secure Relay:


Customer's infrastructure services
Customer's SMTP Servers
Customer's SIEM
Customer's Monitored Domain Controllers
Tenable Identity Exposure Secure Relay
Tenable Identity Exposure Directory Listeners
Tenable Identity Exposure Security Engine Nodes
Tenable Identity Exposure Storage Manager
End-User
TCP/389, TCP/636
LDAP
TCP/445
SMB/CIFS
TCP/88, TCP/464, UDP/464
Kerberos
TCP/53, UDP/53
DNS
TCP/3268, TCP/3269
Global Catalog
TCP/135
RPC Mapper (Replication)
TCP/>1024
Ephemeral RPC (Replication)
TCP/5671, TCP/5672
AMQ Protocol
TCP/443
Tenable Identity Exposure
Internal Rest API
TCP/1433
MS-SQL Queries
TCP/443
Tenable Identity Exposure
Internal Rest API
TCP/4244
Tenable Identity Exposure
EventlogStorage
TCP/443
Web App & REST API
TCP/601, TCP/6515, UDP/514
Syslog (Notification)
TCP/25, TCP/587, TCP/465, TCP/2525
SMTP (Notification)
TLS/80, TLS/443, TCP/389 or TCP/636
Authentication provider (LDAP, SAML, OAUTH)
UDP/123
NTP (Time Synchronization)
UDP/123
NTP (Time Synchronization)
TLS/80 or TLS/443
WSUS (Update Management)
TLS/80 or TLS/443
WSUS (Update Management)

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**.



LINKING KEY

Single-use linking key: eyJjZXRpRG5zIjoicWExc2Fhcy1yZWxheS50ZW5hYmxlLmFkIiwi

The linking key will be asked during a Relay setup. The key will be renewed after each completed setup.

2. Click 🗍 to copy the linking key.

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.

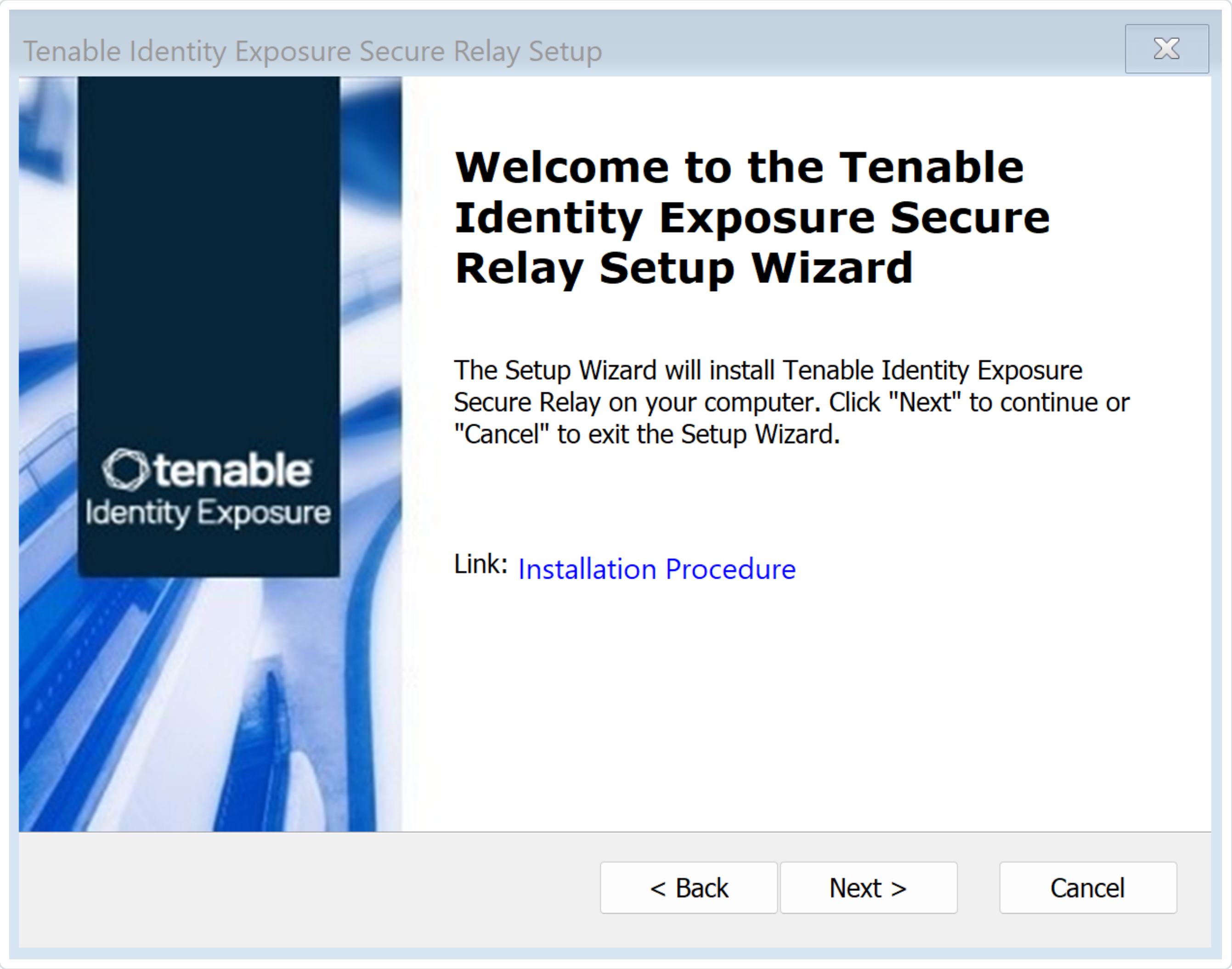
Installation procedure

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.



Tenable Identity Exposure Secure Relay Setup

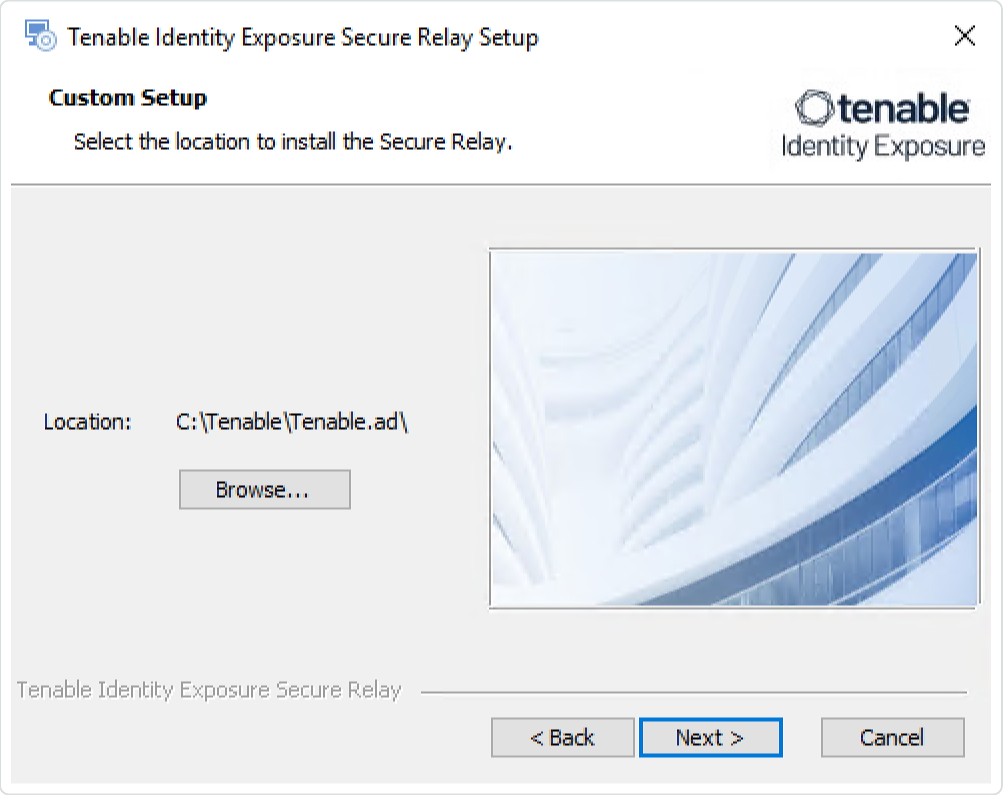
Welcome to the Tenable Identity Exposure Secure Relay Setup Wizard

The Setup Wizard will install Tenable Identity Exposure Secure Relay on your computer. Click "Next" to continue or "Cancel" to exit the Setup Wizard.

Link: Installation Procedure

3. Click **Next**.

   The **Custom Setup** window appears.


Tenable Identity Exposure Secure Relay Setup

Custom Setup

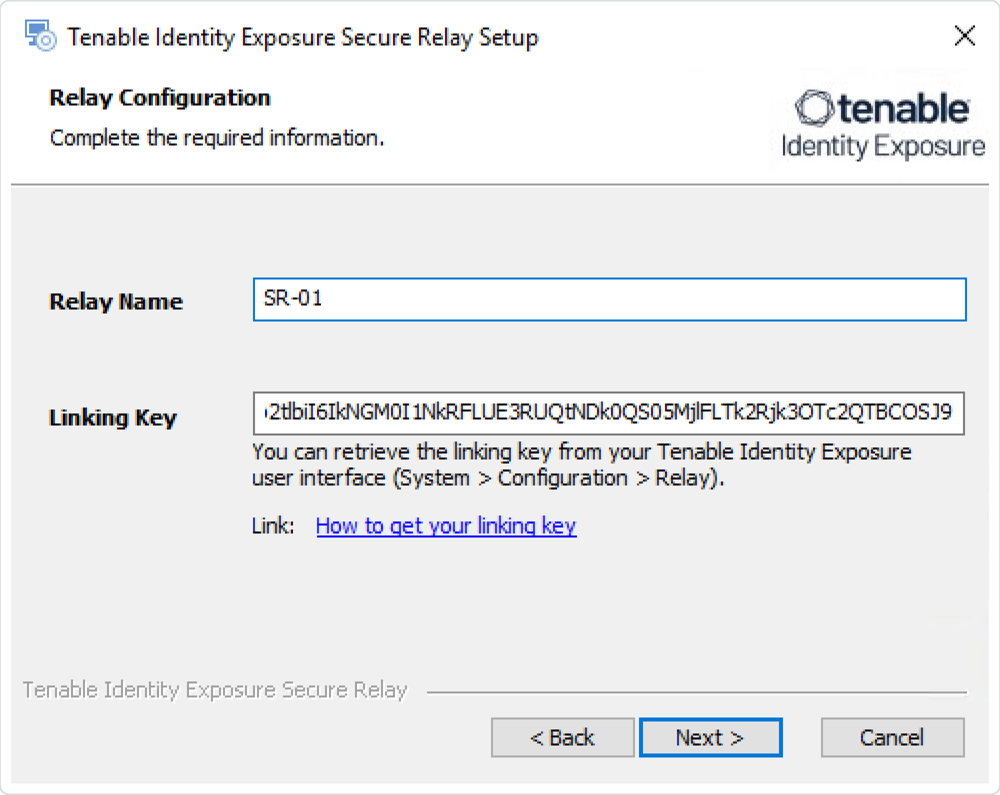
Select the location to install the Secure Relay.

Location: C:\Tenable\Tenable.ad\

4. Click **Browse** to select the disk partition you reserved for Secure Relay (separate from the system partition).

5. Click **Next**.

   The **Relay Configuration** window appears.


Tenable Identity Exposure Secure Relay Setup
tenable
Identity Exposure

Relay Configuration

Complete the required information.

Relay Name SR-01

Linking Key 2tlbiI6IkNGM0I1NkRFLUE3RUQtNDk0QS05MjlFLTk2Rjk3OTc2QTBCOSJ9

You can retrieve the linking key from your Tenable Identity Exposure user interface (System > Configuration > Relay).

Link: How to get your linking key

Tenable Identity Exposure Secure Relay
< Back
Next >
Cancel

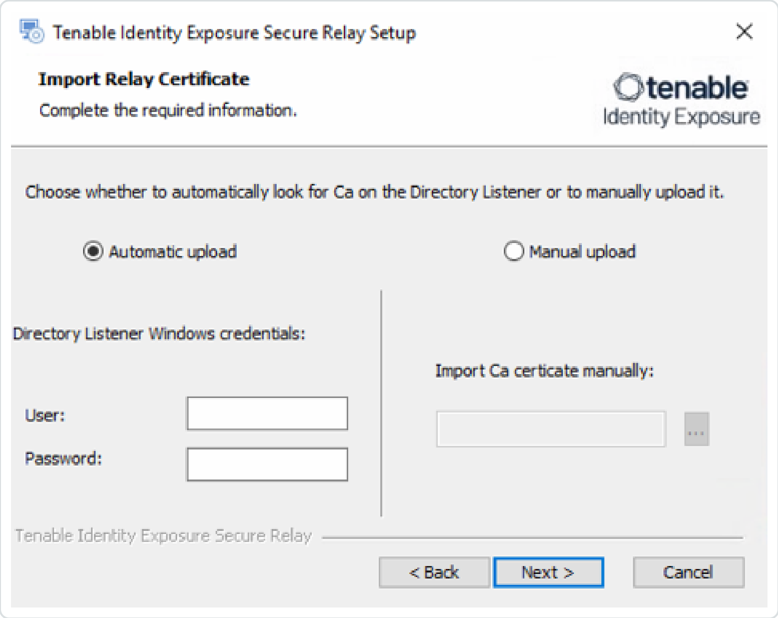
6. Provide the following information:

   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. If you install the Relay on a **separate (standalone) machine** from the Directory Listener: the **Import Relay Certificate** window appears: (if you use the same machine for both the Directory Listener and Relay, go to the next step.)



Tenable Identity Exposure Secure Relay Setup

Import Relay Certificate

Complete the required information.

Choose whether to automatically look for Ca on the Directory Listener or to manually upload it.

● Automatic upload ○ Manual upload

Directory Listener Windows credentials:

User:

Password:

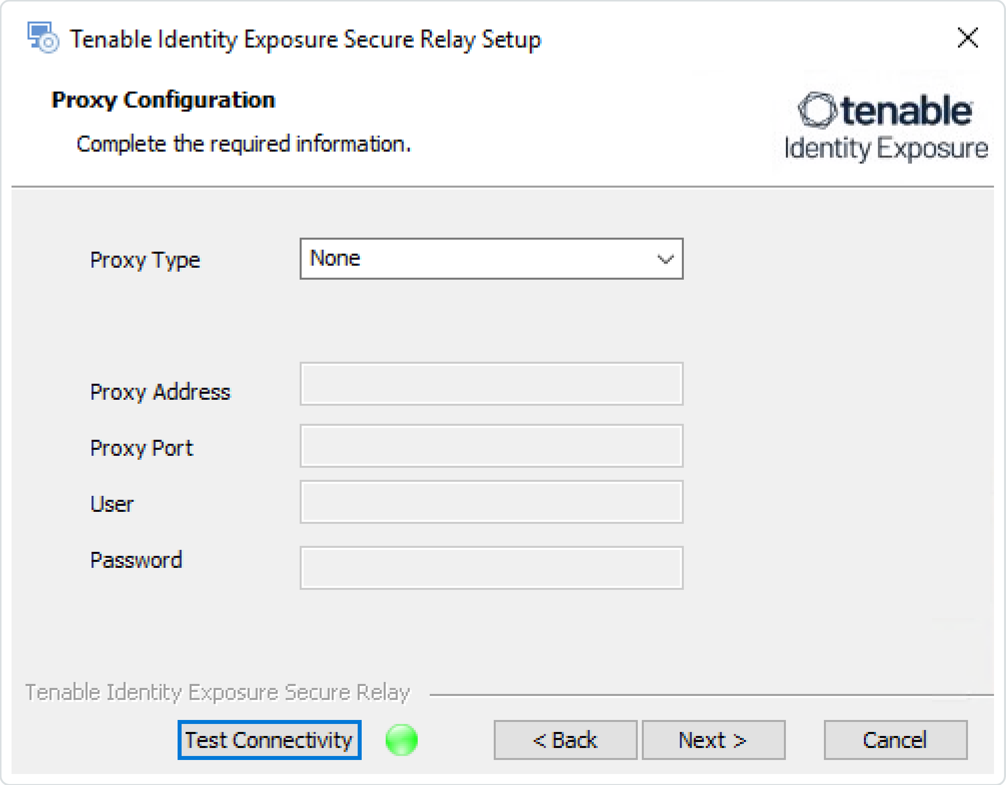
Import Ca certicate manually:

Click on the radio button for one of the following options:

- **Automatic upload** — Retrieve the CA certificate automatically from the Directory Listener: Under **Directory Listener Windows credentials**, type the user name and password for the Windows account used to access the Directory Listener service.
- **Manual upload** — Click **...** to browse for the CA certificate that the Directory Listener uses.

8. Click **Next**.

The Proxy Configuration window appears:



Tenable Identity Exposure Secure Relay Setup

Proxy Configuration

Complete the required information.

Proxy Type: None

Proxy Address

Proxy Port

User

Password

9. 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`.)

10. 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.

11. Click **Next**.

    The **Ready to Install** window appears.

12. Click **Install**.

13. 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

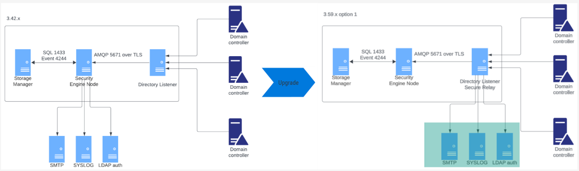
This 3.42 release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

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)

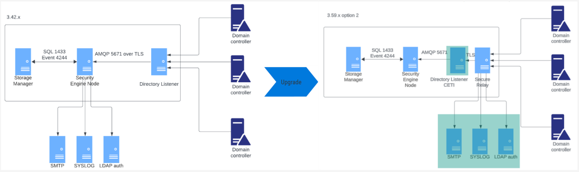
Standard 3 Servers with DL and SR on the Same Server

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	3.59or 3.77
• 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
 3.42.x Storage Manager SQL 1433 Event 4244 Security Engine Node AMQP 5671 over TLS Directory Listener Domain controller Domain controller Domain controller SMTP SYSLOG LDAP auth Upgrade 3.59.x option 1 Storage Manager SQL 1433 Event 4244 Security Engine Node AMQP 5671 over TLS Directory Listener Secure Relay Domain controller Domain controller Domain controller SMTP SYSLOG LDAP auth **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

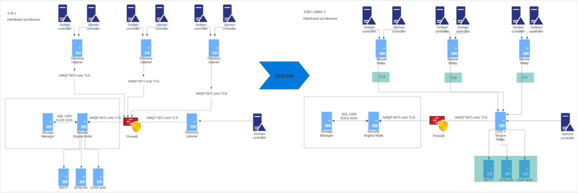
This architecture transitions from a standard 3-servers architecture (SM, SEN, and DL) to one with the DL and SR running on separate servers.

3.42	3.593.77
- The Security Engine Node: ◦ Sends email and Syslog alerts ◦ Provides LDAP authentication	- Requires **a new server for the Directory Listener** - The Secure Relay: ◦ Replaces the Directory Listener ◦ Sends email and Syslog alerts ◦ Provides LDAP authentication
 3.42.x SQL 1433 Event 4244 AMQP 5671 over TLS Storage Manager Security Engine Node Directory Listener Domain controller Domain controller Domain controller SMTP SYSLOG LDAP auth Upgrade 3.59.x option 2 SQL 1433 Event 4244 AMQP 5671 TLS Storage Manager Security Engine Node Directory Listener CETI Secure Relay Domain controller Domain controller Domain controller SMTP SYSLOG LDAP auth	

Multiple DLs to a Single DL Running SR

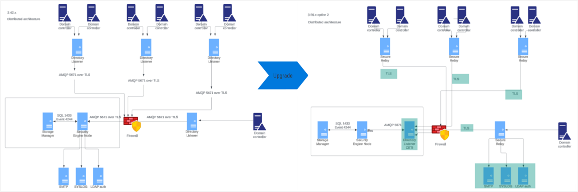
This architecture transitions from a multiple-DLs architecture to one with a single DL running the SR.

3.42	3.593.77
- 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	3.593.77
• 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 3.77

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).

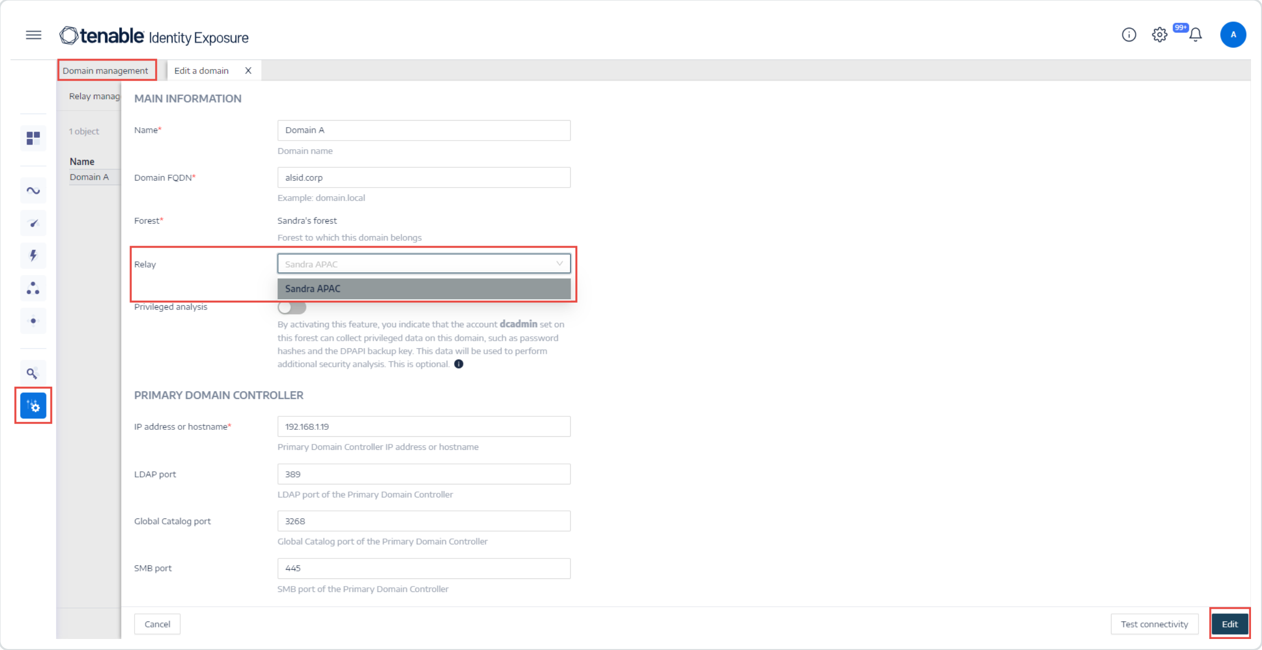
  To map a domain to a Secure Relay:

  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.



MAIN INFORMATION

Name*: Domain A
Domain name

Domain FQDN*: alsid.corp
Example: domain.local

Forest*: Sandra's forest
Forest to which this domain belongs

Relay: Sandra APAC
Sandra APAC

Privileged analysis
By activating this feature, you indicate that the account **dcadmin** set on this forest can collect privileged data on this domain, such as password hashes and the DPAPI backup key. This data will be used to perform additional security analysis. This is optional.

PRIMARY DOMAIN CONTROLLER

IP address or hostname*: 192.168.1.19
Primary Domain Controller IP address or hostname

LDAP port: 389
LDAP port of the Primary Domain Controller

Global Catalog port: 3268
Global Catalog port of the Primary Domain Controller

SMB port: 445
SMB port of the Primary Domain Controller

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):

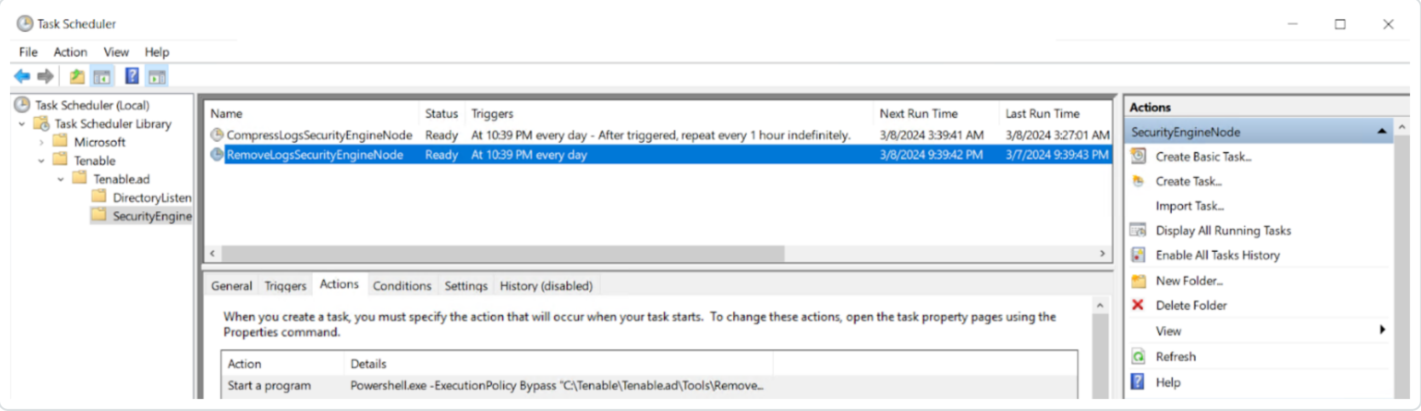
1. In the command line of the local machine, type cd desktop.
2. Type .\installername.exe /LOGS "c:\<path>\logsmsi1.txt".

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.



Name	Status	Triggers	Next Run Time	Last Run Time
CompressLogsSecurityEngineNode	Ready	At 10:39 PM every day - After triggered, repeat every 1 hour indefinitely.	3/8/2024 3:39:41 AM	3/8/2024 3:27:01 AM
RemoveLogsSecurityEngineNode	Ready	At 10:39 PM every day	3/8/2024 9:39:42 PM	3/7/2024 9:39:43 PM

When you create a task, you must specify the action that will occur when your task starts. To change these actions, open the task property pages using the Properties command.

Action	Details
Start a program	Powershell.exe -ExecutionPolicy Bypass "C:\Tenable\Tenable.ad\Tools\Remove...

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.

Post-deployment Tasks

After you successfully installed or upgraded Tenable Identity Exposure, go through the following checks to

Log in to Tenable Identity Exposure

You access Tenable Identity Exposure's web application through a client URL such as `https://<SEN IP-address>` or `https://<SEN hostname>`.

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".

See Log in to Tenable Identity Exposure for complete information.

Health Checks

Use the Health Checks feature to evaluate thoroughly the domain and platform status to ensure that there's no deterioration in health or status post-upgrade compared to the previous state.

Functional Checks

Verify the following functions after an upgrade:

- **Trail Flow** — Check that the Trail Flow page opens normally to display a list of events. Ensure that it loads with the updated date and timestamp. See Trail Flow for complete information.
- **Indicators of Exposure** (IoEs) — Ensure that the Indicators of Exposure pane opens. By default, Tenable Identity Exposure only shows the IoEs containing deviances. Verify that the page loaded correctly for the respective deviances. See Indicators of Exposure for complete information.

- **Indicators of Attack** (IoAs) — Ensure that the Indicators of Attack pane opens. Tenable Identity Exposure presents a timeline and the top 3 incidents that impacted your AD in real time, along with the attack distribution, all in a single pane. If possible, perform a sample test of an IoA (Password Guessing) to confirm whether it triggers an alert. See Indicators of Attack for more information.

Glossary of Terms

This glossary familiarizes you with the commonly used terms in Tenable Identity Exposure.

Cancri — The service that computes the difference between the previous state of an AD object and its new current state. It also sequences events so that Cygni receives them in order.

Cephei — The service that calculates the statistics observable on your dashboard (Widget Active Users count, Compliance Score, Deviance, etc).

Ceti — The service that initially collects AD objects (crawling) and subscribes to replication flows (appearance of new events: listening). The AD objects retrieved currently come from two sources: LDAP and SYSVOL.

Cygni — The service that analyzes the changes in AD objects to deduce whether they involve one or more risks, which, when assembled, would meet the criteria for deviance. This deviance will then be transmitted to the database and then visible in Tenable Identity Exposure.

Deviant objects — The set of deviances that an Indicator Of Exposure (IoE) flags, pointing to an object that carries an attribute that triggered the related IoE.

Directory Listeners — Hosting the Ceti services (on-premises context) that work 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.

Enif — The service that controls authentication at the Web interface.

Eridanis — The API service that stores the business data (configuration and AD objects, deviances, etc.) in MS SQL Server and supplies them to other services.

Kapteyn — The service that hosts the Tenable Identity Exposure web applications. Developed with Javascript technologies, it is a real-time application that allows data updates without user action.

RabbitMQ — RabbitMQ is a third-party tool that Tenable Identity Exposure uses to transfer messages from one service to another. The messages remain in the RabbitMQ queue manager until a receiving application connects and removes a message from the queue. The receiving application subsequently processes the message.

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 (exclusive to versions 3.59 and later).

Security Engine Nodes — As the 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.

Storage Manager — Providing hot and cold storage support, the Storage Managers oversees 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.

Trail Flow — The Trail Flow landing page displays the real-time monitoring and analysis of events affecting your AD infrastructures. The Trail Flow page provides the ability to load previous events to go back in time. The search function at the top of this page can also allow you to perform threat hunting and detect malicious patterns.

Getting Support

When customers encounter challenges with their product usage, Tenable Technical Support is available to provide assistance. For expedited assistance, please consult the following article outlining best practices for opening Support cases: Opening a case with Technical Support: Best Practices.

Tenable empowers our customers to designate an appropriate case priority when creating Technical Support cases via the Tenable Community. These priorities range from P1 to P4, with P1 representing the most critical and P4 the least critical issues. Customers should exercise their best judgment when assigning case priorities to ensure their cases are handled promptly, and Technical Support reserves the right to adjust the priority of a case up or down for accurate classification. We strongly recommend customers with critical P1 issues to contact Technical Support directly to avoid any delays associated with email communication. Below are some examples to assist customers in determining their case priority.

Priority	Description	Examples
P1 — Critical	Product functionality completely degraded – critical impact to business operation	• Product (Nessus, Tenable Identity Exposure, etc - excluding Agents/Clients) service will not start • Product inaccessible to all users • Upgrade failure – Product inaccessible as a result • Nessus/Tenable Identity Exposure/Tenable.io cannot scan (i.e. all scans error/cannot launch)
P2 — High	Product functionality severely degraded – severe impact to business operations	• Reports will not launch/generate (i.e. all reports fail) • Unable to query

		vulnerabilities/all dashboards/all scan results • Linking failure of Scanners/LCE/NNM (excluding agents/clients)
P3 — Medium	General errors/issues – product impaired but business operations remain functional	• Generally the default priority • False Positive/Negative • Scanning/Reporting errors • Errors with non-core functionality - asset/target lists, SMTP/LDAP integration, etc. • Plugin Update Failure • Initial installation/setup issues • Requests for testing upgrades prior to production installation
P4 — Informational	Basic information or assistance with Tenable products – little to no impact on business operations	• How do I [question]? • What ports must be open for the product to work? • Do you have a plugin that scans for 'X'? • What IPs count against my Tenable Identity Exposure license? Do you have 'X' feature?