# Table of Contents

**Welcome to Tenable.ad** ................................................................. 5

**Get Started with Tenable.ad** .......................................................... 6

**On-Premise Architectures** .............................................................. 8
  - Centralized Architecture ......................................................... 10
  - Distributed Architecture ......................................................... 12

**Hosting Specifications** ................................................................. 14

**Installation of Tenable.ad as an Application Package** ......................... 16

**Resource Sizing** ........................................................................ 20
  - Directory Listeners Sizing ....................................................... 21
  - Security Engine Node Sizing ..................................................... 22
  - Storage Manager Sizing ............................................................ 23

**Network Requirements** ................................................................. 28
  - Network Flow Matrix .............................................................. 30
  - Network Matrix for Transport Layer Security (TLS) Mode ................. 37

**Web Portal Requirements** ............................................................. 41

**Integration with an Active Directory Domain** .................................. 42

**Access to AD Objects or Containers** ............................................ 43

**Prerequisite Checklist** .................................................................. 45

**Install Tenable.ad** ......................................................................... 48

**Installation Programs** ................................................................. 49

**Available TLS Installations** .......................................................... 50

**Installation with No TLS** .............................................................. 53
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation with Default TLS</td>
<td>60</td>
</tr>
<tr>
<td>Installation with Default TLS using Autogenerated and Self-signed Certificates</td>
<td>66</td>
</tr>
<tr>
<td>Installation with Custom TLS and without Peer Verification</td>
<td>74</td>
</tr>
<tr>
<td>Installation with Custom TLS and with Peer Verification</td>
<td>83</td>
</tr>
<tr>
<td>Security Probe</td>
<td>92</td>
</tr>
<tr>
<td><strong>Indicators of Attack</strong></td>
<td>95</td>
</tr>
<tr>
<td>Indicators of Attack and the Active Directory</td>
<td>96</td>
</tr>
<tr>
<td>Install Indicators of Attack</td>
<td>98</td>
</tr>
<tr>
<td>Technical Changes and Potential Impact</td>
<td>101</td>
</tr>
<tr>
<td>Install Microsoft Sysmon</td>
<td>102</td>
</tr>
<tr>
<td>Troubleshoot Antivirus Detection</td>
<td>107</td>
</tr>
<tr>
<td>Troubleshoot Advanced Audit Policy Configuration Precedence</td>
<td>108</td>
</tr>
<tr>
<td><strong>Manage Tenable.ad</strong></td>
<td>110</td>
</tr>
<tr>
<td>Connect to an Event Log Collector</td>
<td>112</td>
</tr>
<tr>
<td>Scale Tenable.ad Services</td>
<td>113</td>
</tr>
<tr>
<td>Internet Information Services (IIS) Certificate</td>
<td>116</td>
</tr>
<tr>
<td>View the IIS Certificate</td>
<td>117</td>
</tr>
<tr>
<td>Change the IIS Certificate</td>
<td>119</td>
</tr>
<tr>
<td><strong>Upgrade Tenable.ad</strong></td>
<td>121</td>
</tr>
<tr>
<td>Back Up and Restore the Storage Manager</td>
<td>122</td>
</tr>
<tr>
<td>Upgrade the Directory Listener</td>
<td>124</td>
</tr>
<tr>
<td>Upgrade Security Engine Nodes</td>
<td>135</td>
</tr>
<tr>
<td>Upgrade the Storage Manager</td>
<td>150</td>
</tr>
<tr>
<td>Restart Services</td>
<td>161</td>
</tr>
</tbody>
</table>
Upgrade Indicator of Attack Module ................................................................. 162
Upgrade and Maintenance ................................................................................. 163
Uninstall Tenable.ad ......................................................................................... 164
Uninstall Tenable.ad ......................................................................................... 165
Uninstall the Indicators of Attack Module ...................................................... 166
Uninstall Sysmon .............................................................................................. 167
Welcome to Tenable.ad

Last updated: March 22, 2022

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.

This On-Premise Installation Guide gives the following information:

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

To get started, see Get Started with Tenable.ad.
Get Started with Tenable.ad

Use the following getting started sequence to prepare, install, configure, and manage your Tenable.ad deployment.

1. **Prepare**
2. **Install**
3. **Deploy Indicators of Attack**
4. **Manage**

**Prepare**

Before you install Tenable.ad, review the architectures and the following technical prerequisites to ensure that your platform runs optimally:

- **On-Premise Architectures**
- **Hosting Specifications**
- **Resource Sizing**
- **Upgrade and Maintenance**
- **Network Requirements**
- **Integration with an Active Directory Domain**

**Install**

You download the installation programs from the Tenable.ad portal. Tenable.ad offers several types of TLS installations depending on your infrastructure.

- **Installation Programs**
- **Available TLS Installations**

**Deploy Indicators of Attack**

After you install Tenable.ad, you can deploy the indicator of attack module in your Active Directory.
• **Indicators of Attack and the Active Directory**

• **Install Indicators of Attack**

**Manage**

You use the Tenable.ad portal to review, manage, and receive relevant information about the security state of the monitored infrastructure.

• **Connect to an Event Log Collector**

• **Change the IIS Certificate**

• **Scale Tenable.ad Services**
On-Premise Architectures

Tenable.ad'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**: This model hosts all Tenable.ad components in the same network zone.
- **Distributed architecture**: This model places Directory Listeners in the same network zone as the domain controllers, and hosts other Tenable.ad components—such as the Security Engine Node and the Storage Manager—in another network zone.

Tenable recommends using the centralized architecture as it offers better flexibility and easy-to-achieve deployment.

Supported Infrastructure

The Tenable.ad platform relies on several Windows services hosted on virtual machines (VMs). Your environment must support the infrastructure illustrated below.

For the number and sizing of these VMs, see [Hosting Specifications](#).

The Tenable.ad platform consists of three components: Directory Listeners, Security Engine Nodes, and Storage Managers.

- **The Directory Listeners**: working closely with the monitored domain controllers, the Directory Listeners receive real-time Active Directory flows and apply several treatments to decode, isolate, and correlate security changes.
• The **Security Engine Nodes**: hosting analysis-related services, the security engine nodes support the Tenable.ad 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 **Storage Managers**: 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 2019 and InfluxDB to store internal data and configuration.
Centralized Architecture

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

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

This architecture offers the best balance between manageability and security:

- Each Tenable.ad 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 additional 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.ad network zone.
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 illustration below:

Advantages

This architecture offers several 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.ad 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.ad’s platform only requires one inbound and one outbound network flow, which preserves the security of the isolated infrastructure.

Network security: Tenable.ad’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.
Hosting Specifications

You deploy Tenable.ad as an application package hosted in a dedicated Windows environment that you provide and manage, and which must fulfill specific hosting specifications.

Hardware Requirements

- Supported Microsoft Windows Operating Systems
  - Windows Server 2016
  - Windows Server 2019

- The requirements described in the sizing sections are for the well-being of Tenable.ad’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’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.

Size Your Resources

Tenable.ad runs on three main components:

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

- The Security Engine Nodes support Tenable.ad’s security engine, storage services, and end users.

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

Calculate the Computing Power
The required resources for the Tenable.ad components depend on the size of the Active Directory you monitor. Tenable.ad uses the number of active users to size the resources. This calculation includes the regular user accounts and the service accounts used by applications.

To calculate the volume:

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

  ```powershell
  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.

**What to do next**

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

- [Directory Listener](#)
- [Security Engine Node](#)
- [Storage Manager](#)
Installation of Tenable.ad as an Application Package

You install Tenable.ad as an application package hosted in a dedicated Windows environment that must fulfill specific hosting specifications.

Tenable.ad 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.

Note: Tenable.ad 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.ad on operating systems supporting the micro-services model.

Unsupported Configurations

You must avoid some configurations to allow the platform to run.

The following table details unsupported configurations:

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active anti-virus or End-point Detection and Response (EDR) solution</td>
<td>The Tenable.ad platform requires intensive disk I/O.</td>
</tr>
<tr>
<td></td>
<td>• Using anti-virus and EDR can drastically decrease platform performances.</td>
</tr>
</tbody>
</table>
**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.ad 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.ad 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.ad’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.ad’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.ad components. You must ensure a proper management of your operating systems, including the frequent deployment of security patches. For more information about Tenable.ad releases, see the Tenable.ad Release Notes.

• Tenable.ad’s micro-services architecture supports the immediate application of operating system patches.

Pre-installation Checklist

Use the following checklist to gather the required information before you install Tenable.ad as an application package.

<table>
<thead>
<tr>
<th>Item</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hosting specification</td>
<td>Identify the hosting specifications.</td>
</tr>
<tr>
<td>Configuration review</td>
<td>Identify the following:</td>
</tr>
<tr>
<td></td>
<td>• The list of installed third-party software.</td>
</tr>
<tr>
<td></td>
<td>• All configurations you made on the operating system's master image.</td>
</tr>
<tr>
<td></td>
<td>• All the security hardening you made on the operating system's master image</td>
</tr>
<tr>
<td>Network configuration</td>
<td>• Reserve the resources.</td>
</tr>
<tr>
<td></td>
<td>• Have the private IP addresses.</td>
</tr>
<tr>
<td>Access configuration</td>
<td>• Reserve the resources.</td>
</tr>
<tr>
<td></td>
<td>• Have the DNS name used to access Tenable’s web portal.</td>
</tr>
<tr>
<td>Security configuration</td>
<td>• Reserve the resources.</td>
</tr>
<tr>
<td></td>
<td>• Have the TLS certificate and its associated private key used to secure access to the web portal.</td>
</tr>
<tr>
<td>Platform configuration</td>
<td>Have the following platform configuration information:</td>
</tr>
<tr>
<td></td>
<td>• The first name, last name, and email addresses of the user accounts</td>
</tr>
<tr>
<td>you want to create.</td>
<td></td>
</tr>
<tr>
<td>---------------------</td>
<td></td>
</tr>
<tr>
<td>• The IP address(es) and the domain name of each primary domain controller you want to monitor.</td>
<td></td>
</tr>
</tbody>
</table>
Resource Sizing

To ensure correct behavior, these components require a certain amount of memory and computing power.

- These required resources scale depending on the size of the Active Directory infrastructures to monitor.
- As a metric, Tenable uses the number of active users to compute the required sizing. This includes the regular user accounts and the service accounts used by applications.

To compute the volume:

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

  ```powershell
  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.

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

- [Directory Listener](#)
- [Security Engine Node](#)
- [Storage Manager](#)
## Directory Listeners Sizing

This table describes the required sizing for the system hosting the **Directory Listener** components.

<table>
<thead>
<tr>
<th>Active AD users</th>
<th>Instance required</th>
<th>vCPU (per instance)</th>
<th>Memory (per instance)</th>
<th>Disk space (per instance)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 - 25,000</td>
<td>1 virtual machine</td>
<td>2 cores on 2 sockets</td>
<td>12 GB of RAM</td>
<td>30 GB (silver performance)</td>
</tr>
<tr>
<td>25,001 - 50,000</td>
<td>1 virtual machine</td>
<td>4 cores on 2 sockets</td>
<td>16 GB of RAM</td>
<td>30 GB (silver performance)</td>
</tr>
<tr>
<td>50,001 - 75,000</td>
<td>1 virtual machine</td>
<td>4 cores on 2 sockets</td>
<td>24 GB of RAM</td>
<td>30 GB (silver performance)</td>
</tr>
<tr>
<td>75,001 - 100,000</td>
<td>1 virtual machine</td>
<td>4 cores on 2 sockets</td>
<td>32 GB of RAM</td>
<td>30 GB (silver performance)</td>
</tr>
<tr>
<td>100,001 - 150,000</td>
<td>1 virtual machine</td>
<td>8 cores on 2 sockets</td>
<td>32 GB of RAM</td>
<td>30 GB (silver performance)</td>
</tr>
<tr>
<td>150,001 - 300,000</td>
<td>1 virtual machine</td>
<td>8 cores on 2 sockets</td>
<td>64 GB of RAM</td>
<td>30 GB (silver performance)</td>
</tr>
<tr>
<td>300,001 - 500,001+</td>
<td>1 virtual machine</td>
<td>8 cores on 2 sockets</td>
<td>64 GB of RAM</td>
<td>30 GB (silver performance)</td>
</tr>
</tbody>
</table>
# Security Engine Node Sizing

This table describes the required sizing for the system hosting the Security Engine Node components.

<table>
<thead>
<tr>
<th>Active AD users</th>
<th>Instance required</th>
<th>vCPU (per instance)</th>
<th>Memory (per instance)</th>
<th>Disk space (per instance)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 - 25,000</td>
<td>1 virtual machine</td>
<td>8 cores on 2 sockets</td>
<td>16 GB of RAM</td>
<td>200 GB (gold performance)</td>
</tr>
<tr>
<td>25,001 - 50,000</td>
<td>1 virtual machine</td>
<td>8 cores on 2 sockets</td>
<td>16 GB of RAM</td>
<td>300 GB (gold performance)</td>
</tr>
<tr>
<td>50,001 - 75,000</td>
<td>1 virtual machine</td>
<td>10 cores on 3 sockets</td>
<td>24 GB of RAM</td>
<td>300 GB (gold performance)</td>
</tr>
<tr>
<td>75,001 - 100,000</td>
<td>1 virtual machine</td>
<td>12 cores on 4 sockets</td>
<td>32 GB of RAM</td>
<td>400GB (gold performance)</td>
</tr>
<tr>
<td>100,001 - 150,000</td>
<td>1 virtual machine</td>
<td>16 cores on 4 sockets</td>
<td>32 GB of RAM</td>
<td>400GB (gold performance)</td>
</tr>
<tr>
<td>150,001 - 300,000</td>
<td>1 virtual machine</td>
<td>16 cores on 4 sockets</td>
<td>64 GB of RAM</td>
<td>500GB (gold performance)</td>
</tr>
<tr>
<td>300,001 - 500,001+</td>
<td>4 virtual machine</td>
<td>VM1: 8 cores on 2 sockets</td>
<td>VM1: 16 GB of RAM</td>
<td>VM1: 1 TB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VM2: 12 cores on 4 sockets</td>
<td>VM2: 32 GB of RAM</td>
<td>VM2: 300 GB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VM3: 16 cores on 4 sockets</td>
<td>VM3: 16 GB of RAM</td>
<td>VM3: 100 GB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VM4: 16 cores on 4 sockets</td>
<td>VM4: 32 GB of RAM</td>
<td>VM4: 100 GB</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(gold performance)</td>
</tr>
</tbody>
</table>
Storage Manager Sizing

As part of its security analysis, Tenable.ad stores the differences for each Active Directory (AD) change, whether this change comes from the AD database or from the Sysvol network share.

The Storage Manager component oversees the storage of these events in two databases: a Microsoft SQL Server instance and an InfluxDB instance.

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

- A minimal 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.ad 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.ad is a disk-intensive application. To avoid any bottleneck introduced by the storage (disk or SAN), Tenable.ad offers a minimal and recommended configurations.

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

Minimal and Recommended Computing Power

<table>
<thead>
<tr>
<th>Active AD users</th>
<th>Instance Required</th>
<th>vCPU (per instance)</th>
<th>Memory (per instance)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 - 25,000</td>
<td>1 virtual machine</td>
<td>8 cores on 2 sockets</td>
<td>8 GB of RAM</td>
</tr>
<tr>
<td>25,001 - 50,000</td>
<td>1 virtual</td>
<td>8 cores on 2 sockets</td>
<td>12 GB of RAM</td>
</tr>
</tbody>
</table>

Copyright © 2022 Tenable, Inc. All rights reserved. Tenable, Tenable.io, Tenable Network Security, Nessus, SecurityCenter, SecurityCenter Continuous View and Log Correlation Engine are registered trademarks of Tenable, Inc. Tenable.sc, Tenable.ot, Lumin, Indegy, Assure, and The Cyber Exposure Company are trademarks of Tenable, Inc. All other products or services are trademarks of their respective owners.
<table>
<thead>
<tr>
<th>Machine Range</th>
<th>Machine Type</th>
<th>vCPU Per Instance</th>
<th>Memory Per Instance</th>
</tr>
</thead>
<tbody>
<tr>
<td>50,001 - 75,000</td>
<td>1 virtual machine</td>
<td>12 cores on 4 sockets</td>
<td>16 GB of RAM</td>
</tr>
<tr>
<td>75,001 - 100,000</td>
<td>1 virtual machine</td>
<td>12 cores on 4 sockets</td>
<td>16 GB of RAM</td>
</tr>
<tr>
<td>100,001 - 150,000</td>
<td>1 virtual machine</td>
<td>12 cores on 4 sockets</td>
<td>32 GB of RAM</td>
</tr>
<tr>
<td>150,001 - 300,000</td>
<td>1 virtual machine</td>
<td>16 cores on 4 sockets</td>
<td>64 GB of RAM</td>
</tr>
<tr>
<td>300,001+</td>
<td>1 virtual machine</td>
<td>16 cores on 4 sockets</td>
<td>64 GB of RAM</td>
</tr>
</tbody>
</table>

### Recommended Computing Power

<table>
<thead>
<tr>
<th>Active AD Users Range</th>
<th>Instance Required</th>
<th>vCPU (per instance)</th>
<th>Memory (per instance)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 - 25,000</td>
<td>1 virtual machine</td>
<td>8 cores on 2 sockets</td>
<td>8 GB of RAM</td>
</tr>
<tr>
<td>25,001 - 50,000</td>
<td>1 virtual machine</td>
<td>8 cores on 2 sockets</td>
<td>16 GB of RAM</td>
</tr>
<tr>
<td>50,001 - 75,000</td>
<td>1 virtual machine</td>
<td>12 cores on 4 sockets</td>
<td>32 GB of RAM</td>
</tr>
<tr>
<td>75,001 - 100,000</td>
<td>1 virtual machine</td>
<td>12 cores on 4 sockets</td>
<td>32 GB of RAM</td>
</tr>
<tr>
<td>100,001 - 150,000</td>
<td>1 virtual machine</td>
<td>12 cores on 4 sockets</td>
<td>64 GB of RAM</td>
</tr>
<tr>
<td>150,001 - 300,000</td>
<td>1 virtual machine</td>
<td>16 cores on 4 sockets</td>
<td>64 GB of RAM</td>
</tr>
</tbody>
</table>
300,001 – 500,001+

1 virtual machine

16 cores on 4 sockets

96 GB of RAM

Supported and Recommended Disk Layout

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

- 1 data file disk
- 1 tempDB disk
- 1 log file disk
- (Optional) 1 backup disk

Minimal and Recommended Disk Sizing

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

<table>
<thead>
<tr>
<th>Active AD users</th>
<th>Total Disk Space</th>
<th>Data File Disk Space</th>
<th>Log File Disk Space</th>
<th>TempDb Disk Space</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 - 25,000</td>
<td>450 GB</td>
<td>340 GB</td>
<td>100 GB</td>
<td>10 GB</td>
</tr>
<tr>
<td>25,001 - 50,000</td>
<td>550 GB</td>
<td>400 GB</td>
<td>125 GB</td>
<td>25 GB</td>
</tr>
<tr>
<td>50,001 - 75,000</td>
<td>800 GB</td>
<td>600 GB</td>
<td>150 GB</td>
<td>50 GB</td>
</tr>
<tr>
<td>75,001 - 100,000</td>
<td>1 TB</td>
<td>725 GB</td>
<td>200 GB</td>
<td>75 GB</td>
</tr>
<tr>
<td>100,001 - 150,000</td>
<td>2 TB</td>
<td>1.6 TB</td>
<td>300 GB</td>
<td>100 GB</td>
</tr>
<tr>
<td>150,001 - 300,000</td>
<td>3 TB</td>
<td>2.45 TB</td>
<td>400 GB</td>
<td>150 GB</td>
</tr>
<tr>
<td>300,001 - 500,001+</td>
<td>4 TB</td>
<td>3.3 TB</td>
<td>500 GB</td>
<td>200 GB</td>
</tr>
</tbody>
</table>
## Storage managers - Recommended Disk Sizing Matrix

<table>
<thead>
<tr>
<th>Active AD users</th>
<th>Total Disk Space</th>
<th>Data File Disk Space</th>
<th>Log File Disk Space</th>
<th>TempDb Disk Space</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 - 25,000</td>
<td>600 GB</td>
<td>375 GB</td>
<td>200 GB</td>
<td>25 GB</td>
</tr>
<tr>
<td>25,001 - 50,000</td>
<td>800 GB</td>
<td>500 GB</td>
<td>250 GB</td>
<td>50 GB</td>
</tr>
<tr>
<td>50,001 - 75,000</td>
<td>1.2 TB</td>
<td>775 GB</td>
<td>350 GB</td>
<td>75 GB</td>
</tr>
<tr>
<td>75,001 - 100,000</td>
<td>2 TB</td>
<td>1.3 TB</td>
<td>600 GB</td>
<td>100 GB</td>
</tr>
<tr>
<td>100,001 - 150,000</td>
<td>4 TB</td>
<td>3 TB</td>
<td>800 GB</td>
<td>200 GB</td>
</tr>
<tr>
<td>150,001 - 300,000</td>
<td>6 TB</td>
<td>4.7 TB</td>
<td>1 TB</td>
<td>300 GB</td>
</tr>
<tr>
<td>300,001 - 500,001+</td>
<td>8 TB</td>
<td>6.4 TB</td>
<td>1.2 TB</td>
<td>400 GB</td>
</tr>
</tbody>
</table>

## Minimal and Recommended Disk Performances

The limiting factor of the database is usually the underlying disk performances. The better disk throughput/IOPS, the better overall performances of Tenable.ad will be. A low latency is also required (<5 ms).

## Storage managers - Disk Performance Matrix

<table>
<thead>
<tr>
<th>Active AD users</th>
<th>Minimal Disk Performance</th>
<th>Recommended Disk Performance</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Throughput (MB/sec)</td>
<td>IOPs (read/write)</td>
</tr>
<tr>
<td></td>
<td>Throughput (MB/sec)</td>
<td>IOPs (read/write)</td>
</tr>
<tr>
<td>1 - 25,000</td>
<td>150</td>
<td>2,500</td>
</tr>
<tr>
<td>25,001 - 50,000</td>
<td>200</td>
<td>5,000</td>
</tr>
<tr>
<td>50,001 -</td>
<td>200</td>
<td>5,000</td>
</tr>
</tbody>
</table>
### Example

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

<table>
<thead>
<tr>
<th>Domain</th>
<th>Number of Active AD users</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain A</td>
<td>45,000</td>
</tr>
<tr>
<td>Domain B</td>
<td>15,000</td>
</tr>
<tr>
<td>Domain C</td>
<td>150</td>
</tr>
<tr>
<td><strong>Total:</strong></td>
<td><strong>60,150</strong></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Tenable.ad services</th>
<th>Instance Required</th>
<th>vCPU (per instance)</th>
<th>Memory (per instance)</th>
<th>Disk Space (per instance)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory Listeners</td>
<td>1</td>
<td>4 cores, at least 2.6 GHz</td>
<td>12 GB of RAM</td>
<td>30 GB</td>
</tr>
<tr>
<td>Security Engine Nodes</td>
<td>1</td>
<td>10 cores, at least 2.6 GHz</td>
<td>24 GB of RAM</td>
<td>300 GB</td>
</tr>
<tr>
<td>Storage Managers</td>
<td>1</td>
<td>12 cores, at least 2.6 GHz</td>
<td>16 GB of RAM</td>
<td>1.2 TB with 10,000 IOPs</td>
</tr>
</tbody>
</table>
Network Requirements

Tenable.ad requires access to your Active Directory infrastructures to initiate security monitoring. You must allow some network flows between the different services of the platform, as described in Network Flow Matrix.

Bandwidth

As a monitoring platform, Tenable.ad 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.ad's for analysis in a reasonable amount of time.

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

<table>
<thead>
<tr>
<th>Active AD Users</th>
<th>Average Number of Objects Received (per minute)</th>
<th>Minimum Bandwidth</th>
<th>Recommended Bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 - 5,000</td>
<td>10</td>
<td>1 Mbps/sec</td>
<td>2 Mbps/sec</td>
</tr>
<tr>
<td>5,001 - 75,000</td>
<td>150</td>
<td>5 Mbps/sec</td>
<td>10 Mbps/sec</td>
</tr>
<tr>
<td>75,001 - 400,000</td>
<td>700</td>
<td>15 Mbps/sec</td>
<td>30 Mbps/sec</td>
</tr>
</tbody>
</table>

Microsoft APIs

To subscribe to the replication flows and begin monitoring them, Tenable.ad must contact standard directory APIs from Microsoft. Tenable.ad 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.

Architecture

For an on-premise architecture, Tenable.ad is a software package that you deploy on your Windows Server environment. Tenable.ad must communicate with the monitored Active Directory infrastructure.
Regular Upgrades

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.ad regularly.

Network Protocols

Specific network protocols (such as Syslog, SMTP or HTTP) allow Tenable.ad 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.ad 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 take into account other network flows, such as:

- Access to the end user services
- The network flows between Tenable.ad services
- The network flows from the support services that Tenable.ad 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.
Based on this diagram, the following table describes each required protocol and port that Tenable.ad uses.

<table>
<thead>
<tr>
<th>Network Flows</th>
<th>From</th>
<th>To</th>
<th>Tenable.ad’s Usage</th>
<th>Type of Traffic</th>
<th>Protocol and Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Tenable.ad ’s Directory Listeners</td>
<td>Domain controllers</td>
<td>Directory, Replication, User and Computer Authentication, Group Policy,</td>
<td>LDAP/LDAPS</td>
<td>TCP/389 and TCP/636 ICMP/echo-request</td>
</tr>
<tr>
<td>Trusts</td>
<td>Protocol</td>
<td>Ports</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>----------</td>
<td>------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Replication, User and Computer Authentication, Group Policy, Trusts</td>
<td>ICMP/echo-response</td>
<td>TCP/445</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Replication, User and Computer Authentication, Forest Level Trusts</td>
<td>Kerberos</td>
<td>TCP/88, TCP/464 and UDP/464</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User and Computer Authentication, Name Resolution, Trusts</td>
<td>DNS</td>
<td>UDP/53 and TCP/53</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Replication, User and Computer Authentication, Group Policy, Trusts</td>
<td>RPC, DCOM, EPM, DRSUAPI, NetLogonR, SamR, FRS</td>
<td>TCP Dynamic (&gt; 1024)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Directory, Replication, User and Computer Authentication, Group Policy, Trusts</td>
<td>Global Catalog</td>
<td>TCP/3268 and TCP/3269</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Replication</td>
<td>RPC Endpoint Mapper</td>
<td>TCP/135</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>Tenable.ad's Directory Listeners</td>
<td>Tenable.ad's Security engine nodes</td>
<td>Tenable.ad's communication bus</td>
<td>Advanced Message Queuing Protocol</td>
<td>TCP/5671 and TCP/5672</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Tenable.ad's internal API flows (optional)</td>
<td>TLS/HTTP</td>
<td>TCP/443</td>
</tr>
<tr>
<td>3.</td>
<td>End users</td>
<td>Tenable.ad's Security engine nodes</td>
<td>Tenable.ad's end user services (Web portal, REST API, etc.)</td>
<td>TLS/HTTP</td>
<td>TCP/443</td>
</tr>
<tr>
<td>4.</td>
<td>Tenable.ad Support services</td>
<td>Time synchronization</td>
<td>NTP</td>
<td>UDP/123</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Update infrastructure (e.g., WSUS or SCCM)</td>
<td>HTTP/HTTPS</td>
<td>TCP/80 or TCP/443</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>PKI infrastructure</td>
<td>HTTP/HTTPS</td>
<td>TCP/80 or TCP/443</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Identity provider SAML server</td>
<td>TLS/HTTP</td>
<td>TCP/443</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Identity provider LDAP</td>
<td>LDAP/LDAPS</td>
<td>TCP/389 and TCP/636</td>
</tr>
</tbody>
</table>
In addition to the Active Directory protocols, certain Tenable.ad configurations require additional flows. These protocols and ports must be open between Tenable.ad and the targeted service.

<table>
<thead>
<tr>
<th>Network flows</th>
<th>From</th>
<th>To</th>
<th>Tenable.ad’s Usage (optional)</th>
<th>Type of Traffic</th>
<th>Protocol and Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.</td>
<td>Tenable.ad’s Security Engine Nodes</td>
<td>Cybersecurity services</td>
<td>Tenable.ad Web Application</td>
<td>HTTP/TLS</td>
<td>TCP/443</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Email notifications</td>
<td>SMTP</td>
<td>TCP/25, TCP/587, TCP/465, TCP/2525, TCP/25025 (depending on the SMTP server’s configuration)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Syslog notifications</td>
<td>Syslog</td>
<td>TCP/601, TCP/6515, UDP/514 (depending on the event log server’s configuration)</td>
</tr>
<tr>
<td></td>
<td>Tenable REST API</td>
<td>HTTP/TLS</td>
<td></td>
<td></td>
<td>TCP/443</td>
</tr>
</tbody>
</table>
If you split the Security Engine Nodes and the Storage Managers into two different subnets, Tenable.ad 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.

<table>
<thead>
<tr>
<th>Network flows</th>
<th>From</th>
<th>To</th>
<th>Tenable.ad’s Usage</th>
<th>Type of Traffic</th>
<th>Protocol and Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.</td>
<td></td>
<td>Tenable.ad’s</td>
<td>MS SQL Server database</td>
<td>MS SQL queries</td>
<td>TCP/1433</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Security Engine</td>
<td>base access</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Nodes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Tenable.ad’s</td>
<td>InfluxDB Server database</td>
<td>InfluxDB queries over</td>
<td>TCP/8086</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Storage Managers</td>
<td>base access</td>
<td>HTTP</td>
<td></td>
</tr>
</tbody>
</table>

**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.ad initiates all network connections, except those from end users. You can use network address translation (NAT) to connect to Tenable.ad through network interconnection.
Network Matrix for Transport Layer Security (TLS) Mode

The illustration below shows the network matrix for a TLS platform with the required protocol and port.

Based on this diagram, the networks flows are as follows:

<table>
<thead>
<tr>
<th>Network Flows</th>
<th>To</th>
<th>From</th>
<th>Tenable's Usage</th>
<th>Type of Traffic</th>
<th>Protocol and Port</th>
</tr>
</thead>
</table>

Copyright © 2022 Tenable, Inc. All rights reserved. Tenable, Tenable.io, Tenable Network Security, Nessus, SecurityCenter, SecurityCenter Continuous View and Log Correlation Engine are registered trademarks of Tenable, Inc. Tenable.sc, Tenable.ot, Lumin, Indegy, Assure, and The Cyber Exposure Company are trademarks of Tenable, Inc. All other products or services are trademarks of their respective owners.
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>User and Computer Authentication, Forest Level Trusts</td>
<td>Kerberos</td>
<td>TCP/88, TCP/464 and UDP/464</td>
</tr>
<tr>
<td>User and Computer Authentication, Name Resolution, Trusts</td>
<td>DNS</td>
<td>UDP/53 and TCP/53</td>
</tr>
<tr>
<td>Replication, User and Computer Authentication, Group Policy, Trusts</td>
<td>RPC, DCOM, EPM, DRSUAPI, NetLogonR, SamR, FRS</td>
<td>TCP Dynamic (&gt;1024)</td>
</tr>
<tr>
<td>Directory, Replication, User and Computer Authentication, Group Policy, Trusts</td>
<td>Global Catalog</td>
<td>TCP/3268 and TCP/3269</td>
</tr>
<tr>
<td>Replication</td>
<td>RPC Endpoint Mapper</td>
<td>TCP/135</td>
</tr>
<tr>
<td>2.</td>
<td>Tenable</td>
<td>Tenable.ad</td>
</tr>
<tr>
<td>Network Flows</td>
<td>To</td>
<td>From</td>
</tr>
<tr>
<td>---------------</td>
<td>----</td>
<td>------</td>
</tr>
<tr>
<td>3.</td>
<td>End-users</td>
<td>Tenable.ad SaaS platform</td>
</tr>
</tbody>
</table>

Depending on your Tenable.ad configuration, you may need to allow additional flows by opening these protocols and ports between Tenable.ad and the targeted service.

<table>
<thead>
<tr>
<th>Network Flows</th>
<th>To</th>
<th>From</th>
<th>Tenable’s Usage (optional)</th>
<th>Type of Traffic</th>
<th>Protocol and Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.</td>
<td>Tenable.ad SaaS platform</td>
<td>Support services</td>
<td>Email notifications</td>
<td>SMTP</td>
<td>TCP/25, TCP/587, TCP/465, TCP/2525, TCP/25025 (depending on the SMTP server’s configuration)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>TCP/601, TCP/6515, UDP/514 (depending on the event log server’s con-</td>
</tr>
<tr>
<td>Configuration</td>
<td>Protocol</td>
<td>Port</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>--------------</td>
<td>------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tenable REST API</td>
<td>TLS/HTTP</td>
<td>TCP/443</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PKI infrastructure</td>
<td>HTTP/HTTPS</td>
<td>TCP/80 or TCP/443</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identity provider SAML server</td>
<td>TLS/HTTP</td>
<td>TCP/443</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identity provider LDAP</td>
<td>LDAP/LDAPS</td>
<td>TCP/389 and TCP/636</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identity provider OAuth</td>
<td>HTTPS</td>
<td>TCP/443</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Web Portal Requirements

Tenable.ad 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.

<table>
<thead>
<tr>
<th>Supported Web Browsers including minimum version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft</td>
</tr>
<tr>
<td>Google</td>
</tr>
<tr>
<td>Mozilla</td>
</tr>
<tr>
<td>Apple</td>
</tr>
</tbody>
</table>

TLS Server Certificate

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

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

<table>
<thead>
<tr>
<th>Supported TLS configuration and version</th>
<th>• TLS 1.1 to TLS 1.3</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Self-signed certificate from Tenable</td>
</tr>
<tr>
<td></td>
<td>• Certificate issued from your private PKI</td>
</tr>
<tr>
<td>Recommended TLS configuration and version</td>
<td>• Alternative TLS certificate</td>
</tr>
<tr>
<td></td>
<td>• TLS 1.2</td>
</tr>
<tr>
<td></td>
<td>• Certificate issued from your private PKI</td>
</tr>
</tbody>
</table>
Integration with an Active Directory Domain

Tenable.ad 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.ad 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.ad). In this configuration, an attacker with initial access or limited privileges on the monitored domain cannot directly access Tenable.ad and its security analysis results.

- If you have a trustful infrastructure, you can choose to run Tenable.ad 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’s 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.ad.
  - 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.ad’s security monitoring by hiding a security incident.

The following table summarizes the supported and recommended AD integrations:

<table>
<thead>
<tr>
<th>Supported AD integration</th>
<th>Recommended AD integration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tenable.ad’s joined to an AD domain</td>
<td>Tenable.ad’s isolated from the AD infrastructure</td>
</tr>
<tr>
<td>Tenable.ad’s isolated from the AD infrastructure</td>
<td></td>
</tr>
</tbody>
</table>

Copyright © 2022 Tenable, Inc. All rights reserved. Tenable, Tenable.io, Tenable Network Security, Nessus, SecurityCenter, SecurityCenter Continuous View and Log Correlation Engine are registered trademarks of Tenable, Inc. Tenable.sc, Tenable.ot, Lumin, Indegy, Assure, and The Cyber Exposure Company are trademarks of Tenable, Inc. All other products or services are trademarks of their respective owners.
Access to AD Objects or Containers

**Note:** This section only applies for a Tenable.ad license for the Indicator of Exposure module.

Tenable.ad does not require administrative privileges to achieve its security monitoring.

This approach relies on the ability of the user account that Tenable.ad uses to read all Active Directory objects stored in a domain (including user accounts, organizational units, groups, etc.).

By default, most objects have a read access for the group Domain Users that the Tenable.ad service account uses. However, you must manually configure some containers to allow read access for the Tenable.ad user account.

The following table details the Active Directory objects and containers that require manual configuration for read access on each domain that Tenable.ad monitors.

<table>
<thead>
<tr>
<th>Location of the Container</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CN=Deleted Objects, DC=&lt;DOMAIN&gt;, DC=&lt;TLD&gt;</td>
<td>A container that hosts deleted objects.</td>
</tr>
<tr>
<td>CN=Password Settings Container, CN=System, DC=&lt;DOMAIN&gt;, DC=&lt;TLD&gt;</td>
<td>(Optional) A container that hosts Password Strategy Objects.</td>
</tr>
</tbody>
</table>

To grant access to AD objects and containers:

- In the domain controller’s command line interface, run the following command to grant access to Active Directory objects or containers:

  ```
  dsacls "<__CONTAINER__>" /takeownership
  dsacls "<__CONTAINER__>" /g <__SERVICE_ACCOUNT__>:LCRP /I:T
  ```

  where:

  - `<__CONTAINER__>`
  - `<__SERVICE_ACCOUNT__>`
- `<__CONTAINER__>` refers to the container that requires access.
- `<__SERVICE_ACCOUNT__>` refers to the service account that Tenable.ad uses.
Prerequisite Checklist

- Tenable.ad works with Windows Server 2016 with the latest available update.
- Tenable.ad installation program requires Local Administrator rights on Windows Server 2016. If the account used for the installation is the default account, ensure that this account can run programs without restrictions.
- Tenable.ad services require Local Administrator rights to run local services on the machine.
- Tenable.ad requires a dedicated data partition. Do not run Tenable.ad on the OS partition to prevent system freeze if the partition is full.
- Tenable.ad SQL instance requires the virtual accounts usage feature.
- Tenable.ad must run as a black box. You must dedicate each machine to Tenable.ad and not share it with another product.
- Tenable.ad 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.

This table resumes the prerequisites in a handy checklist prior to installation.

<table>
<thead>
<tr>
<th>Information or Resource to Reserve</th>
<th>Status</th>
<th>Specifics</th>
</tr>
</thead>
<tbody>
<tr>
<td>The required agreements (NDA, Evaluation Software License), if applicable</td>
<td>YES/NO</td>
<td></td>
</tr>
<tr>
<td>The choice of architecture (centralized or distributed)</td>
<td>YES/NO</td>
<td></td>
</tr>
<tr>
<td>The number of active AD users in the targeted domains to monitor</td>
<td>YES/NO</td>
<td></td>
</tr>
<tr>
<td>The computing and memory resources based on Tenable.ad’s sizing matrix.</td>
<td>YES/NO</td>
<td></td>
</tr>
<tr>
<td>The private IP of each virtual machine used to deploy Tenable’s platform</td>
<td>YES/NO</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>YES/NO</td>
<td></td>
</tr>
<tr>
<td>----------------------------------------------------------------------------</td>
<td>--------</td>
<td></td>
</tr>
<tr>
<td>The type and IP address of the update management infrastructure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The type and IP address of the time server</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The type and IP address of the PKI server</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The type and IP address of the identity provider</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Open required network flows for each service that Tenable.ad requires.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The private IP addresses of each Primary Domain Controller emulator</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Creation of a regular user account on each Active Directory forest to monitor.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>On the specific Active Directory containers, grant access right to the Tenable service account.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The domain user accounts information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Format: NetBIOSName\SamAccountName</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A TLS certificate issued for Tenable.ad's Web Portal issued from the customer’s PKI</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Otherwise, inform Technical Lead of the use of self-signed certificate.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The list of Tenable.ad user accounts to create</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Required information: first and last name, email address and desired login.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The list of optional configurations to activate (email notification, Syslog event forwarding, etc.)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>An identified and available project coordinator to work with Tenable.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Technical staff to respond to potential technical issues such as network filtering issue and Punreachable DCe.</td>
<td>YES/NO</td>
<td></td>
</tr>
</tbody>
</table>
Install Tenable.ad

Tenable.ad's installation program installs the following components:

- A Storage Manager to host all data based on MSSQL and InfluxDB.
- A Directory Listener to target audited domains.
- A Security Engine Node to perform security analysis and serve the Web interface.

All three 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).

For more information about different TLS setups, see Available TLS Installations
Installation Programs

The Tenable.ad Platform Installer, available on Tenable’s Downloads site, is the main installer for most on-premises and SaaS (excluding SaaS-TLS) deployments.

For SaaS-TLS deployments, you must download the Tenable.ad Security Probe Installer. You must also have your customized certs.zip file containing the required certificates that the Tenable.ad team provides.

Note that starting from version 3.11, the Tenable.ad Security Probe Installer is only compatible with SaaS-TLS deployments. To install a Directory Listener node, you must use the Tenable.ad Platform Installer file and select the "Directory Listener" component only.

**Note:** Tenable requires that you reboot all machines before you start a new installation.

Installation Log File

If the installation program cannot install Tenable.ad 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`.

Available TLS Installations

Tenable.ad offers the possibility to encrypt internal communications between Tenable.ad components (micro-services) for eventual cybersecurity policy requirements or regulatory reasons using Transport Layer Security (TLS).

Tenable.ad 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.ad web portal using an Internet Information Services (IIS) certificate.

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

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

<table>
<thead>
<tr>
<th>Installation Type</th>
<th>Recommended For</th>
<th>Encryption Between Internal Communications and Tenable.ad Components</th>
<th>Peer Verification</th>
<th>Installation Option to Select</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>No TLS</strong></td>
<td>A trusted network of machines. An easy installation with little configuration.</td>
<td>Not encrypted</td>
<td>N/A</td>
<td><em>No TLS option in &quot;Expert mode&quot;</em></td>
</tr>
</tbody>
</table>
| **Default TLS**   | An organization without its own internal public key infrastructure (PKI) that requires | Encrypted, using an internal PKI for Tenable.ad with its own certificates and private keys, Disabled | Tenable.ad does not check server certificates. This setup is | • Default (no "Expert mode")  
• Installation with Default TLS using |

Copyright © 2022 Tenable, Inc. All rights reserved. Tenable, Tenable.io, Tenable Network Security, Nessus, SecurityCenter, SecurityCenter Continuous View and Log Correlation Engine are registered trademarks of Tenable, Inc. Tenable.sc, Tenable.ot, Lumin, Indegy, Assure, and The Cyber Exposure Company are trademarks of Tenable, Inc. All other products or services are trademarks of their respective
| **Custom TLS Without Peer Verification** | An organization with its own internal PKI that requires protection against passive eavesdropping. | **Encrypted**, using certificates from your internal PKI. Certificates must contain the IP address of the corresponding machine in the Subject Alternative Name (SAN) extension and be signed by the provided Certificate Authority (CA). | **Disabled** Tenable.ad does not check server certificates. This setup is not resistant to active MITM attacks. | **TLS with Custom certificates without peer verification option in "Expert mode"** |
| **Custom TLS With Peer Verification** | An organization with its own internal public key infrastructure (PKI) that requires protection against both passive eavesdropping and | **Encrypted**, using certificates from your internal PKI. Certificates must contain the IP address of the corresponding machine in the Subject Alternative Name | **Enabled** Tenable.ad checks server certificates. This setup is resistant to active MITM attacks. | **TLS with Custom certificates with peer verification option in "Expert mode"** |
| man-in-the-middle (MITM) attacks. | (SAN) extension and be signed by the provided Certificate Authority (CA). |   |
Installation with No TLS

**Required User Role:** Administrator on the local machine

This installation type installs the following Tenable.ad components without TLS.

- Storage Manager
- Security Engine Node
- Directory Listener

To install the Storage Manager with no TLS:

1. On the local machine, run the installation file Tenable.ad_v3.11.x.exe.
   
   The **Setup Wizard** appears.

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

3. Click **Next**.
   
   The **Custom Setup** window appears.

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

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

6. Click **Next**.
   
   The **TLS Options** window appears.

7. Select the **No TLS** option.
8. Click Next.

   The **Storage Manager** window appears.

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

   ![Storage Manager window]

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

10. Click Next.

    The **Ready to Install** window appears.
11. Click **Install** to begin the installation.

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

12. Click **Finish**.

   A dialog box asks you to restart your machine.

13. Click **Yes**.

   The machine restarts.

To install the Security Engine Node with no TLS:

1. On the local machine, run the installation file Tenable.ad_v3.11.x.exe.

   The **Setup Wizard** appears.

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

3. Click **Next**.

   The **Custom Setup** window appears.

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

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

6. Click **Next**.

   The **TLS Options** window appears.

7. Select the **No TLS** option.
8. Click **Next**.

The **Storage Manager** window appears.

9. Provide the following information:

   - In the **MSSQL** box, type the IP address of the Storage Manager.
   - In the **InfluxDB** 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.

10. Click **Next**.

    The **Security Engine Node** window appears.
11. 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.ad.

![Tenable.ad Setup window](image)

**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 **Ready to Install** window appears.

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

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

14. Click **Finish**.

   A dialog box asks you to restart your machine.

15. Click **Yes**.

   The machine restarts.

**To install the Directory Listener with no TLS:**

1. On the local machine, run the installation file `Tenable.ad_v3.11.x.exe`.

   The **Setup Wizard** appears.

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

   The **Custom Setup** window appears.

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

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

6. Click **Next**.

   The **TLS Options** window appears.

7. Select the **No TLS** option.

8. Click **Next**.

   The **Security Engine Node** window appears.
9. In the IP box for RabbitMQ, type the address of the Security Engine Node hosting RabbitMQ.

10. Click **Next**.

    The **Ready to Install** window appears.

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

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

12. Click **Finish**.

    A dialog box asks you to restart your machine.

13. Click **Yes**.

    The machine restarts.
Installation with Default TLS

**Required User Role:** Administrator on the local machine

This installation process installs the following Tenable.ad components in default TLS mode without peer verification and with self-signed certificates.

- Storage Manager
- Security Engine Node
- Directory Listener

To install the Storage Manager with default TLS:

1. On the local machine, run the installation file `Tenable.ad_v3.11.x.exe`.
   
   The **Setup Wizard** appears.
   
   **Note:** Do not select the "Expert Mode" checkbox.

2. Click **Next**.
   
   The **Custom Setup** window appears.

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

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

5. Click **Next**.
   
   The **Storage Manager** window appears.
6. In the **Password** box, type a password for the MSSQL database.

![Password box screenshot](image)

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

7. Click **Next**.

   The **Ready to Install** window appears.

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

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

9. Click **Finish**.

   A dialog box asks you to restart your machine.

10. Click **Yes**.

    The machine restarts.

To install the Security Engine Node with default TLS:

1. On the local machine, run the installation file `Tenable.ad_v3.11.x.exe`.

   The **Setup Wizard** appears.

   **Note**: Do not select the "Expert Mode" checkbox.
2. Click **Next**.

   The **Custom Setup** window appears.

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

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

5. Click **Next**.

   The **Storage Manager** window appears.

6. Provide the following information:
   
   - In the **MSSQL** box, type the IP address of the Storage Manager.
   - In the **InfluxDB** 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.

7. Click **Next**.

   The **Security Engine Node** window appears.

8. 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.ad.
9. Click Next.

The Ready to Install window appears.

10. Click Install to begin the installation.

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

11. Click Finish.

A dialog box asks you to restart your machine.

12. Click Yes.

The machine restarts.

To install the Directory Listener with default TLS:

1. On the local machine, run the installation file Tenable.ad_v3.11.x.exe.

The Setup Wizard appears.

Note: Do not select the "Expert Mode" checkbox.
2. Click **Next**.

   The **Custom Setup** window appears.

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

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

5. Click **Next**.

   The **Security Engine Node** window appears.

6. In the **IP** box for RabbitMQ, type the address of the Security Engine Node hosting RabbitMQ.

7. Click **Next**.

   The **Directory Listener** window appears.

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

   The **Ready to Install** window appears.

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

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

11. Click **Finish**.

    A dialog box asks you to restart your machine.

12. Click **Yes**.

    The machine restarts.
Installation with Default TLS using Autogenerated and Self-signed Certificates

**Required User Role:** Administrator on the local machine

This installation process installs the following Tenable.ad components in TLS mode without peer verification and with autogenerated and self-signed certificates. It requires the "Expert Mode" setting in the Setup Wizard.

- **Storage Manager**
- **Security Engine Node**
- **Directory Listener**

To install the Storage Manager with default TLS using the "Expert Mode":

1. On the local machine, run the installation file `Tenable.ad_v3.11.x.exe`.

   The **Setup Wizard** appears.

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

3. Click **Next**.

   The **Custom Setup** window appears.

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

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

6. Click **Next**.

   The **TLS Options** window appears.

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

    The **Storage Manager** window appears.

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

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

10. Click **Next**.

    The **Ready to Install** window appears.
11. Click **Install** to begin the installation.

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

12. Click **Finish**.

    A dialog box asks you to restart your machine.

13. Click **Yes**.

    The machine restarts.

To install the Security Engine Node with default TLS using the "Expert Mode":

1. On the local machine, run the installation file `Tenable.ad_v3.11.x.exe`.

    The **Setup Wizard** appears.

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

3. Click **Next**.

    The **Custom Setup** window appears.

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

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

6. Click **Next**.

    The **TLS Options** window appears.

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

The **Storage Manager** window appears.

9. Provide the following information:

   - In the MSSQL box, type the IP address of the Storage Manager.
   - In the InfluxDB 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.

10. **Click Next.**

    The **Security Engine Node** window appears.
11. 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.ad.

![Tenable.ad Setup](image)

**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 **Ready to Install** window appears.

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

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

14. Click **Finish**.

A dialog box asks you to restart your machine.

15. Click **Yes**.

The machine restarts.

To install the Directory Listener with default TLS using the "Expert Mode":

1. On the local machine, run the installation file `Tenable.ad_v3.11.x.exe`.

   The **Setup Wizard** appears.

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

   The **Custom Setup** window appears.

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

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

6. Click **Next**.

   The **TLS Options** window appears.

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

![TLS Options window](image)

8. Click **Next**.

   The **Security Engine Node** window appears.
9. In the **IP** box for RabbitMQ, type the address of the Security Engine Node hosting RabbitMQ.

![Image of the IP box for RabbitMQ]

10. Click **Next**.

   The **Directory Listener** window appears.

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

![Image of the Directory Listener window]

12. Click **Next**.

   The **Ready to Install** window appears.

13. Click **Install** to begin the installation.
After the installation completes, the **Completing the Tenable.ad Setup Wizard** window appears.

14. Click **Finish**.

   A dialog box asks you to restart your machine.

15. Click **Yes**.

   The machine restarts.
Installation with Custom TLS and without Peer Verification

**Required User Role:** Administrator on the local machine

This installation type installs the following Tenable.ad components with custom TLS and without peer verification.

- **Storage Manager**
- **Security Engine Node**
- **Directory Listener**

To install the Storage Manager with custom TLS and without peer verification:

1. On the local machine, run the installation file `Tenable.ad_v3.11.x.exe`.
   
   The **Setup Wizard** appears.

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

3. Click **Next**.
   
   The **Custom Setup** window appears.

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

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

6. Click **Next**.
   
   The **TLS Options** window appears.

7. Select the **TLS with custom certificates without peer verification** option.
8. Click Next.

The TLS certificates window appears.

9. 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.

10. Click Next.

    The Storage Manager window appears.
11. In the **Password** box, type a password for the MSSQL database.

![Password box screenshot](image1)

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

12. Click **Next**.

   The **Ready to Install** window appears.

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

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

14. Click **Finish**.

   A dialog box asks you to restart your machine.

15. Click **Yes**.

   The machine restarts.

To install the Security Engine Node with custom TLS and without peer verification:

1. On the local machine, run the installation file `Tenable.ad_v3.11.x.exe`.

   The **Setup Wizard** appears.

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

3. Click **Next**.
The Custom Setup window appears.

4. Deselect the Storage Manager and Directory Listener components.

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

6. Click Next.

The TLS Options window appears.

7. Select the TLS with custom certificates without peer verification option.

8. Click Next.

The TLS certificates window appears.

9. 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.

10. Click Next.

The Storage Manager window appears.

11. Provide the following information:
   - In the MSSQL box, type the IP address of the Storage Manager.
   - In the InfluxDB 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.
12. Click **Next**.

   The **Security Engine Node** window appears.

13. 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.ad.

![Security Engine Node window](image)

   **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.

14. Click **Next**.

   The **Ready to Install** window appears.

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

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

16. Click **Finish**.

   A dialog box asks you to restart your machine.

17. Click **Yes**.

   The machine restarts.

To install the Directory Listener with custom TLS and without peer verification:
1. On the local machine, run the installation file Tenable.ad_v3.11.x.exe.

   The **Setup Wizard** appears.

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

3. Click **Next**.

   The **Custom Setup** window appears.

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

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

6. Click **Next**.

   The **TLS Options** window appears.

7. Select the **TLS with custom certificates without peer verification** option.

8. Click **Next**.

   The **TLS certificates** window appears.
9. Nothing is required in this screen. Click **Next**.

The **Security Engine Node** window appears.

10. In the **IP** box for RabbitMQ, type the address of the Security Engine Node hosting RabbitMQ.

11. Click **Next**.

The **Directory Listener** window appears.

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

   The **Ready to Install** window appears.

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

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

15. Click **Finish**.

   A dialog box asks you to restart your machine.

16. Click **Yes**.

   The machine restarts.
Installation with Custom TLS and with Peer Verification

**Required User Role:** Administrator on the local machine

This installation type installs the following Tenable.ad components with custom TLS and peer verification.

- **Storage Manager**
- **Security Engine Node**
- **Directory Listener**

To install the Storage Manager with custom TLS and peer verification:

1. On the local machine, run the installation file `Tenable.ad_v3.11.x.exe`.
   
   The **Setup Wizard** appears.

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

3. Click **Next**.
   
   The **Custom Setup** window appears.

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

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

6. Click **Next**.
   
   The **TLS Options** window appears.

7. Select the **TLS with custom certificates with peer validation** option.
8. Click **Next**.

   The **TLS certificates** window appears.

9. 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.

10. Click **Next**.

    The **Storage Manager** window appears.
11. In the **Password** box, type a password for the MSSQL database.

![Password box](image)

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

12. Click **Next**.

   The **Ready to Install** window appears.

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

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

14. Click **Finish**.

   A dialog box asks you to restart your machine.

15. Click **Yes**.

   The machine restarts.

To install the Security Engine Node with custom TLS and peer verification:

1. On the local machine, run the installation file `Tenable.ad_v3.11.x.exe`.

   The **Setup Wizard** appears.

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

3. Click **Next**.
The **Custom Setup** window appears.

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

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

6. Click **Next**.

   The **TLS Options** window appears.

7. Select the **TLS with custom certificates with peer validation** option.

8. Click **Next**.

   The **TLS certificates** window appears.

9. 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.

10. Click **Next**.

The **Storage Manager** window appears.

11. Provide the following information:
   - In the **MSSQL** box, type the IP address of the Storage Manager.
   - In the **InfluxDB** 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.

12. Click **Next**.
The **Security Engine Node** window appears.

13. 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.ad.

![Security Engine Node window](image)

**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](#).

14. Click **Next**.

   The **Ready to Install** window appears.

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

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

16. Click **Finish**.

   A dialog box asks you to restart your machine.

17. Click **Yes**.

   The machine restarts.

To install the Directory Listener with custom TLS and peer verification:

1. On the local machine, run the installation file `Tenable.ad_v3.11.x.exe`.

   The **Setup Wizard** appears.
2. Select the **Expert Mode** check box.

3. Click **Next**.

   The **Custom Setup** window appears.

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

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

6. Click **Next**.

   The **TLS Options** window appears.

7. Select the **TLS with custom certificates with peer validation** option.

8. Click **Next**.

   The **TLS certificates** window appears.

9. In the **CA Cert File** box, click **...** to browse to your CA certificate file.
10. Click **Next**.

11. The **Security Engine Node** window appears.

12. In the **IP** box for RabbitMQ, type the address of the Security Engine Node hosting RabbitMQ.

13. Click **Next**.

   The **Directory Listener** window appears.

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

   The Ready to Install window appears.

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

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

17. Click **Finish**.

   A dialog box asks you to restart your machine.

18. Click **Yes**.

   The machine restarts.
Security Probe

**Required User Role:** Administrator on the local machine

You install Tenable.ad's security probe in a SaaS-TLS deployment.

Before you start

- Obtain from Tenable.ad the `certs.zip` archive that contains the required certificate files to configure the SaaS-TLS installation.
- Extract the required certificate files to a local directory.
- Obtain from Tenable.ad the public IP address for RabbitMQ.

To install the security probe:

1. On the local machine, run the installation file `Tenable.ad_Security_Probe_v3.11.x.exe`.
   
   The *Security Probe Setup Wizard* appears.

2. Click *Next*.
   
   The *TLS certificates* window appears.

3. Provide the following information extracted from the `certs.zip` archive:
○ In the **Client PFX Archive** box, click ... to browse to your PFX archive.

○ In the **PFX Password** box, type the password for the PFX file.

![Image of PFX Archive and Password boxes]

4. Click **Next**.

   The **Security Engine Node** window appears.

5. In the **IP** box, type the public IP address for RabbitMQ that you obtained from Tenable.ad.

![Image of IP entry in Security Engine Node]

6. Click **Next**.

   The **Security Probe** window appears.
7. In the **Subnets** box, type the subnet address for the security probe. For multiple subnets, use a comma to separate the addresses.

8. Click **Next**.

   The **Ready to Install** window appears.

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

   When the installation completes, the **Completing the Tenable.ad Security Probe Setup Wizard** window appears.

10. Click **Finish**.

    A dialog box message asks you to restart your machine.

11. Click **Yes**.

    The machine restarts.
Indicators of Attack

The indicator of attack module requires the deployment of a new GPO on the monitored infrastructure using a PowerShell script from Tenable. You must run this script once per feature deployment using an administrative account that can create a new GPO and link it to the organizational unit hosting the Domain Controllers of the monitored domain, as described in Install Indicators of Attack.

**Note:** This information only applies to licenses benefiting from the indicator of attack module.

For more information, see:

- [Indicators of Attack and the Active Directory](#)
- [Install Indicators of Attack](#)
- [Install Microsoft Sysmon](#), a Windows system tool that some of Tenable.ad’s indicators of attack require to get relevant system data.
- [Troubleshoot Antivirus Detection](#)
- [Troubleshoot Advanced Audit Policy Configuration Precedence](#)
Indicators of Attack and the Active Directory

Tenable.ad works as a non-intrusive solution that monitors an Active Directory infrastructure without deploying agents and with minimal configuration change in your environment.

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

Tenable.ad leverages the Active Directory replication mechanisms to retrieve the relevant information, which incurs only limited bandwidth costs between each domain’s PDC and Tenable.ad’s Directory Listener.

To detect efficiently security incidents using indicators of attack, Tenable.ad uses the Event Tracing for Windows (ETW) information and the replication mechanisms available on each Domain Controller. To collect this set of information, you deploy a dedicated Group Policy Object (GPO) using a script from Tenable.ad as described in Install Indicators of Attack.

This GPO activates a Windows Management Instrumentation (WMI) filter on all domain controllers which writes to the system volume (SYSVOL) to benefit from the AD replication engine and Tenable.ad’s ability to listen to SYSVOL events. The GPO creates a file in SYSVOL for each domain controller and flushes its contents periodically.

To initiate security monitoring, Tenable.ad must contact standard directory APIs from Microsoft.
Tenable.ad only requires communication with the Primary Domain Controller emulator (PDCe) using the network protocols described in the Network Flow Matrix.

In the case of multiple monitored domains or forests, Tenable.ad must reach each domain's PDCe. For best performance, Tenable recommends that you host Tenable.ad on a physical network close to the PDCe to monitor.

**User Account**

Tenable.ad authenticates to the monitored infrastructure using a non-administrator user account to access the replication flow.

A simple Tenable.ad user can access all collected data. Tenable.ad does not access secret attributes such as credentials, password hashes, or Kerberos keys.

Tenable recommends that you create a service account that is a member of the group “Domain Users” as follows:

- The service account is on the main monitored domain.
- The service account is in any Organizational Unit (OU), preferably where you create other security service accounts.
- The service account has standard user group membership (such as member of the Domain Users AD default group).
Install Indicators of Attack

Tenable.ad's Indicators of Attack (IoA) module requires you to run a Powershell installation script with an administrative account having the ability to create and link a new Group Policy Object (GPO) to an organizational unit (OU).

You can run this script from any machine joined to your Active Directory domain that Tenable.ad monitors and that can reach domain controllers via the network.

You only have to run this installation script once in each AD domain: through the GPO, it will automatically apply to all existing and new domain controllers (DC).

To activate this module, the installation script carries out the following tasks:

- Creation of a GPO that configures the PowerShell Event Tracing for Windows (ETW) script, which runs on each domain controller (DC) to extract ETW information.
- Installation of a Windows Management Instrumentation (WMI) filter to restart the PowerShell script at boot.

Before you begin

- Review the limitations and potential impacts of installing IoAs, as described in Technical Changes and Potential Impact.
- Check that the DC has the PowerShell modules for ActiveDirectory and GroupPolicy installed and available.
- Check that the DC has the Distributed File System Tools feature RSAT-DFS-Mgmt-Con enabled so that the deployment script can check for replication status because it cannot create a GPO while the DC is replicating.

To download the installation script:

1. In Tenable.ad, click System and the Configuration tab.

   The Configuration pane appears.

2. Click Indicators of Attack.
3. Check the boxes for each indicators of attack and domain to monitor. Be mindful not to exceed the workload quota.

4. Click **Save**.

   A confirmation window appears.

5. Click **Confirm**.

6. Click **Download the installation file**.

To run the installation script:

1. Copy and paste the downloaded installation file to the DC in the monitored domain.
2. Open a PowerShell terminal with administrative rights.
3. In Tenable.ad, copy the command under the **Indicators of Attack** section at the bottom of the window.

4. In the PowerShell window, paste the command to run the script.

For more information, see:
• Troubleshoot Antivirus Detection
• Troubleshoot Advanced Audit Policy Configuration Precedence
**Technical Changes and Potential Impact**

The installation script for the indicators of attack (IoA) module creates a GPO that applies the following changes transparently on the monitored DCs:

- A new GPO named “Tenable.ad” by default linked to the domain controller's organization unit (OU) by default.
- Modification of a registry key to activate the Microsoft Advanced logging policy.
- Activation of a new Event Log policy to force Domain Controllers to generate the ETW information that IoAs require.

**Note:** The Event Log policy is mandatory so that the ETW engine can generate the insertion strings that Tenable.ad requires. This policy does not disable any existing logging policy but adds to them. If there is a conflict, the deployment script stops with an error message.

**Limitation and Potential Impacts**

The **Indicator of Attack** (IoA) module can pose the following limitations:

- The IoA module relies on the ETW data and is bound by their limitations as defined by Microsoft.
- The installed GPO must replicate over the entire domain, and the GPO refresh interval must elapse for the installation process to complete. During this replication period, false positives and false negatives can happen, even though Tenable.ad minimizes this effect by not starting the checks in the Indicator of Attack engine immediately.
- Tenable uses the SYSVOL file share to retrieve ETW information from domain controllers. As SYSVOL replicates to every domain controller in the domain, a significant increase of the replication activity appears during a high peak of Active Directory activity.
- Replicating files between domain controllers and Tenable.ad also consumes some network bandwidth. Tenable.ad controls these impacts with the automatic removal of the files it collects, and limits the size of these files (500 MB maximum by default.)
Install Microsoft Sysmon

Some Tenable.ad’s Indicators of Attack (IoAs) require the Microsoft System Monitor (Sysmon) service to activate.

Sysmon monitors and logs system activity to the Windows event log to provide more security-oriented information in the Event Tracing for Windows (ETW) infrastructure.

Because installing an additional Windows service and driver can affect performances of the domain controllers hosting the Active Directory infrastructure. Tenable does not deploy automatically Microsoft Sysmon. You must install it manually or use a dedicated GPO.

The following IoAs require Microsoft Sysmon.

<table>
<thead>
<tr>
<th>Name</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS Credential Dumping: LSASS Memory</td>
<td>Detects Process Injection</td>
</tr>
</tbody>
</table>

**Note:** If you choose to install Sysmon, then you must install it on all domain controllers and not just the PDC to collect all necessary events.

**Note:** Test your Sysmon installation for compatibility issues before a full deployment of Tenable.ad.

To install Sysmon:

1. Download Sysmon from the Microsoft website.

2. In the command line interface, run the following command to install Microsoft Sysmon on the local machine:

   ```
   .\Sysmon64.exe -accepteula -i C:\TenableSysmonConfigFile.xml
   ```

   **Note:** See the commented `Sysmon configuration file` for configuration explanations.

3. Run the following command to add a registry key to indicate to WMI filters that Sysmon is installed:
For more information, see Uninstall Sysmon.

Sysmon Configuration File

```xml
<Sysmon schemaversion="4.40">
  <EventFiltering>
    <!--- SYSMON EVENT ID 1 : PROCESS CREATION [ProcessCreate]-->
    <RuleGroup name="" groupRelation="or">
      <ProcessCreate onmatch="exclude">
        <!--- NOTE: Using "exclude" with no rules means everything in this section will be logged-->
      </ProcessCreate>
    </RuleGroup>
    <!--- SYSMON EVENT ID 2 : FILE CREATION TIME RETROACTIVELY CHANGED IN THE FILESYSTEM [FileCreateTime]-->
    <RuleGroup name="" groupRelation="or">
      <FileCreateTime onmatch="include">
        <!--- NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </FileCreateTime>
    </RuleGroup>
    <!--- SYSMON EVENT ID 3 : NETWORK CONNECTION INITIATED [NetworkConnect]-->
    <RuleGroup name="" groupRelation="or">
      <NetworkConnect onmatch="include">
        <!--- NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </NetworkConnect>
    </RuleGroup>
    <!--- SYSMON EVENT ID 4 : RESERVED FOR SYSMON SERVICE STATUS MESSAGES-->
    <!--- Cannot be filtered.-->
    <!--- SYSMON EVENT ID 5 : PROCESS ENDED [ProcessTerminate]-->
    <RuleGroup name="" groupRelation="or">
      <ProcessTerminate onmatch="exclude">
        <!--- NOTE: Using "exclude" with no rules means everything in this section will be logged-->
      </ProcessTerminate>
    </RuleGroup>
    <!--- SYSMON EVENT ID 6 : DRIVER LOADED INTO KERNEL [DriverLoad]-->
    <RuleGroup name="" groupRelation="or">
      <DriverLoad onmatch="include">
        <!--- NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </DriverLoad>
    </RuleGroup>
    <!--- SYSMON EVENT ID 7 : DLL (IMAGE) LOADED BY PROCESS [ImageLoad]-->
    <RuleGroup name="" groupRelation="or">
      <ImageLoad onmatch="include">
        <!--- NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </ImageLoad>
    </RuleGroup>
  </EventFiltering>
</Sysmon>
```
<!-- SYSMON EVENT ID 8: REMOTE THREAD CREATED [CreateRemoteThread]-->
<RuleGroup name="" groupRelation="or">
  <CreateRemoteThread onmatch="include">
    <TargetImage name="lsass" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
  </CreateRemoteThread>
</RuleGroup>

<!-- SYSMON EVENT ID 9: RAW DISK ACCESS [RawAccessRead]-->
<RuleGroup name="" groupRelation="or">
  <RawAccessRead onmatch="include">
    <!-- NOTE: Using "include" with no rules means nothing in this section will be logged-->
  </RawAccessRead>
</RuleGroup>

<!-- SYSMON EVENT ID 10: INTER-PROCESS ACCESS [ProcessAccess]-->
<RuleGroup name="" groupRelation="or">
  <ProcessAccess onmatch="include">
    <!-- Detect Access to LSASS-->
    <Rule groupRelation="and">
      <TargetImage name="technique_id=T1003,technique_name=Credential Dumping" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
      <GrantedAccess>0x1FFFFF</GrantedAccess>
    </Rule>
    <Rule groupRelation="and">
      <TargetImage name="technique_id=T1003,technique_name=Credential Dumping" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
      <GrantedAccess>0x1F1FFF</GrantedAccess>
    </Rule>
    <Rule groupRelation="and">
      <TargetImage name="technique_id=T1003,technique_name=Credential Dumping" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
      <GrantedAccess>0x1010</GrantedAccess>
    </Rule>
    <Rule groupRelation="and">
      <TargetImage name="technique_id=T1003,technique_name=Credential Dumping" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
      <GrantedAccess>0x143A</GrantedAccess>
    </Rule>
    <!-- Detect process hollowing to LSASS-->
    <Rule groupRelation="and">
      <TargetImage name="technique_id=T1003,technique_name=Credential Dumping" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
      <GrantedAccess>0x0800</GrantedAccess>
    </Rule>
    <Rule groupRelation="and">
      <TargetImage name="technique_id=T1003,technique_name=Credential Dumping" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
      <GrantedAccess>0x800</GrantedAccess>
    </Rule>
  </ProcessAccess>
</RuleGroup>

<!-- Detect process process injection to LSASS-->
<Rule groupRelation="and">
  <TargetImage name="technique_id=T1055,technique_name=Process Injection" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
  <GrantedAccess>0x8820</GrantedAccess>
</Rule>
<!DOCTYPE html>
<html xmlns="http://www.w3.org/1999/xhtml">
<body>

<!-- SYMOM EVENT ID 11: FILE CREATED [FileCreate] -->

[RuleGroup name="" groupRelation="or">
  [FileCreate onmatch="include">
    <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
    </FileCreate>
  </RuleGroup>

<!-- SYMOM EVENT ID 12 & 13 & 14: REGISTRY MODIFICATION [RegistryEvent] -->

[RuleGroup name="" groupRelation="or">
  [RegistryEvent onmatch="include">
    <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
    </RegistryEvent>
  </RuleGroup>

<!-- SYMOM EVENT ID 15: ALTERNATE DATA STREAM CREATED [FileCreateStreamHash] -->

[RuleGroup name="" groupRelation="or">
  [FileCreateStreamHash onmatch="include">
    <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
    </FileCreateStreamHash>
  </RuleGroup>

<!-- SYMOM EVENT ID 16: SYMOM CONFIGURATION CHANGE -->

<!-- Cannot be filtered.--> 

<!-- SYMOM EVENT ID 17 & 18: PIPE CREATED / PIPE CONNECTED [PipeEvent] -->

[RuleGroup name="" groupRelation="or">
  [PipeEvent onmatch="include">
    <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
    </PipeEvent>
  </RuleGroup>


[RuleGroup name="" groupRelation="or">
  [WmiEvent onmatch="include">
    <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
    </WmiEvent>
  </RuleGroup>

<!-- SYMOM EVENT ID 22: DNS QUERY [DnsQuery] -->

[RuleGroup name="" groupRelation="or">
  [DnsQuery onmatch="include">
    <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
    </DnsQuery>
  </RuleGroup>

<!-- SYMOM EVENT ID 23: FILE DELETED [FileDelete] -->

[RuleGroup name="" groupRelation="or">
  [FileDelete onmatch="include">
    <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
    </FileDelete>
  </RuleGroup>

</body>
</html>
<!-NOTE: Using "include" with no rules means nothing in this section will be logged-->
Troubleshoot Antivirus Detection

Tenable does not recommend installing antivirus, Endpoint Protection Platform (EPP), or Endpoint Detection and Response (EDR) software on domain controllers (or any other tool with a central management console). If you choose to do so, note that your antivirus/EPP/EDR might detect and even block or delete required items for the collection of Indicator of Attack (IoA) events on domain controllers.

Tenable.ad's deployment script for Indicators of Attack does not include malicious code, nor is it even obfuscated. However, occasional detections are normal given its usage of PowerShell and WMI and the agentless nature of the implementation.

If you encounter issues such as:

- Error messages during installation
- False-positive or false-negative in detection

To troubleshoot installation scripts antivirus detection:

1. Review your antivirus/EPP/EDR security logs to check for any detection, blocking, or deletion of Tenable.ad components. Antivirus/EPP/EDR can affect the following components:
   - ScheduledTasks.xml file in the Tenable.ad GPO applied to domain controllers
   - The Tenable.ad scheduled task on domain controllers that launches PowerShell.exe

2. Add security exceptions in your tools for the affected components.

In particular, Symantec Endpoint Protection is known to raise CL.Downloaderagen27 detections during the IoA installation process. You can add this specific known risk to your exceptions policy.
Troubleshoot Advanced Audit Policy Configuration Precedence

The group policy object (GPO) that Tenable.ad creates to enable required events logging is linked to the organization unit (OU) domain controllers with Enforced mode enabled.

This gives the GPO a very high priority, but an enforced GPO configured at a higher level (such as domain or site) takes precedence over it.

If the higher priority GPO that defines the Advanced Audit Policy Configuration settings conflicts with Tenable.ad’s needs, it takes precedence and Tenable.ad misses required events for attack detection.

Since Windows merges Advanced Audit Policy Configuration settings defined by GPOs, different GPOs can define different settings.

However, at each setting level, it only uses the GPO-defined value with the higher precedence. For example, Tenable.ad needs the Success and Failure value for the Audit Credential Validation setting. However, if a GPO with higher precedence only defines Success for Audit Credential Validation, then Windows only collects Success events and Tenable.ad misses the required Failure events.

To check for GPO precedence:

1. In the command line interface, run the following command on a domain controller.

   It outputs the effective Advanced Audit Policy Configuration after considering all GPOs and precedence.

   ```
   auditpol.exe /get /category:*
   ```

2. Compare the output with the Tenable.ad advanced audit policy requirements. For each setting that Tenable.ad requires, check that the effective policy also covers it.

   - It is not an issue if the effective policy is more exhaustive, such as when Tenable.ad needs "Success" or "Failure" and the setting is "Success and Failure".
   - If the effective policy is insufficient, it means that a GPO with a higher precedence defines conflicting settings.

To fix the GPO precedence:
1. Look for GPOs linked to higher levels (domain or site) in "enforced" mode that define the Advanced Audit Policy Configuration.

2. In the command line interface, run the following command on a domain controller to pinpoint the winning GPO:

   ```
   gpresult /scope:computer /h gpo.html
   ```

3. Modify the corresponding Advanced Audit Policy Configuration setting in the GPO to meet Tenable.ad's minimum requirements. For example:
   - If Tenable.ad requires "Success" and the higher priority GPO defines "Failure," then modify the setting to "Success and Failure."
   - If Tenable.ad requires "Success and Failure" and the higher priority GPO defines "Success," then modify the setting to "Success and Failure."

4. After you modify the setting, you can either wait for the updated GPO to apply or force it with the `gpupdate` command.

5. Repeat the procedure `To check for GPO precedence:` to check the new effective policy.
Manage Tenable.ad

Using its web portal, Tenable.ad 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.ad can also forward its security monitoring flows to other services such as internal application logs for further correlation.

Alerts and Notifications

Tenable.ad 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.ad raises notifications to inform security teams to take immediate action.

Tenable.ad 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.ad with credentials for a user account with permissions to send emails to the selected SMTP server. This can be the same user account as the one you use to connect to your Active Directory.

The following is a generic email template for a security incident detected by Tenable:
Tenable REST v3 API

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

Tenable.ad 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.ad API Reference Portal.
Connect to an Event Log Collector

You can configure Tenable.ad to send notifications, such as alerts or security offenses, to an event log collector. Tenable.ad 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.ad uses the Syslog protocol to carry messages in LEEF format.

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

- IBM QRadar
- Splunk
- RSA Netwitness
- LogRhythm
- Micro Focus ArcSight
- Tibco Loglogic
- McAfee Enterprise Security Manager
Scale Tenable.ad Services

**Required User Role:** Administrator on the local machine

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

**Cancri**

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.
   ```

   ```powershell
   [Environment]::SetEnvironmentVariable("ALSID_CASSIOPEIA_CANCRI_Application__MaxConcurrentPublishToEridanis", "IntegerValue", "Machine")
   ```

3. Restart Cancri:

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

   **Example:**

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

**Caroli**

Caroli's scaling up mechanism is fully automated.

To scale Caroli:
1. Open a PowerShell (x64) terminal.

2. Define the environment variable ALSID_CASSIOPEIA_CAROLI_Application__SpeedCoefficient:

   ```powershell
   [Environment]::SetEnvironmentVariable("ALSID_CASSIOPEIA_CAROLI_Application__SpeedCoefficient", "IntegerValue", "Machine")
   ```

   **Note:** The default value is 100.

3. Restart Caroli:

   ```powershell
   Restart-Service -Name Alsid_Caroli
   ```

   **Example**

   ```powershell
   [Environment]::SetEnvironmentVariable("ALSID_CASSIOPEIA_CAROLI_Application__SpeedCoefficient", "200", "Machine")
   ```

---

**Eridanis**

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):

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

3. Restart Eridanis:

   ```powershell
   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
```
Internet Information Services (IIS) Certificate

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

The certificate name is the same as the webAppHostName.

Often, this name is the IP address of the SEN server where the Web Server (IIS) role runs.

For example, if the IP address of the SEN server is 10.0.48.55, you can log in to the Tenable.ad Web application at https://10.0.48.55 after installation.

For more information, see:

- View the IIS Certificate
- Change the IIS Certificate
View the IIS Certificate

The Tenable.ad 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.

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.

---

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

1. Install your certificate in IIS.
2. Edit site binding to use your installed certificate.

To install the IIS certificate:

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

To change the IIS certificate:

1. Navigate to the "Edit Site Binding" window.
2. From the drop-down list of SSL certificates, select the certificate you just installed.
3. Click OK.
4. Right-click on the website in the Connections panel and select Manage Website > Restart for the new certificate to take effect.
Upgrade Tenable.ad

Before you upgrade, Tenable strongly recommends that you perform a backup of your databases, as described in Back Up and Restore the Storage Manager.

To upgrade Tenable.ad, proceed in the following order:

1. Upgrade the Directory Listener
2. Upgrade Security Engine Nodes
3. Upgrade the Storage Manager

**Note:** During the upgrade, the Tenable.ad installer asks you to choose a TLS installation type. For more information, see Available TLS Installations.

For more information about how to upgrade Indicators of Attack, see:

- Upgrade Indicator of Attack Module
Back Up and Restore the Storage Manager

**Required User Role:** Administrator on the local machine

Tenable strongly recommends that you back up the Storage Manager before you upgrade Tenable.ad.

**MSSQL**

For instructions on how to back up or restore MSSQL, see the official Microsoft documentation.

**InfluxDB**

You can back up and restore InfluxDB remotely and locally.

To back up InfluxDB remotely:

1. Open a PowerShell (x64) terminal as an administrator.
2. Browse to the folder `C:\Tenable\Tenable.ad\StorageManager\AfadInfluxDB\InfluxDB`.
3. In the command line interface, run the following command to back up InfluxDB remotely. Replace the value inside the brackets with the real expected value:

   ```bash
   influxd backup -portable -host <host:port> <path-to-backup>
   ```

To back up InfluxDB locally:

1. Open a PowerShell (x64) terminal as an administrator.
2. Browse to the folder `C:\Tenable\Tenable.ad\StorageManager\AfadInfluxDB\InfluxDB`.
3. In the command line interface, run the following command to back up InfluxDB locally. Replace the value inside the brackets with the real expected value:

   ```bash
   influxd backup -portable <path-to-backup-files>
   ```

**Note:** The backup is a folder, not a file. See the InfluxDB documentation for details: https://docs.influxdata.com/influxdb/v1.7/administration/backup_and_restore/
To restore InfluxDB remotely:

1. Open a PowerShell (x64) terminal as an administrator.
2. Browse to the folder C:\Tenable\Tenable.ad\StorageManager\AfadInfluxDB\InfluxDB.
3. In the command line interface, run the following command to restore InfluxDB remotely. Replace the value inside the brackets with the real expected value:

   ```
   influxd restore -portable -host <host:port> <path-to-backup-files>
   ```

To restore InfluxDB locally:

1. Open a PowerShell (x64) terminal as an administrator.
2. Browse to the folder C:\Tenable\Tenable.ad\StorageManager\AfadInfluxDB\InfluxDB.
3. In the command line interface, run the following command to restore InfluxDB locally. Replace the value inside the brackets with the real expected value:

   ```
   influxd restore -portable <path-to-backup-files>
   ```
Upgrade the Directory Listener

**Required User Role:** Administrator on the local machine

The first Tenable.ad component to upgrade is the Directory Listener. This process upgrades the Tenable component **Ceti**.

**Note:** During the upgrade, the Tenable.ad installer asks you to choose a TLS installation type. For more information, see **Available TLS Installations**.

**Caution:** Tenable strongly advises you to make a backup of your databases and/or make a snapshot of your environment prior to the update procedure.

To upgrade the Directory Listener with default TLS:

1. Run `Tenable.ad_v3.11.x.exe`.
   
   The **Setup Wizard** appears.

2. Click **Next**.
   
   The **Custom Setup** window appears.

3. The installation program automatically preselects the features and location based on the previous installation. Check that the **Directory Listener** is selected.

4. Click **Next**.

5. The installation program automatically fills in the Storage Manager’s IP address in the **MSSQL** and **InfluxDB** boxes. Check that this information is still valid.

6. Click **Next**.
   
   The **Security Engine Node** window appears.

7. The installation program automatically fills in the RabbitMQ’s IP address based on the previous installation. Check that this information is still valid.
8. Click Next to upgrade Tenable.ad.

9. Click Finish.

A dialog box asks you to restart your machine.

10. Click No.

**Caution**: Do NOT reboot the server now.

To upgrade the Directory Listener with default TLS using the "Expert Mode":

1. On the local machine, run the installation file Tenable.ad_v3.11.x.exe.

   The Setup Wizard appears.

2. Select the Expert Mode check box.

3. Click Next.

   The Custom Setup window appears.

4. The installation program automatically preselects the features and location based on the previous installation. Check that the Directory Listener is selected.

5. Click Next.

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

![Image of TLS options](image)

7. Click **Next**.

The **Security Engine Node** window appears.

8. In the **IP** box for RabbitMQ, type the address of the Security Engine Node hosting RabbitMQ.

![Image of Security Engine Node window](image)

9. Click **Next**.

The **Directory Listener** window appears.

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

   The **Ready to Install** window appears.

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

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

13. Click **Finish**.

   A dialog box asks you to restart your machine.

14. Click **No**.

   **Caution**: Do NOT reboot the server now.

To upgrade the Directory Listener with custom TLS and without peer verification:

1. On the local machine, run the installation file `Tenable.ad_v3.11.x.exe`.

   The **Setup Wizard** appears.

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

3. Click **Next**.

   The **Custom Setup** window appears.

4. The installation program automatically preselects the features and location based on the previous installation. Check that the **Directory Listener** is selected.
5. Click **Next**.
   
   The **TLS Options** window appears.

6. Select the **TLS with custom certificates without peer verification** option.

![TLS Options window](image)

7. Click **Next**.
   
   The **TLS certificates** window appears.

![TLS certificates window](image)

8. Nothing is required in this screen. Click **Next**.
   
   The **Security Engine Node** window appears.
9. In the **IP** box for RabbitMQ, type the address of the Security Engine Node hosting RabbitMQ.

![Tenable.ad Setup](image)

10. Click **Next**.

    The **Directory Listener** window appears.

11. 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](image)

12. Click **Next**.

    The **Ready to Install** window appears.

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

    After the upgrade completes, the **Completing the Tenable.ad 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.

To upgrade the Directory Listener with custom TLS and peer verification:

1. On the local machine, run the installation file `Tenable.ad_v3.11.x.exe`.
   
   The **Setup Wizard** appears.

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

3. Click **Next**.
   
   The **Custom Setup** window appears.

4. The installation program automatically preselects the features and location based on the previous installation. Check that the **Directory Listener** is selected.

5. Click **Next**.
   
   The **TLS Options** window appears.

6. Select the **TLS with custom certificates with peer validation** option.
7. Click **Next**.

The **TLS certificates** window appears.

8. In the **CA Cert File** box, click ... to browse to your CA certificate file.

9. Click **Next**.

10. The **Security Engine Node** window appears.

11. In the **IP** box for RabbitMQ, type the address of the Security Engine Node hosting RabbitMQ.

12. Click **Next**.

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

![](image)

14. Click **Next**.

   The **Ready to Install** window appears.

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

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

16. Click **Finish**.

   A dialog box asks you to restart your machine.

17. Click **No**.

   **Caution**: Do NOT reboot the server now.

---

**To install the Directory Listener with no TLS:**

1. On the local machine, run the installation file `Tenable.ad_v3.11.x.exe`.

   The **Setup Wizard** appears.

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

3. Click **Next**.

   The **Custom Setup** window appears.
4. The installation program automatically preselects the features and location based on the previous installation. Check that the Directory Listener is selected.

5. Click Next.

The TLS Options window appears.

6. Select the No TLS option.

7. Click Next.

The Security Engine Node window appears.

8. In the IP box for RabbitMQ, type the address of the Security Engine Node hosting RabbitMQ.
9. Click **Next**.

The **Ready to Install** window appears.

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

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

11. Click **Finish**.

A dialog box asks you to restart your machine.

12. Click **No**.

**Caution**: Do NOT reboot the server now.

**What to do next**

- [Upgrade Security Engine Nodes](#)
- [Upgrade the Storage Manager](#)
Upgrade Security Engine Nodes

Required User Role: Administrator on the local machine

The standard architecture for the Tenable.ad on-premises solution comprises three virtual machines (VMs) by default.

However, you can split the Security Engine Nodes (SEN) into multiple machines to improve performance on large infrastructures.

Note: During the upgrade, the Tenable.ad installer asks you to choose a TLS installation type. For more information, see Available TLS Installations.

Before you start

You must first upgrade the Directory Listener, as described in Upgrade the Directory Listener.

Caution: Tenable strongly advises you to make a backup of your databases and/or make a snapshot of your environment prior to the update procedure.

The installation process upgrades the following Tenable components:

- Cancri
- Ceti-Bridge
- Enif
- Kapteyn
- Caroli
- Cygni
- Equuleus
- IIS
- Cephei
- Electra
To upgrade the SEN with default TLS on one machine:

1. Run Tenable.ad_v3.11.x.exe.

   The **Setup Wizard** appears.

2. Click **Next**.

   The **Custom Setup** window appears.

3. The installation program automatically preselects the features and location based on the previous installation. Check that the **Security Engine Node** is selected.

4. Click **Next**.

   The **Storage Manager** window appears.

5. The installation program automatically fills in the Storage Manager’s IP address in the MSSQL and InfluxDB boxes. Check that this information is still valid.

   ![Storage Manager Window](image)

6. Click **Next**.

   The **Security Engine Node** window appears.
7. Click **Next**.

   The **Ready to Install** window appears.

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

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

9. Click **Finish**.

   A dialog box asks you to restart your machine.

10. Click **No**.

    **Caution**: Do NOT reboot the server now.

To upgrade the SEN with default TLS using the "Expert Mode" on one machine:

1. On the local machine, run the installation file *Tenable.ad_v3.11.x.exe*.

   The **Setup Wizard** appears.

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

3. Click **Next**.

   The **Custom Setup** window appears.

4. The installation program automatically preselects the features and location based on the previous installation. Check that the **Security Engine Node** is selected.
5. Click **Next**.

The **TLS Options** window appears.

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

7. Click **Next**.

The **Storage Manager** window appears.

8. Provide the following information:

   - In the **MSSQL** box, type the IP address of the Storage Manager.
   - In the **InfluxDB** 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.

9. Click **Next**.

The **Security Engine Node** window appears.

10. 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.ad.

11. Click **Next**.

The **Ready to Install** window appears.

**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 **Install** to begin the upgrade.

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

13. Click **Finish**.

A dialog box asks you to restart your machine.

14. Click **No**.

**Caution:** Do NOT reboot the server now.

To upgrade the SEN with custom TLS and without peer verification on one machine:

1. On the local machine, run the installation file `Tenable.ad_v3.11.x.exe`.

   The **Setup Wizard** appears.

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

3. Click **Next**.

   The **Custom Setup** window appears.

4. The installation program automatically preselects the features and location based on the previous installation. Check that the **Security Engine Node** is selected.

5. Click **Next**.

   The **TLS Options** window appears.

6. Select the **TLS with custom certificates without peer verification** option.
7. Click Next.

The TLS certificates window appears.

8. 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.

9. In the CA Cert File box, click ... to browse to your CA certificate file.

10. Click Next.

The Storage Manager window appears.

11. Provide the following information:
- In the **MSSQL** box, type the IP address of the Storage Manager.
- In the **InfluxDB** 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.

12. Click **Next**.

The **Security Engine Node** window appears.

13. 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.ad.
14. Click **Next**.

The **Ready to Install** window appears.

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

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

16. Click **Finish**.

A dialog box asks you to restart your machine.

17. Click **No**.

**Caution:** Do NOT reboot the server now.

To upgrade the SEN with custom TLS and peer verification on one machine:

1. On the local machine, run the installation file `Tenable.ad_v3.11.x.exe`.

   The **Setup Wizard** appears.

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

3. Click **Next**.

   The **Custom Setup** window appears.

4. The installation program automatically preselects the features and location based on the previous installation. Check that the **Security Engine Node** is selected.

5. Click **Next**.

   The **TLS Options** window appears.

6. Select the **TLS with custom certificates with peer validation** option.
7. Click **Next**.

The **TLS certificates** window appears.

8. 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.

9. In the **CA Cert File** box, click ... to browse to your CA certificate file.

10. Click **Next**.

    The **Storage Manager** window appears.

11. Provide the following information:
12. Click **Next**.

The **Security Engine Node** window appears.

13. 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.ad.
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.

14. Click Next.

    The Ready to Install window appears.

15. Click Install to begin the upgrade.

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

16. Click Finish.

    A dialog box asks you to restart your machine.

17. Click No.

Caution: Do NOT reboot the server now.

To upgrade the SEN with no TLS on one machine:

1. On the local machine, run the installation file Tenable.ad_v3.11.x.exe.

    The Setup Wizard appears.

2. Select the Expert Mode check box.

3. Click Next.

    The Custom Setup window appears.

4. The installation program automatically preselects the features and location based on the previous installation. Check that the Security Engine Node is selected.

5. Click Next.

    The TLS Options window appears.

6. Select the No TLS option.
7. Click **Next**.

   The **Storage Manager** window appears.

8. Provide the following information:
   
   a. In the **MSSQL** box, type the IP address of the Storage Manager.
   
   b. In the **InfluxDB** box, type the IP address of the Storage Manager.
   
   c. In the **Password** box, type the service account password for the MSSQL database defined in the Storage Manager installation.
   
9. Click **Next**.

   The **Security Engine Node** window appears.
10. 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.ad.

![Tenable.ad Setup](image)

**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](#).

11. Click **Next**.

The **Ready to Install** window appears.

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

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

13. Click **Finish**.

A dialog box asks you to restart your machine.

14. Click **No**.

**Caution:** Do NOT reboot the server now.

To upgrade the SEN on **multiple** virtual machines:

- **Perform the update procedure as for one machine, in the following order** on each machine running these services:
1. Cygni
2. Cancri
3. Caroli
4. Others (Eridanis, Kapteyn, etc.)
5. RabbitMQ

What to do next

- Upgrade the Storage Manager
Upgrade the Storage Manager

**Required User Role:** Administrator on the local machine

The Storage Manager is the last component that you upgrade, after you upgrade the Directory Listener and the Security Engine Node.

**Note:** During the upgrade, the Tenable.ad installer asks you to choose a TLS installation type. For more information, see Available TLS Installations.

**Before you start**

Upgrade Tenable.ad components in the following order:

1. Upgrade the Directory Listener
2. Upgrade Security Engine Nodes

**Caution:** Tenable strongly advises you to make a backup of the Storage Manager and/or make a snapshot of your environment before you upgrade.

To upgrade the Storage Manager with default TLS:

1. On the local machine, run the installation file Tenable.ad_v3.11.x.exe.
   
   The **Setup Wizard** appears.

2. Click **Next**.
   
   The **Custom Setup** window appears.

3. The installation program automatically preselects the features and location based on the previous installation. Check that the Storage Manager feature is selected.

4. Click **Next**.
   
   The **Storage Manager** window appears.

5. The installation program automatically fills in the Storage Manager’s IP address in the **MSSQL** and **InfluxDB** boxes. Check that this information is still valid.
Note: Tenable strongly recommends that you keep the default TENABLE instance name.

6. Click **Next**.

The **Ready to Install** window appears.

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

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

8. Click **Finish**.

A dialog box asks you to restart your machine.

9. Click **No**.

**Caution:** Do NOT reboot the server now.

To upgrade the Storage Manager with default TLS using the "Expert Mode":

1. On the local machine, run the installation file **Tenable.ad_v3.11.x.exe**.

   The **Setup Wizard** appears.

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

3. Click **Next**.

   The **Custom Setup** window appears.
4. The installation program automatically preselects the features and location based on the previous installation. Check that the Storage Manager feature is selected.

5. Click **Next**.

   The **TLS Options** window appears.

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

7. Click **Next**.

   The **Storage Manager** window appears.

8. The installation program automatically fills in the Storage Manager’s IP address in the **MSSQL** and **InfluxDB** boxes based on the previous installation. Check that this information is still valid.
9. Click **Next**.

   The **Ready to Install** window appears.

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

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

11. Click **Finish**.

   A dialog box asks you to restart your machine.

12. Click **No**.

**Caution:** Do NOT reboot the server now.

To upgrade the Storage Manager with custom TLS and without peer verification:

1. On the local machine, run the installation file `Tenable.ad_v3.11.x.exe`.

   The **Setup Wizard** appears.

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

3. Click **Next**.

   The **Custom Setup** window appears.

4. The installation program automatically preselects the features and location based on the previous installation. Check that the Storage Manager feature is selected.

5. Click **Next**.

   The **TLS Options** window appears.

6. Select the **TLS with custom certificates without peer verification** option.
7. Click **Next**.

   The **TLS certificates** window appears.

8. 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.

9. Click **Next**.

   The **Storage Manager** window appears.
10. In the **Password** box, type a password for the MSSQL database.

![Password box screenshot](image)

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

11. Click **Next**.

   The **Ready to Install** window appears.

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

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

13. Click **Finish**.

   A dialog box asks you to restart your machine.

14. Click **No**.

   **Caution:** Do NOT reboot the server now.

To upgrade the Storage Manager with custom TLS and peer verification:

1. On the local machine, run the installation file `Tenable.ad_v3.11.x.exe`.

   The **Setup Wizard** appears.

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

   The **Custom Setup** window appears.

4. The installation program automatically preselects the features and location based on the previous installation. Check that the Storage Manager feature is selected.

5. Click **Next**.

   The **TLS Options** window appears.

6. Select the **TLS with custom certificates with peer validation** option.

![TLS Options window](image)

7. Click **Next**.

   The **TLS certificates** window appears.

8. Provide the following information:
9. Click **Next**.

The **Storage Manager** window appears.

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

   ![Storage Manager](image)

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

11. Click **Next**.

   The **Ready to Install** window appears.
12. Click **Install** to begin the upgrade.

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

13. Click **Finish**.

   A dialog box asks you to restart your machine.

14. Click **No**.

   **Caution:** Do NOT reboot the server now.

To upgrade the Storage Manager with no TLS:

1. On the local machine, run the installation file `Tenable.ad_v3.11.x.exe`.

   The **Setup Wizard** appears.

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

3. Click **Next**.

   The **Custom Setup** window appears.

4. The installation program automatically preselects the features and location based on the previous installation. Check that the Storage Manager feature is selected.

5. Click **Next**.

   The **TLS Options** window appears.

6. Select the **No TLS** option.
7. Click **Next**.

The **Storage Manager** window appears.

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

9. Click **Next**.

The **Ready to Install** window appears.

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

After the upgrade completes, the **Completing the Tenable.ad Setup Wizard** window appears.
11. Click Finish.

A dialog box asks you to restart your machine.

12. Click No.

Caution: Do NOT reboot the server now.

What to do next

- Restart Services
Restart Services

After you finish upgrading the Tenable.ad components Storage Manager, Security Engine Node, and Directory Listener, you can restart the services.

Security Engine Node

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

To restart the SEN machine:

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

Directory Listener

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

To restart Directory Listener services:

- At the prompt from the installation program, click Yes.
Upgrade Indicator of Attack Module

**Required Role:** Administrator on the local machine.

Before you upgrade the indicator of attack (IoA) module on domain controllers, you must first uninstall it as described in [Uninstall the Indicators of Attack Module](#).

To upgrade the IoA module:

1. After you uninstall, wait a few hours for the cleaning GPO to replicate and apply properly on all domain controllers.

   **Note:** The script enforces a 4-hour delay.

2. Delete the cleaning GPO.

3. Download and install the new version of the IoA module as described in [Install Indicators of Attack](#).
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.ad Release Notes for more information.
- You can access them on Tenable Downloads site.

To update Tenable.ad, deploy the update installation packages on each Windows Server machine. For more information about the update process, see Update.

Maintenance and Support Services

To keep servers in good security conditions the Tenable.ad platform requires access to the following support services. For more information about the required network flows, see Network Flow Matrix.

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

<table>
<thead>
<tr>
<th>Service Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update management infrastructure</td>
<td>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.</td>
</tr>
<tr>
<td>Time Server</td>
<td>Your company's time server (e.g., NTP server). This service synchronizes Tenable.ad’s platform internal clock to your reference time. Time synchronization offers consistent security monitoring.</td>
</tr>
<tr>
<td>Identity provider</td>
<td>Your identity and access provider. This service activates SAML, LDAP, or OAUTH authentication to Tenable.ad’s web services (portal, API, etc.).</td>
</tr>
</tbody>
</table>
Uninstall Tenable.ad

See the following sections:

- [Uninstall Tenable.ad](#)
- [Uninstall the Indicators of Attack Module](#)
- [Uninstall Sysmon](#)
Uninstall Tenable.ad

**Required User Role:** Administrator on the local machine

The uninstallation process removes all Tenable.ad components.

To uninstall Tenable.ad:

1. In Windows, go to **Control Panel > Programs > Programs and Features**.
2. Select Tenable.ad.
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.
Uninstall the Indicators of Attack Module

Required Role: Administrator on the local machine.

To uninstall the Indicators of Attack (IoA) module, you run a command that creates a new Group Policy Object (GPO) called Tenable.ad cleaning.

The uninstallation process uses this new GPO by default to clean out previously installed GPOs as well as its SYSVOL files, the registry setting, the advanced logging policy, and the WMI filters.

Note: If you changed the initial GPO's name, you must pass it to the uninstaller so that it knows which GPO to uninstall.

To uninstall the IoA module:

1. In the command line interface, run the following command to uninstall the IoA module:

```
Register-TenableIOA.ps1 -Uninstall
```

2. Replicate this new GPO over the entire domain.

3. Wait for the GPO refresh interval to pass for the entire uninstallation process to complete.

   Tenable recommends letting this cleaning GPO run for a week and then manually remove it.
Uninstall Sysmon

To uninstall Sysmon:

1. Open a PowerShell terminal.
2. Browse to the folder that contains Sysmon64.exe.
3. Type the following command:
   
   ```ps
c:\> .\Sysmon64.exe -u
   ```

To delete the registry key:

- In the command line interface, type the following command on all machines running Sysmon:

   ```reg delete "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Microsoft-Windows-Sysmon\Operational"
   ```

For more information, see Install Microsoft Sysmon.