Tenable Identity Exposure On-Premises Installation Guide

Last Revised: April 17, 2024

Table of Contents

Welcome to Tenable Identity Exposure

Last updated: April 17, 2024

Tenable Identity Exposure (formerly Tenable.ad) 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 on-premises Installation Guide for Tenable Identity Exposure **versions 3.42 and earlier** 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 Tenable Identity Exposure Installation Roadmap.

Tenable Identity Exposure Installation Roadmap

The following roadmap to perform your deployment of Tenable Identity Exposure **version 3.42 or earlier**.

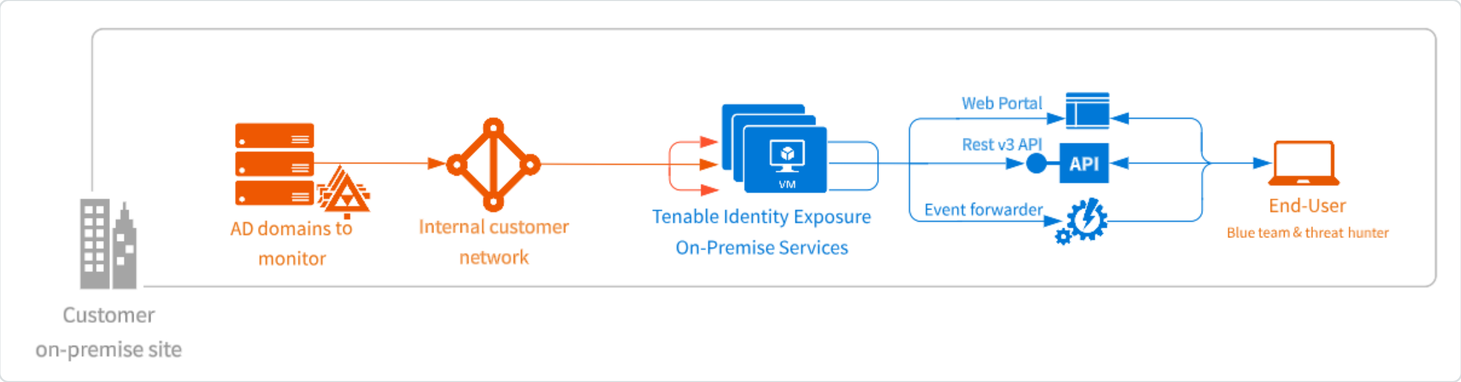
1. **Review** the Release Notes.
2. **Select your architecture** — Tenable Identity Exposure offers two deployment options depending on your specific needs. See On-premises Architectures.
3. **Check** Pre-deployment Requirements: For optimal performance, Tenable Identity Exposure requires careful resource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

   Technical Prerequisites

   - Resource Sizing
   - Hardware Requirements
   - Network Requirements
   - Web Portal Requirements
   - Integration with an Active Directory Domain
4. Install Tenable Identity Exposure.
5. Upgrade Tenable Identity Exposure.
6. **Post-deployment** — Restart Services, Logs for Troubleshooting.
7. **Review** Tenable Identity Exposure Licensing.

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
VM
Tenable Identity Exposure On-Premise Services
Web Portal
Rest v3 API
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.

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

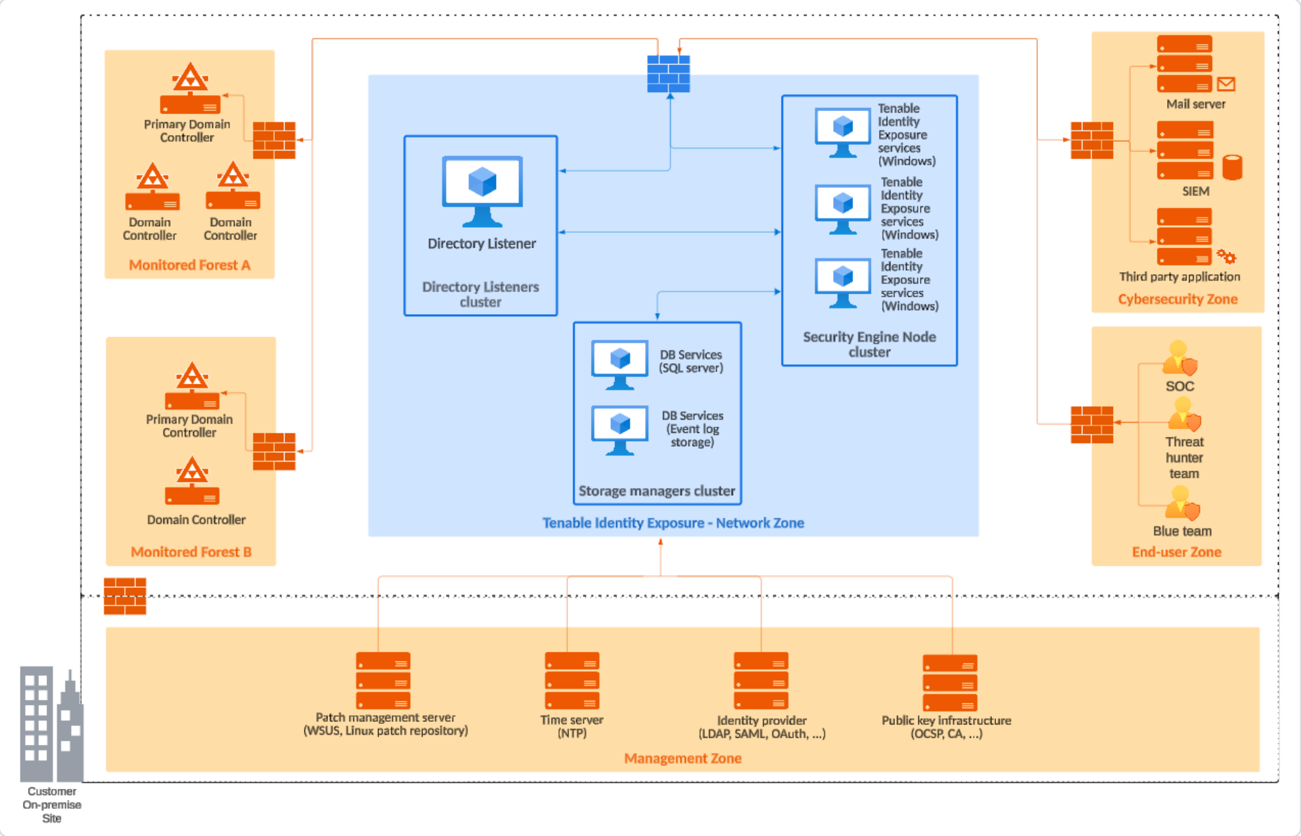
Architectures

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
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:

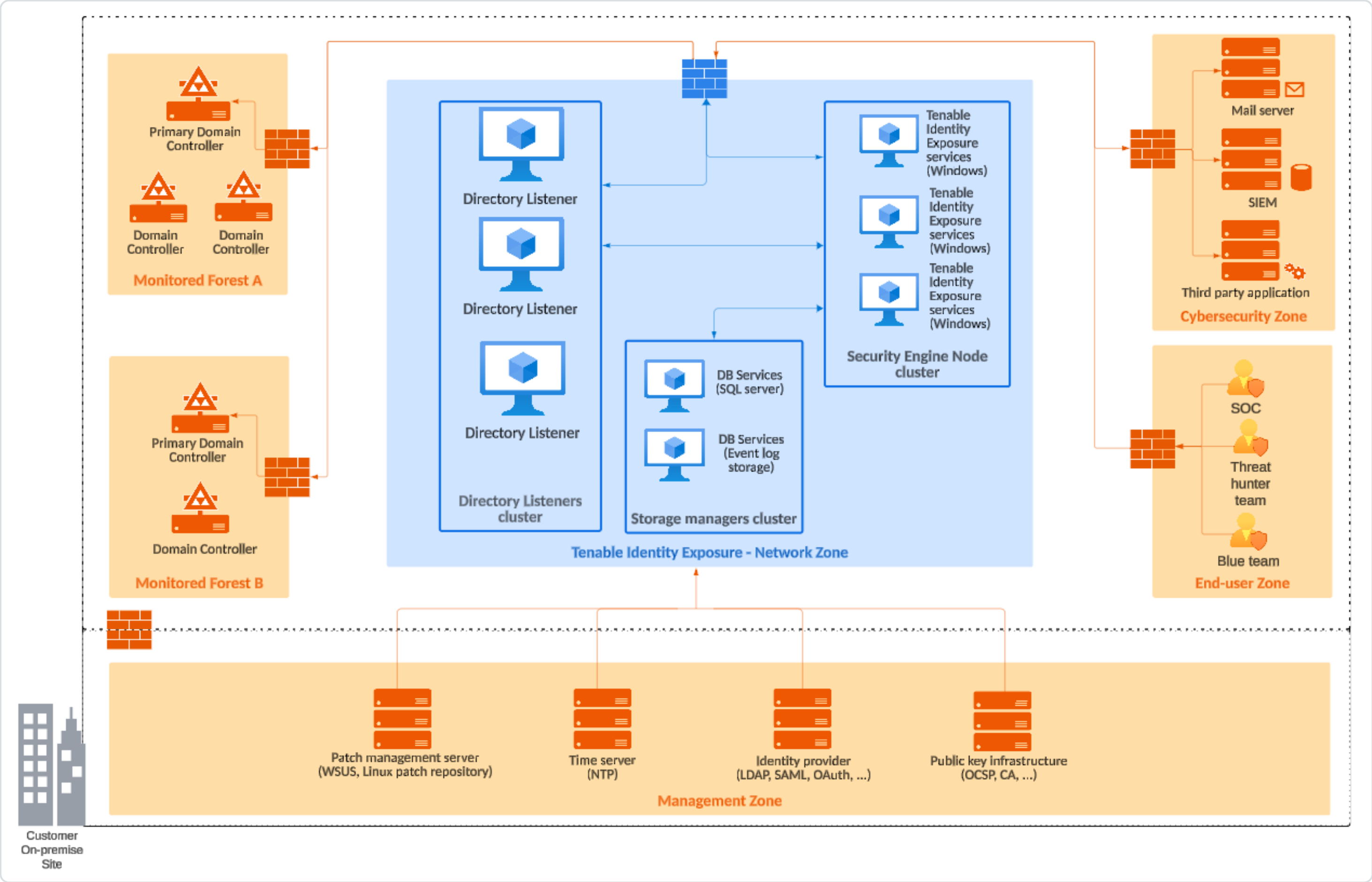
- Each Tenable Identity Exposure service is at the same logical place behind a unique firewall.
- Each service flow (Active Directory, end-users, alerts, etc.) goes through the same network equipment.
- This architecture links new Active Directory domains easily because it does not need service or extra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

- 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

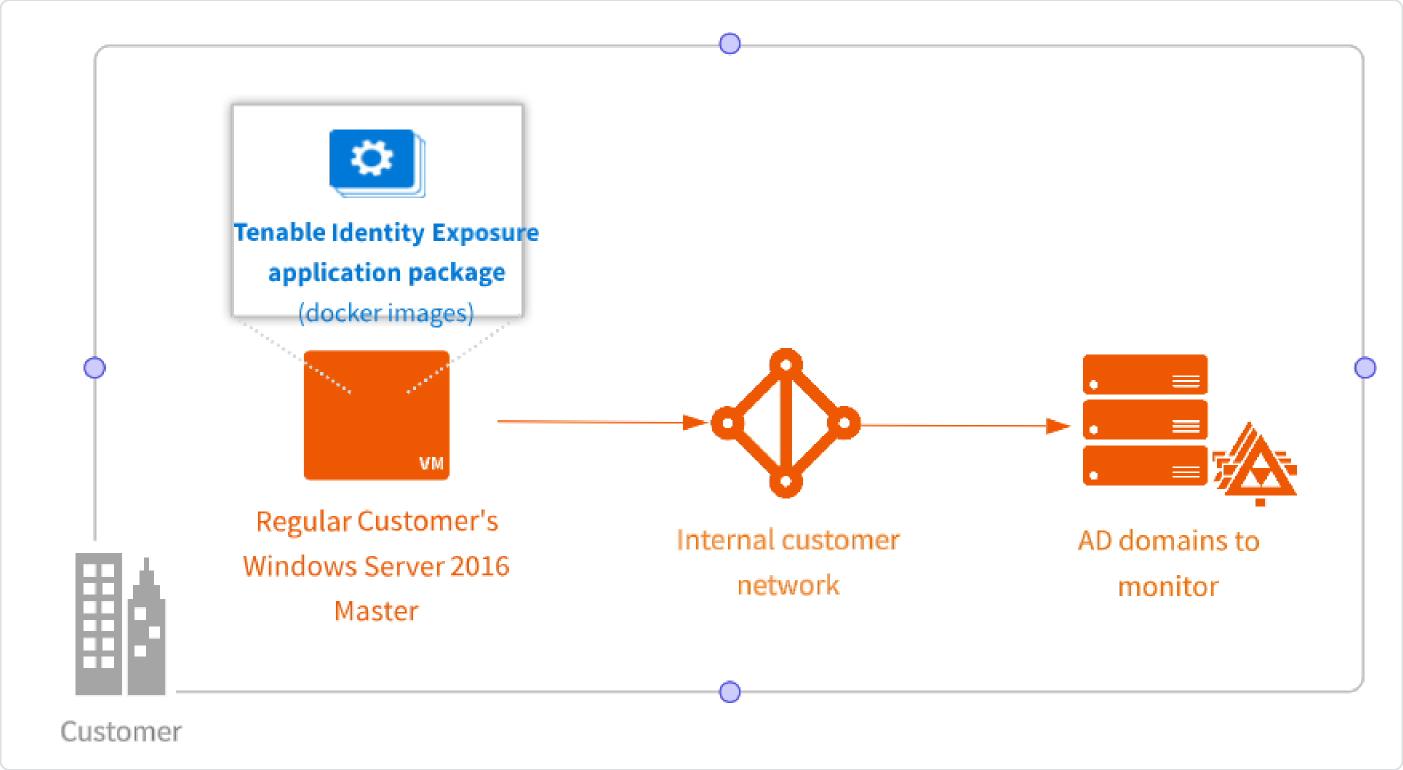
Before you begin, check that you meet the following prerequisites to ensure a smooth installation process.

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.



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.

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.

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.
FIPS-compliant algorithms	For data privacy reasons, do not activate Federal Information Processing Standards (FIPS)-compliant algorithms for encryption.
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 Server 2016 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 Technical Lead 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**, 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 **Directory Listeners** receive real-time Active Directory flows.

  Required sizing for the system hosting the Directory Listener components:

Directory Listener				
Active AD users	Instance	vCPU (per instance)	Memory	Disk space

	required		(per instance)	(per instance)
1 – 25,000	1 virtual machine	2 cores on 2 sockets	16 GB of RAM	30 GB (Silver)
25,001 – 50,000	1 virtual machine	4 cores on 2 sockets	16 GB of RAM	30 GB (Silver)
50,001 - 75,000	1 virtual machine	4 cores on 2 sockets	32 GB of RAM	30 GB (Silver)
75,001 – 100,000	1 virtual machine	4 cores on 2 sockets	32 GB of RAM	30 GB (Silver)
100,001 – 150,000	1 virtual machine	8 cores on 2 sockets	64 GB of RAM	30 GB (Silver)
150,001 – 300,000	1 virtual machine	8 cores on 2 sockets	64 GB of RAM	30 GB (Silver)
300,001 – 500,001+	1 virtual machine	8 cores on 2 sockets	64 GB of RAM	30 GB (Silver)

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

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 -	1 virtual	10 cores on 3	32 GB of RAM	300 GB

75,000	machine	sockets		(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

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
300,001 – 500,001+	8 TB	3.3 TB	6.4 TB	500 GB	1.2 TB	200 GB	400 GB

Minimum and Recommended Disk Performance

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

Storage managers – Disk Performance Matrix

Active AD users	Minimal Disk Performance		Recommended Disk Performance	
	Throughput (MB/sec)	IOPs (read/write)	Throughput (MB/sec)	IOPs (read/write)
1 – 25,000	150	2,500	300	5,000
25,001 – 50,000	200	5,000	400	10,000
50,001 - 75,000	200	5,000	400	10,000
75,001 – 100,000	200	5,000	400	10,000
100,001 – 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
- 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/sec	2 Mbps/sec
5,001 – 75,000	150	5 Mbps/sec	10 Mbps/sec
75,001 – 400,000	700	15 Mbps/sec	30 Mbps/sec

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.

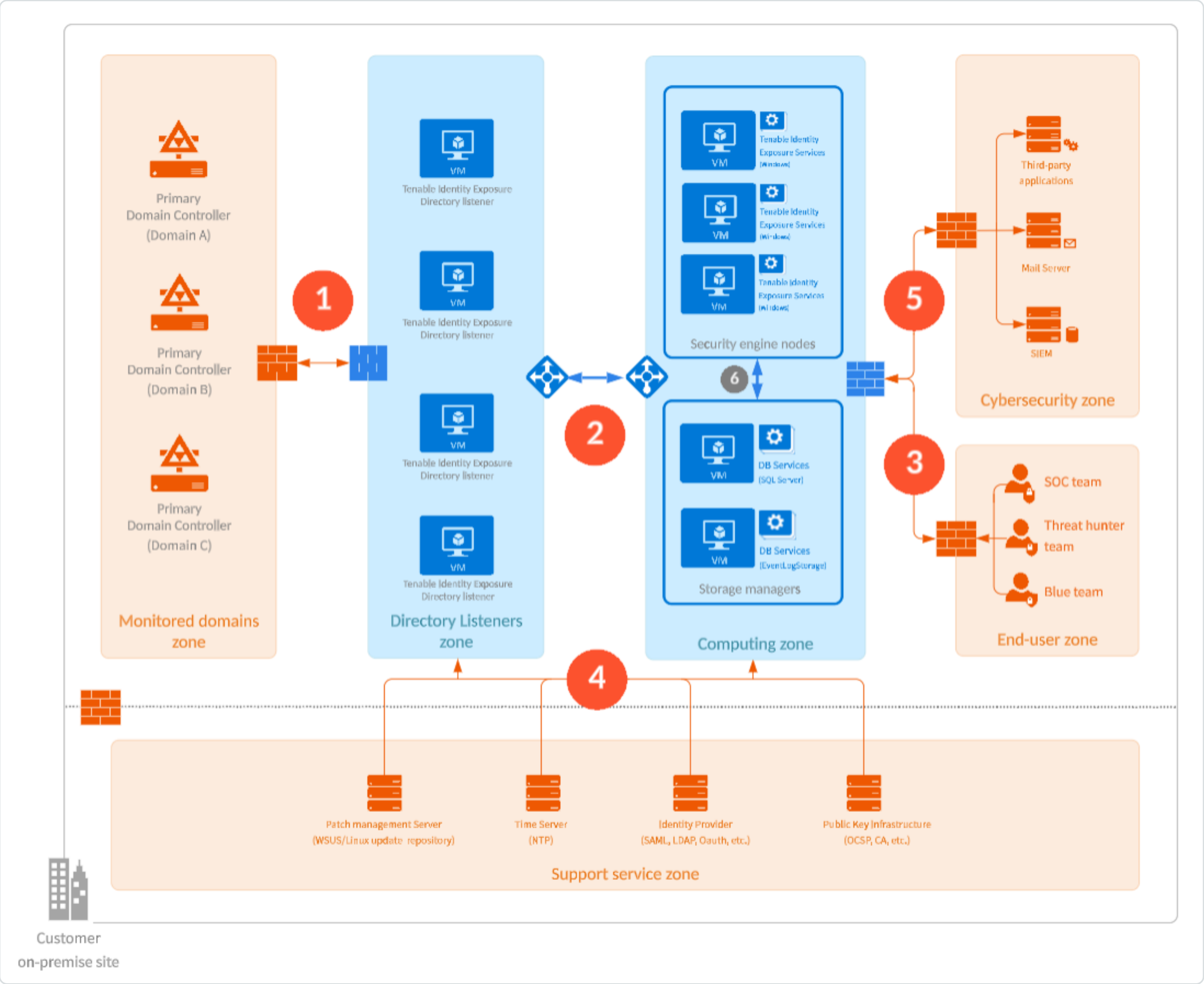
Network Flow Matrix

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.


Primary
Domain Controller
(Domain A)
Primary
Domain Controller
(Domain B)
Primary
Domain Controller
(Domain C)
Monitored domains zone
1
VM
Tenable Identity Exposure Directory listener
VM
Tenable Identity Exposure Directory listener
VM
Tenable Identity Exposure Directory listener
VM
Tenable Identity Exposure Directory listener
Directory Listeners zone
2
VM
Tenable Identity Exposure Services (Windows)
VM
Tenable Identity Exposure Services (Windows)
VM
Tenable Identity Exposure Services (Windows)
Security engine nodes
6
VM
DB Services (SQL Server)
VM
DB Services (EventLogStorage)
Storage managers
Computing zone
5
3
Third-party applications
Mail Server
SIEM
Cybersecurity zone
SOC team
Threat hunter team
Blue team
End-user zone
4
Patch management Server (WSUS/Linux update repository)
Time Server (NTP)
Identity Provider (SAML, LDAP, Oauth, etc.)
Public Key Infrastructure (OCSP, CA, etc.)
Support service 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	Domain controllers	Directory, Replication, User	LDAP/LDAPS	TCP/389 and TCP/636

	Exposure’s Secure Relay(s)		and Computer Authentication, Group Policy, Trusts		ICMP/echo-request ICMP/echo-response
			Replication, User and Computer Authentication, Group Policy, Trusts	SMB, CIFS, SMB2, DFSN, LSARPC, NbtSS, NetLogonR, SamR, SrvSvc	TCP/445
			User and Computer Authentication, Forest Level Trusts	Kerberos	TCP/88, TCP/464 and UDP/464
			User and Computer Authentication, Name Resolution, Trusts	DNS	UDP/53 and TCP/53
			Replication, User and Computer Authentication, Group Policy, Trusts	RPC, DCOM, EPM, DRSUAPI, NetLogonR, SamR, FRS	TCP Dynamic (> 1024)
			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
3.	End users	Tenable Identity Exposure’s Security engine nodes	Tenable Identity Exposure’s end-user services (Web portal, REST API, etc.)	HTTPS	TCP/443
4.	Tenable Identity Exposure	Support services	Time synchronization	NTP	UDP/123
			Update infrastructure (for example WSUS or SCCM)	HTTP/HTTPS	TCP/80 or TCP/443
			PKI infrastructure	HTTP/HTTPS	TCP/80 or TCP/443
			Identity provider SAML server	HTTPS	TCP/443
			Identity provider LDAP	LDAP/LDAPS	TCP/389 and TCP/636
			Identity provider OAuth	HTTPS	TCP/443

Additional Flows

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

Network flows	From	To	Tenable Identity Exposure's Usage (optional)	Type of Traffic	Protocol and Port
5.	Tenable Identity Exposure's Secure Relay(s)	Cybersecurity services	Email notifications	SMTP	TCP/25, TCP/587, TCP/465, TCP/2525, TCP/25025 (depending on the SMTP server's configuration)
			Syslog notifications	Syslog	TCP/601, TCP/6515, UDP/514 (depending on the event log server's configuration)
			Tenable REST API	HTTP/TLS	TCP/443

Internal Ports

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

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

Network flows	From	To	Tenable Identity Exposure’s Usage	Type of Traffic	Protocol and Port
6.	Tenable Identity Exposure ’s Security Engine Nodes	Tenable Identity Exposure’s Storage Managers	MS SQL Server database access	MS SQL queries	TCP/1433
			`EventLogStorage` database access	`EventLogStorage` queries	TCP/4244

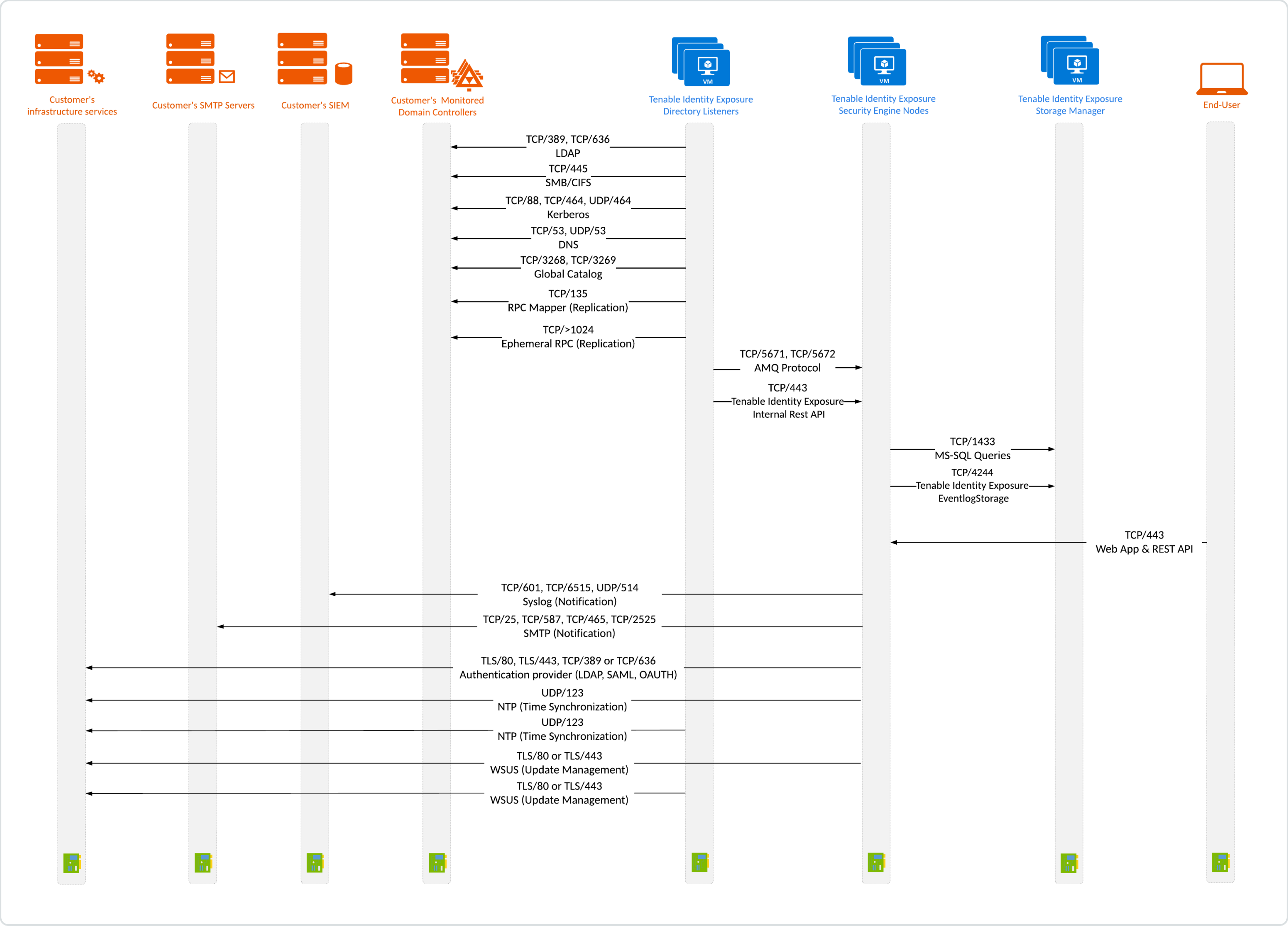
Support Services

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

Network Address Translation (NAT) support

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

On-premise platform


Customer's infrastructure services
Customer's SMTP Servers
Customer's SIEM
Customer's Monitored Domain Controllers
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/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)

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.

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:

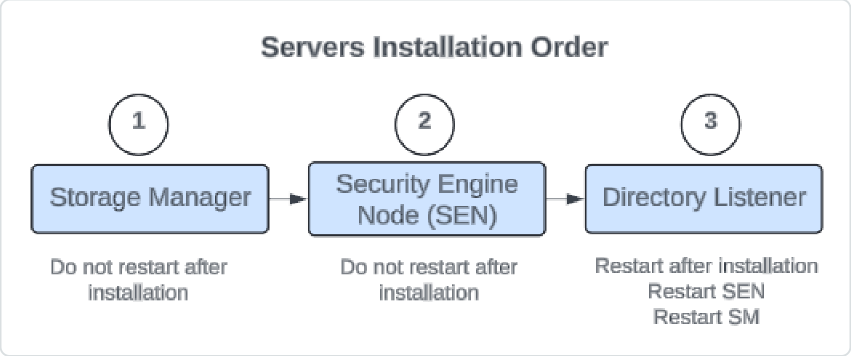
- A **Storage Manager** (SM) to host all data based on MSSQL.
- A **Directory Listener** (DL) to target audited domains.
- A **Security Engine Node** (SEN) to perform security analysis and serve the user interface.

  For more information about how to install the SEN on several machines, see Split Security Engine Node (SEN) Services.

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 3.42**, proceed in the following order:


Servers Installation Order
1
2
3
Storage Manager
Security Engine Node (SEN)
Directory Listener
Do not restart after installation
Do not restart after installation
Restart after installation
Restart SEN
Restart SM

Before you start

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

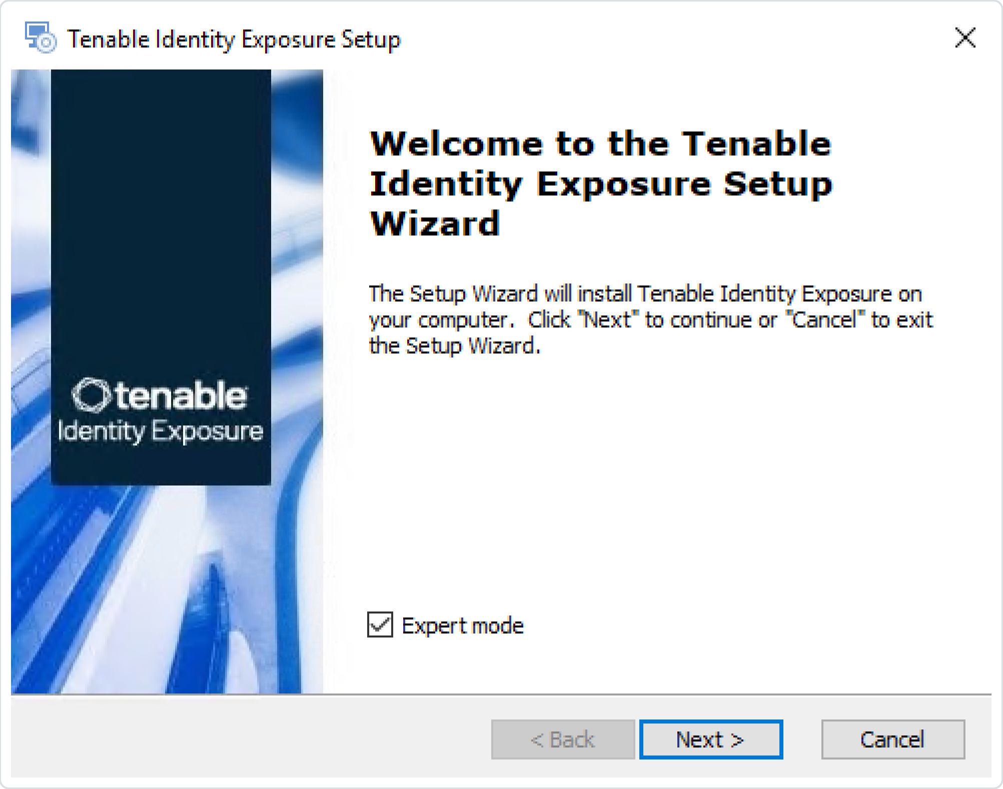
To install the Storage Manager:

1. On the local machine, run the **Tenable Identity Exposure 3.42** 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

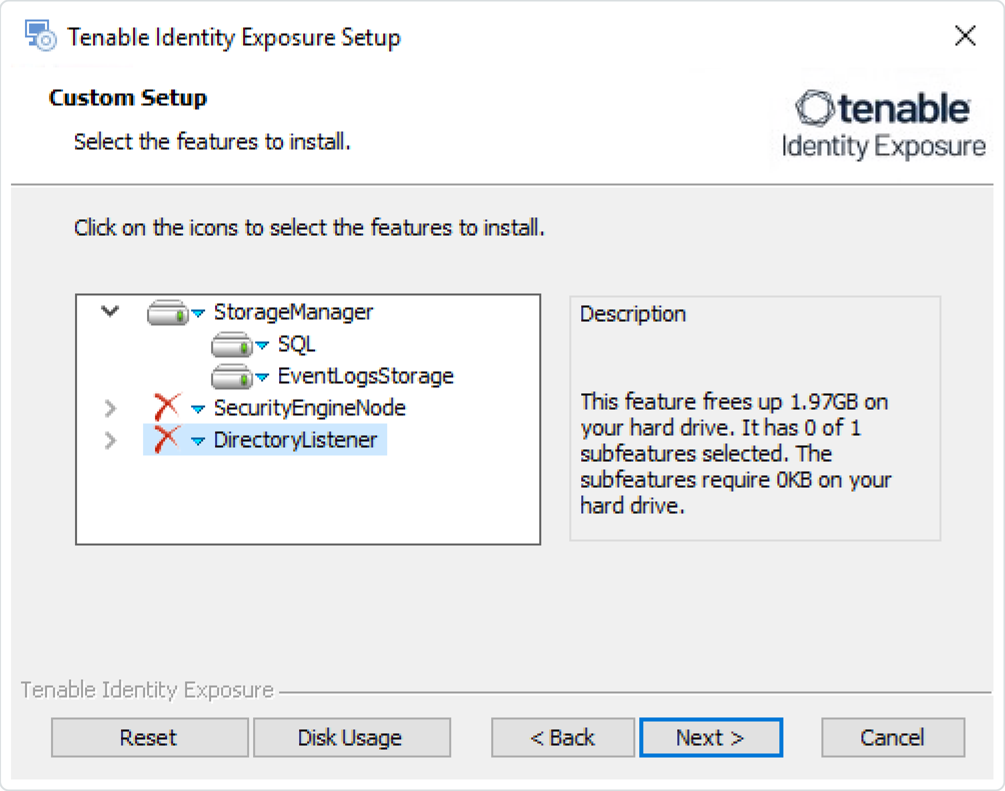
The Setup Wizard will install Tenable Identity Exposure on your computer. Click "Next" to continue or "Cancel" to exit the Setup Wizard.

☑ Expert mode

4. Click **Next**.

   The **Custom Setup** window appears.

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



Custom Setup

Select the features to install.

Click on the icons to select the features to install.

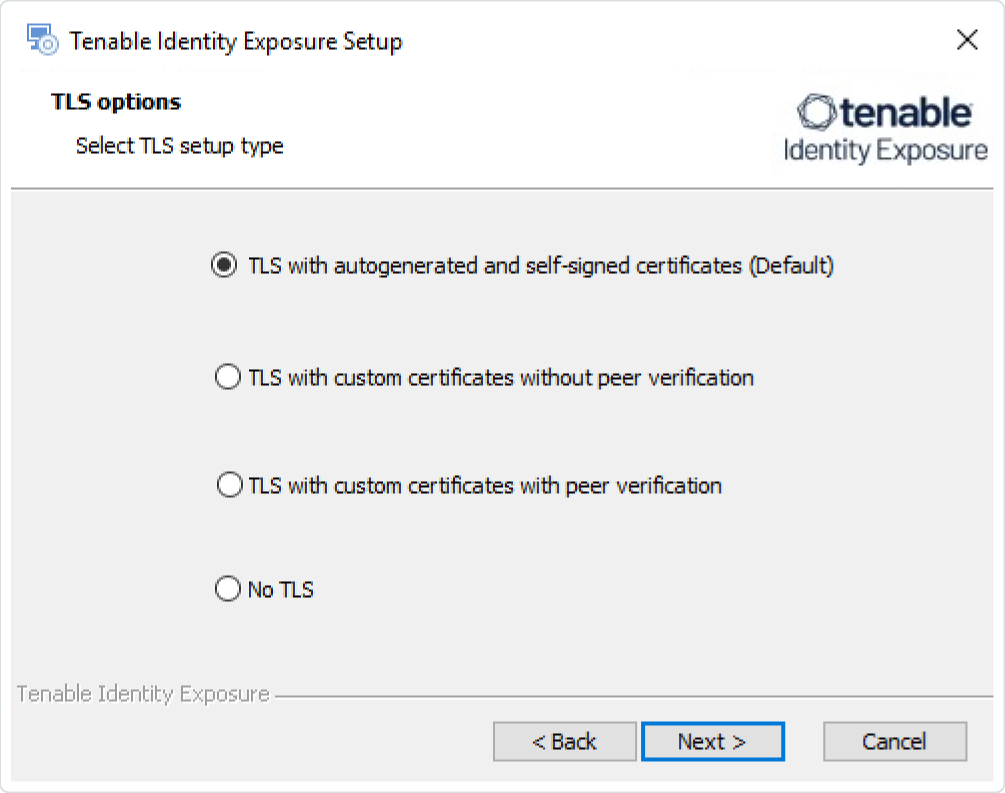
Description

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.

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)

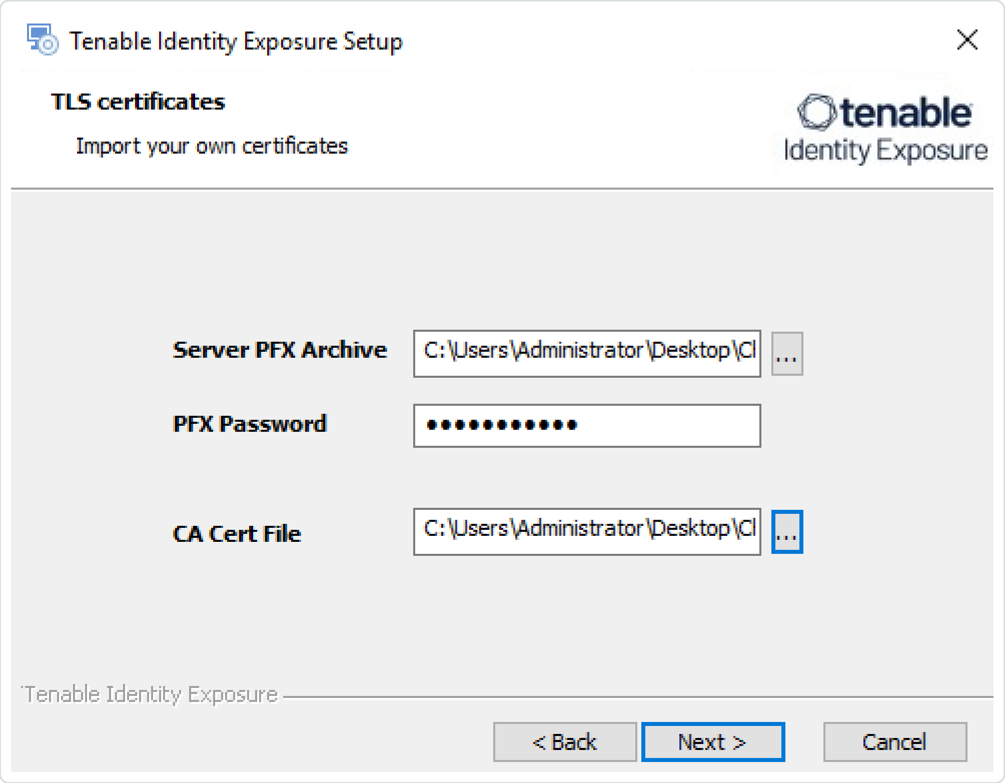
○ TLS with custom certificates without peer verification

○ 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

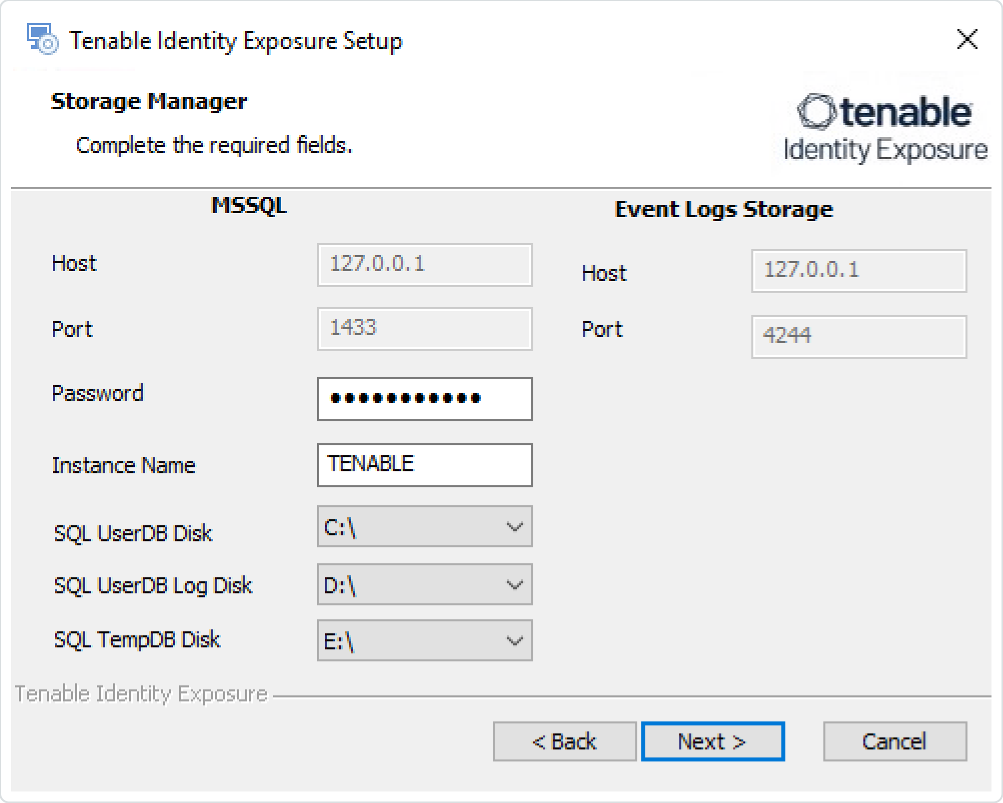
8. Click **Next**.

   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

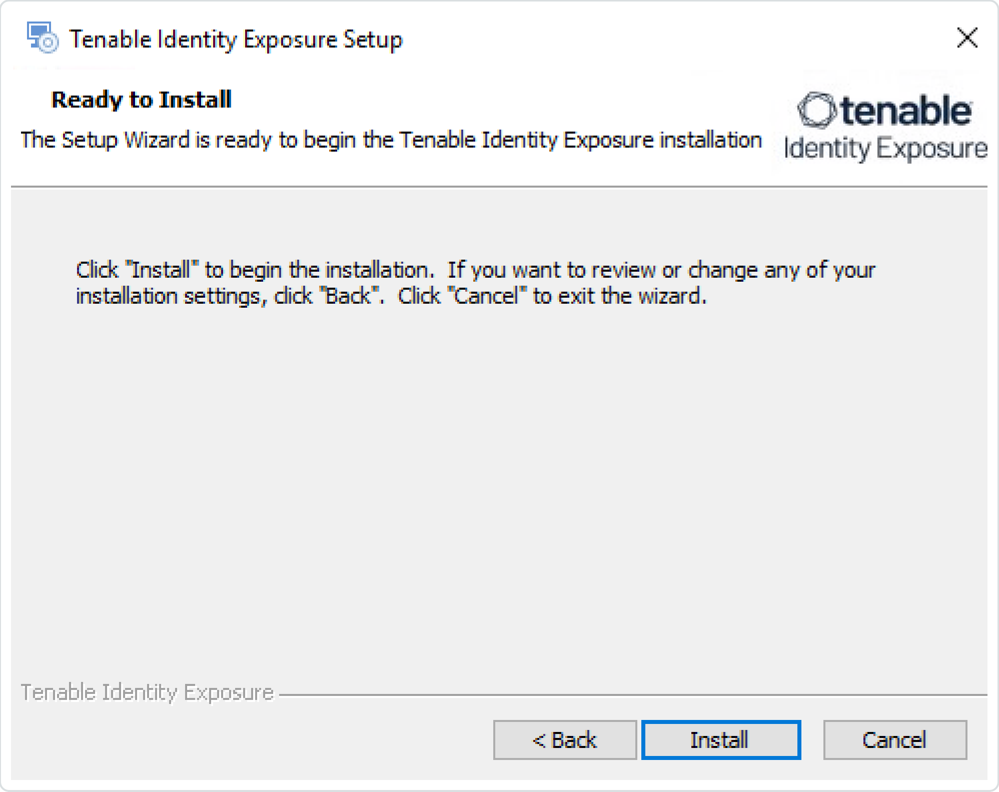
Host: 127.0.0.1

Port: 4244

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

10. Click **Next**.

    The **Ready to Install** window appears.



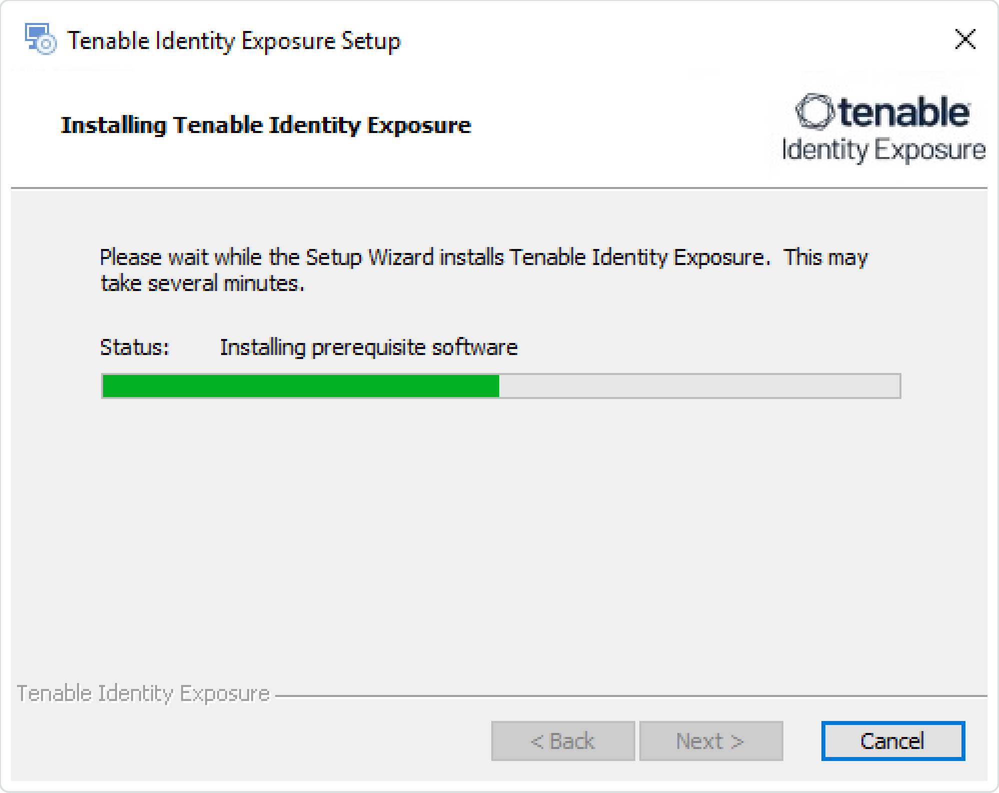
Tenable Identity Exposure Setup

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:

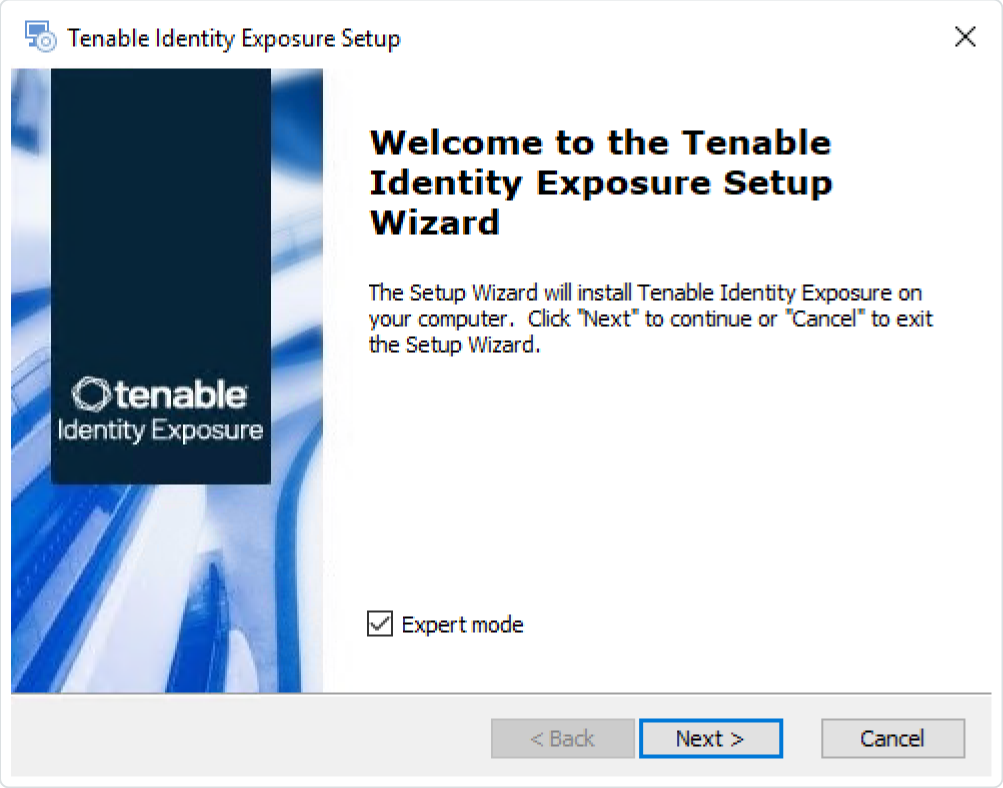
1. On the local machine, run the **Tenable Identity Exposure 3.42** On-premises installer.

   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.

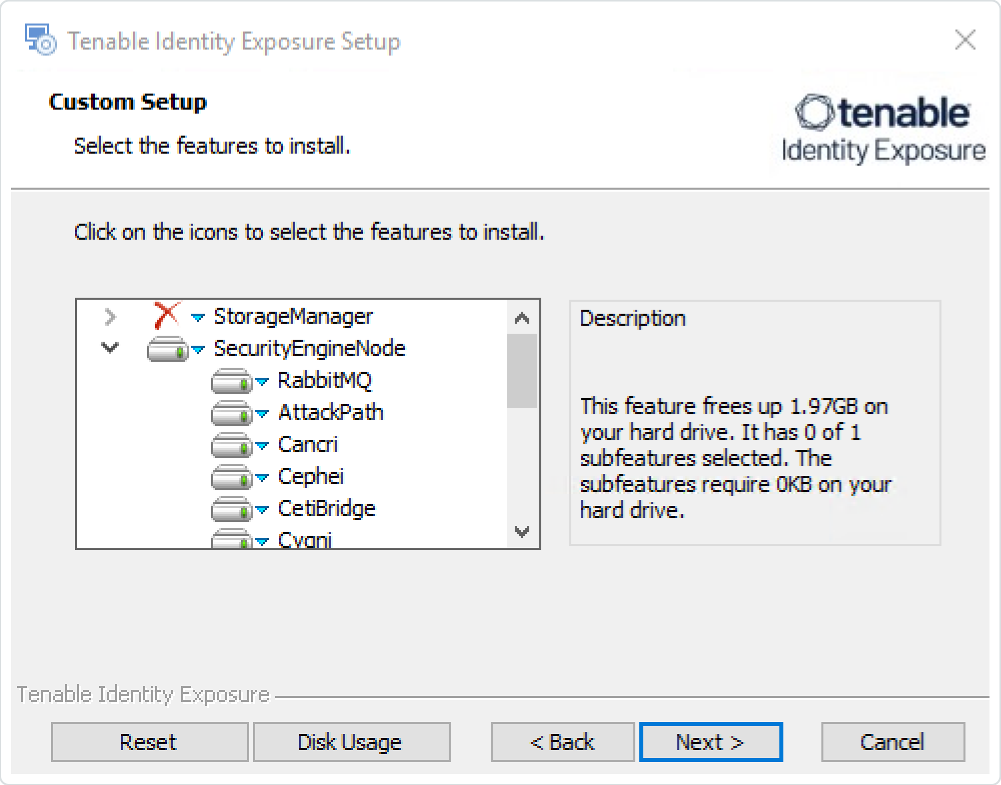
☑ Expert mode

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 Security Engine Node (SEN) Services.



Tenable Identity Exposure Setup

Custom Setup

Select the features to install.

Click on the icons to select the features to install.

- StorageManager
- SecurityEngineNode
  - RabbitMQ
  - AttackPath
  - Cancri
  - Cephei
  - CetiBridge
  - Cygni

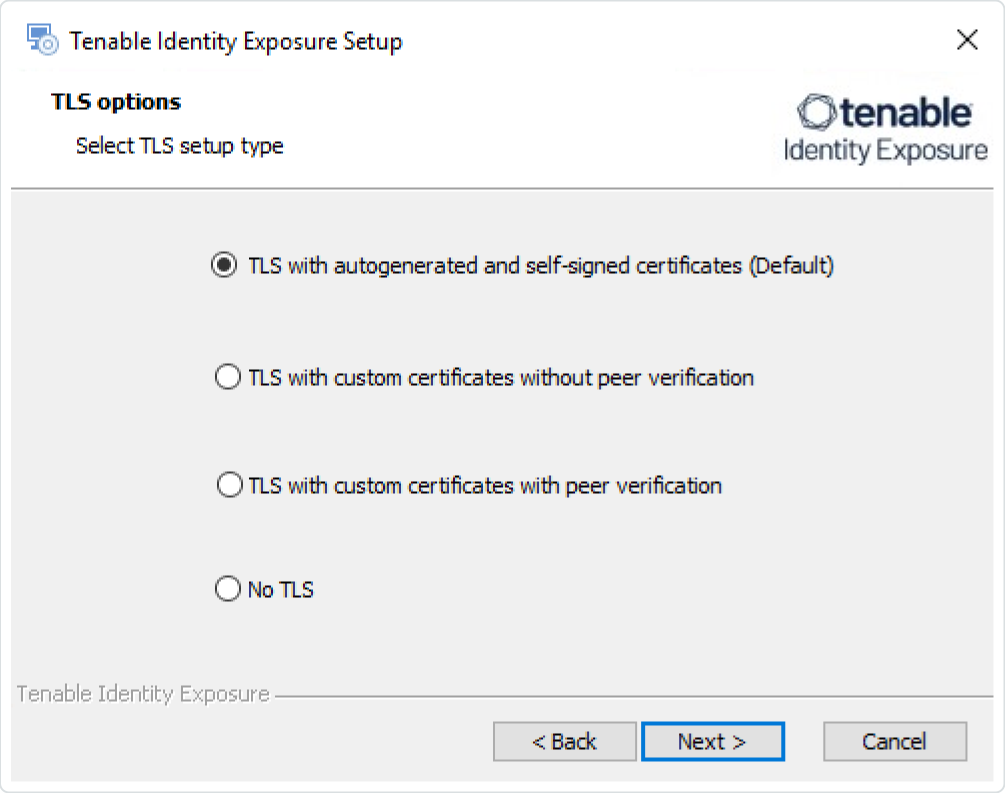
Description

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.

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)

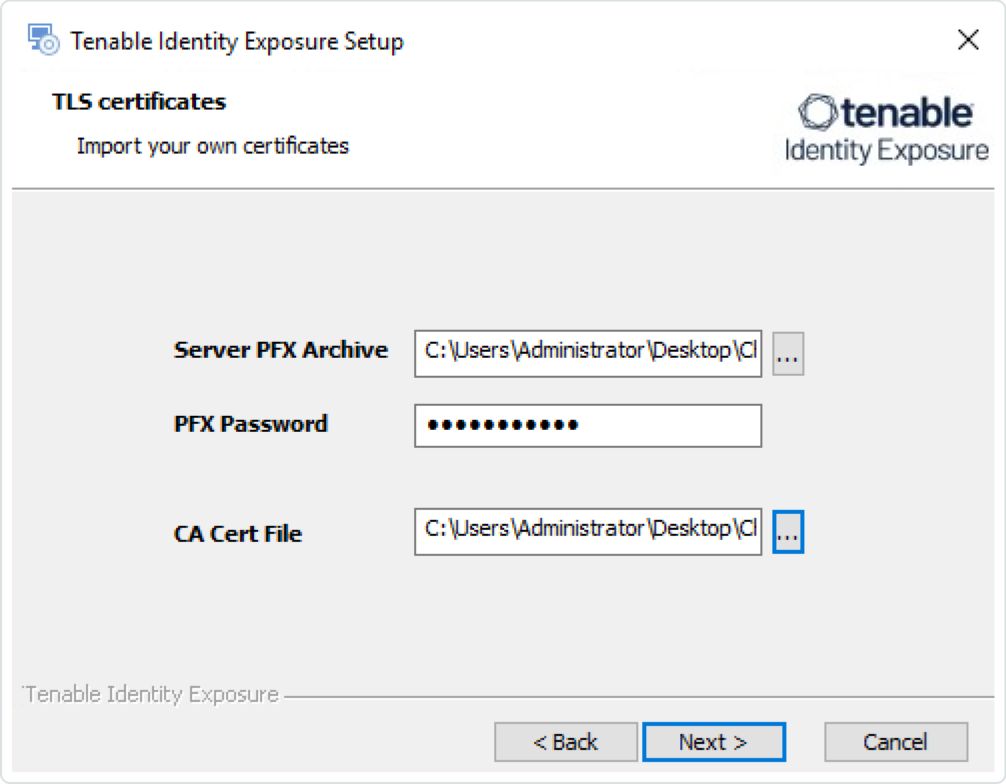
○ TLS with custom certificates without peer verification

○ 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.

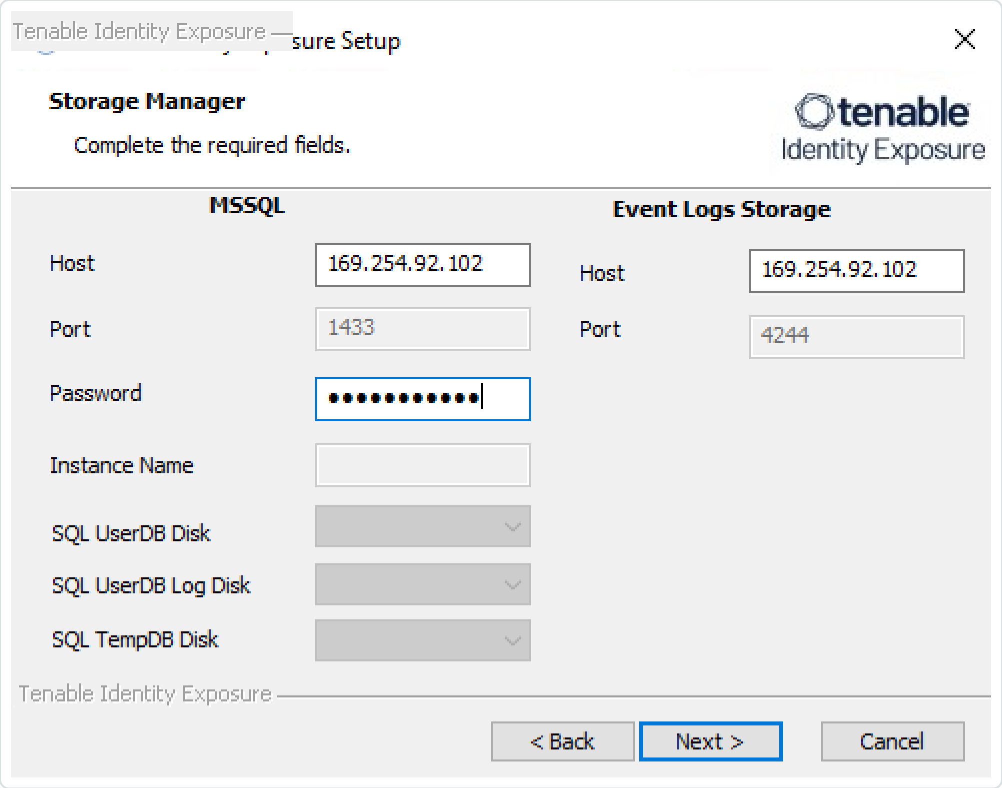
9. Provide the following information:

   - 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

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

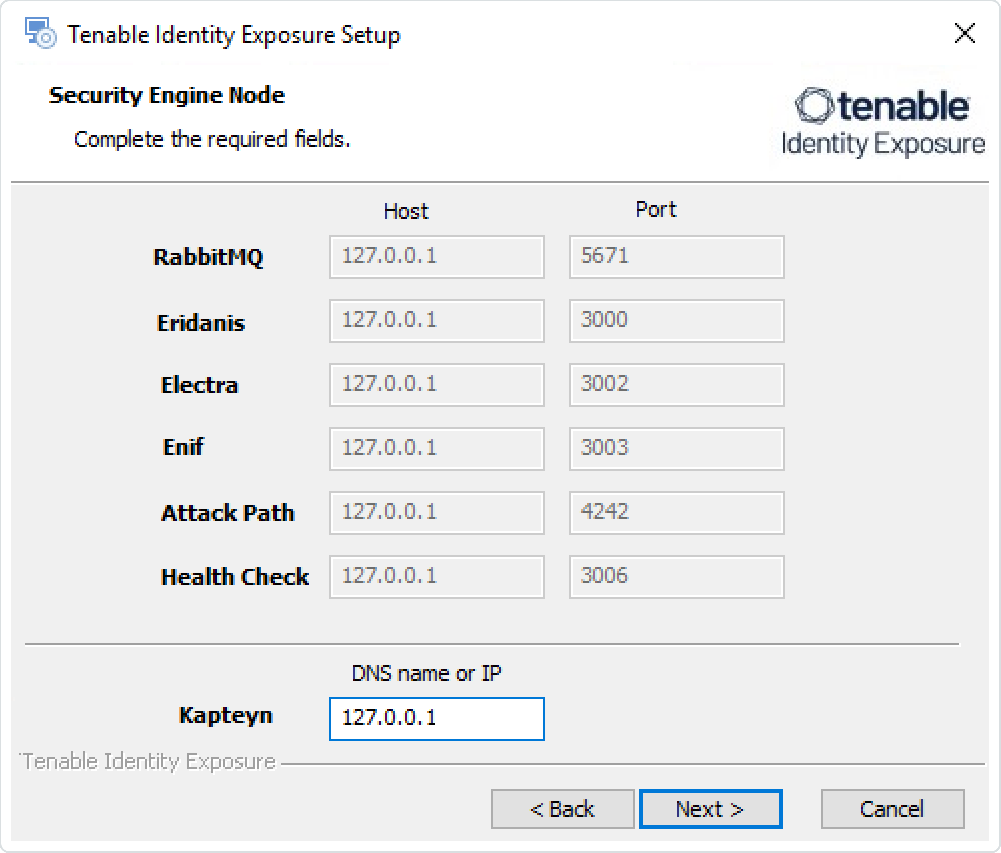
Host: 169.254.92.102

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

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

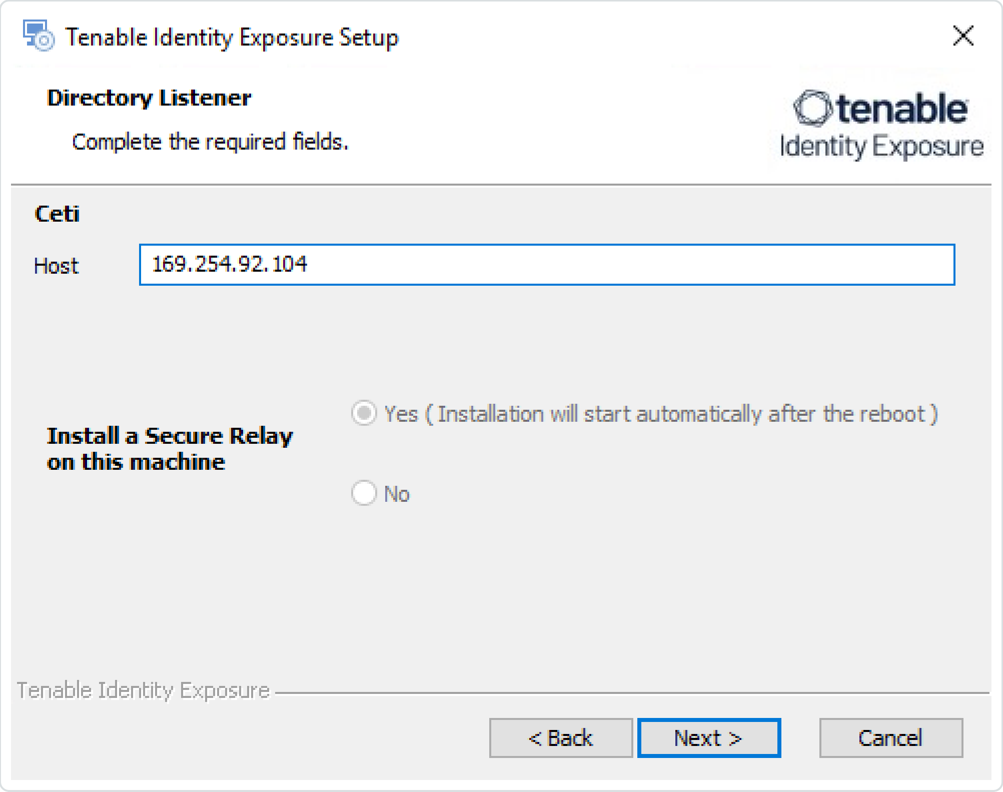
	DNS name or IP
Kapteyn	127.0.0.1

> **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.



Tenable Identity Exposure Setup

Directory Listener

Complete the required fields.

Ceti

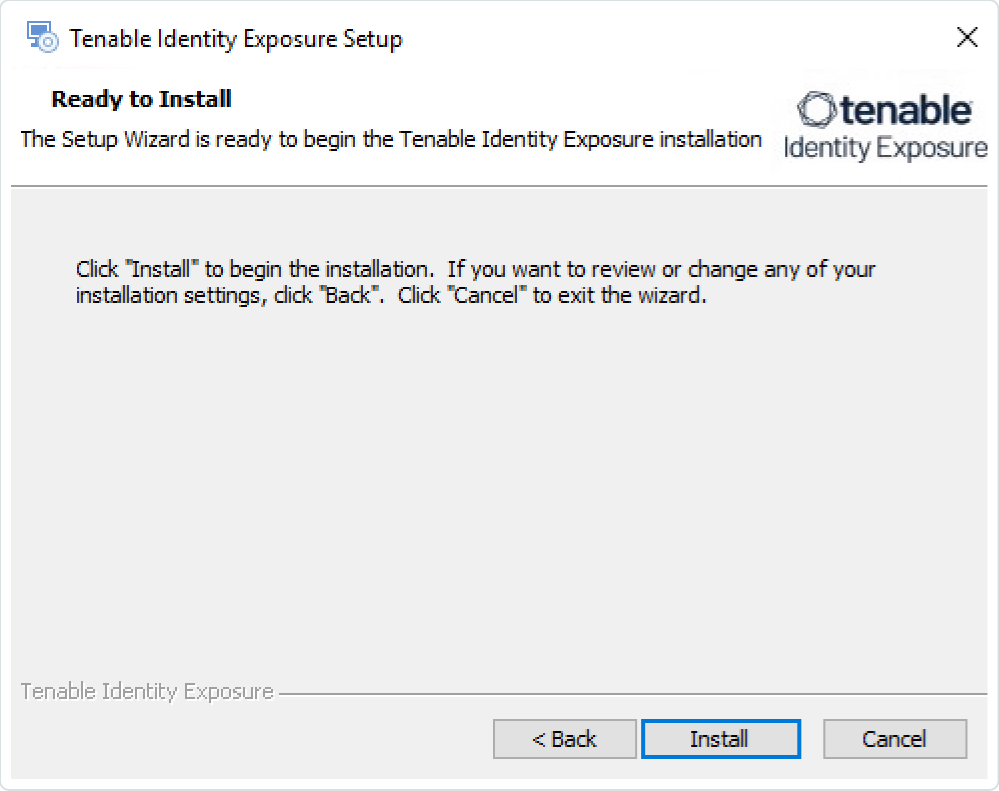
Host: 169.254.92.104

Install a Secure Relay on this machine

● Yes (Installation will start automatically after the reboot)

○ No

The **Ready to Install** window appears.



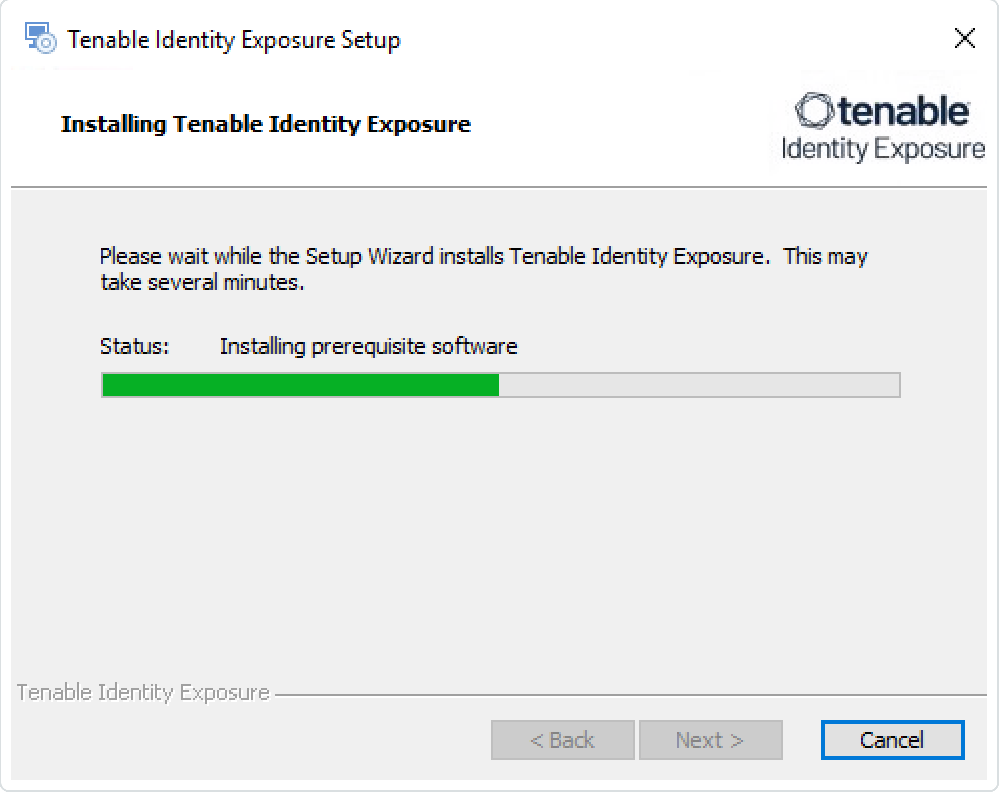
Tenable Identity Exposure Setup

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.

14. 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.

15. Click **Finish**.

    A dialog box asks you to restart your machine.

16. Click **No**.

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

17. Install the Directory Listener.

To install the Directory Listener:

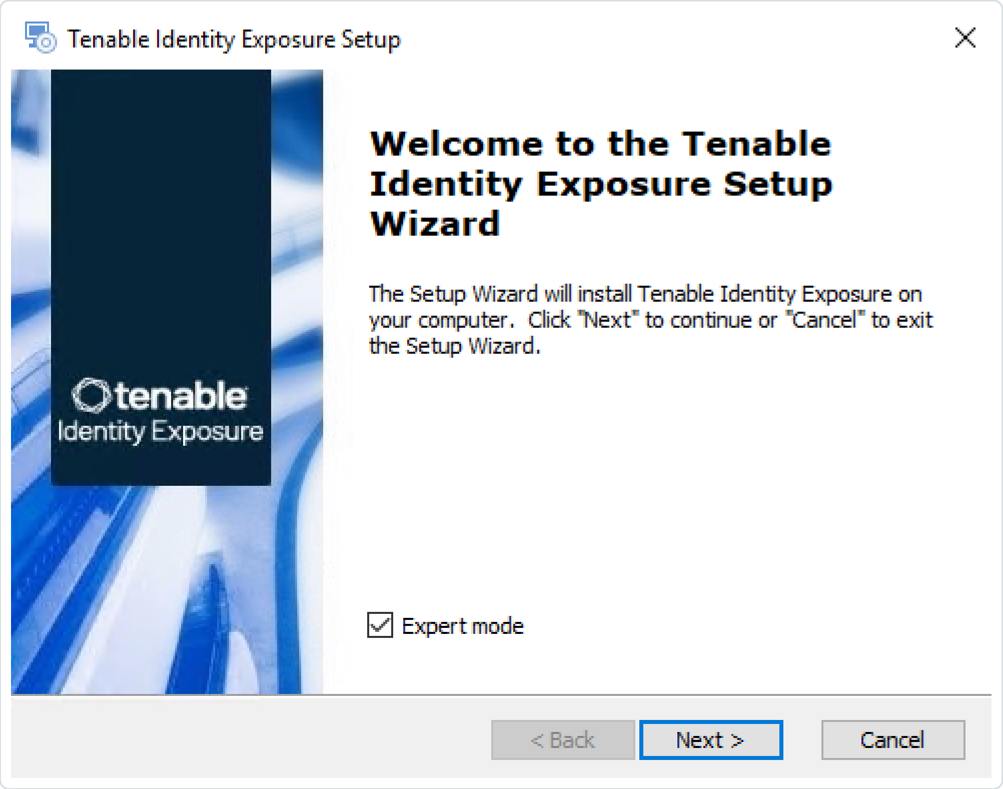
1. On the local machine, run the **Tenable Identity Exposure 3.42** On-premises installer.

   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

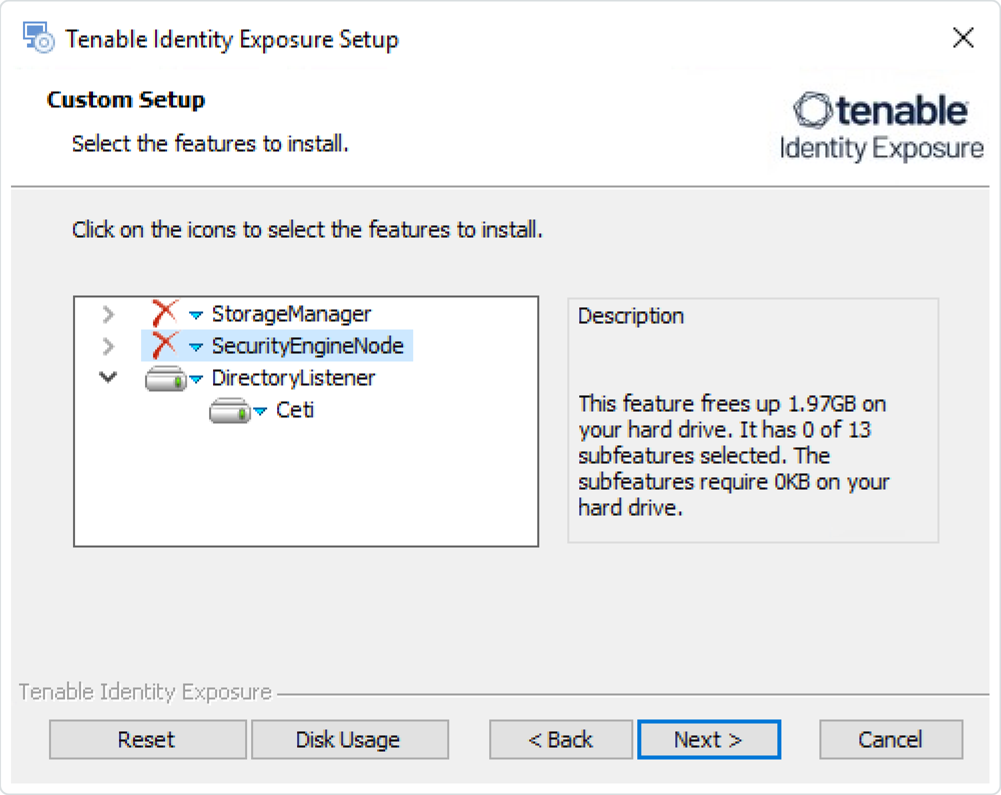
The Setup Wizard will install Tenable Identity Exposure on your computer. Click "Next" to continue or "Cancel" to exit the Setup Wizard.

☑ Expert mode

4. Click **Next**.

   The **Custom Setup** window appears.

5. Deselect the *Storage Manager* and 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.

- StorageManager
- SecurityEngineNode
- DirectoryListener
  - Ceti

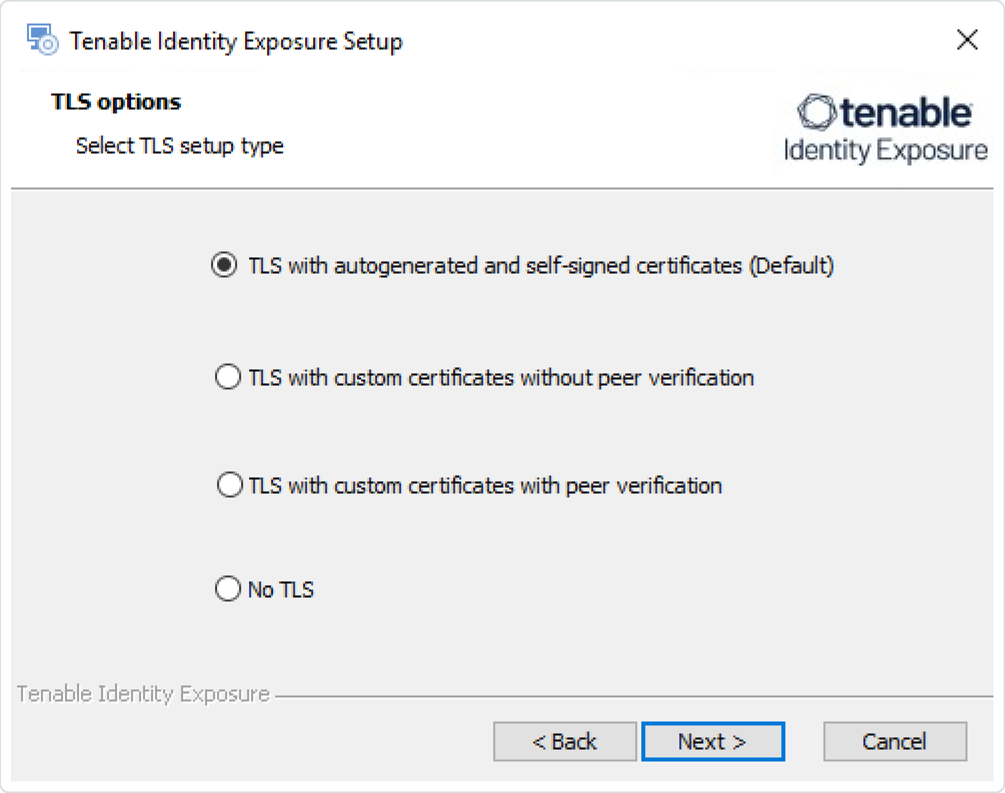
Description

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.

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)

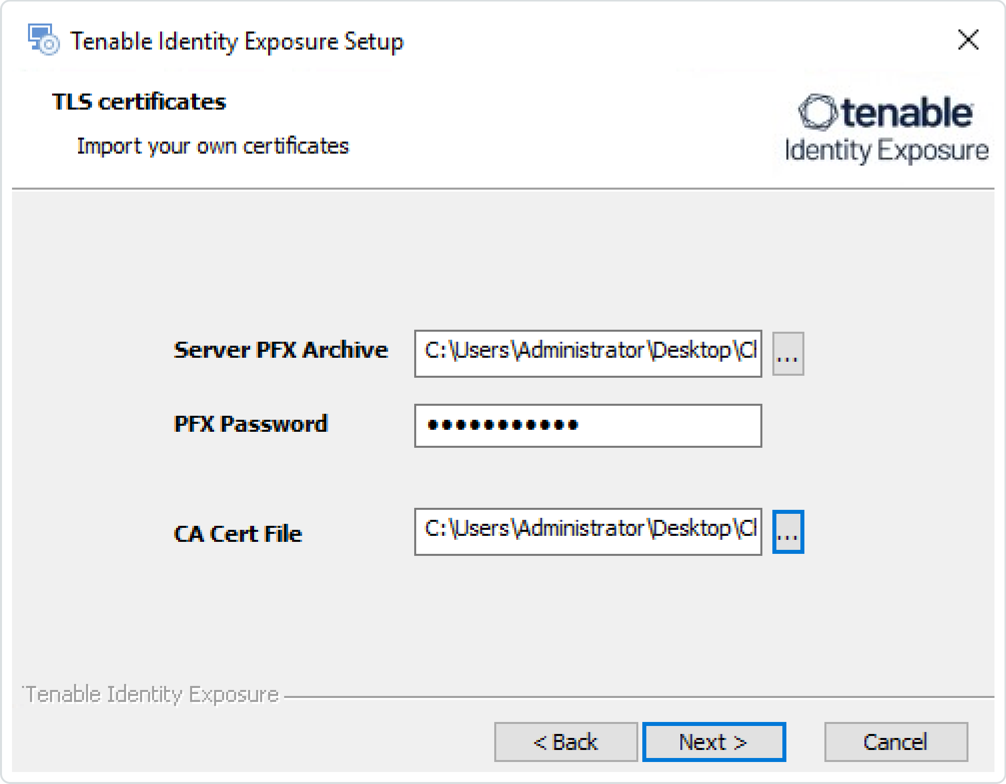
○ TLS with custom certificates without peer verification

○ 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

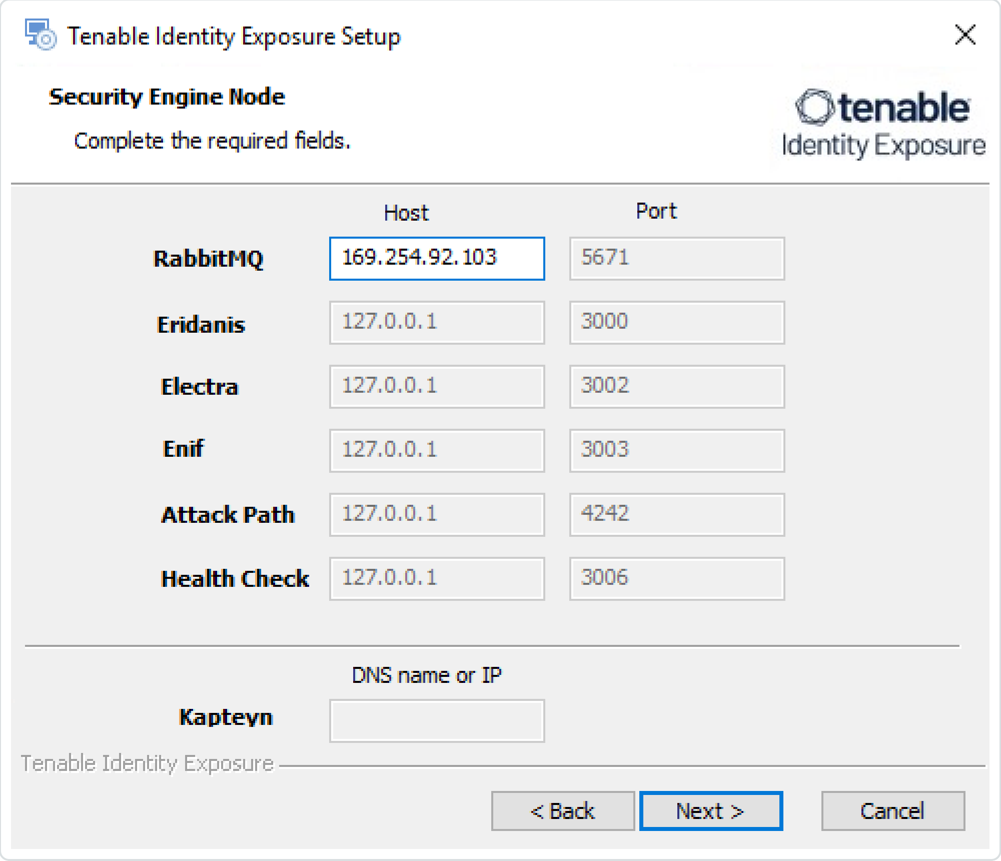
PFX Password: ●●●●●●●●●●●

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.



Security Engine Node

Complete the required fields.

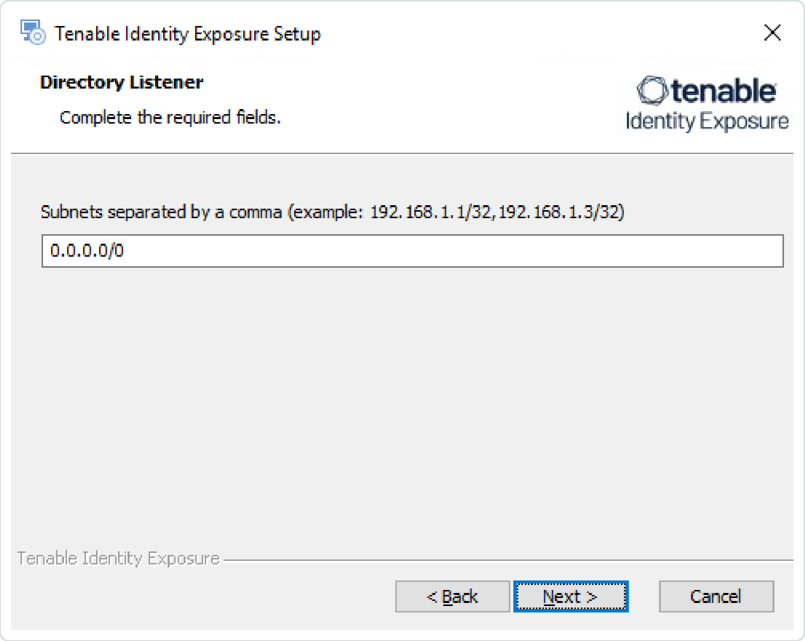
	Host	Port
RabbitMQ	169.254.92.103	5671
Eridanis	127.0.0.1	3000
Electra	127.0.0.1	3002
Enif	127.0.0.1	3003
Attack Path	127.0.0.1	4242
Health Check	127.0.0.1	3006

	DNS name or IP
Kapteyn	

10. Click **Next**.

    The **Directory Listener** window appears.

11. In the **Subnets** box (if applicable), type the subnet information for the Directory Listener.



Tenable Identity Exposure Setup

Directory Listener

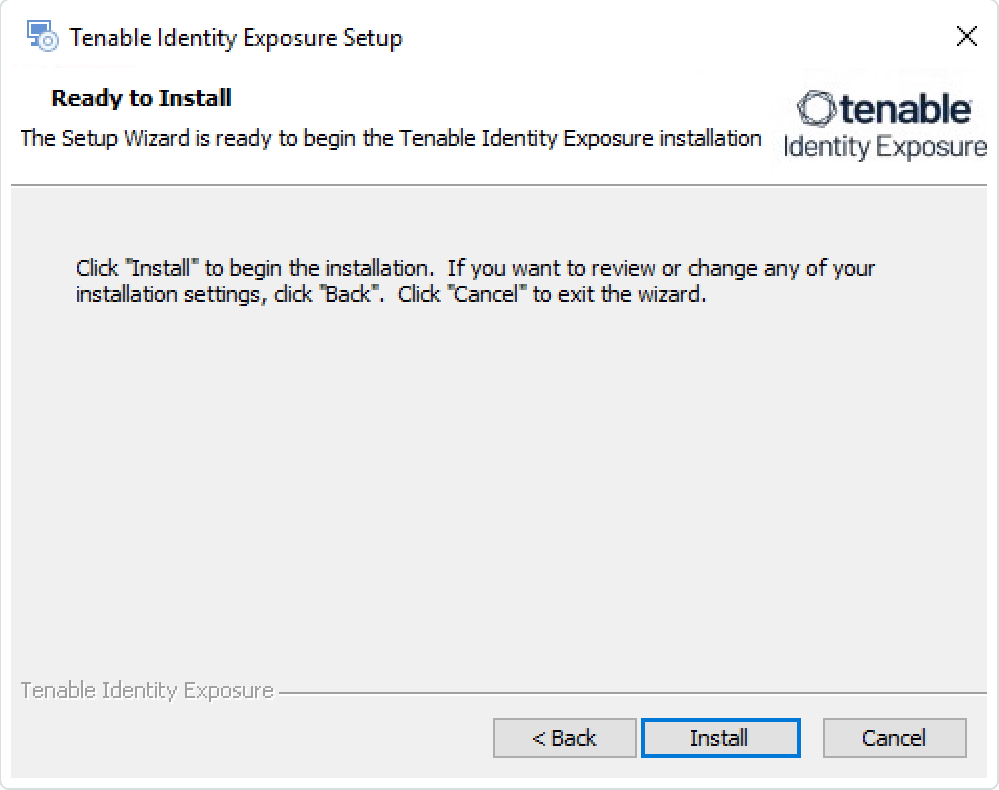
Complete the required fields.

Subnets separated by a comma (example: 192.168.1.1/32,192.168.1.3/32)

0.0.0.0/0

12. Click **Next**.

    The **Ready to Install** window appears.



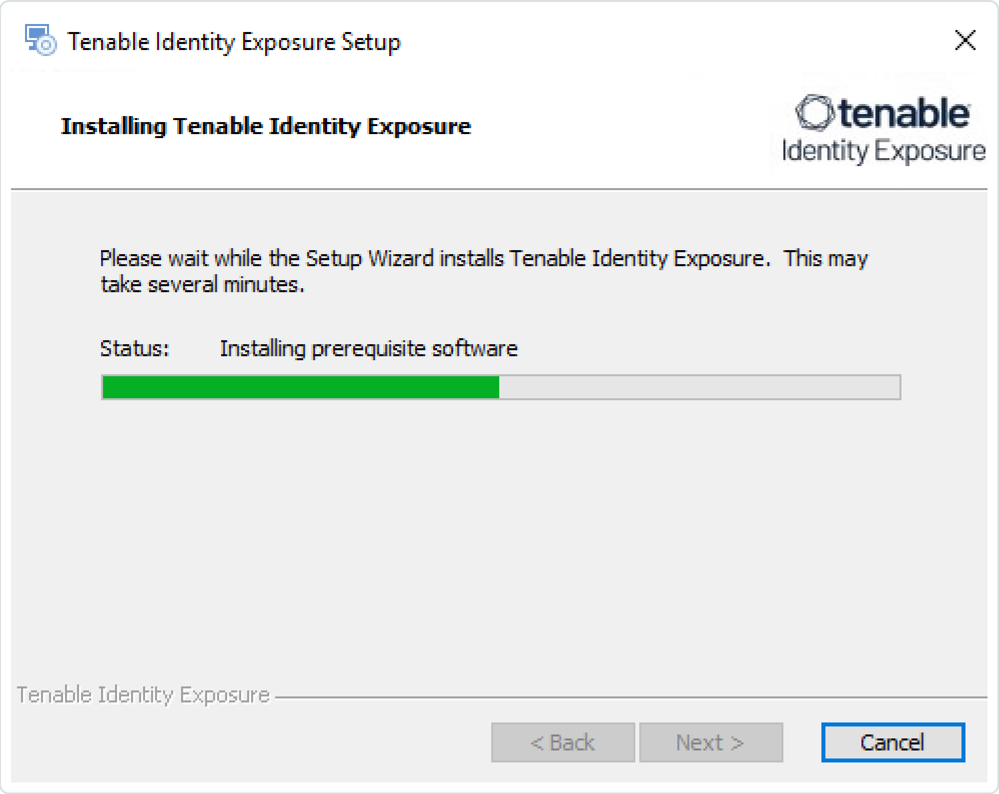
Tenable Identity Exposure Setup

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.

TLS Installation Types

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

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

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

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

TLS Installation Types

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

Installation Option	Recommended For	Encryption Between Internal Communications and Tenable Identity Exposure Components	Peer Verification
No TLS	A trusted network of machines. An easy installation with little configuration. This option falls back to the "Default TLS" option.	**Not encrypted**. Every component communicates in plain text, except for the Secure Relay that interacts with the Directory Listener.	**Disabled** Tenable Identity Exposure does not check server certificates. This setup is not resistant to active MITM attacks.
Default TLS (no "Expert mode")	An organization without its own internal public key infrastructure (PKI) that requires protection against passive eavesdropping.	**Encrypted** using an internal PKI for Tenable Identity Exposure with its own certificates and private keys, which the installation automatically generates and stores on the disk of the first machine.	
Default TLS ("Expert mode")			
Note: The default TLS installations — one that uses the "Expert" mode and one that does not — are essentially the same.			
Custom TLS	An organization	**Encrypted**, using certificates from	**Disabled**

Without Peer Verification	with its own internal PKI that requires protection against passive eavesdropping.	your internal PKI. Certificates must contain the IP address of the corresponding machine in the Subject Alternative Name (SAN) extension and a signature from the provided Certificate Authority (CA).	Tenable Identity Exposure does not check server certificates. This setup is not resistant to active MITM attacks.
Custom TLS With Peer Verification	An organization with its own internal public key infrastructure (PKI) that requires protection against both passive eavesdropping and man-in-the-middle (MITM) attacks.	**Encrypted**, using certificates from your internal PKI. Certificates must contain the IP address of the corresponding machine in the Subject Alternative Name (SAN) extension and have a signature from the provided Certificate Authority (CA).	**Enabled** Tenable Identity Exposure checks server certificates. This setup is resistant to active MITM attacks.

Update the TLS certificate

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

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

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

2. Restart Services.

Split Security Engine Node (SEN) Services

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

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

The installation process installs the following Tenable Identity Exposure components:

VM #	vCPU (per instance)	Memory (per instance)	Disk Space (per instance)	Recommended Service	Service Description
1	8 cores — at least 2.6 GHz	16 GB of RAM	1 TB	RabbitMQ	A message broker between services.
2	8 cores — at least 2.6 GHz	16 GB of RAM	100 GB	Attack Path	Computes attack path relations and maintaining them over time.
3	12 cores — at least 2.6 GHz	32 GB of RAM	300 GB	Cephei	Computes values for different analytics used for the Tenable Identity Exposure dashboards.
				CetiBridge	Communication plugins and service in charge of communicating with the Active Directory.
				Electra	Manages web sockets to

					update information without reloading the user interface.
				Enif	Authenticates web users.
				Eridanis	Connects to the SQL Server; ensures the exactness of Tenable Identity Exposure's information.
				Eltanin	Sends data to the Tenable Cloud, if enabled in Tenable Identity Exposure.
				Health Check	Alerts configuration anomalies leading to connectivity or other issues in the infrastructure.
				Kapteyn	Runs in the end user's browser to show the user interface.
4	16 cores —	16 GB of	100 GB	Cancri	Decodes raw

	at least 2.6 GHz	RAM			information; fetches delta between events; computes event type.
				EventLogsDecoder	Decodes information related to IOA events.
5	16 cores — at least 2.6 GHz	32 GB of RAM	100 GB	Cygni	Computes deviances and attacks.

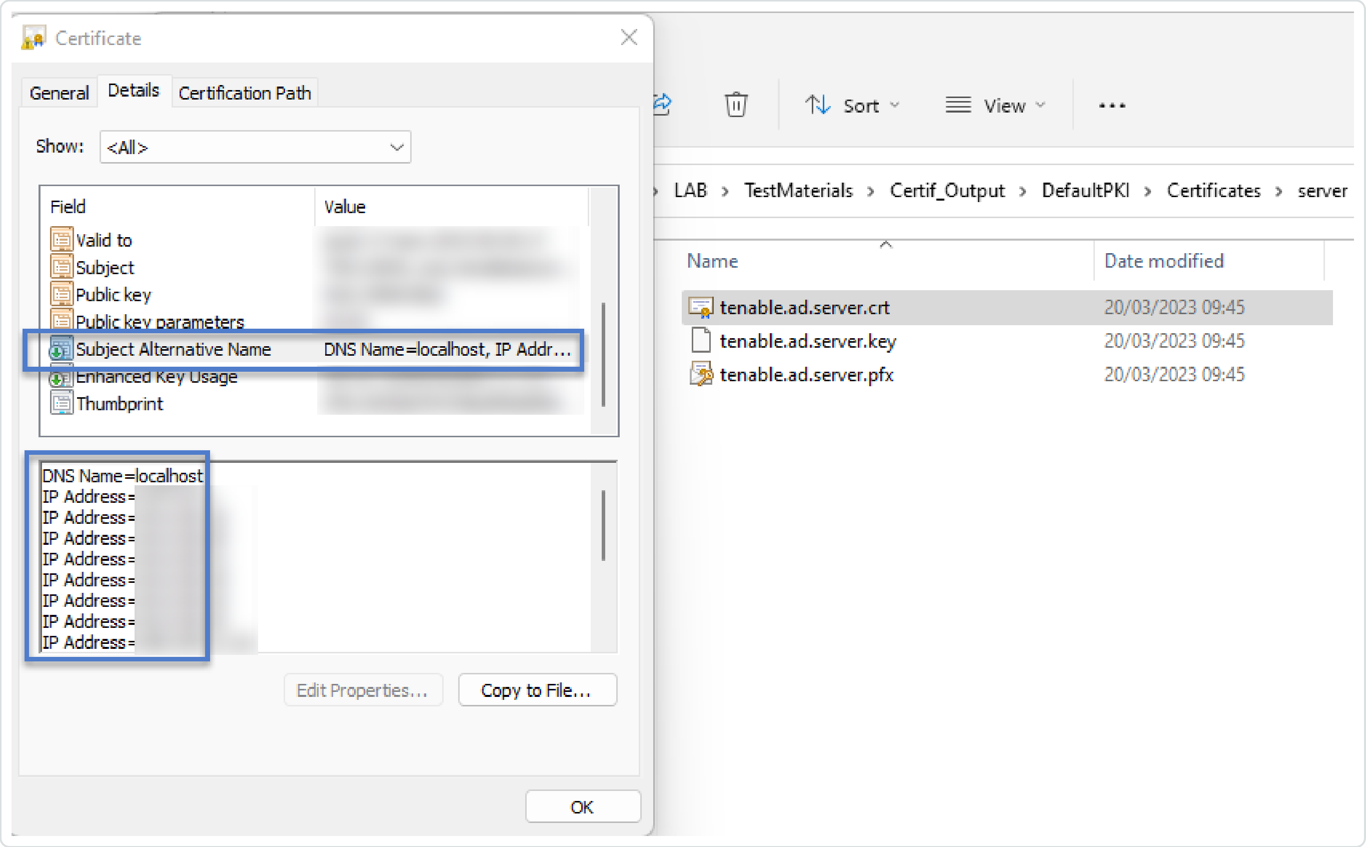
For more information, see Resource Sizing for requirements.

SEN Installation on Several Machines

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

Public Key Infrastructure (PKI) Certificate

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



Field	Value
Valid to	[redacted]
Subject	[redacted]
Public key	[redacted]
Public key parameters	[redacted]
Subject Alternative Name	DNS Name=localhost, IP Addr...
Enhanced Key Usage	[redacted]
Thumbprint	[redacted]

```
DNS Name=localhost
IP Address=[redacted]
IP Address=
IP Address=
IP Address=
IP Address=
IP Address=
IP Address=
IP Address=
```

Name	Date modified
tenable.ad.server.crt	20/03/2023 09:45
tenable.ad.server.key	20/03/2023 09:45
tenable.ad.server.pfx	20/03/2023 09:45

Example

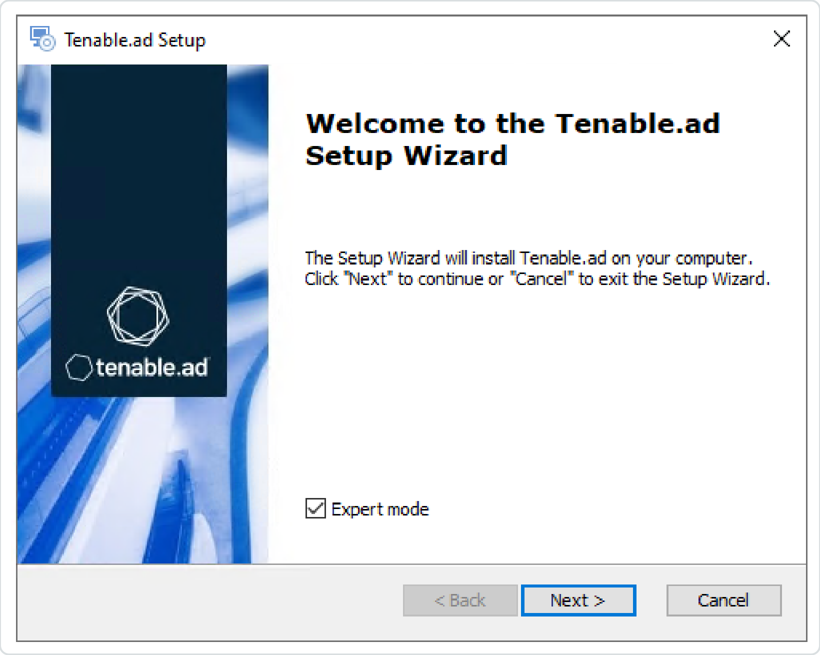
The following example shows an installation of RabbitMQ and Attack Path on one virtual machine.

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

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

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

   The **Setup Wizard** appears.


Tenable.ad Setup

Welcome to the Tenable.ad Setup Wizard

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

☑ Expert mode

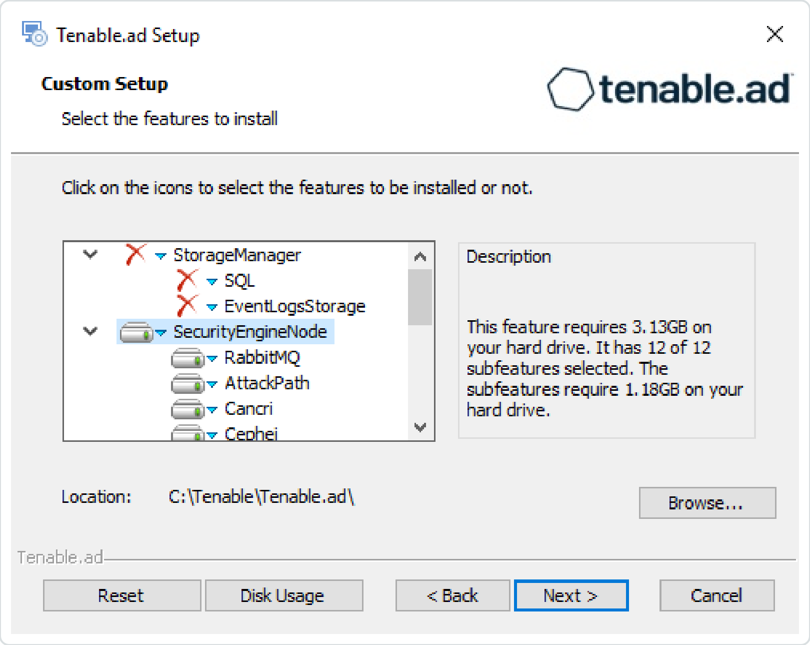
2. Select the **Expert Mode** check box.

3. Click **Next**.

   The **Custom Setup** window appears.

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

5. Deselect all SEN services except for *RabbitMQ* and *AttackPath*.


Tenable.ad Setup

Custom Setup

Select the features to install

Click on the icons to select the features to be installed or not.

Description

This feature requires 3.13GB on your hard drive. It has 12 of 12 subfeatures selected. The subfeatures require 1.18GB on your hard drive.

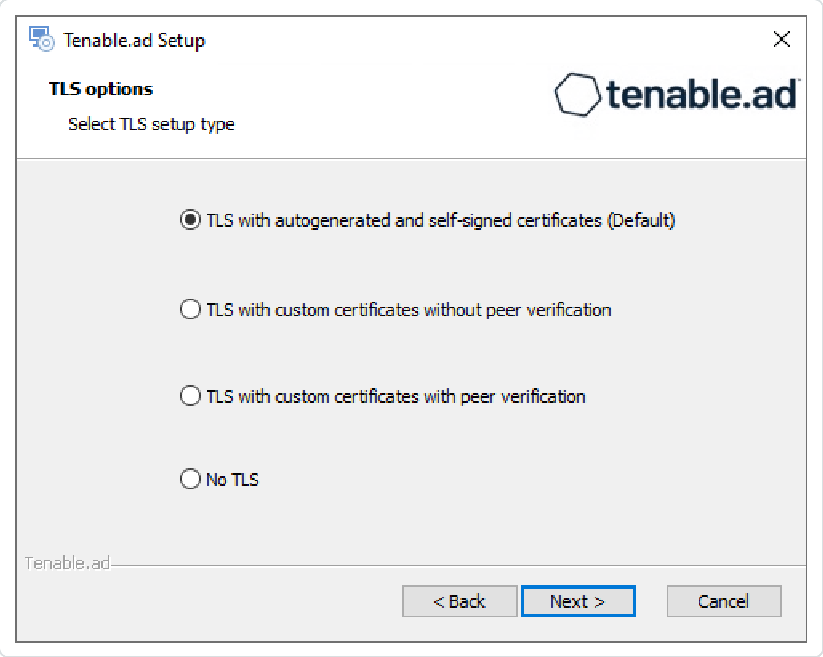
Location: C:\Tenable\Tenable.ad\

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

7. Click **Next**.

   The **TLS Options** window appears.

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



Tenable.ad 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

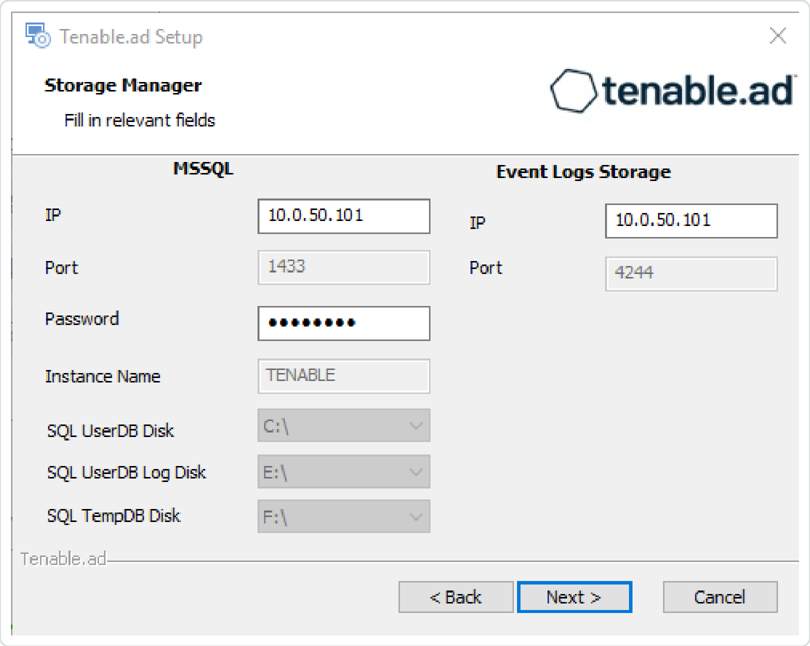
○ No TLS

9. Click **Next**.

   The **Storage Manager** window appears.

10. Provide the following information:

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



Storage Manager

Fill in relevant fields

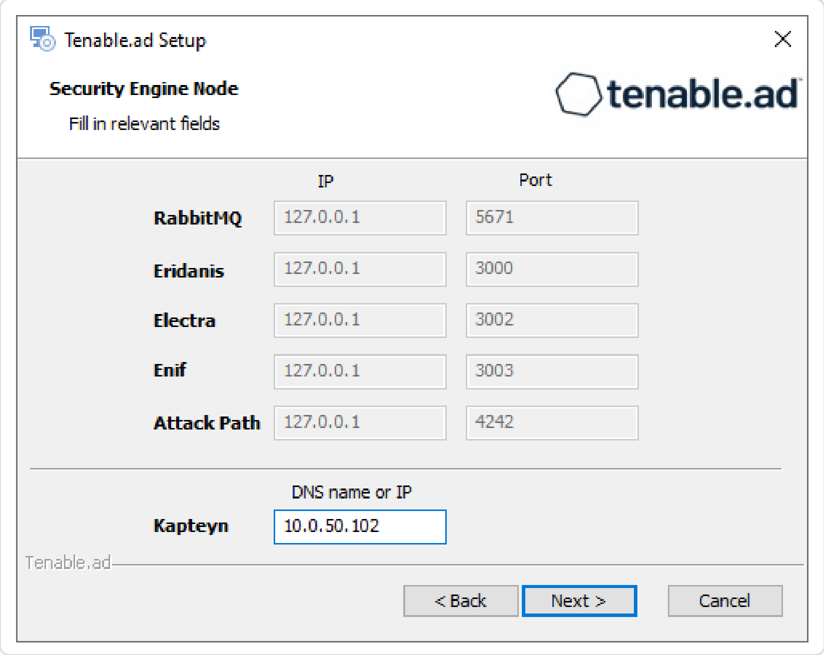
	MSSQL
IP	10.0.50.101
Port	1433
Password	••••••••
Instance Name	TENABLE
SQL UserDB Disk	C:\
SQL UserDB Log Disk	E:\
SQL TempDB Disk	F:\

	Event Logs Storage
IP	10.0.50.101
Port	4244

11. Click **Next**.

    The **Security Engine Node** window appears.

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



Security Engine Node

Fill in relevant fields

	IP	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

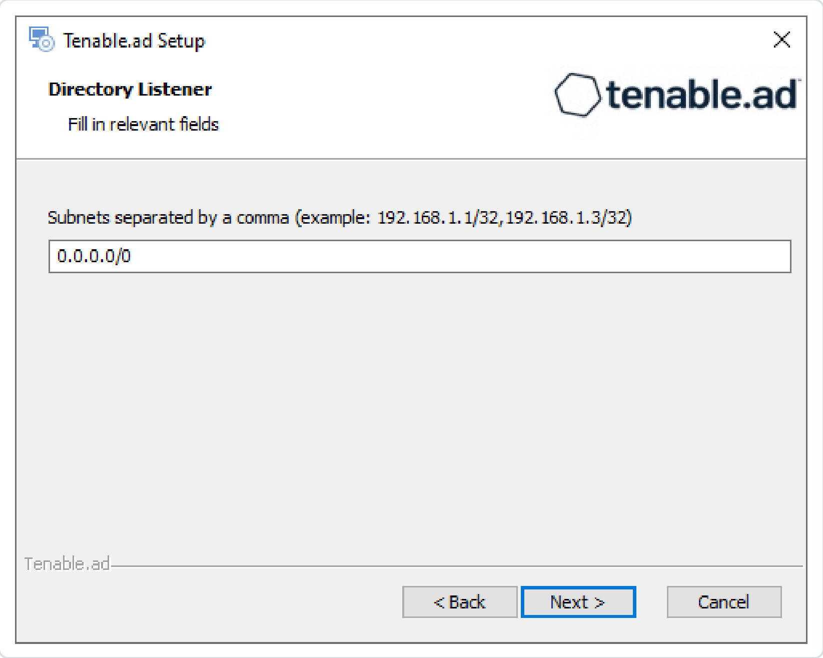
	DNS name or IP
Kapteyn	10.0.50.102

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

13. Click **Next**.

14. The **Directory Listener** window appears.

15. In the **Subnets** box, type the subnet address for the Directory Listener. For multiple subnets, use a comma to separate the addresses.



Tenable.ad Setup

Directory Listener

Fill in relevant fields

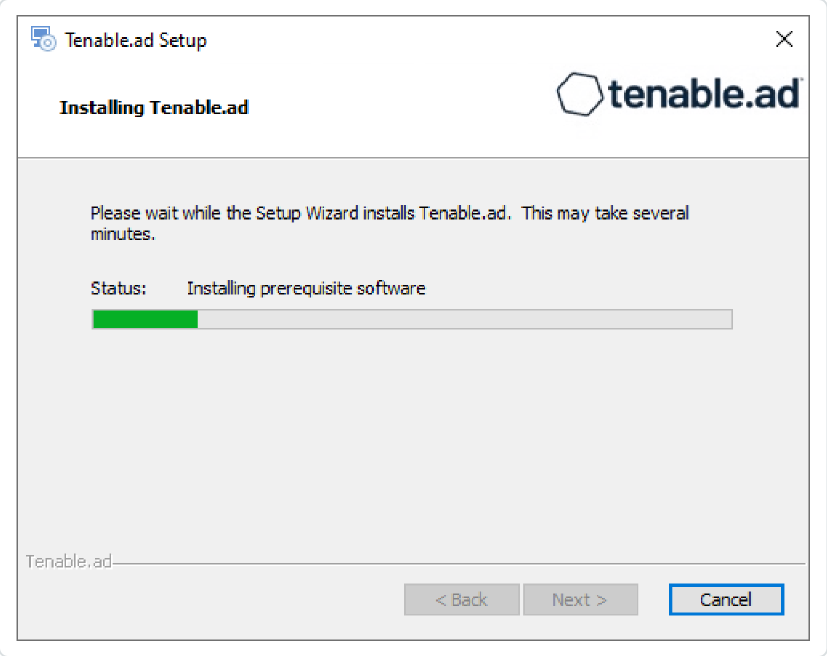
Subnets separated by a comma (example: 192.168.1.1/32,192.168.1.3/32)

0.0.0.0/0

16. Click **Next**.

    The **Ready to Install** window appears.

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



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

Status: Installing prerequisite software

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

18. Click **Finish**.

A dialog box asks you to restart your machine.

19. Click **No**.

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

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

See also

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

Upgrade Tenable Identity Exposure

Required User Role: Administrator on the local machine

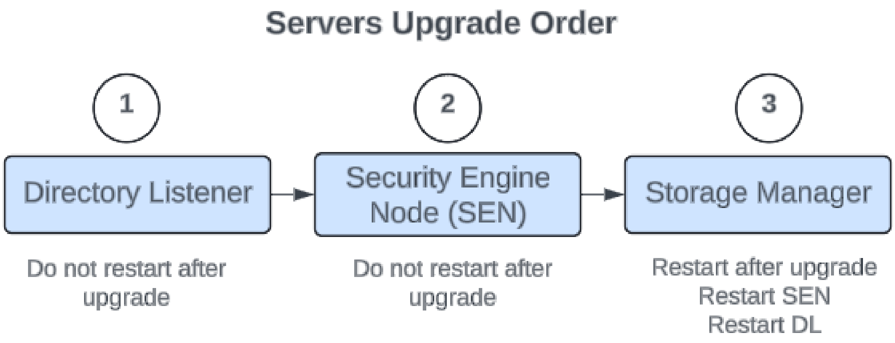
Upgrade Path

To upgrade to the latest version of Tenable Identity Exposure, you must follow this installation path: 2.7 -> 3.1 -> 3.11 -> 3.19 -> 3.29 -> 3.42.

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

Upgrade Order

To upgrade to **Tenable Identity Exposure 3.42**, proceed in the following order:



Before you start

- **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.
- **Back up and restore the Storage Manager**. Tenable strongly recommends that you back up the Storage Manager before you upgrade. For instructions on how to back up or restore MSSQL, see the official Microsoft documentation.
- **Consider the downtime**: Depending on your environment and the magnitude of the upgrade, downtime can range from minutes to several hours. Factor this into your scheduling and communication plan. Inform impacted users of the scheduled downtime and potential service disruption.

- **Download the executable programs** for Tenable Identity Exposure and Secure Relay from Tenable’s Downloads site.
- **Run the installer as a local user or a domain user** who is a member of the **Local Administrators** group.
- **Restart your server** before launching the Tenable Identity Exposure installer for each component.

Upgrade Procedures

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

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

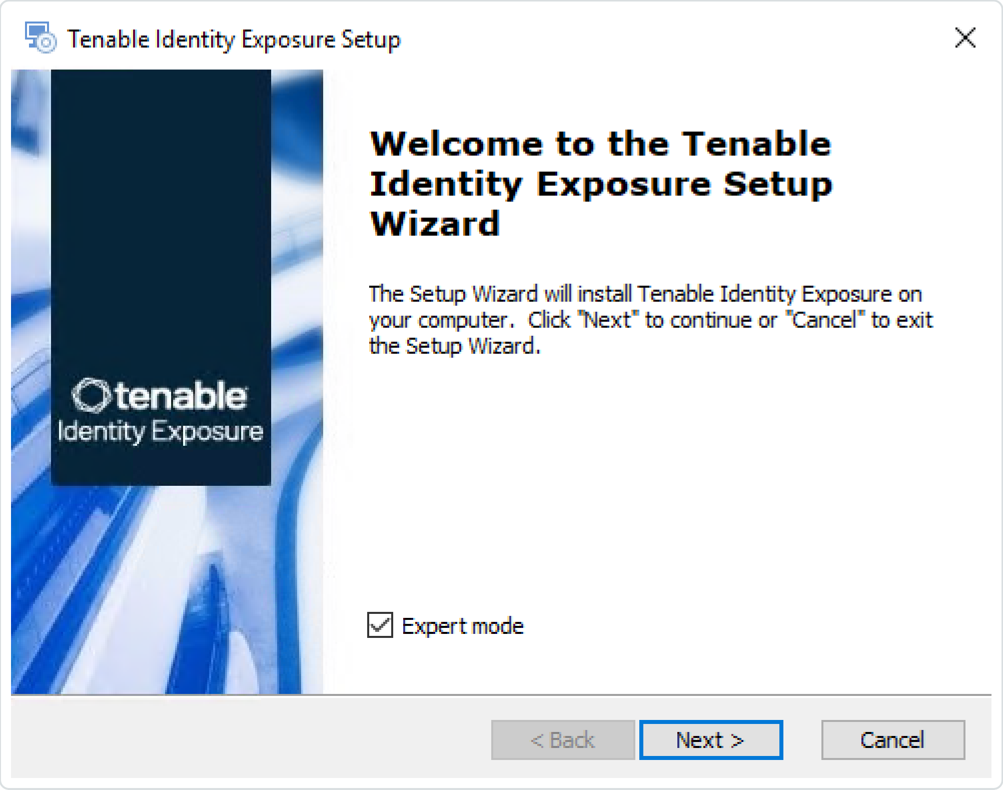
To upgrade the Directory Listener:

1. On the local machine, restart the server and run the **Tenable Identity Exposure 3.42** 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.



Tenable Identity Exposure Setup

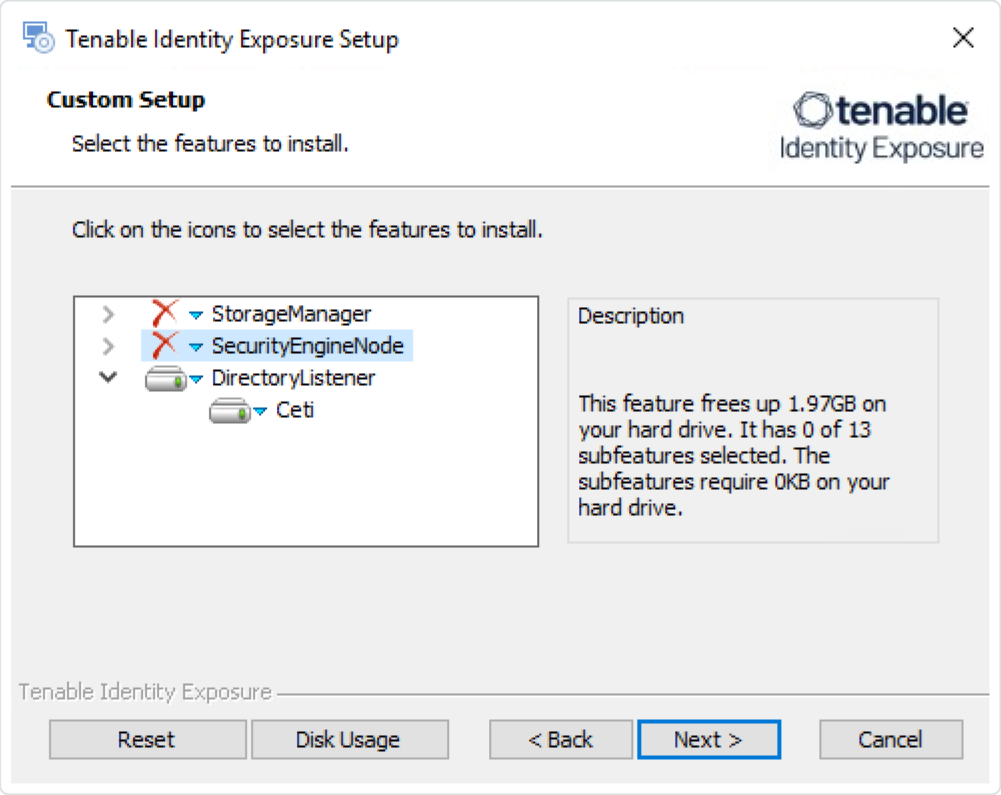
Welcome to the Tenable Identity Exposure Setup Wizard

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.



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

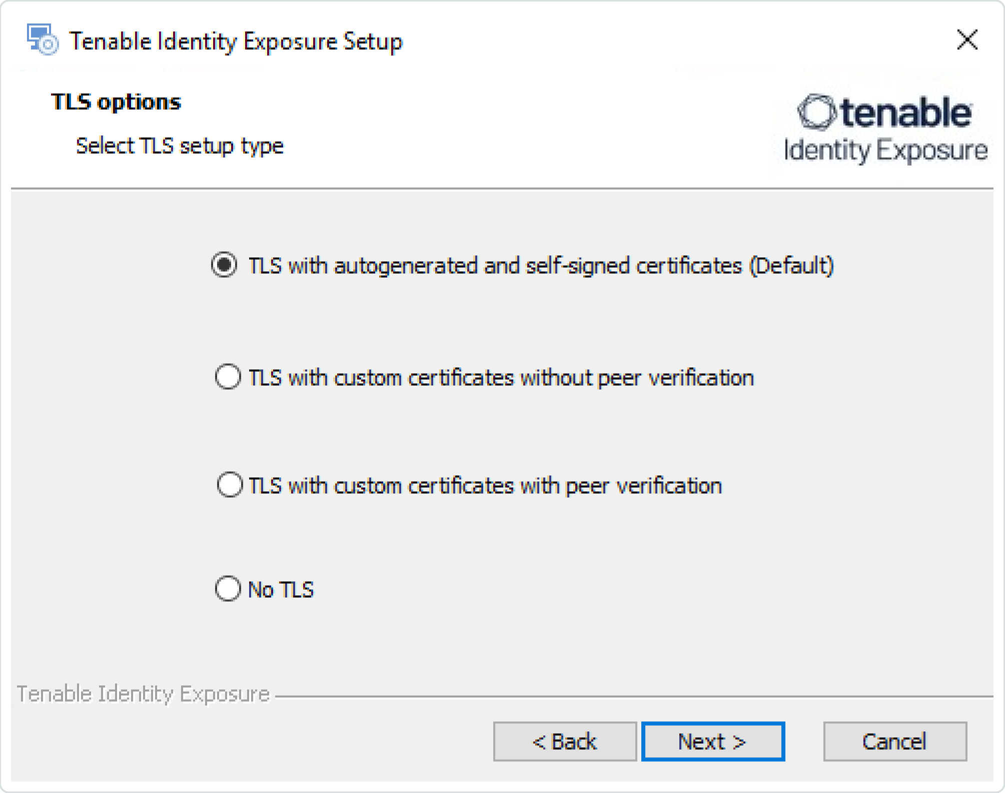
Description

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)

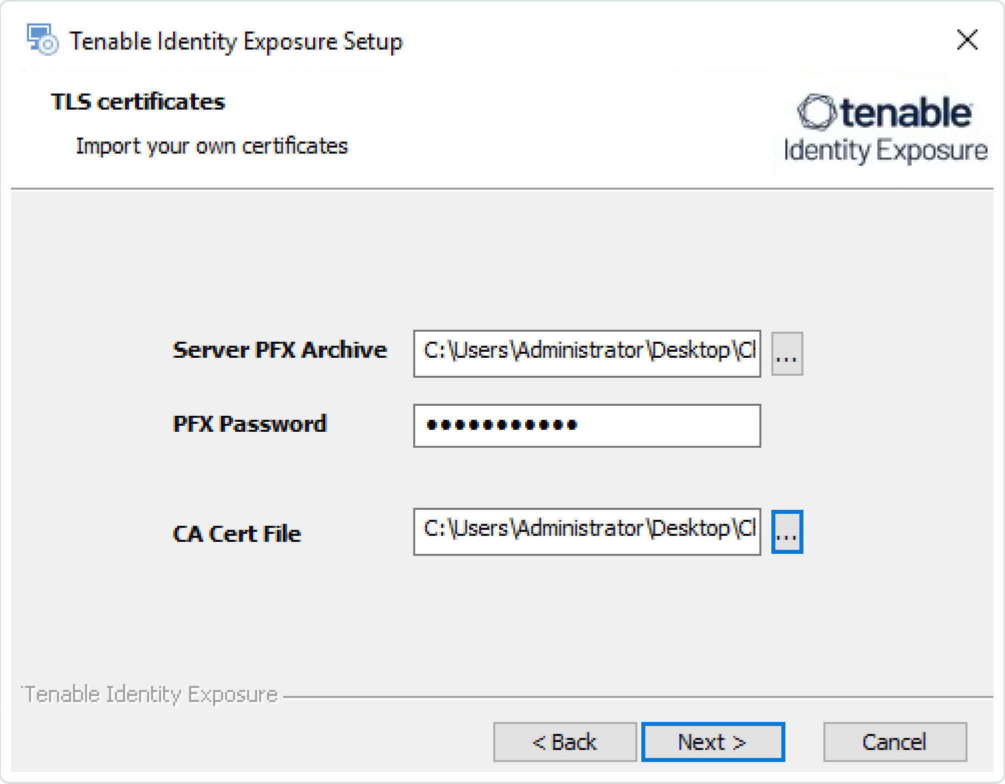
○ TLS with custom certificates without peer verification

○ 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.


Tenable Identity Exposure Setup
TLS certificates
Import your own certificates
tenable
Identity Exposure
Tenable Identity Exposure
< Back
Next >
Cancel

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

PFX Password: ●●●●●●●●●●●●

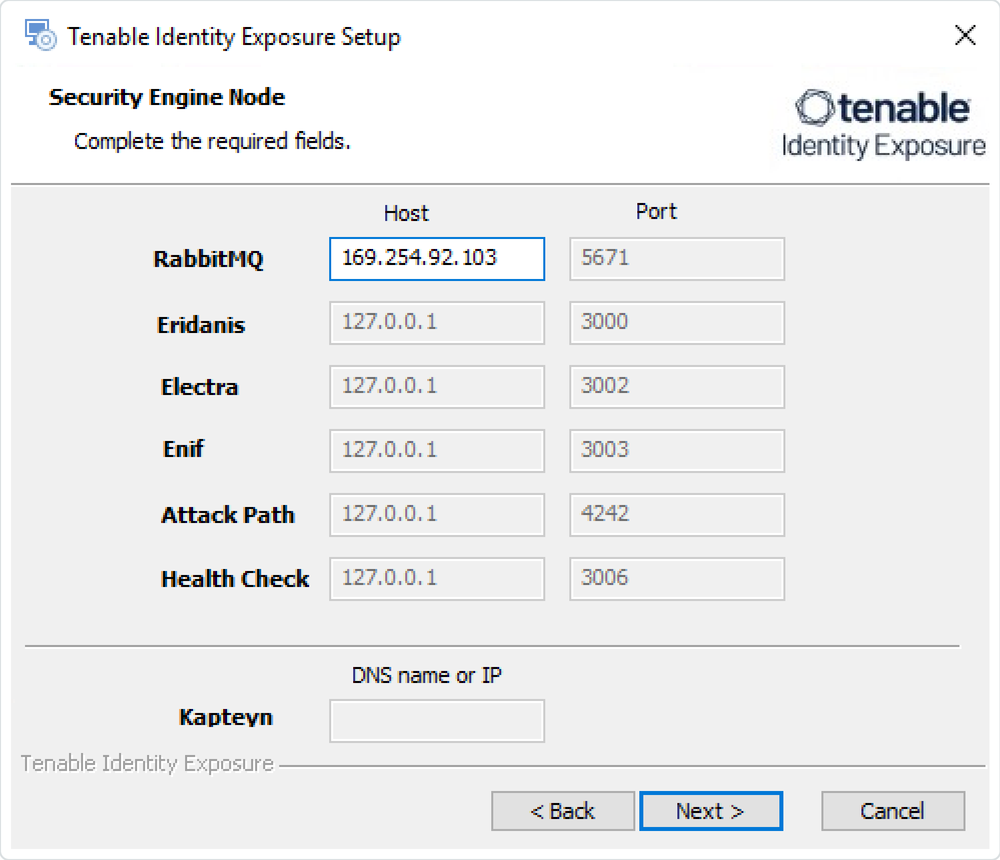
CA Cert File: C:\Users\Administrator\Desktop\Cl

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.

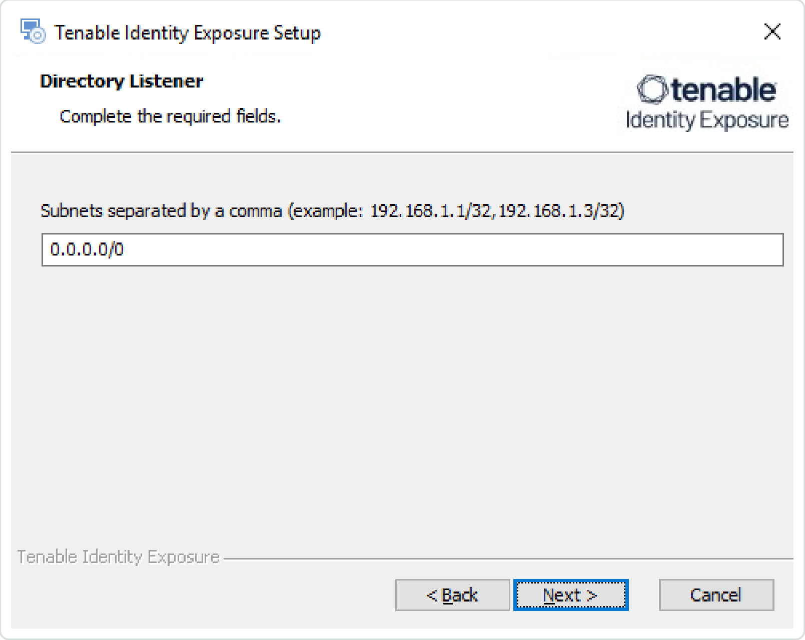
	Host	Port
RabbitMQ	169.254.92.103	5671
Eridanis	127.0.0.1	3000
Electra	127.0.0.1	3002
Enif	127.0.0.1	3003
Attack Path	127.0.0.1	4242
Health Check	127.0.0.1	3006

	DNS name or IP
Kapteyn	

8. Click **Next**.

   The **Directory Listener** window appears.

9. In the **Subnets** box (if applicable), type the subnet information for the Directory Listener.



Tenable Identity Exposure Setup

Directory Listener

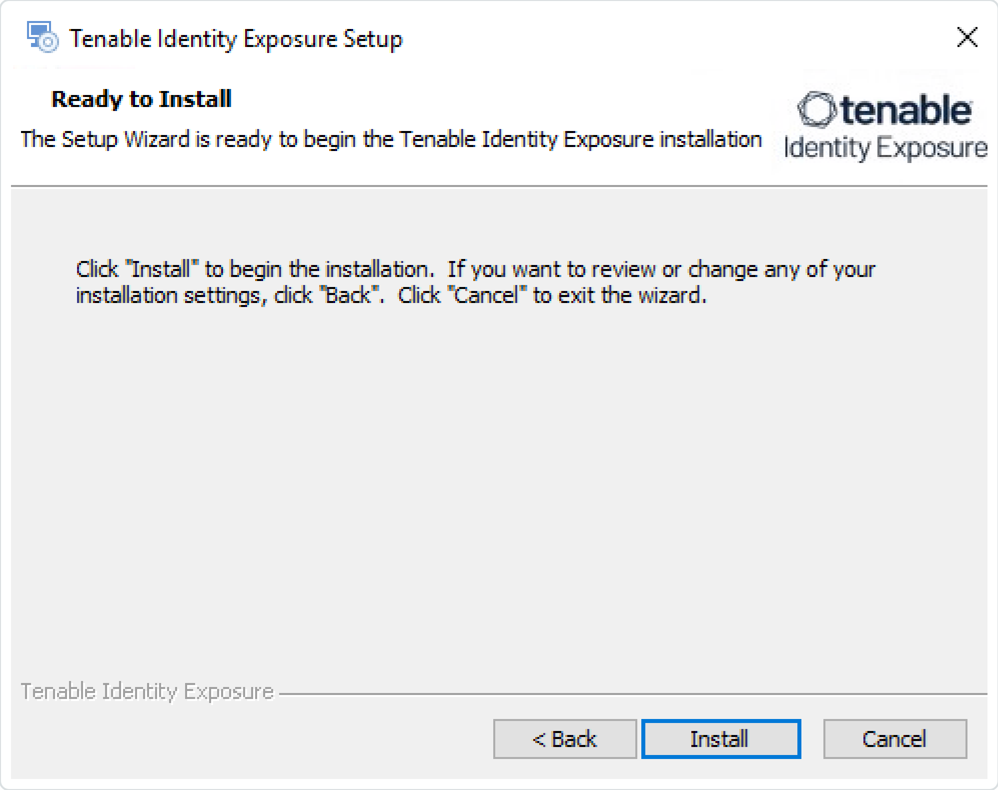
Complete the required fields.

Subnets separated by a comma (example: 192.168.1.1/32,192.168.1.3/32)

0.0.0.0/0

10. Click **Next**.

    The **Ready to Install** window appears.



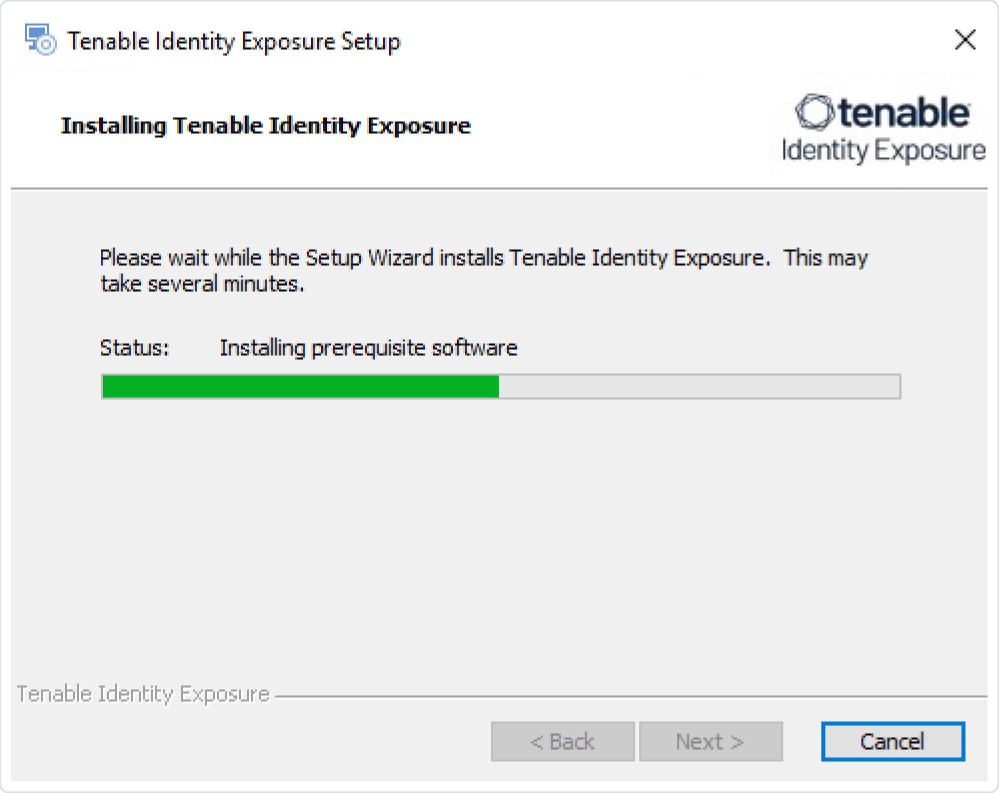
Tenable Identity Exposure Setup

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).

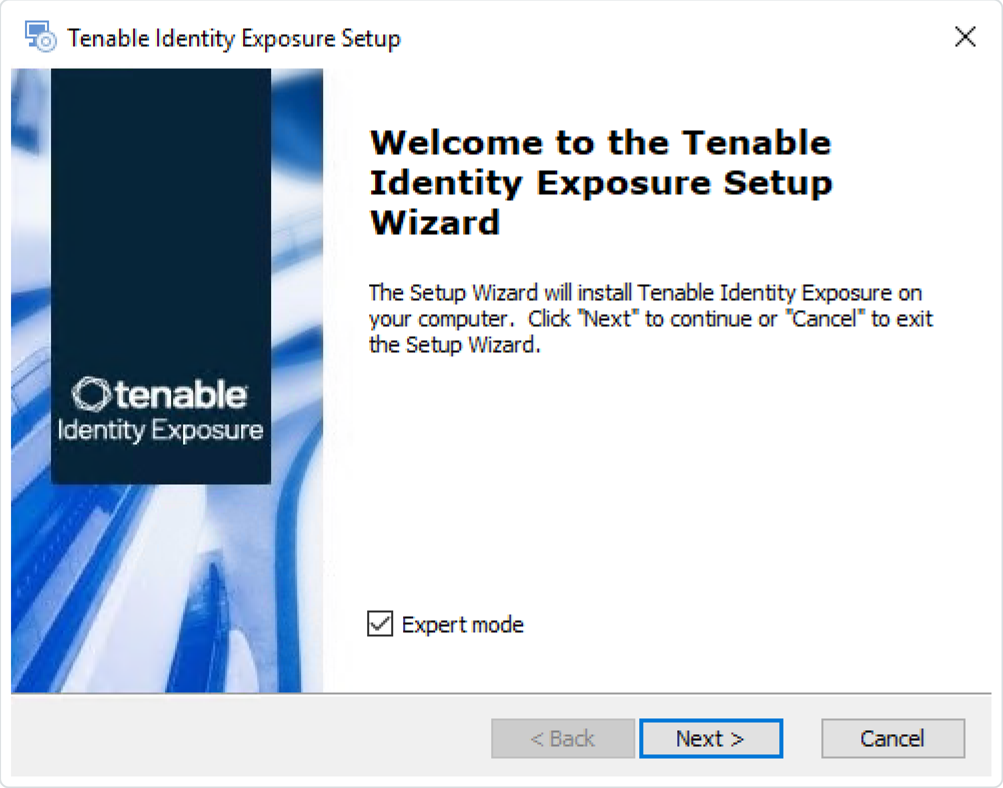
To upgrade the SEN:

1. On the local machine, restart the server and run the **Tenable Identity Exposure 3.42** 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

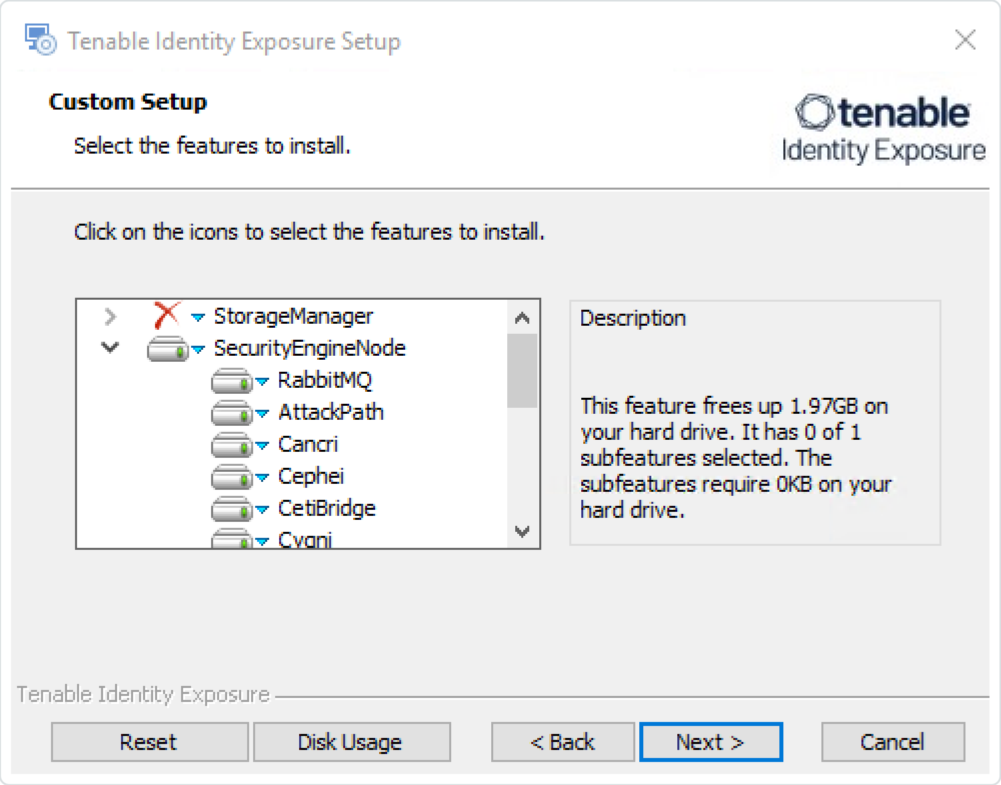
Welcome to the Tenable Identity Exposure Setup Wizard

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.

- StorageManager
- SecurityEngineNode
  - RabbitMQ
  - AttackPath
  - Cancri
  - Cephei
  - CetiBridge
  - Cygni

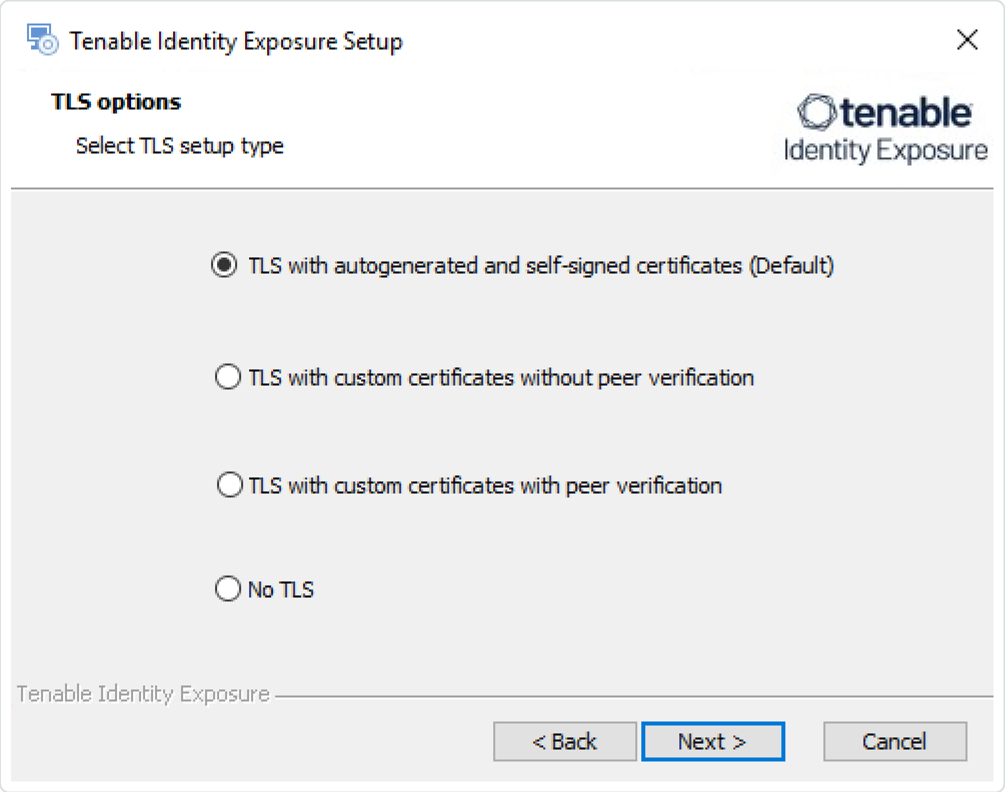
Description

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.

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.



Tenable Identity Exposure Setup

TLS options

Select TLS setup type

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

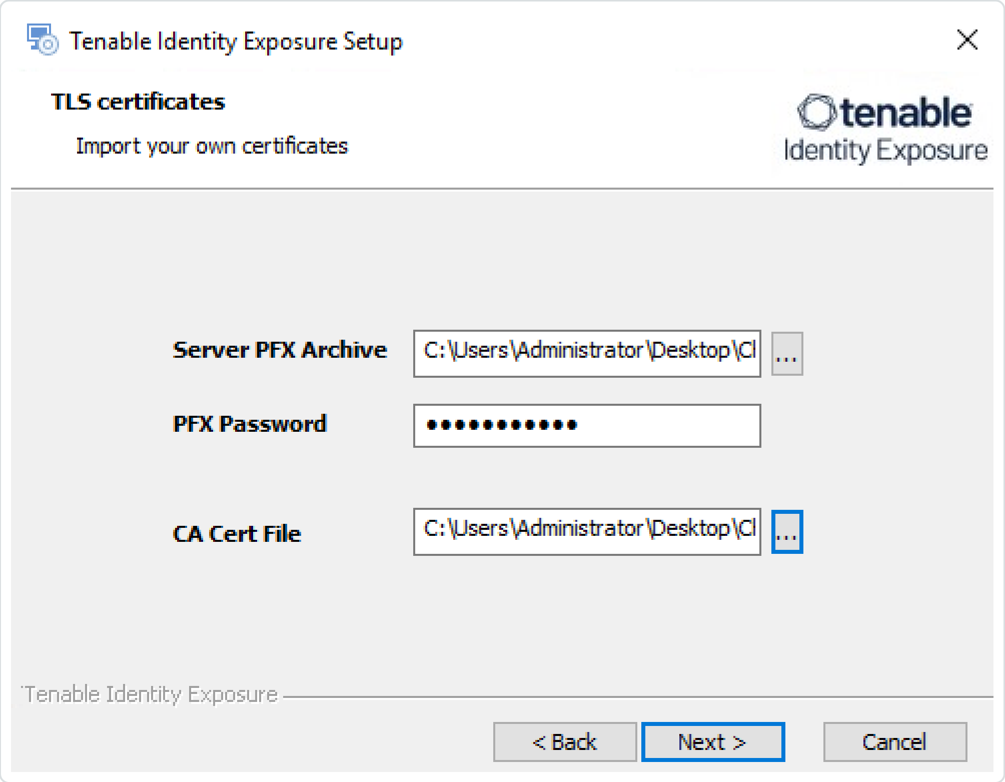
○ TLS with custom certificates without peer verification

○ 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

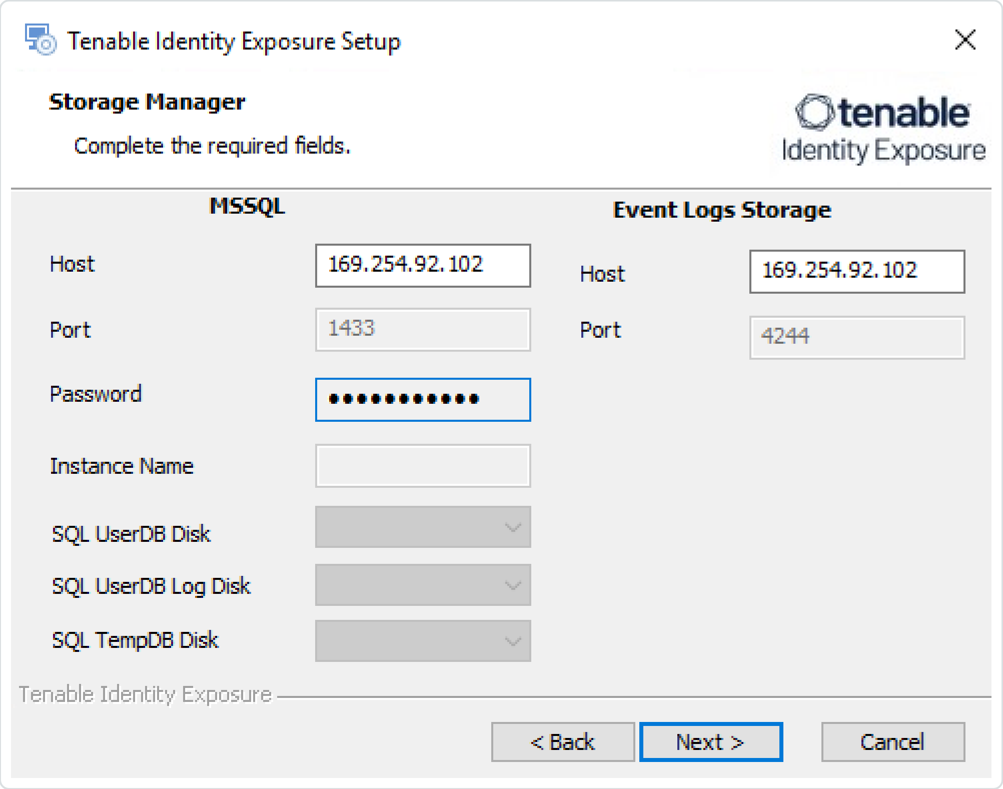
6. Click **Next**.

   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.

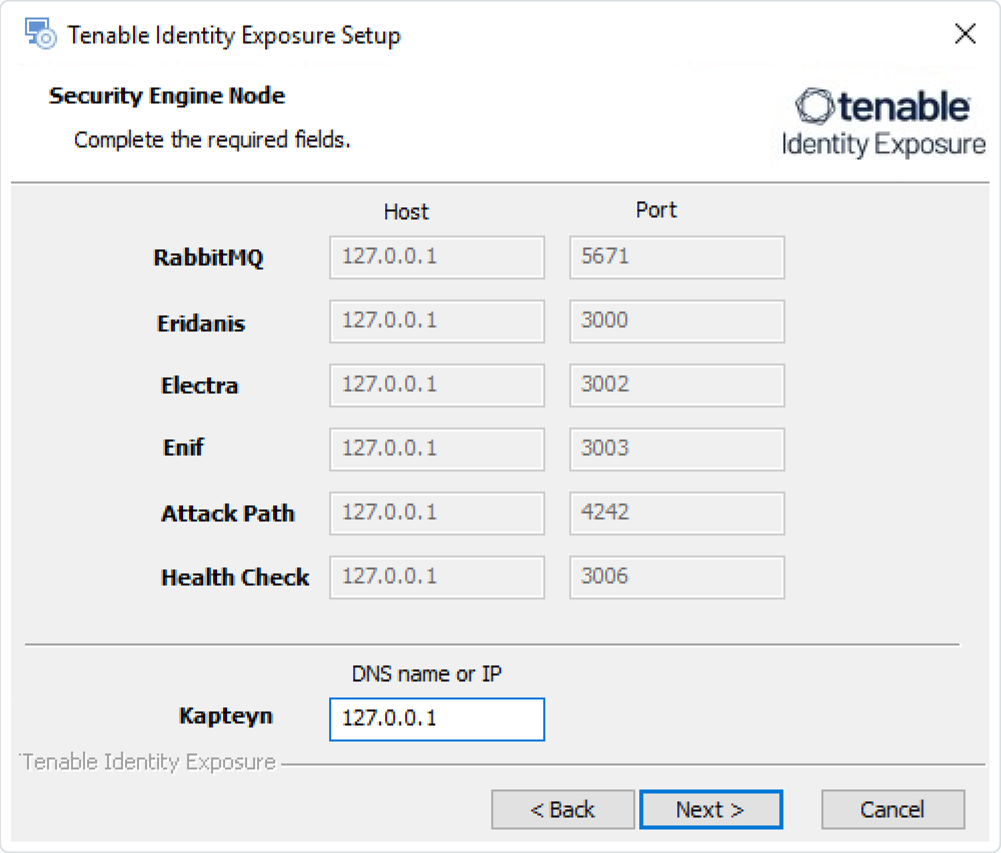
MSSQL		**Event Logs Storage**	
Host	169.254.92.102	Host	169.254.92.102
Port	1433	Port	4244
Password	●●●●●●●●●●●		
Instance Name			
SQL UserDB Disk			
SQL UserDB Log Disk			
SQL TempDB Disk			

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 `ALSID_CASSIOPEIA_CYGNI_Service__EventLogsStorage__Host` and `ALSID_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

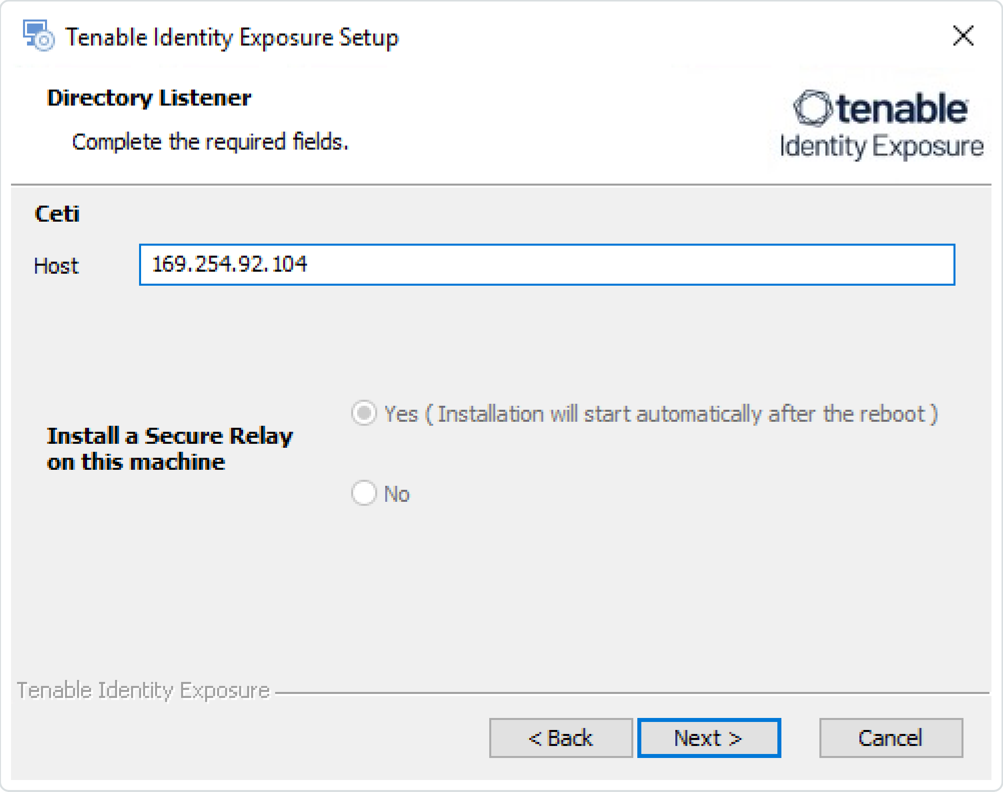
	DNS name or IP
Kapteyn	127.0.0.1

Tenable Identity Exposure

10. Click **Next**.

    The **Directory Listener** window appears.

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



Tenable Identity Exposure Setup

Directory Listener

Complete the required fields.

Ceti

Host: 169.254.92.104

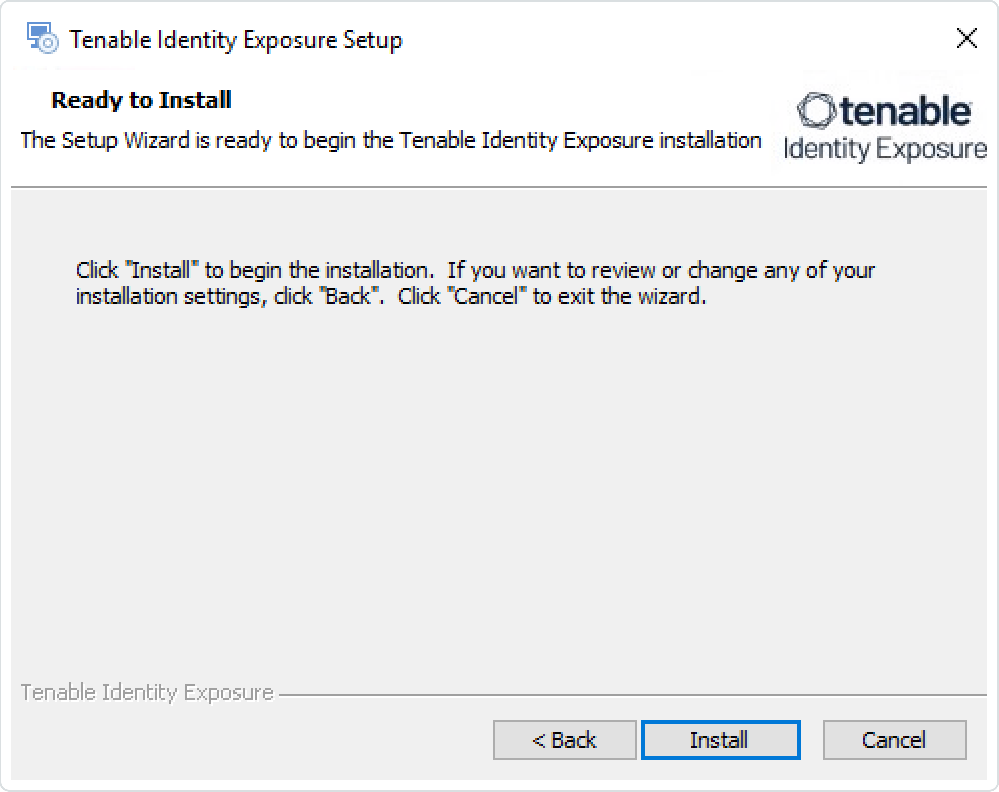
Install a Secure Relay on this machine

● Yes (Installation will start automatically after the reboot)

○ No

12. Click **Next**.

    The **Ready to Install** window appears.



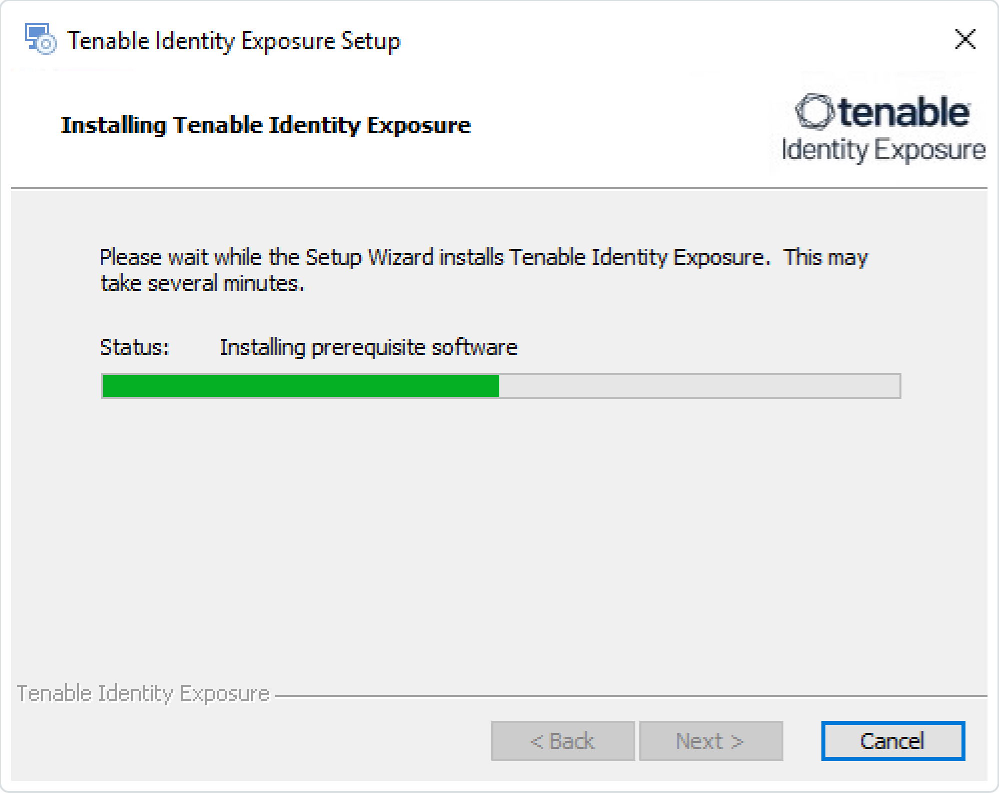
Tenable Identity Exposure Setup

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 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.

14. Click **Finish**.

    A dialog box asks you to restart your machine.

15. Click **No**.

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

16. Upgrade the Storage Manager.

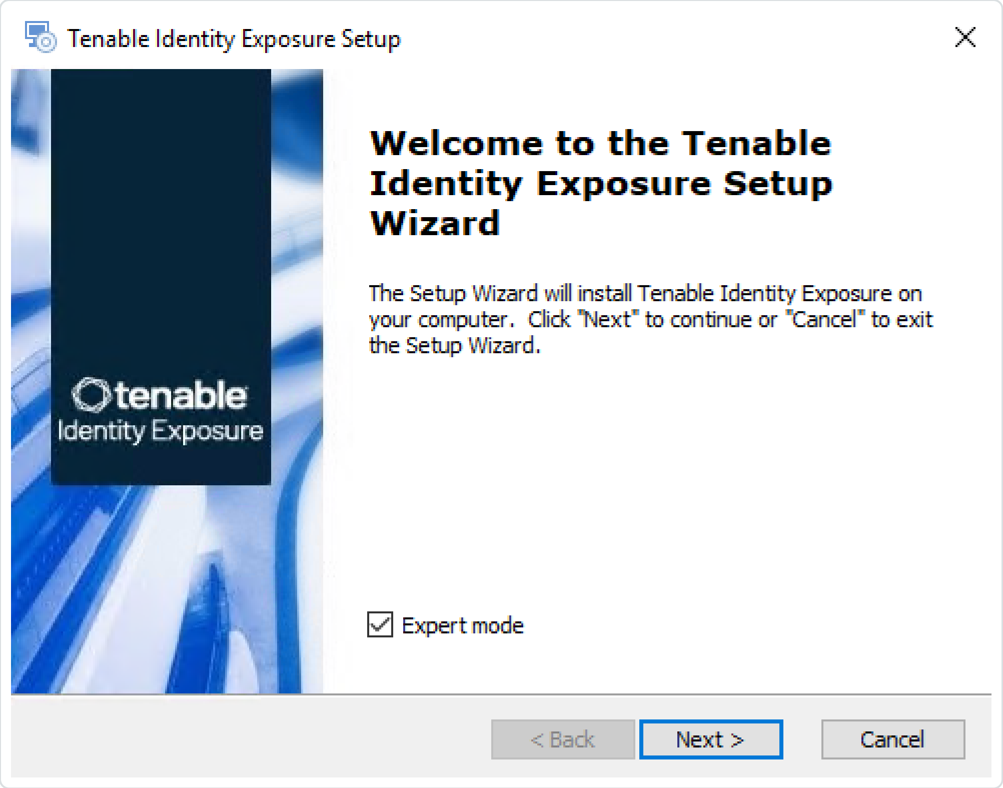
To upgrade the Storage Manager:

1. On the local machine, restart the server and run the **Tenable Identity Exposure 3.42** 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

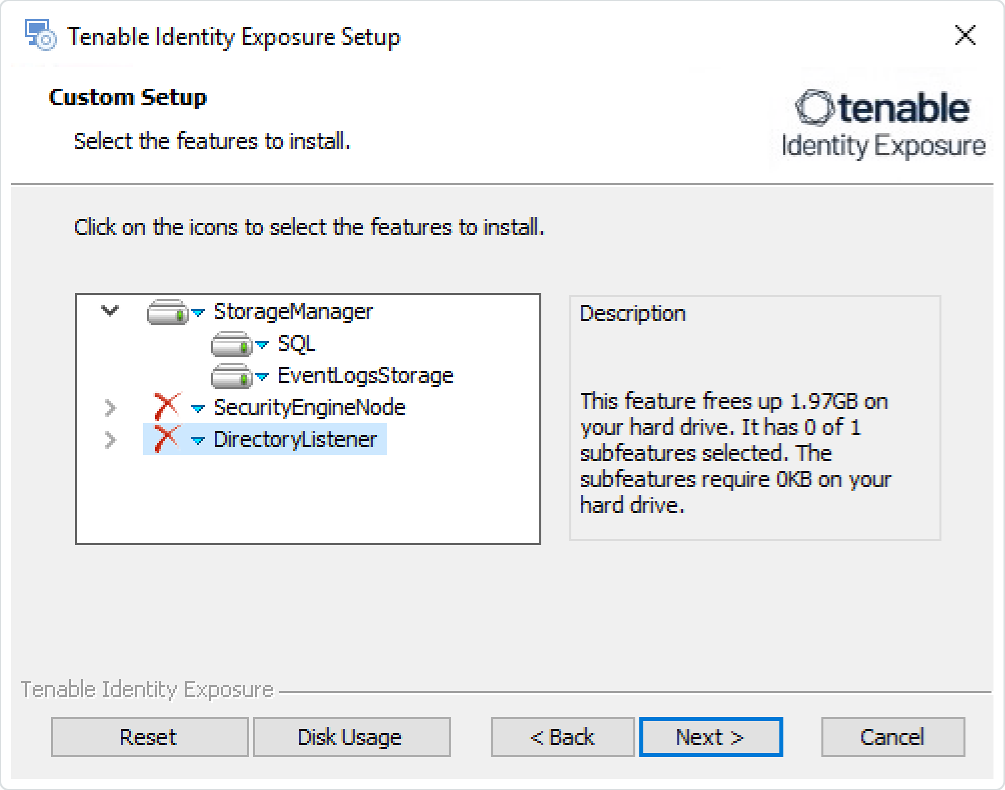
Welcome to the Tenable Identity Exposure Setup Wizard

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.

   - StorageManager
     - SQL
     - EventLogsStorage
   - SecurityEngineNode
   - DirectoryListener

   Description

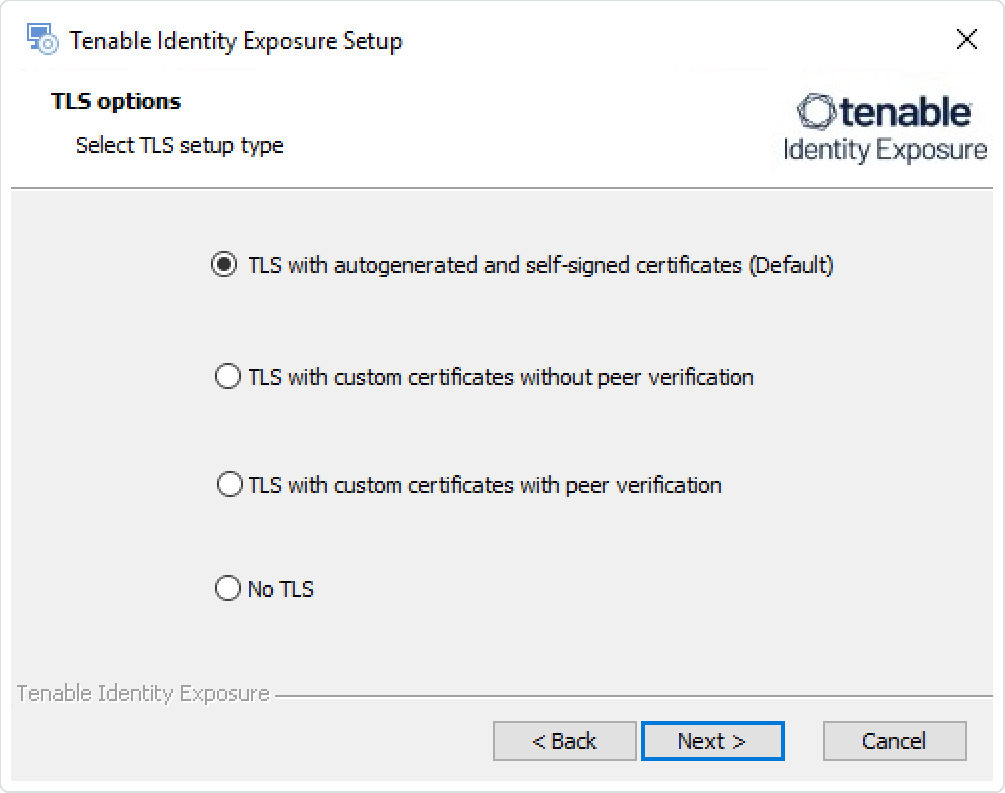
   This feature frees up 1.97GB on your hard drive. It has 0 of 1 subfeatures selected. The subfeatures require 0KB on your hard drive.

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.



Tenable Identity Exposure Setup

TLS options

Select TLS setup type

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

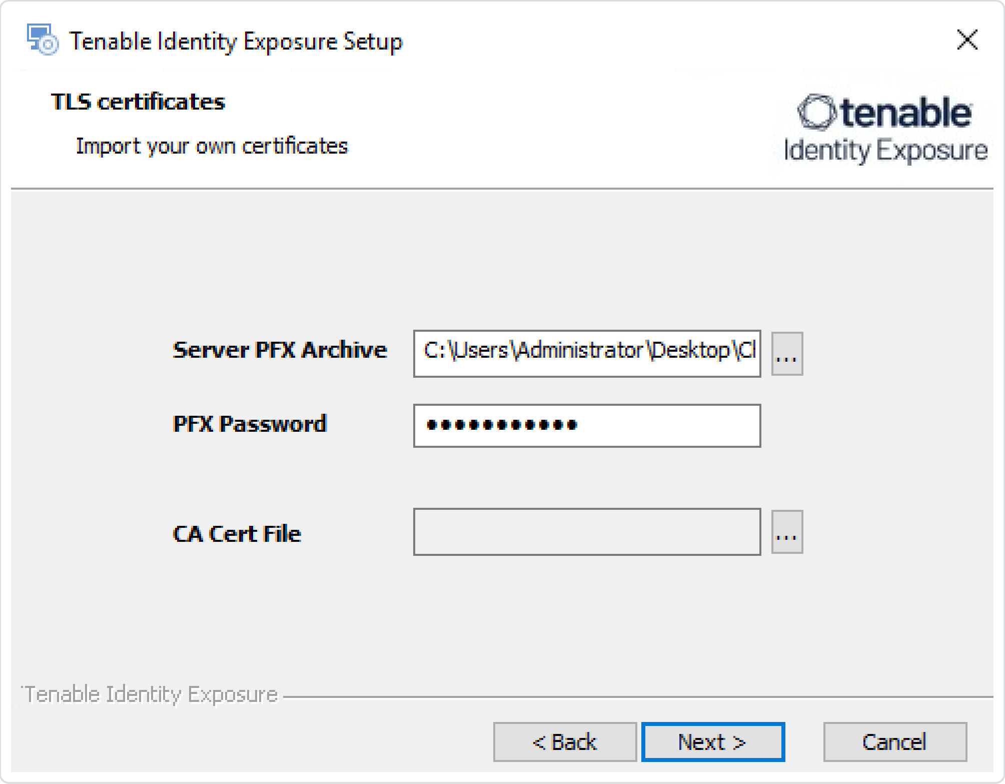
○ TLS with custom certificates without peer verification

○ 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 **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: ●●●●●●●●●●●●

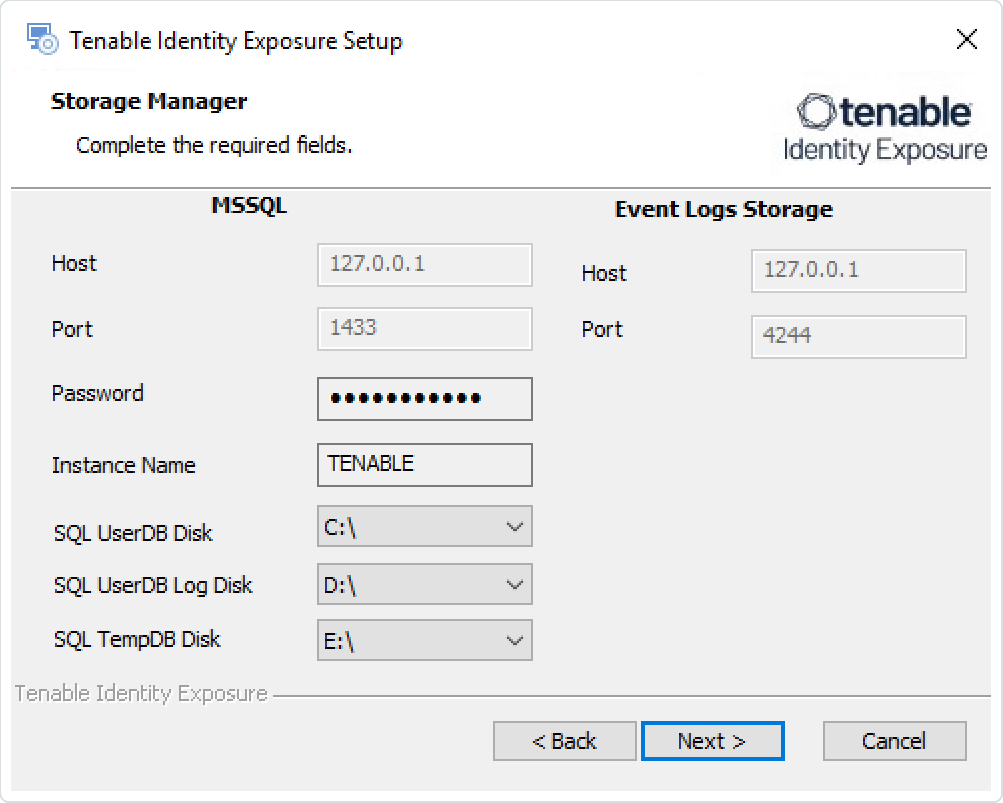
CA Cert File:

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

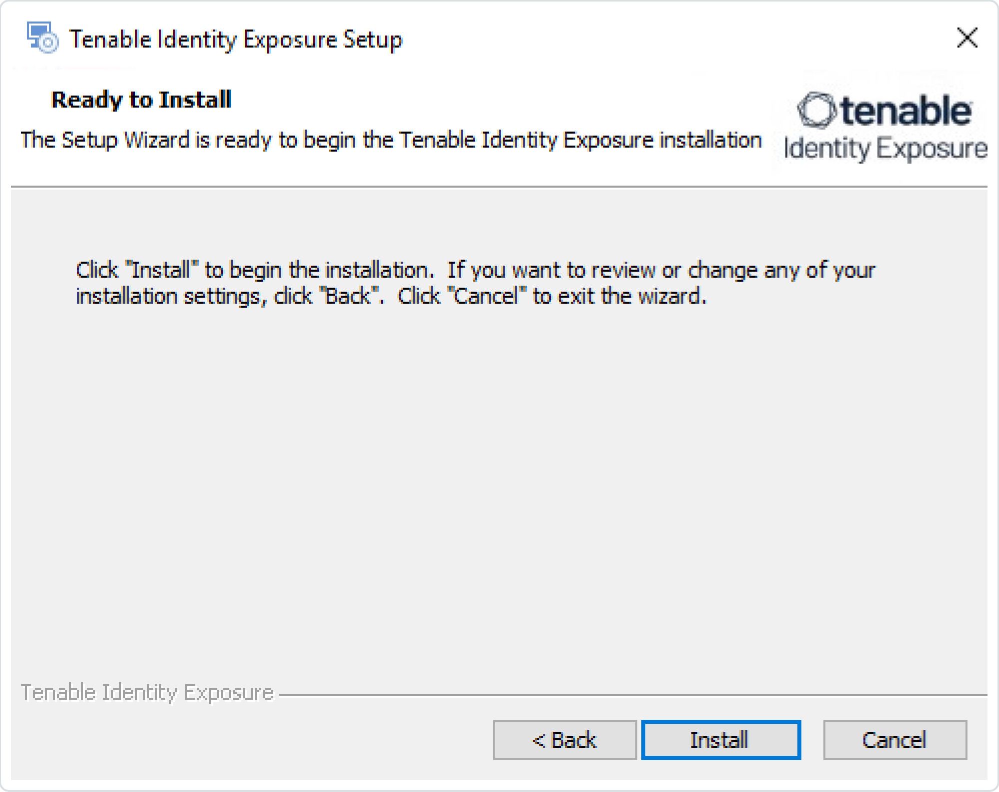
Host	127.0.0.1
Port	1433
Password	●●●●●●●●●●●●
Instance Name	TENABLE
SQL UserDB Disk	C:\
SQL UserDB Log Disk	D:\
SQL TempDB Disk	E:\

Event Logs Storage

Host	127.0.0.1
Port	4244

9. Click **Next**.

   The **Ready to Install** window appears.



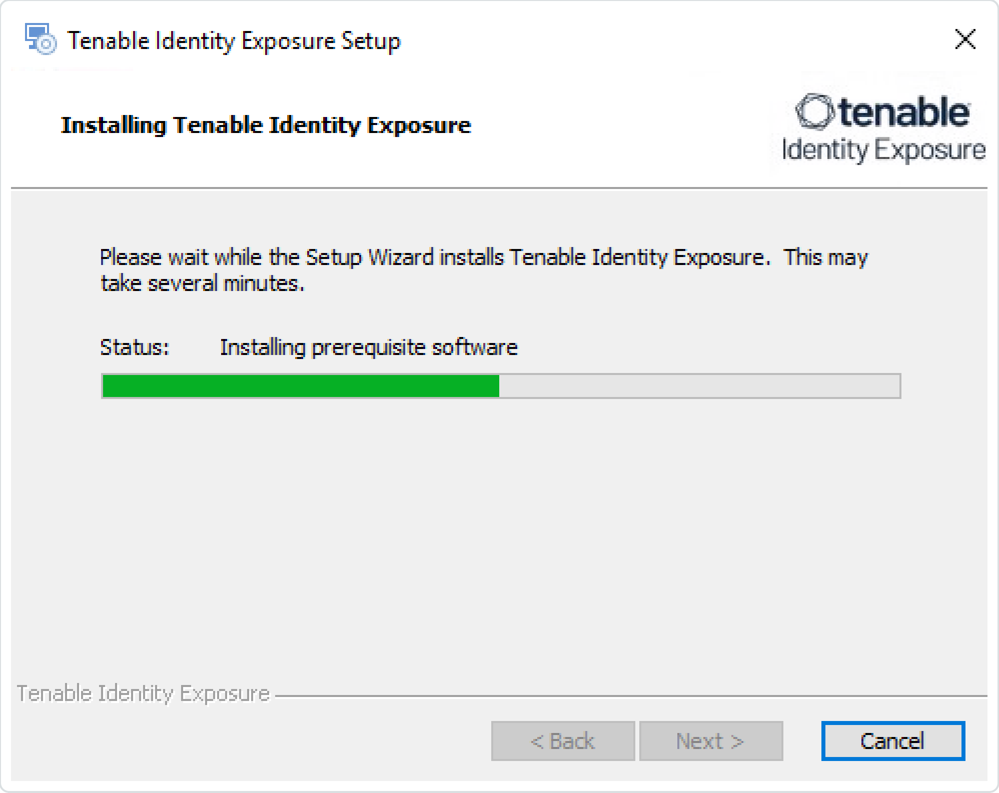
Tenable Identity Exposure Setup

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.

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)
    - `alsid_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:

    - `alsid_AttackPath1`
    - `alsid_Cancri`
    - `alsid_Cephei`
    - `alsid_CetiBridge`
    - `alsid_Cygni`
    - `alsid_Electra`
    - `alsid_Eltanin`
    - `alsid_Enif`
    - `alsid_Eridanis`
    - `alsid_EventLogsDecoder1`
    - `alsid_HealthCheck`
    - `alsid_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`

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):

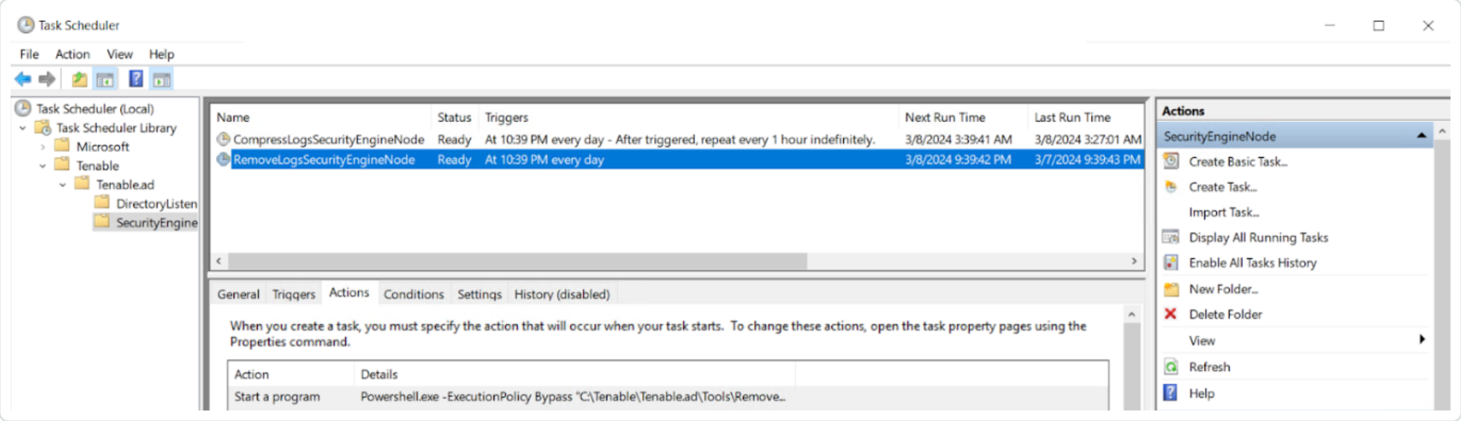
1. In the command line of the local machine, type cd desktop.
2. Type .\installername.exe /LOGS "c:\<path>\logsmsi1.txt".

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.

Manage Tenable Identity Exposure

Using its web portal, Tenable Identity Exposure allows you to review, manage, and receive relevant information about the security state of the monitored infrastructure. The web portal displays the following:

- Live Active Directory security flows to allow security teams to perform security compliance tasks, threat hunting, or incident response tasks.
- Administrative panes to manage the monitoring of new infrastructures.
- Access rights of each user or service connected to the platform.

Tenable Identity Exposure can also forward its security monitoring flows to other services such as internal application logs for further correlation.

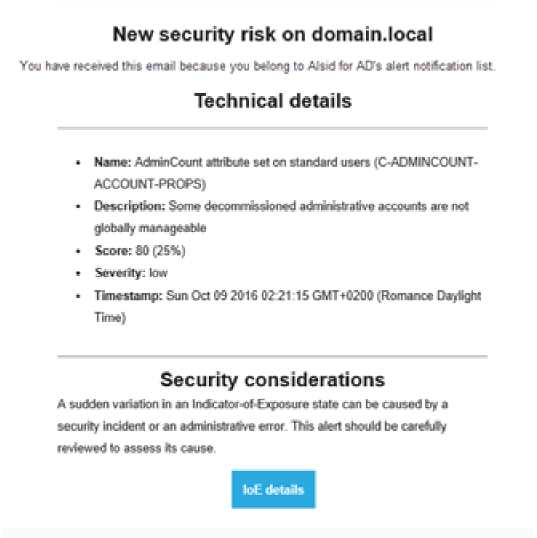
Alerts and Notifications

Tenable Identity Exposure includes notifications and alerts that you can connect to third-party services, such as an event log collector (for example, a Security Information and Event Management), an email service provider using SMTP, or a ticketing system. When a new security incident appears, Tenable Identity Exposure raises notifications to inform security teams to take immediate action.

Tenable Identity Exposure uses email notifications to send general purpose information to users, such as password recovery information, as well as notifications about security incidents.

To enable alerts, provide Tenable Identity Exposure with credentials for a user account with permissions to send emails to the selected SMTP server. This can be the same user account as the one you use to connect to your Active Directory.

The following is a generic email template for a security incident detected by Tenable:



New security risk on domain.local

You have received this email because you belong to Alsid for AD's alert notification list.

Technical details

- **Name:** AdminCount attribute set on standard users (C-ADMINCOUNT-ACCOUNT-PROPS)
- **Description:** Some decommissioned administrative accounts are not globally manageable
- **Score:** 80 (25%)
- **Severity:** low
- **Timestamp:** Sun Oct 09 2016 02:21:15 GMT+0200 (Romance Daylight Time)

Security considerations

A sudden variation in an Indicator-of-Exposure state can be caused by a security incident or an administrative error. This alert should be carefully reviewed to assess its cause.

IoE details

Tenable REST v3 API

You can integrate Tenable Identity Exposure into a security ecosystem using its RESTv3 (Representational State Transfer) API to enable management, logging. or notification capabilities.

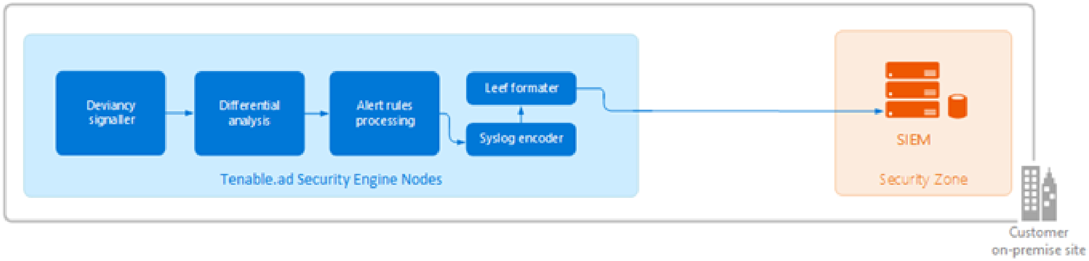
Tenable Identity Exposure provides a public API that you can use to connect the platform to third-party services. This API supports the REST v3 standard which you access using HTTP.

For more information, see the Tenable Identity Exposure API Reference Portal.

Connect to an Event Log Collector

You can configure Tenable Identity Exposure to send notifications, such as alerts or security offenses, to an event log collector. Tenable Identity Exposure also allows you to redirect a subset of the traffic flows to a collector for further correlation.

The following illustration shows an integrated process managing Security Information and Event Management (SIEM) events.



Tenable Identity Exposure uses the Syslog protocol to carry messages in LEEF format.

Tenable Identity Exposure supports most SIEMs or event log collectors. Tenable Identity Exposure supports the following event collectors:

- IBM QRadar
- Splunk
- RSA Netwitness
- LogRhythm
- Micro Focus ArcSight
- Tibco Loglogic
- McAfee Enterprise Security Manager

Scale Tenable Identity Exposure Services

Required User Role: Administrator on the local machine

To improve data processing performance, you can scale up or down these Tenable Identity Exposure services.

Cancri

Cancri is the service in charge of translating and decoding the raw data it receives.

Cancri's scaling up mechanism goes through its reconfiguration using an environment variable.

To scale Cancri:

1. Open a PowerShell (x64) terminal.
2. Define the environment variable `ALSID_CASSIOPEIA_CANCRI_Application__MaxConcurrentPublishToEridanis`:

   Note: The default value is 100.

   ```
   [Environment]::SetEnvironmentVariable("ALSID_CASSIOPEIA_CANCRI_Application__
   MaxConcurrentPublishToEridanis", "IntegerValue", "Machine")
   ```

3. Restart Cancri:

```
Restart-Service -Name Alsid_Cancri
```

Example:

```
[[Environment]::SetEnvironmentVariable("ALSID_CASSIOPEIA_CANCRI_Application__
MaxConcurrentPublishToEridanis", "200", "Machine")
Restart-Service -Name Alsid_Cancri
```

Cygni

The Cygni service analyzes changes in AD objects to identify potential risks. If these changes collectively meet deviance criteria, it transmits the deviance to the database and it becomes visible in Tenable Identity Exposure.

If your security requirements do not align with the default settings of the Tenable security profile, you can deactivate it to enhance performance by circumventing the computation associated with this profile. Alternatively, you can create a new profile by duplicating the Tenable security profile and customizing it to your specific needs. This allows you to create a personalized profile aligned with your own security standards based on Tenable recommendations. You can then deactivate the default Tenable profile, ensuring that your system adheres to your security requirements.

> **Note**: Disabling analysis on this profile pauses the results.

To disable IoE analysis on the Tenable security profile:

1. On the Security Engine Node machine, open a PowerShell (x64) terminal.
2. Run the following command:

   ```
   [Environment]::SetEnvironmentVariable("ALSID_CASSIOPEIA_CYGNI_Application__IOE__
   IgnoreDefaultProfile", "true", [System.EnvironmentVariableTarget]::Machine)
   ```

3. Restart the Cygni service:

   ```
   Restart-Service -Name 'alsid_Cygni'
   ```

Eridanis

Eridanis is the API service that stores the business data (configuration and AD objects, deviances, etc.) in the MSSQL Server and forwards it to other services.

To scale up the total number of Eridanis instances, you must update the `ERIDANIS_WORKER_COUNT` environment variable.

To scale Eridanis:

1. Open a PowerShell (x64) terminal.
2. Run the following command (replace the value in brackets with the real expected value):

   ```
   [System.Environment]::SetEnvironmentVariable('ERIDANIS_WORKER_COUNT', <number of Eridanis
   instances>, 'Machine')
   ```

3. Restart Eridanis:

   ```
   Restart-Service -Name 'alsid_Eridanis'
   ```

Example: For 3 Instances of Eridanis

```
[System.Environment]::SetEnvironmentVariable('ERIDANIS_WORKER_COUNT', 3, 'Machine')
Restart-Service -Name 'alsid_Eridanis' -Force
```

EventLogsDecoder

The `EventLogsDecoder` component needs to process data at a high speed. It's possible that a single instance of `EventLogsDecoder` may not suffice, so consider running multiple instances of this component concurrently.

To determine when to initiate additional instances, you monitor a specific metric, which is the number of messages queued in the RabbitMQ queue named `event-logs-decoder-ioa-input-queue`. When this metric reaches a threshold of 8000 messages, it's imperative to launch a new instance of the EventLogsDecoder component.

To scale a new instance of EventLogsDecoder on a new machine, launch the installation program on this machine and follow the same procedure as the one you used for the first instance:

- Default TLS
- Default TLS in "Expert Mode"
- TLS without Peer Verification
- TLS with Peer Verification
- No TLS

You do not need to restart any service because Tenable Identity Exposure automatically takes in account this new instance.

> **Note**: It is not possible to add several instances of `EventLogsDecoder` on the same machine.

Change IP Addresses or FQDNs for Tenable Identity Exposure Nodes

Changing the IP addresses or fully qualified domain names (FQDNs) of machines running the Storage Manager (SM), Security Engine Nodes (SEN), and Directory Listener (DL) is a required task in certain situations, such as disaster recovery testing. Using scripts to modify environment variables with the new IPs or FQDNs and to restart services is the most efficient way to perform this operation which also minimizes downtime.

To change the IP addresses or FQDN for Tenable Identity Exposure nodes:

1. If your Tenable Identity Exposure installation type uses:
    - **Default TLS**: Generate and replace all self-signed TLS certificates with the new IP addresses or FQDNs.
    - **Custom TLS**: Generate and replace all custom TLS certificates with the new IP addresses or FQDNs.
    - **No TLS**: Proceed to the next step.
2. In PowerShell, list all the IP/FQDN-related environment variables with the new IPs or FQDNs, such as in the following example:

    > **Note**: The following scripts only show the environment variables that you would need to update in a conventional setup of Tenable Identity Exposure. It excludes any setup using split SENs or multiple

DLs.

- Security Engine Node (SEN):

Update environment variables with new IPs or FQDNs for SEN

```
$vars = @{
    ERIDANIS_MSSQL_HOST                 = $MssqlNodeIp            # Storage Manager 
Node IP Address
    ERIDANIS_MSSQL_PORT                 = $MssqlNodePort         # Storage Manager 
Node Default Port 1433
    ERIDANIS_KAPTEYN_PUBLIC_DOMAIN      = $WebAppHostName        # FQDN or IP Address 
of Web UI
    ALSID_CASSIOPEIA_EVENT_LOGS_DECODER_Service__EventLogsStorage__Host        = 
$DecoderIP        # Storage Manager Node IP Address
    ALSID_CASSIOPEIA_EVENT_LOGS_DECODER_Service__EventLogsStorage__Port        = 
$DecorderPort        # Default Port 4244
    ALSID_CASSIOPEIA_CYGNI_Service__EventLogsStorage__Host                    = 
$DecoderIP        # Storage Manager Node IP Address
    ALSID_CASSIOPEIA_CYGNI_Service__EventLogsStorage__Port                    = 
$DecorderPort        # Default Port 4244
}

ForEach ($var in $vars.GetEnumerator()) {
    [System.Environment]::SetEnvironmentVariable($var.Name, $var.Value, 'Machine')
}
```

- Directory Listener (DL):

Update environment variables with new IPs or FQDNs for DL

```
$vars = @{
    ALSID_CASSIOPEIA_CETI_Service__Broker__Host                 = 
$SecurityEngineNodeIP            # Security EngineNode IP Address
    ALSID_CASSIOPEIA_CETI_Service__Broker__Port                 = 
$SecurityEngineNodePort            # Security EngineNode Port
}

ForEach ($var in $vars.GetEnumerator()) {
    [System.Environment]::SetEnvironmentVariable($var.Name, $var.Value, 'Machine')
}
```

3. Restart all services on each machine.

Restart services on each machine

```
# Restart all services
Get-Service alsid* | Restart-Service
Get-Service tenable* | Restart-Service
```

HTTPS for Tenable Identity Exposure Web Application

When the Tenable Identity Exposure installation process installs the Security Engine Node (SEN), it creates a self-signed certificate and binds it to the Tenable Identity Exposure web application to let you access Tenable Identity Exposure via HTTPS.

For example, if the SEN server's IP address is `10.0.48.55`, you can log in to the Tenable Identity Exposure web application at `https://10.0.48.55` after installation.

Tenable Identity Exposure provides a default self-signed certificate for your convenience. But to secure fully the web application, you must change this IIS certificate for a valid one, such as a signed certificate from the organization’s PKI/internal Certificate Authority.

Moreover, the SSL/TLS protocols versions and their enabled cipher suites have globally configured settings in the underlying Windows operating system (OS). Tenable Identity Exposure does not modify these settings, so you must configure them to obtain the desired level of security in line with your organization’s requirements.

In the absence of specific requirements and within a modern environment, Tenable recommends that you enable TLS 1.2. You can enable TLS 1.3 if you use Windows Server 2022 with the compatible Tenable Identity Exposure version. You should also disable weak cipher suites (DES, 3DES, RC2, RC4, AES 128, etc.)

Refer to the Microsoft documentation to Restrict the use of certain cryptographic algorithms and protocols in Schannel.dll. Use the configuration method that your organization recommends to deploy those settings (for example local configuration, GPO, third-party tool, etc.) However, Tenable does not offer support around this.

For more information, see:

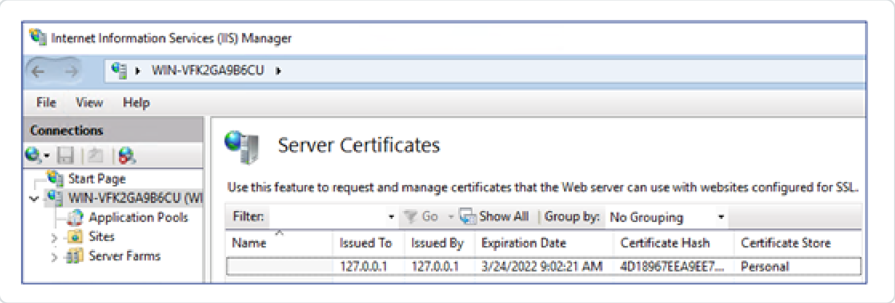
- View the IIS Certificate
- Change the IIS Certificate

View the IIS Certificate

The Tenable Identity Exposure installation process creates and places a self-signed certificate in Internet Information Services (IIS) Manager.

To view the IIS certificate:

1. Go to **Windows Start** > **Windows Administrative Tools** > **Internet Information Services (IIS) Manager**.
2. In the **Connections** panel on the left, click on the server name.
3. Double-click on **Server Certificates** to display certificates in the IIS Manager.



Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.

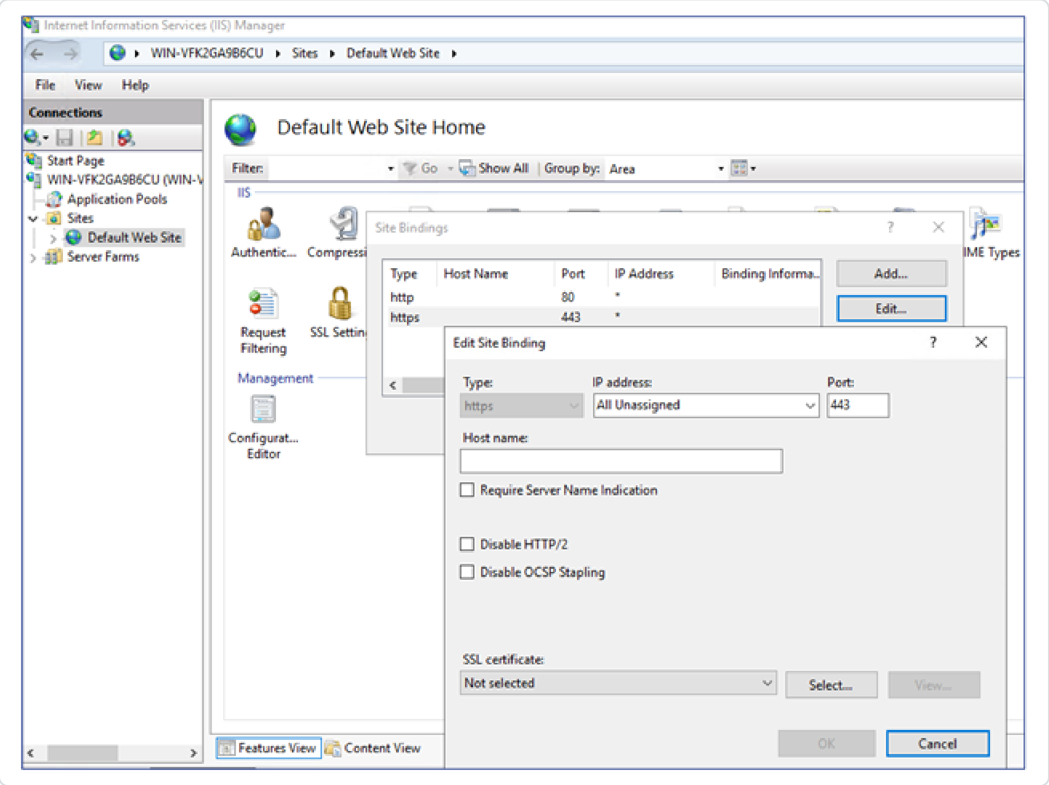
Name	Issued To	Issued By	Expiration Date	Certificate Hash	Certificate Store
	127.0.0.1	127.0.0.1	3/24/2022 9:02:21 AM	4D18967EEA9EE7...	Personal

> **Note**: By default, the installation process creates the self-signed certificate and the IIS site binding by using HTTPS port 443.

4. To explore the binding, expand **Sites** on the left panel.
5. Right-click your website and choose **Edit Bindings**.

   The **Site Bindings** window appears.
6. Select the **https** binding.
7. Click **Edit**.

   The **Edit Site Binding** window appears.



Type	Host Name	Port	IP Address	Binding Informa...
http		80	*	
https		443	*	

Type: https

IP address: All Unassigned

Port: 443

Host name:

☐ Require Server Name Indication

☐ Disable HTTP/2

☐ Disable OCSP Stapling

SSL certificate: Not selected

8. Under SSL Certificates, click on the drop-down menu to view installed certificates.

Change the IIS Certificate

To use your certificate for the Tenable Identity Exposure web application, you must:

1. Install your certificate in IIS.

2. Edit site binding to use your installed certificate.

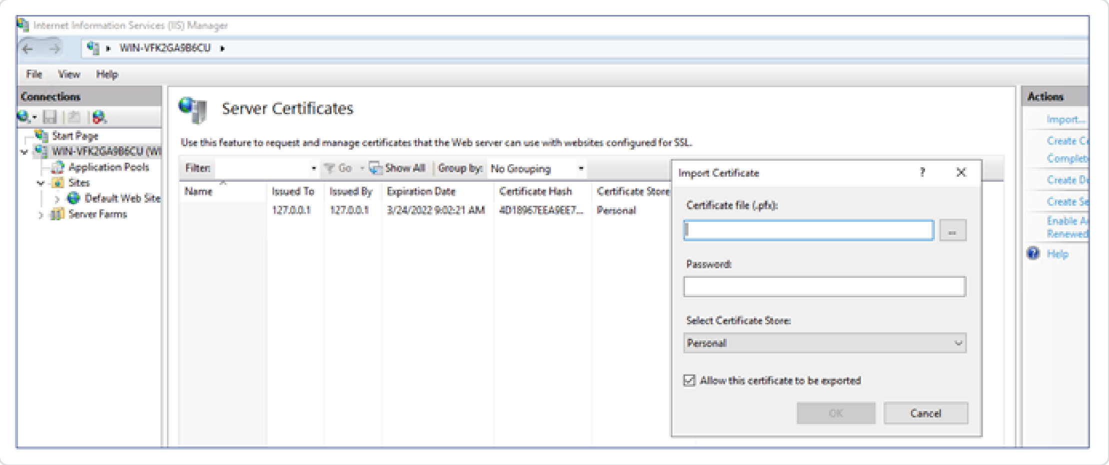
To install the IIS certificate:

1. Go to **Windows Start** > **Windows Administrative Tools** > **Internet Information Services (IIS) Manager**.

2. In the **Connections** panel on the left, click on the server name.

3. Double-click on **Server Certificates** to display certificates in the IIS Manager.

4. In the right panel, click **Import** to import your certificate.



Internet Information Services (IIS) Manager

Server Certificates

Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.

Filter: Go · Show All | Group by: No Grouping

Name	Issued To	Issued By	Expiration Date	Certificate Hash	Certificate Store
	127.0.0.1	127.0.0.1	3/24/2022 9:02:21 AM	4D18967EEA9EE7...	Personal

Import Certificate

Certificate file (.pfx):

Password:

Select Certificate Store: Personal

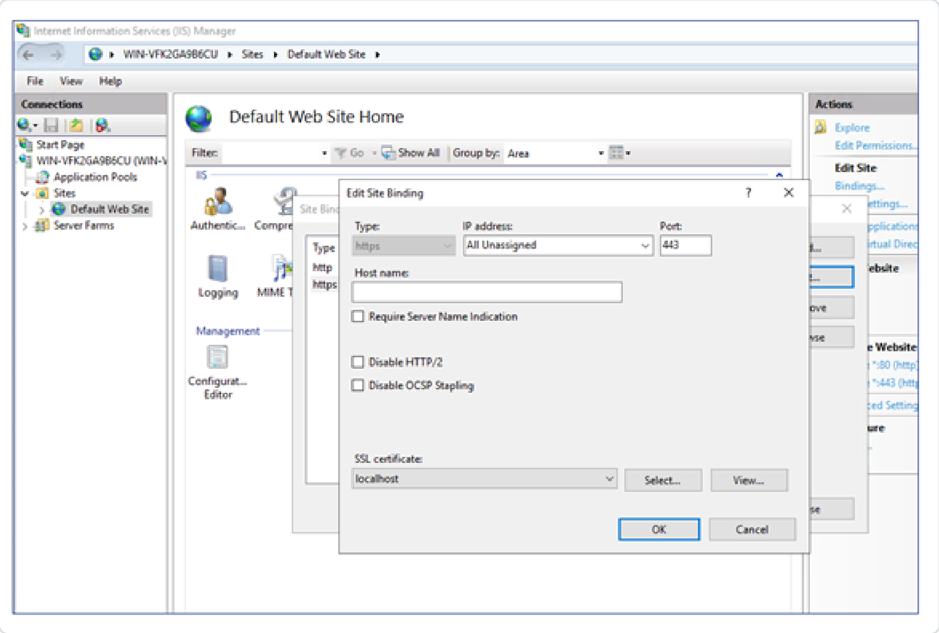
☑ Allow this certificate to be exported

To change the IIS certificate:

1. View the IIS Certificate.

2. From the drop-down list of SSL certificates, select the certificate you just installed.

3. Click **OK**.



Internet Information Services (IIS) Manager

Default Web Site Home

Filter: Go · Show All | Group by: Area

Edit Site Binding

Type: https

IP address: All Unassigned

Port: 443

Host name:

□ Require Server Name Indication

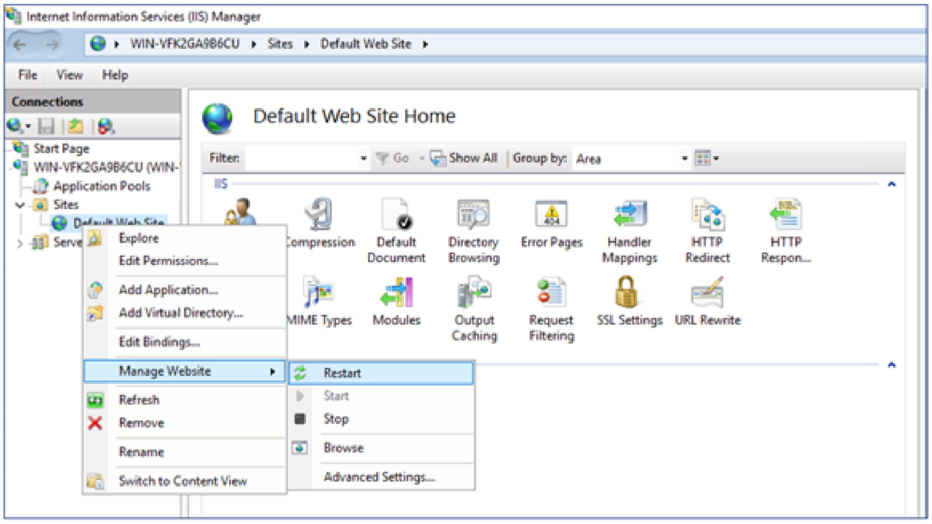
□ Disable HTTP/2

□ Disable OCSP Stapling

SSL certificate: localhost

4. Right-click on the website in the **Connections** panel and select **Manage Website** > **Restart** for

the new certificate to take effect.



Upgrade and Maintenance

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

- These upgrades include security patches for the underlying operating system. See the latest Tenable Identity Exposure Release Notes for more information.
- You can access them on Tenable Downloads site.

To upgrade Tenable Identity Exposure, deploy the installation packages on each Windows Server machine. For more information about the upgrade process, see Upgrade Tenable Identity Exposure.

Maintenance and Support Services

To keep servers in good security conditions the Tenable Identity Exposure platform requires access to the following support services.

During maintenance operations, Tenable Support requires administrative access to the operating systems that host Tenable Identity Exposure.

Service Name	Description
Update management infrastructure	Your company's update management infrastructure (e.g., WSUS or SCCM) or Microsoft update servers on the Internet. This service applies security patches on the underlying operating system.
Time Server	Your company's time server (e.g., NTP server). This service synchronizes Tenable Identity Exposure's platform internal clock to your reference time. Time synchronization offers consistent security monitoring.
Identity provider	Your identity and access provider. This service activates SAML, LDAP, or OAUTH authentication to Tenable Identity Exposure's web services (portal, API, etc.).

Uninstall Tenable Identity Exposure

Required User Role: Administrator on the local machine

The uninstallation process removes all Tenable Identity Exposure components.

To uninstall Tenable Identity Exposure:

1. In Windows, go to **Control Panel** > **Programs** > **Programs and Features**.
2. Select Tenable Identity Exposure.
3. Click **Uninstall**. A dialog box asks for confirmation:
4. Click **Yes**.
    - The confirmation dialog box disappears after the uninstallation completes.
    - An icon in the system tray indicates that a second uninstallation phase is in process. This icon disappears when the uninstallation has fully completed.