# Tenable Patch Management Installation Guide

Last Revised: December 20, 2024

# Table of Contents

# About Adaptiva Components

Since Tenable Patch Management is powered by Adaptiva, this documentation references Adaptiva components. These include databases, binaries, and directories. Tenable's collaboration with Adaptiva brings advanced patch management to customers, ensuring you benefit from the combined expertise of both companies.

# Prerequisites

Before installing the Tenable Server, review the following details, complete the configuration requirements, and record information for use during the installation process.

Follow the sequence of prerequisites in the order presented.

# Accounts and Permissions

The Tenable Server installation requires an installation account with local administrator permissions on the chosen server. The installation creates a local service named AdaptivaServer, which runs under the Local System account by default.

If you use SQL Server Standard Edition or SQL Server Enterprise Edition, the installation account must also have sysadmin permissions on the SQL Server that hosts the database (see Choosing the SQL Server Edition after you finish setting up permissions, exclusion, and so on).

You may change this permission after the installation. In addition, you may also change the service account from local system to a specified service account after installation.

| Server | Account | Permissions |
|---|---|---|
| Tenable Server | Installation account<br><br>Optional Service account<br><br>Reporting Account | Domain (recommended) or Local account add to Local Administrators group<br><br>If used, the account must be granted the Log On As A Service User right.<br><br>Domain (recommended) or Local account |
| SQL Server hosting the Adaptiva Database | Tenable Server SYSTEM Account<br><br>Installation Account | Prior to installation of the Tenable Server, grant `sysadmin` permission to the Tenable Server SYSTEM account (see Set System Account Permission in SQL Management Studio). After completing the Tenable Server installation, you may reduce these permissions for day-to-day operations if necessary. |

| Server | Account | Permissions |
|---|---|---|
| | Option Service Account | SQL Server Role Sysadmin (installation account for initial installation)<br><br>Minimum permissions (after installation) Adaptiva Database Security User Mapping (account running the AdaptivaServer service)<br><br>db_datareader<br><br>db_datawriter<br><br>db_ddladmin<br><br>db_executer |
| Content Library | <domain>\ Tenable Server $ or<br><br>Optional Service Account | If you choose to relocate the Adaptiva Content Library to a remote drive/share, you must modify the Tenable Server service account to allow permission for this location. |
| Adaptiva Database | Reporting Account | Server Setup automatically grants db_datareader permissions |

## Set System Account Permissions in SQL Management Studio

Before installing the Tenable Server, you must grant `sysadmin` SQL permission to the Tenable Server SYSTEM account.

1. Open SQL Server Management Studio, and then connect to the target database server.
2. Expand the **Security** folder.
3. Right-click the **Logins** folder, and then select **New Login...**.
4. Select **Search...**, and then verify that the **Location** shows the **domain**.
5. Enter the new login details:
    a. Enter the **username** of the account you will use to perform the Tenable Server installation.
    b. Select **Check Names**, and then select **OK**.

c. Select the **Server Roles** page, and then select `sysadmin` to add a check mark.

d. Click **OK** to add the login information.

6. Complete changes on the Tenable Server SYSTEM account using the following syntax:

   `domain\servername$`

# Firewall and Communication Ports

As a network application, Tenable Vulnerability Manager facilitates activity between servers and clients, which requires access using specific ports. For a list of all the required ports, see Communication Port and Flow Diagrams.

Exclude all required ports from any network filtering or intervening network security devices to prevent a disruption in network communication. Tenable Server installation automatically creates Windows Firewall rules for ports in the currently connected profile during the Tenable Server installation. If customized ports use the following options, you must manually configure these ports as rules or exceptions in the firewall to enable the necessary communication:

- Tenable Server
- Tenable Client
- Tenable Workbench
- Other firewalls
- Security software between the server

# Antivirus Exceptions

Tenable Patch Management acquires content directly from the Adaptiva Content Library on the Tenable Server and from the `AdaptivaCache` folder on individual devices.

Because antivirus scanning of these files can cause performance degradation, Tenable recommends excluding Tenable folders from antivirus scans. Tenable uses a secure hash to protect all distributed content against tampering or corruption, either in transit or when stored.

## Excluding Adaptiva Folders and Processes

There are two types of exclusions:

- **Folders:** Excludes Parent folders, including sub-folders.
- **Process:** Excludes processes. For use when aggressive antivirus programs identify `.exe` processes as high-risk.

### *Creating Antivirus Folder Exclusions*

Exclude the folders listed in the server and client exclusion tables below. The tables list the parent folders only. Make sure to exclude all sub folders.

| **Adaptiva Server Exclusion Description** | **Exclusion Type** | **Exclusion** |
|---|---|---|
| Server Installation Folder | Folder | <path>\Tenable \AdaptivaServer |
| Adaptiva Content Library (if different from the default location) | Folder | The location of the Adaptiva Content Library depends on the installation path chosen during the Tenable Server installation. |
| Client Installation Folder | Folder | <path>\Tenable\AdaptivaClient |

| **Adaptiva Client Exclusion Description** | **Exclusion Type** | **Exclusion** |
|---|---|---|
| Client Installation Folder | Folder | *<path>*\Tenable\AdaptivaClient |
| Content Cache | Folder | \ AdaptivaCache (exists at the root of every fixed logical drive by default) |

### *Creating Antivirus Process Exclusions*

In some cases, administrators prefer to exclude processes rather than folders, particularly when aggressive antivirus programs consider the executables to be a high-risk process.

| **Server Process Exclusion Description** | **Process Exclusion** |
|---|---|
| Server Service | *<path>*\Tenable\AdaptivaServer\bin\AdaptivaServerService.exe<br>*<path>*\Tenable\AdaptivaServer\cloud-ui\node-adaptiva.exe<br>*<path>*\Tenable\AdaptivaServer\cloud-ui\nginx-adaptiva.exe |
| Client Service | *<path>*\Tenable\AdaptivaClient\bin\AdaptivaAIT.exe<br>*<path>*\Tenable\AdaptivaClient\bin\AdaptivaClientService.exe<br>*<path>*\Tenable\AdaptivaClient\bin\AdaptivaUserPortal.exe |

| Server Process Exclusion Description | Process Exclusion |
|---|---|
| | *<path>*\Tenable\AdaptivaClient\bin\OneSiteClient64.exe |

| Client Process Exclusion Description | Process Exclusion |
|---|---|
| Client Service | *<path>*\Tenable\AdaptivaClient\bin\AdaptivaAIT.exe<br>*<path>*\Tenable\AdaptivaClient\bin\AdaptivaClientService.exe<br>*<path>*\Tenable\AdaptivaClient\bin\AdaptivaUserPortal.exe<br>*<path>*\Tenable\AdaptivaClient\bin\OneSiteClient.exe<br>*<path>*\Tenable\AdaptivaClient\bin\OneSiteClient64.exe<br>*<path>*\Tenable AdaptivaClient\bin\amd64\OneSiteDownloader.exe |

*ConfigMgr Process Exclusion*

| ConfigMgr Process Description | Process Exclusion |
|---|---|
| Client Exclusions | `%windir%\CCM\CCMExec.exe`<br>`%windir%\CCM\CMRCService.exe` |

# Internet Access

The Tenable Server requires an internet connection. This is an outbound connection only and uses the TCP ports 80 or 443.

## Internet Access Best Practices

Use the following best practices when connecting the Tenable Server to the Internet:

- Provide Tenable Server access to URLs formatted as `http[s]://*adaptiva.cloud`.
- Use the `HEAD`, `GET`, and `POST` request methods when using proxies.

## Connect to Internet Destinations

The Tenable Server and Internet-based clients must connect to the Internet destinations in the table below.

| Source | Description | Destination | Port |
|---|---|---|---|
| Tenable Internet-based Clients | Adaptiva Services | *.Adaptiva.cloud<br>*.opendns.com | http:// or https:// (TCP port 80, port 443, Internet Control Message Protocol (ICMP), or User Datagram Protocol (UDP) 3478) |
| Tenable Internet-based Clients | Adaptiva Content Delivery Network (CDN) | *.Adaptivacdn.cloud | http:// or https (TCP port 80 or port 443) |
| Tenable Server | Tenable Vulnerability Manager | Cloud.tenable.com | https:// (TCP port 443) |
| Internet-based Clients | Azure storage | *.windows.net | https:// (TCP port 443) |
| Adaptiva Server All Clients | Azure (for Intune) | *.microsoft.com<br>*.windows.net | https:// (TCP port 443) |

# Admin Portal Communication

For the Admin Portal, the Tenable Server installation defaults to using the standard HTTP TCP port 443. The Admin Portal does not require IIS. If there are other services listening on port 443, enter a different port during installation. To find a custom port, run `NETSTAT -nabo` to get a current list of the ports used in your environment.

# Tenable Server Installation Folder

The first user input required for the Tenable Server installation is the installation folder location. The default is C:\Program Files\Tenable\ Tenable Patch Management.

You may choose a custom installation folder location, and Tenable recommends either not installing on the Operating System C:\ drive or moving the Content Library after the installation.

**Important**

Do not install the Server on the Operating System (OS) C: drive. The product log files and the Adaptiva Content Library installed with the Server grow over time, which impacts storage and performance on the OS C: drive.

Consider which folder location you want to use for Tenable Server installation and be prepared to enter this information when you install the Tenable Server .

# Licensing Tenable Products

Tenable Patch Management requires a license for each active client. The license key contains the licensed company name and client count. The Tenable Server periodically counts all active, healthy, reporting clients as licensed clients.

Make sure you have your license key available for the Server installation. You may enter the license key when installing the Server, or enter the license key using the Admin Portal after completing the installation. If you are starting the Admin Portal for the first time or your key has expired, the software prompts you for a license key at login.

# TLS Certificates

The Server installation requires data entry for Transport Layer Security (TLS). When deciding on the type of TLS certificate to use for your Server installation, consider whether your security organization has any requirements for using certificates, such as the following:

- Self-signed certificates versus CA certificates.
- Wildcard certificates versus a certificate specific to a server.
- Key size, Hash algorithm, and expiration length requirements.

In addition, identify all administrators who require access to the Admin Portal and whether they require access from a remote device. after completing the Server installation, install the Server certificate in the certificate store of each remote device that requires secure access to the Admin Portal (see Import the TLS Certificate to the Root Store).

Make note of the TLS certificate option to use so you can enter the information during the installation.

The Tenable Server, installation provides the following TLS security options:

- Add your own TLS certificate, authorized through a CA such as Active Directory Certificate Services or a third-party CA like GoDaddy, DigiCert, Let's Encrypt and so on.
- Use the self-signed TLS certificate that the Tenable Server creates during Server installation. This certificate is 4096 bits, uses SHA-512 hash, and expires in 12 years from the date of creation.

- Use plain HTTP protocol. The Tenable Server, installation allows this option for lab testing only. Tenable does not support this choice on product servers.

## Using a Certificate Authority

Certificate Authorities issue Secure Socket Layer (SSL) certificates as `.pfx` files, which you must convert to `.pem` files for use with the Tenable Server. The two separate `.pem` files required by the Tenable Server include a certificate file and a private key file in `UTF-8` format. You can convert the `.pfx` files to `.pem` with a converter, such as openssl, GitHub, and so on.

## Using a Self-signed Certificate

List the x.500 protocol common and alternate comma-separated names you want to use for the self-signed certificate. These include server FQDNs, DNS aliases, IP addresses, and so on.

## Import the TLS Certificate to the Root Store

After choosing your TLS Certificate option and completing the Server installation, import your TLS Certificate into the Trusted Root Certification Authorities container on the Tenable Server. Each administrator who uses the Admin Portal from a remote device must import the certificate. Alternatively, users may deploy certificates using a Group Policy Object (GPO) or an Intune profile.

To import the certificate, run the following command from a command prompt as an administrator:

```
Certutil.exe -addstore root
"<path>\Tenable\AdaptivaServer\data\security\webui\cert.pem"
```

# HTTP Communication

Tenable Clients use the User Datagram Protocol (UDP) to communicate with the Tenable Server. When Clients are unable to use UDP, such as when the company uses cloud-based VPN products like ZScaler, Microsoft Direct Access, or other Network Address Translation (NAT) scenarios, the Tenable Server installation allows you to configure HTTP Bindings.

The Server installation HTTP Binding settings default to port 80 for both Web UI HTTP Port and for Enable Client HTTP Communications. You must change one of these ports so that they are different. Tenable recommends using port 443 for the Web UI or enter a custom port. You may use 80 for the Client HTTP port, or enter a custom port.

If you use a custom port for the Web UI, the URL to access the Admin Portal must include the custom port. For example, `https://<adaptivaserverfqdn>:<customport>`.

# Adaptiva Database

The Tenable Server requires its own SQL Server database (Adaptiva Database). Depending on the SQL Server Edition you choose, the Server installation wizard may require details for the host SQL database.

Make note of your Edition choice and configuration details such as database name, location, communication port, domain, and read-only login information.

To prepare, choose a host location for the Adaptiva Database, and choose the SQL Server Edition you intend to use.

**Adaptiva Database Host Server**

- **Local server**: This is the server that also hosts the Tenable Server.
- **Remote server**: This is any remote server you choose, including an existing SQL database or a SQL database associated with an integrated third-party product (ConfigMgr or Workspace ONE).

**Adaptiva Database SQL Server Edition**

- SQL Server Express Edition
- SQL Server Standard or Enterprise Edition
- An existing SQL Server instance

# Choosing the SQL Server Edition

The Tenable Server installation wizard requires specific input depending on the SQL Server Edition you choose to use. Make note of your Edition choice and configuration details such as database name, location, communication port, domain, and read-only login information for the database reporting account.

Use the information below to help determine which SQL Server Edition works best in your environment to host the Adaptiva Database. For a full list of the differences between Editions, download the *SQL Server Editions Datasheet* available from the URL below. This link takes you outside of the Adaptiva domain:

https://www.microsoft.com/en-us/sql-server/sql-server-2022-comparison

# SQL Server Express Edition

The Tenable Patch Management installation wizard provides a choice to download and install the free SQL Server Express Edition as part of the Server installation. The SQL Server Express Edition has no licensing requirement.

Downloading and installing the free SQL Server Express Edition from Microsoft requires an Internet connection and specific Internet Settings. See Internet Settings for SQL Server Express Download for details and to make the required changes. In addition, using this version requires enabling Microsoft .NET Framework 3.5 SP1 or downloading and installing Microsoft .NET Framework 4.0.

SQL Server Express Edition has the following conditions:

- No Built-In Scheduled Backups (work around available).
- Maximum Allowed Memory Capacity - 1410MB
- Maximum Database Size – 10GB
- Maximum Number of Cores – 1 socket, up to 8 Cores.
- No High Availability.

For a full list of differences, see https://www.microsoft.com/en-us/sql-server/sql-server-2022-comparison

Although the installer configures all necessary settings, consider the following server installation defaults:

- Installs SQL Server 2022 Express Edition.
- Does not include SQL Server Management Studio.
- Names the SQL Express instance `AdaptivaSQL`.

You may also pre-download `SQLEXPR_x64_ENU.exe` for SQL Server 2022 Express Edition, and then specify the path to that database when requested during installation. To succeed in this case, the file size must match exactly 279,293,816 bytes (version 2022).

# SQL Standard Edition

- Use the SQL Standard Edition when you expect the Tenable estate to support more than 2000 licensed devices.
- Install on the Tenable Server or to a remote location.
- Standard SQL licensing requirements apply. Consult with a Microsoft licensing specialist to ensure you have purchased the proper licenses.
- If you choose this option, see Accounts and Permissions for required settings.

## SQL Enterprise Edition

- SQL Server Standard Edition statements, plus:
- If you use high availability, you must use the SQL Server Enterprise Edition.

## SQL Server Component Requirements

Review the requirements in the table below when deciding which SQL Server Edition to install with the Tenable Server. A SQL Server Always On availability group may also host the Adaptiva database.

Tenable Patch Management requires a Database Compatibility Level of SQL Server 2016 SP2 or newer for SQL Standard and Enterprise versions. Each of the following versions apply to SQL Express, SQL Standard, and SQL Enterprise.

| Component | Requirement |
|---|---|
| SQL Server Version | • **SQL Server 2022**<br>• **SQL Server 2019**<br>• **SQL Server 2017**<br>• **SQL Server 2016 SP2** |
| Database Compatibility Level | Minimum level is SQL 2016 (103). |
| Database Sizing | Minimum database size is 5 GB. Storage allocation per managed device is approximately 2.5MB. Use the following equation to determine your database size requirements:<br>5GB + (2.5MB x licensed clients) = xGB<br>SQL Server Express supports no more than 10GB. |
| Memory | Minimum RAM memory requirement is 64GB. |
| Disk Infrastructure | SSD or NVMe drives for the database files (recommended). |

## Database Reporting Read Only Account

The Adaptiva Database requires a Read-Only SQL Login for reporting purposes. If the login does not exist, the Server installation creates one. If you use Windows Authentication, the Windows account must exist before running the Server installation. In either case, the Tenable Server installation automatically grants the necessary read permissions to the login.

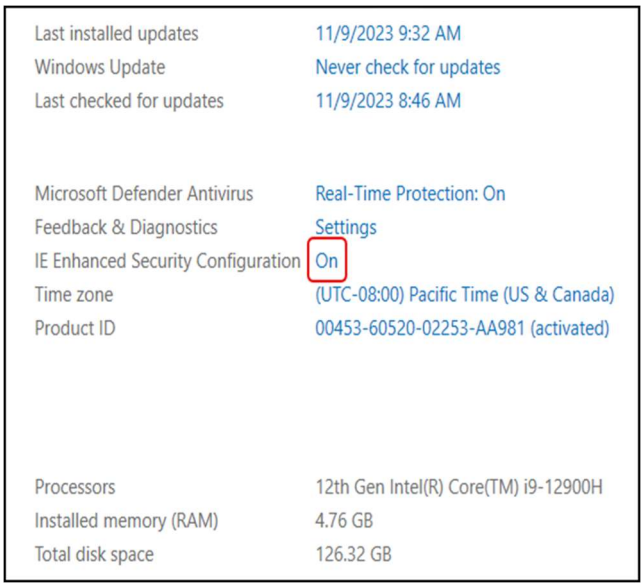
Use the best practices below when creating a Database Reporting account using Windows Authentication. Make note of the Domain Name, User Name, and Password so you are prepared to enter that information during the Server installation.

- Tenable recommends creating this account to operate the Tenable Server at the highest security level for your SQL Server environment.
- Tenable recommends using a domain account for this account. When the SQL Server is remote, the Tenable Server installer requires using domain account.
- All Tenable Server data providers require this account to query the Adaptiva database.

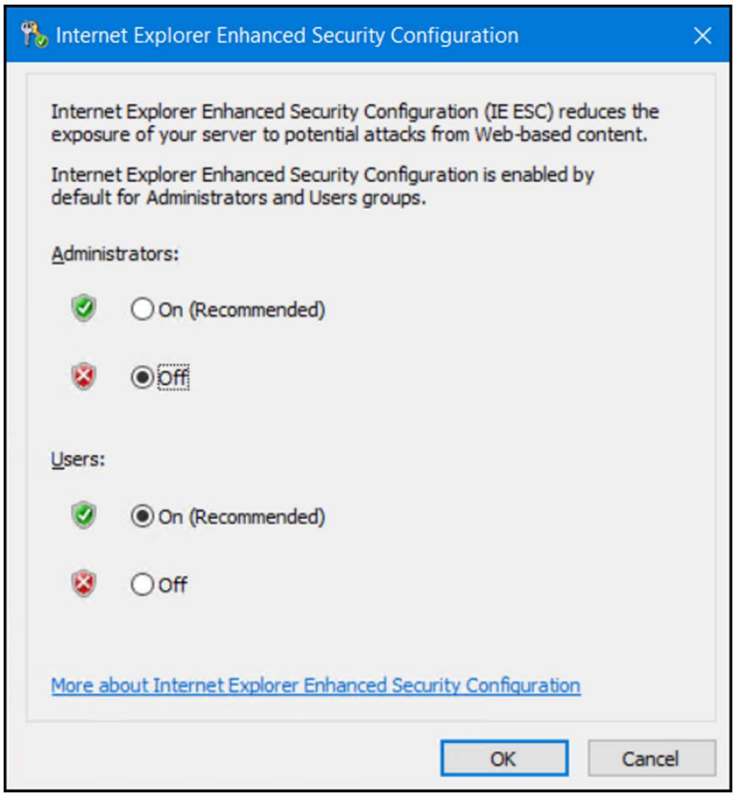
## Internet Settings for SQL Server Express Download

When you choose the SQL Server Express Edition during the Tenable Server installation, the installation wizard automatically downloads and extracts the SQL Server Express media from Microsoft. To ensure a successful download, make the following configuration changes to the Windows Internet settings on the target Server prior to installation.

1. Turn off IE Enhanced Security configuration on the target Tenable Server:
    a. Open **Server Manager**, and then select **Local Server**.
    b. Locate **IE Enhanced Security Configuration** under **Properties** and select the current setting (either On or Off).




    c. Verify that the **Administrators** setting is **Off**, and then click **OK**.




d. Refresh the page to see changes.

2. Configure Internet on the target Tenable Server

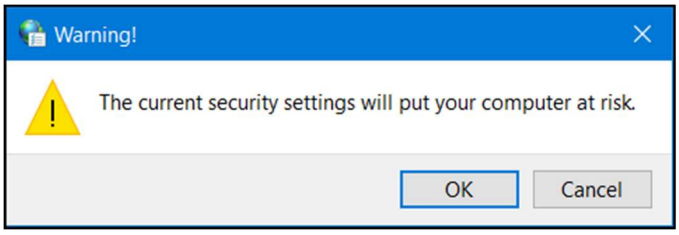
   a. Navigate to **Internet Options** on the Server.

   b. Select the **Security** tab, and then select **Enable Protected Mode** to clear the checkbox.

   c. Select **Internet**, and then select **Custom Level**.

   d. Scroll down to **Downloads**, and then set **File download** to **enabled**.

   e. Click OK to exit the Custom level, and then click OK to exit Internet Properties. The following Warning displays:




   f. Click **OK**. After a successful Server installation with SQL Express Edition, return to these settings and make the necessary changes for security.

# Tenable Platform Installation

Tenable provides the Platform files in a compressed (.zip) file. The compressed file includes an Installers folder and a Tools folder. Platform installation requires two files from the Installer folder:

- TenableServerSetup.exe
- TenableClientSetup.exe

All components require local administrator privileges to install.

# Prepare the Installation Files

Extract the files for installation from the .zip file provided by Tenable, complete the following steps:

1. Download or move the file to the server acting as the Server instance.
2. Right click the file, and then select **Extract All...**.
3. Select **Browse** and navigate to the location on the Server where you want to save the files.

   **Important**

   Do not install the Server on the Operating System (OS) C: drive. The product log files and the Tenable Content Library installed with the Tenable grow over time, which impacts storage and performance on the OS C: drive.
4. Select **Show Extracted Files When Complete**, and then click **Extract**. This extracts the files and displays them in a folder structure.

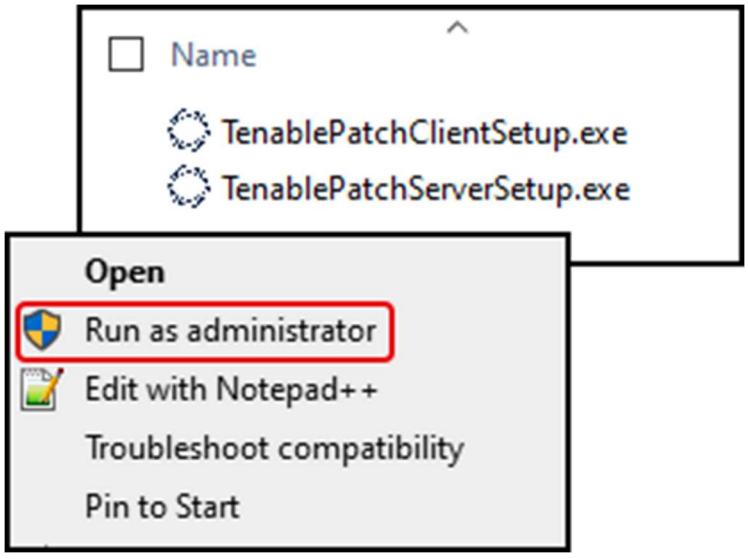

5. Continue to /document/preview/8543#UUID-1c3be5f3-06e7-9f34-fd2b-b623fad75027.

# Launch the Tenable Server Installer

**Important**

Always run the installation files with administrator privileges.

1. Right click the **TenableServerSetup.exe**, and then select **Run as administrator**.



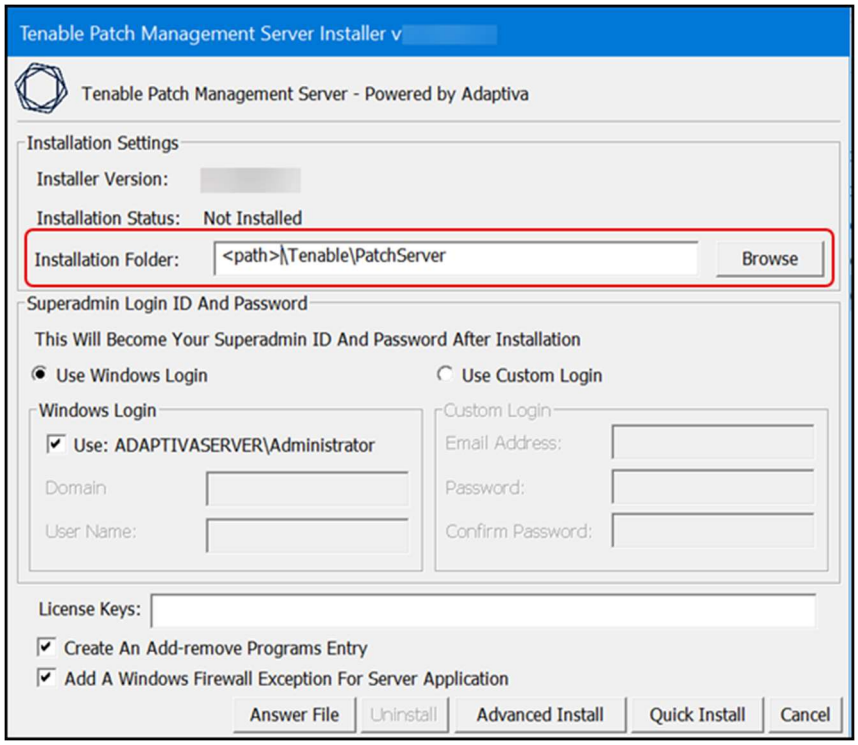

# Configure Tenable Server Installation Settings

After launching the Server installer, configure the installation settings.

**Important**

Do not install the Server on the Operating System (OS) C: drive. The product log files and the Tenable Content Library installed with the Tenable grow over time, which impacts storage and performance on the OS C: drive.

1. Select **Browse** under **Installation Settings** and navigate to the location where you want the AdaptivaServer instance installed. The installer copies files to the default file structure (`Program Files\Tenable\AdaptivaServer`). Tenable recommends using a primary drive designation other than `Operating System (OS) C:`.

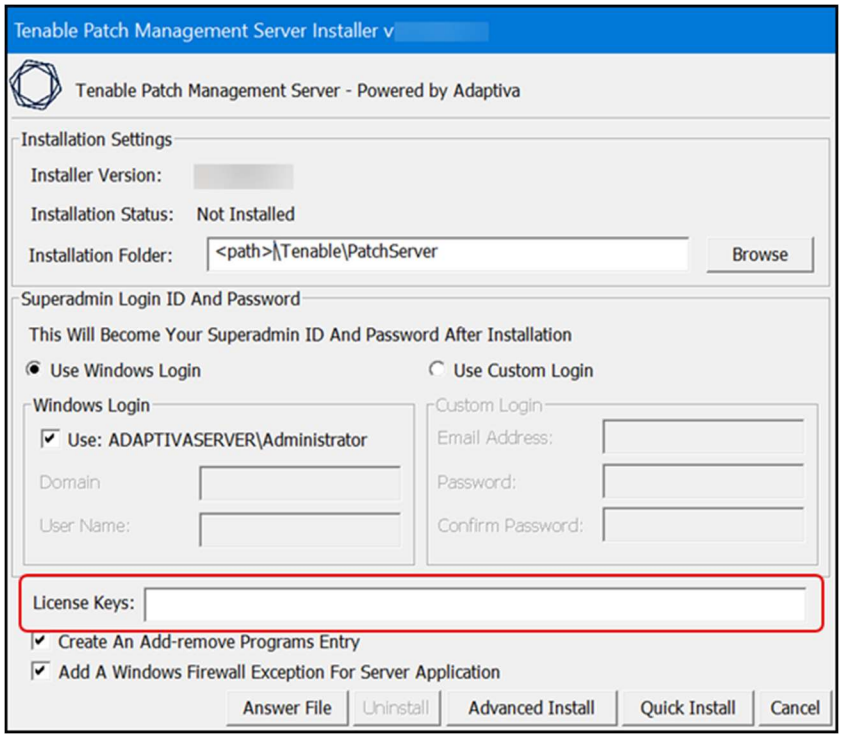



2. Set the **Superadmin Login ID and Password** using one of the following options:

    a. Select **Use Windows Login** to use the same account details you used to log in to the Windows server. The installation adds the domain name and username specified here to the `superadmin` role. (Recommended)

    b. Select **Use Custom Login** and supply a correctly formatted email address (does not need to be real) and password to create an internal login. Tenable recommends this for lab/test environments only.

3. (Optional) Enter the license key for Tenable Patch Management. You may enter the license key here or in the Admin Portal after installation.




4. Review the options below. These categories default enabled:

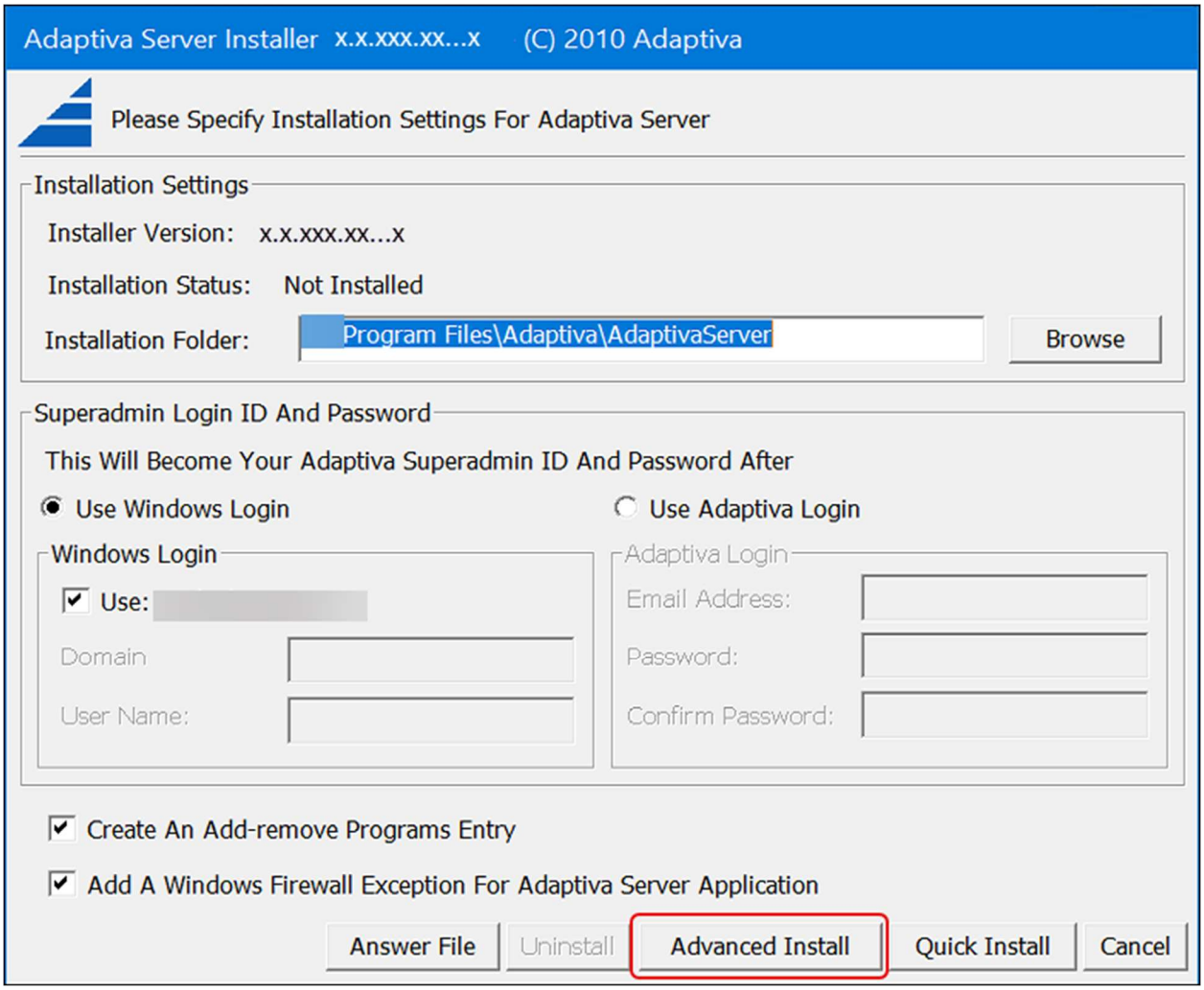
    c. **Create an Add/Remove Programs Entry**: When enabled (default), the installer creates a program entry from the Windows `Control Panel > Programs > Programs and Features` menu.

    d. **Add a Windows Firewall Exception for Server Application**: When enabled (default), automatically adds local exceptions in the Windows firewall for the default server ports.

    **Important**

    Review any existing domain-based group policies (GPO) that may configure or restrict Windows firewall rules to make sure they do not conflict with the Tenable Server-created firewall exceptions.

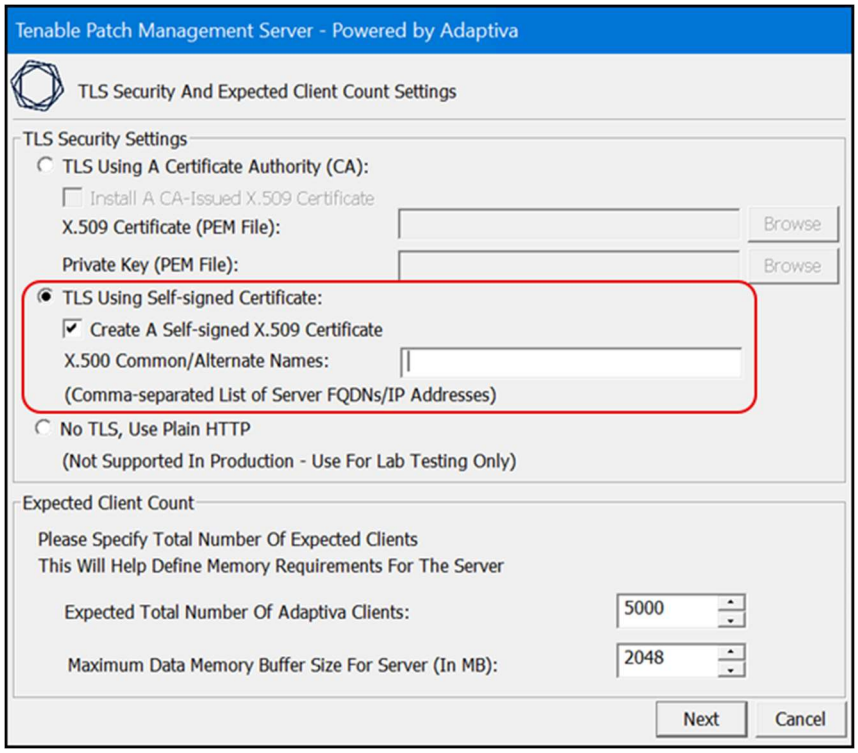
5. Select Advanced Install to continue with a new installation:




This opens the TLS Security Settings dialog.

# Configure Transport Layer Security Settings and Client Count

Use the Transport Layer Security (TLS) Settings to choose the certificate ensure secure communication between the administrator and the Admin Portal. See Prerequisites for information about these settings.




1. Select one of the following TLS security settings, based on the preferences of your organization. These settings allow secure access to the Admin Portal from the identified servers:

    a. Select **TLS Using A Certificate Authority (CA)** to use a certificate you exported from a Certificate Authority.

        i. Select **Install A CA-Issued X.509 Certificate**.

        ii. Select **Browse**, and then navigate to the location of the downloaded or exported **Certificate PEM** file.

        iii. Select **Browse**, and then navigate to the location of the **Private Key PEM** file.

    **Important**

    CA certificates must use a `.pem` extension. If your certificate has a `.pfx` extension, convert it using the instructions in Using a Certificate Authority.

    b. Select **TLS Using Self-signed Certificate** to use a self-signed certificate.

        i. Select **Create A Self-signed X.509 Certificate** and remove any prepopulated information from the text box.

ii. Enter the **names or IP addresses** associated with the servers that host the Admin Portal.

For example, include server details for Netbios, FQDN, DNS Alias, and so on. Separate multiple server names with commas.

c. Select **No TLS, Use Plain HTTP** if your organization does not require TLS to access the Admin Portal. The installer prompts you to confirm that this is a lab server.

2. Set the number of clients (endpoints) you expect this installation to support.

3. The **Expected Total Number Of Tenable Clients** defaults to 5000, which automatically sets the the **Maximum Data Memory Buffer Size** to **2048 MB**.

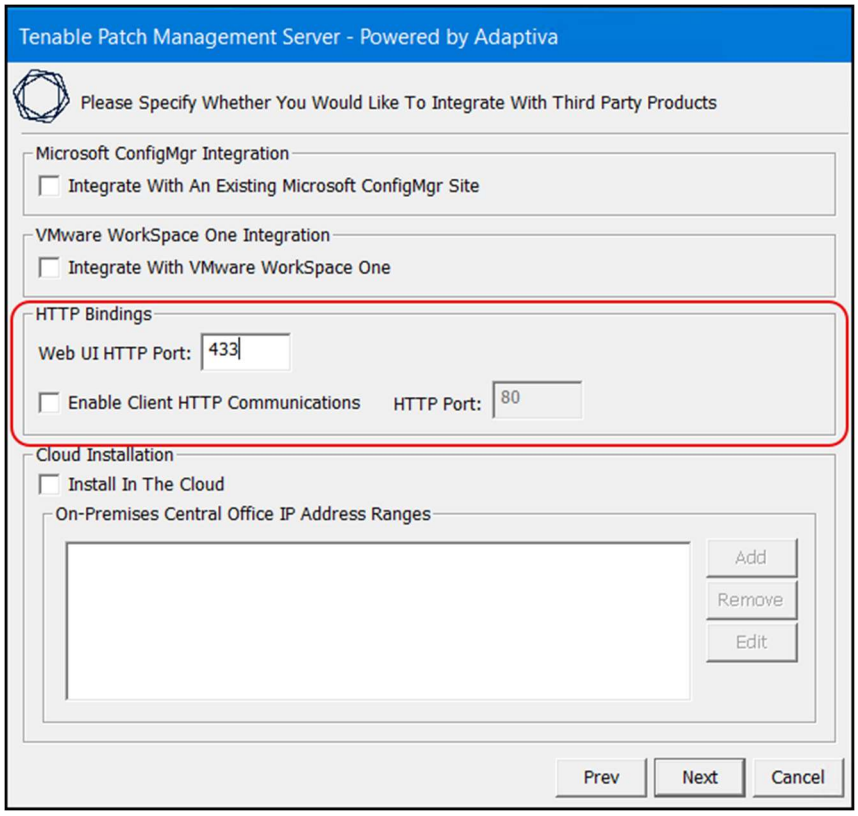
4. Select **Next**.

5. Continue with Set HTTP Bindings for Adaptiva Server (Required).

# Set HTTP Bindings for Adaptiva Server (Required)

The Tenable Server requires HTTP Binding to ensure secure communication between the administrator and the Admin Portal. Configure the HTTP Bindings only. Do not select any integrations or cloud installations.

1. Complete one or both of the following options for HTTP Bindings, and then click **Next**:




2. Configure the HTTP Bindings:

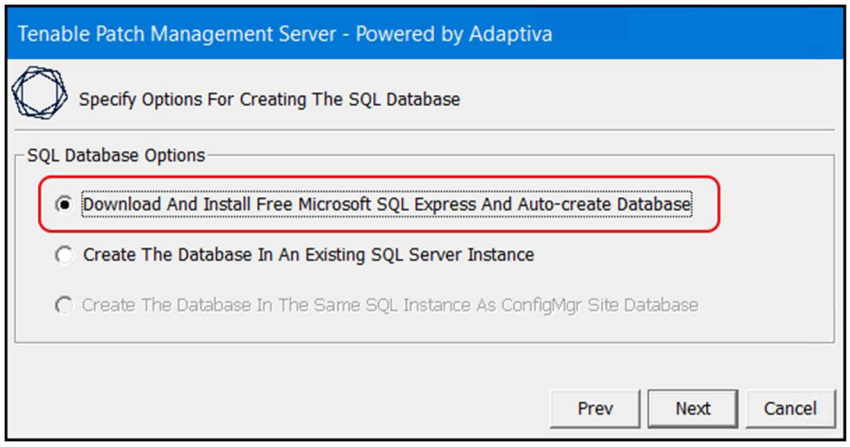
    a. Enter the **Web UI HTTP Port** that allows communication between the administrator and the Tenable Admin Portal.

    b. Select **Enable Client HTTP Communications** only if User Datagram Protocol (UDP) does not work in the environment. Clients use this Transmission Control Protocol (TCP) port to communicate with the Tenable Server when they cannot connect using UDP ports. Defaults to disabled.

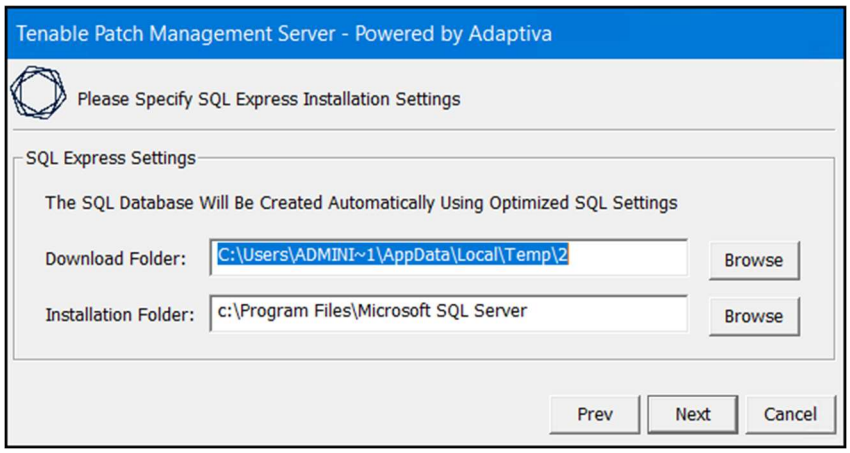
# Auto-create Adaptiva Database using Free Microsoft SQL Express

After specifying the Free Microsoft SQL Express option for creating the Tenable SQL database, the installer creates the Tenable SQL Database automatically using optimized SQL. To ensure a successful download, be sure to modify the Internet Settings as outlined in the Prerequisites.

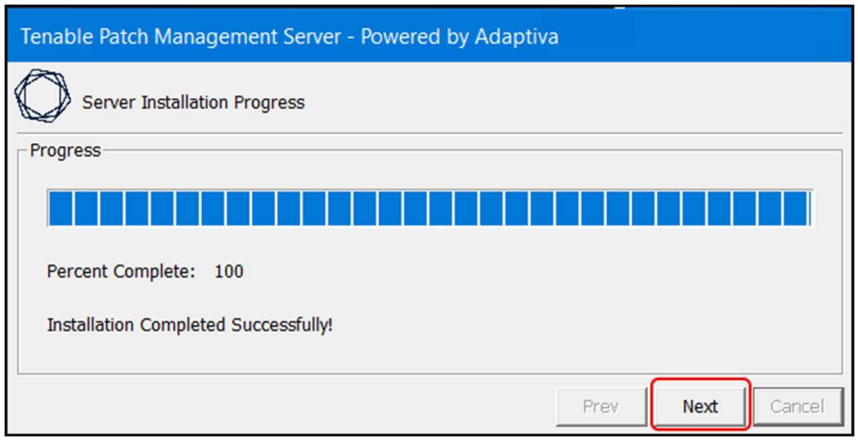
1. Select the **Free Microsoft...** option, and then click **Next**.




2. Browse to and choose the SQL Express download and installation locations or use the default settings:




3. Click **Next**. The Server installation downloads, installs, and configures SQL Server Express.

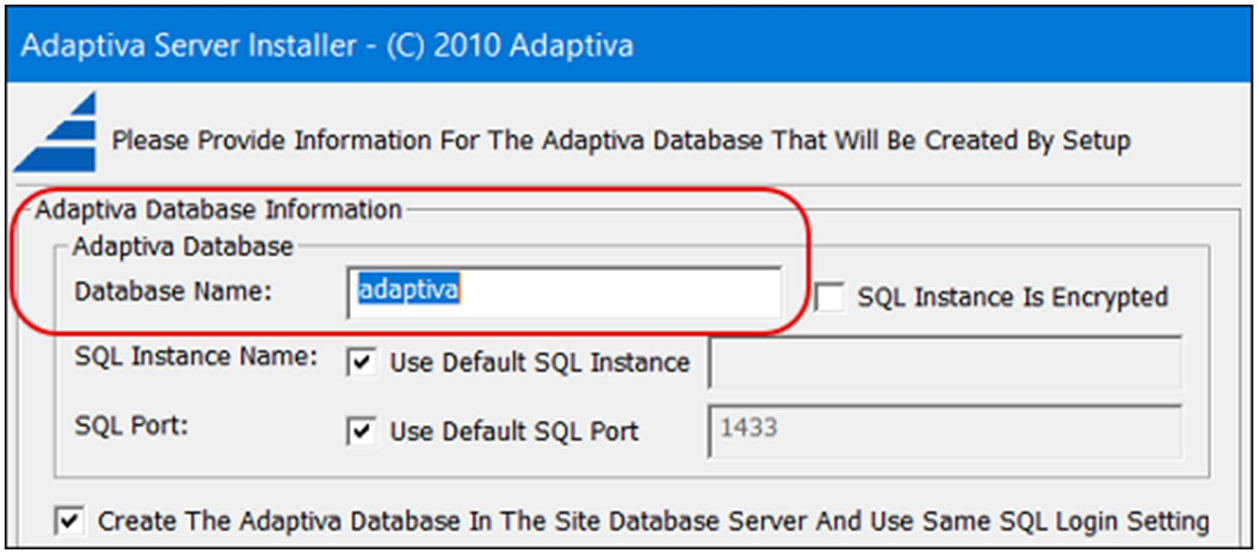



4. Create a SQL Read-Only Login for Tenable reporting.

# Create the Adaptiva SQL Database in an Existing SQL Server Instance

Name the Adaptiva SQL Database and identify the existing SQL Server instance that will host it.

1. Verify or enter the name of the Adaptiva SQL database.

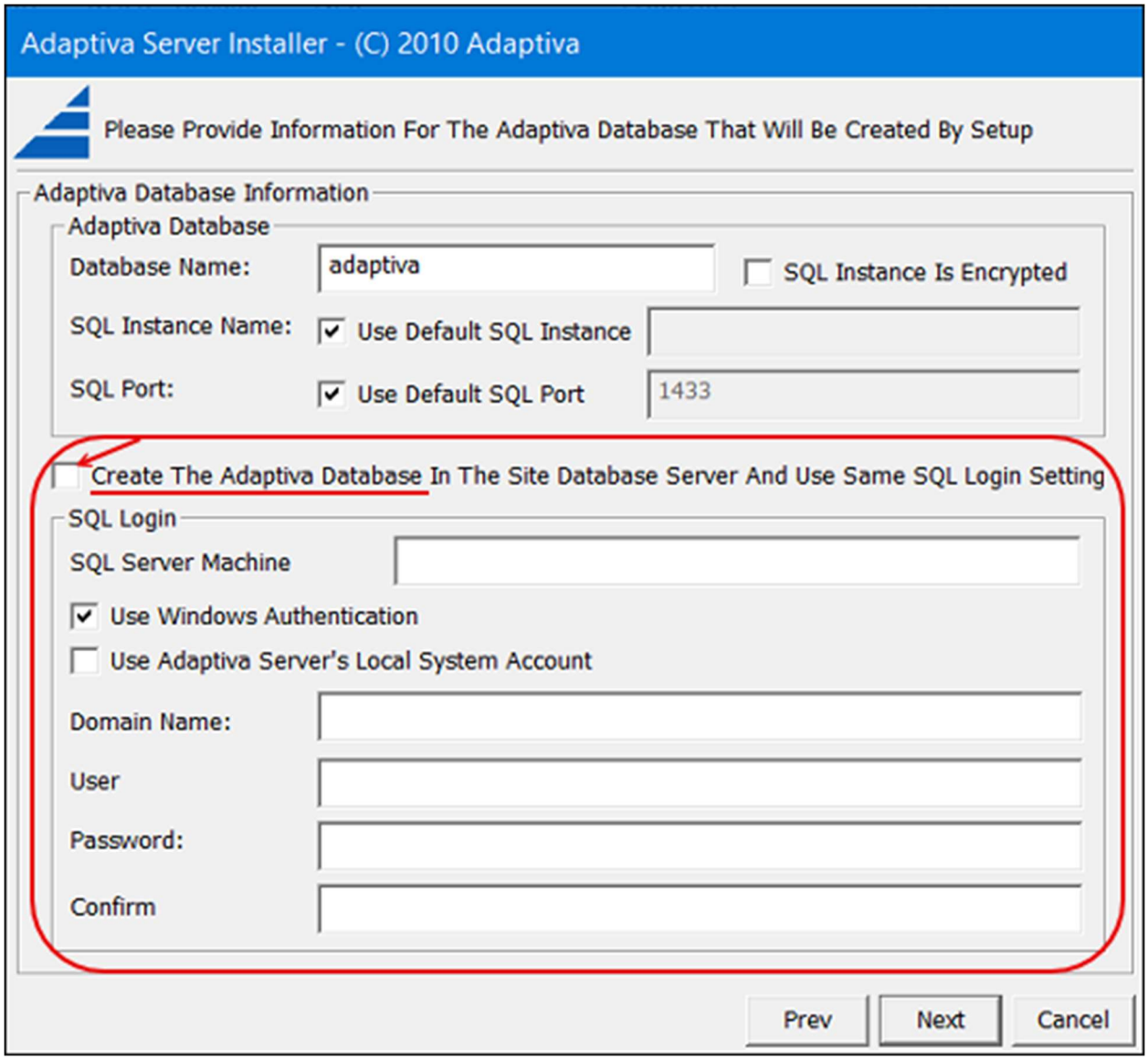



2. Choose which SQL Instance and port to use as the Adaptiva SQL Database host:

    a. To specify a SQL Instance Name, click Use Default SQL Instance to remove the check, and then enter the SQL instance name to use.

    b. To specify a SQL Port, click Use Default SQL Port to remove the check, and then enter the SQL port to use. This is the port used to connect the SQL instance.

3. Enter the SQL Server Machine and login details.




a. Enter the name of the SQL Server Machine. This is the FQDN of the SQL server that will host the Adaptiva database.

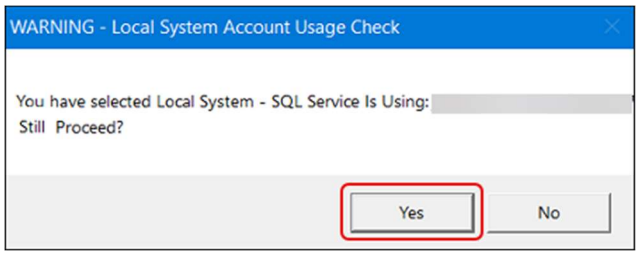
b. Decide whether to use Windows Authentication details (recommended), details from the Adaptiva SQL Server local system account, or enter a username and password:

   i. To use Windows Authentication (default, enter the domain and login details for Windows Authentication.

   ii. To use the local system account, select **Use Adaptiva Server...** to add a check mark.

iii. Check this box to authenticate using the Adaptiva server computer account, otherwise enter the User's credentials with permissions to access this SQL Server.

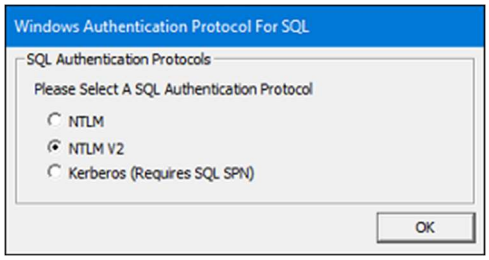
4. Verify your selection:




   a. If the settings are correct, select **Yes**.

   b. If the settings are incorrect, select **No** and update the Adaptiva SQL Database information.

5. Select the NTLM V2 as the Authentication Protocol for SQL:

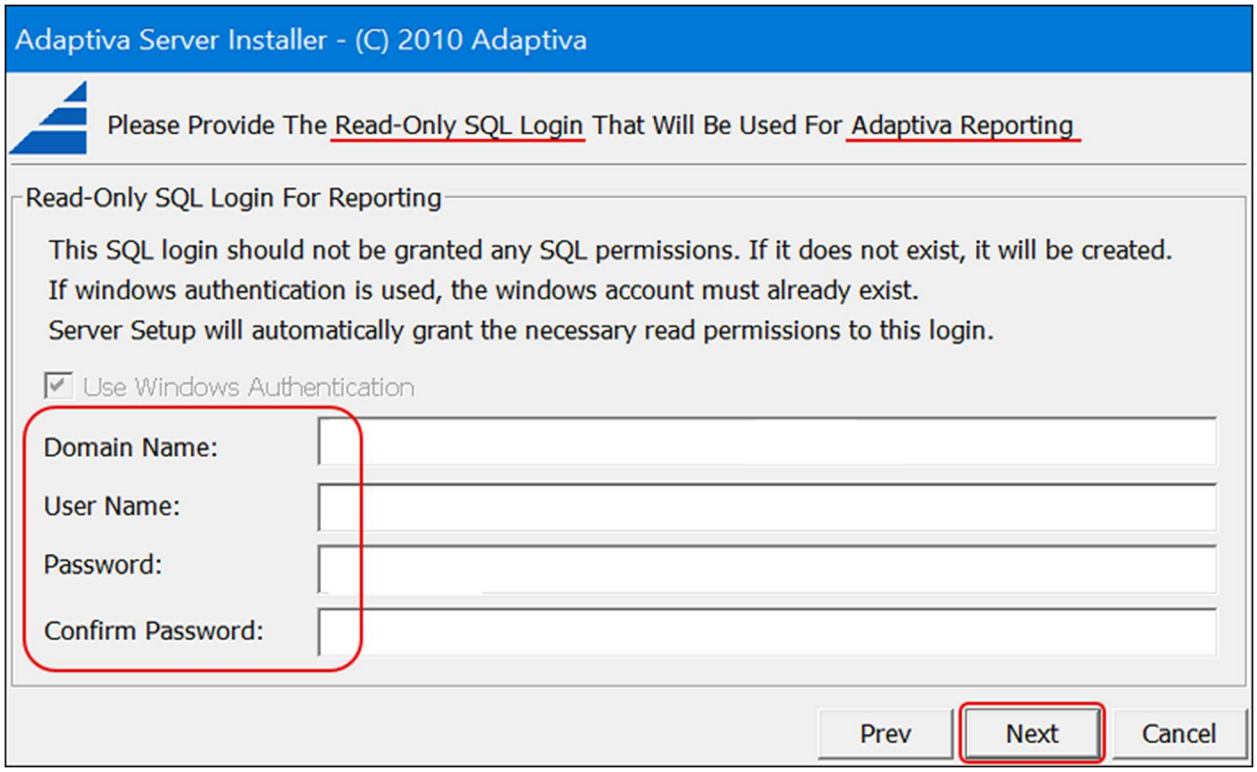



6. Click **OK** to continue with the SQL reporting details.

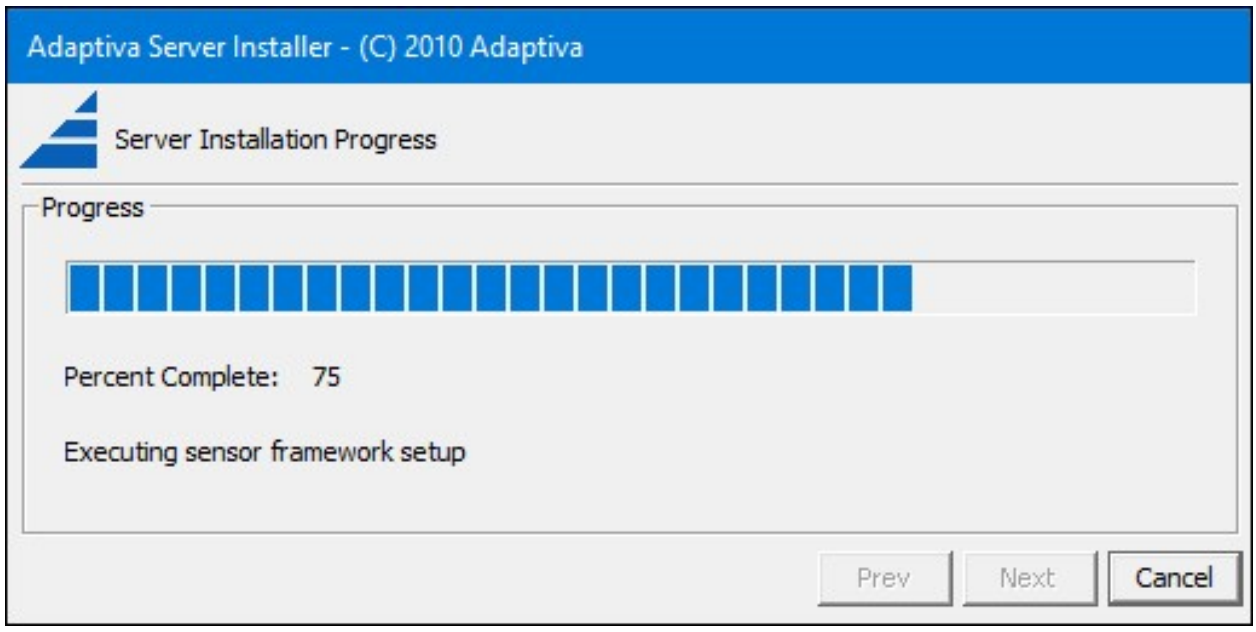
# Provide SQL Reporting Credentials

After completing the SQL setup for your chosen database options, enter the read-only log in details for SQL reporting. . See Accounts and Permissions for required permission settings.

1. Enter the NETBIOS Domain, User Name and Password for SQL reporting.



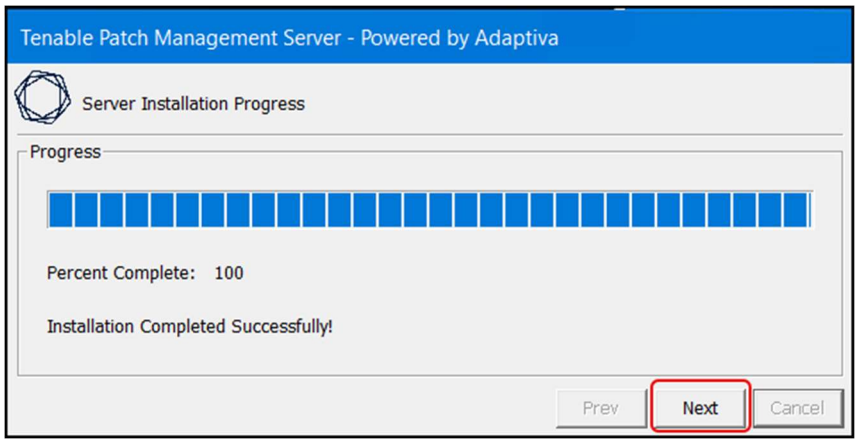

2. Click **Next**. This launches the installation program and displays the installation status. :



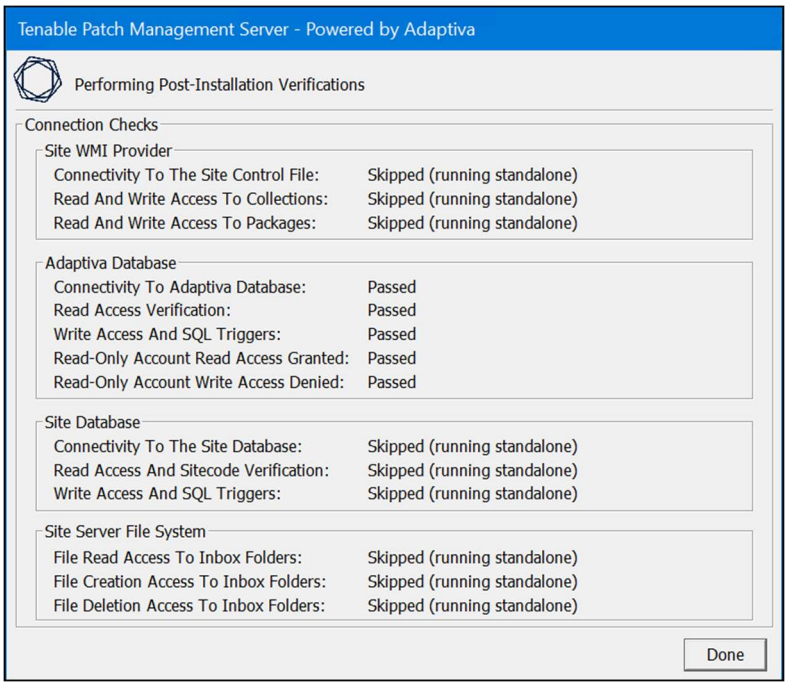

3. See Finalize the Server Installation to continue.

# Finalize Server Installation

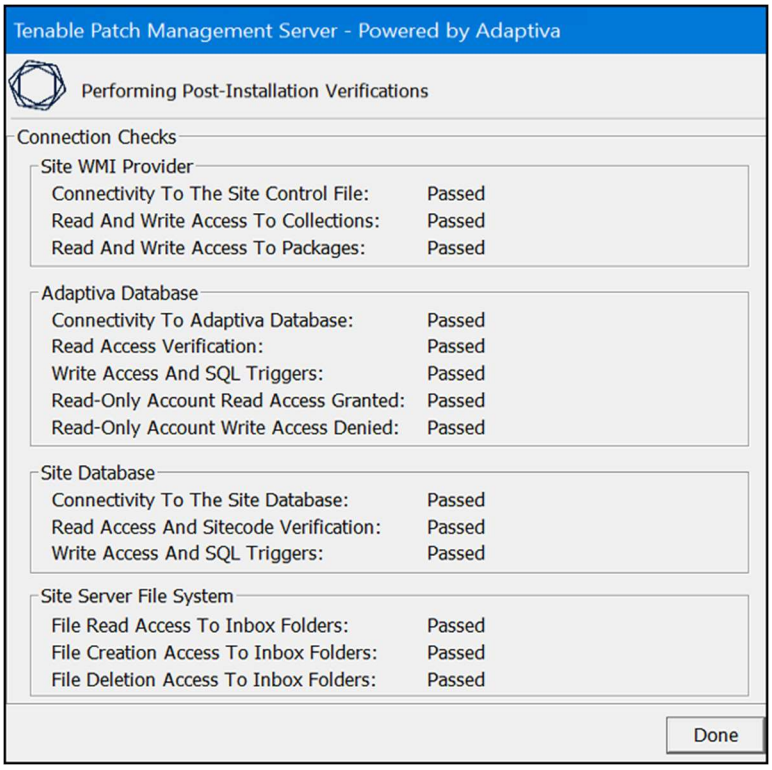
When the Server Installation Progress reaches 100% successfully, the Server Installation Progress shows the following:




1. Click **Next** to see the post-installation verifications:
2. For a SQL Standard or SQL Enterprise version:
    a. For a SQL Express version:




    b. For a SQL Standard or SQL Enterprise version:

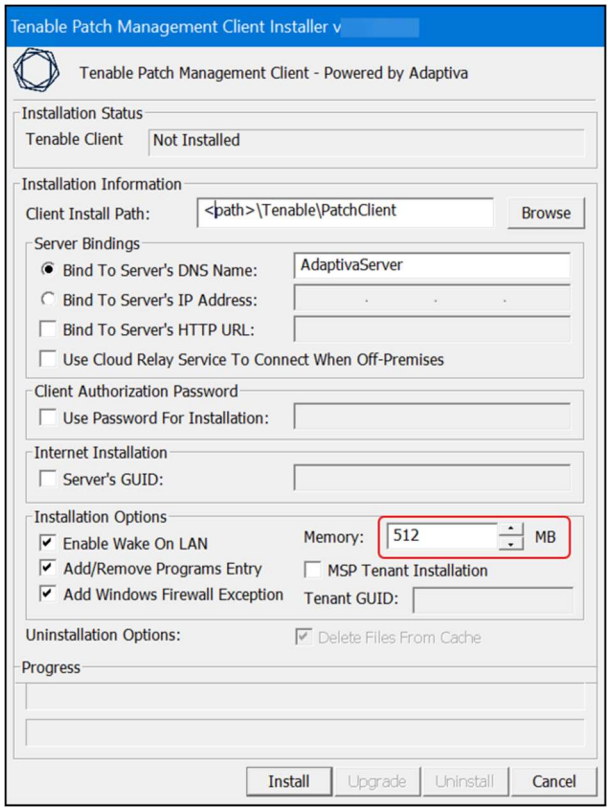



3. Click **Done**. Because every Tenable Server also requires a Tenable Client, the wizard prompts you to verify whether you want to continue with that installation:

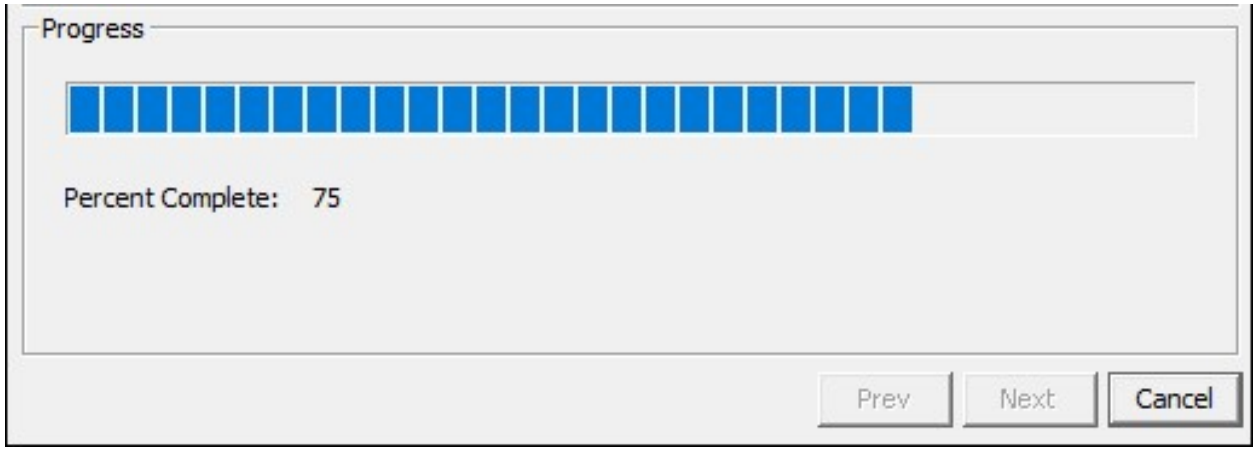
    e. To continue with the Tenable Client installation, click **Yes** (Recommended), and continue with the next step.

    f. To skip the Tenable Client installation, click **No**. If you have no Client installed on the Server, you must install the Client manually before you can use Tenable Patch Management.

4. Increase the **Memory** to 512 MB, otherwise, accept the default settings.




5. Click **Install**. The installer presents an install status:




6. Click **Next** when the installation finishes to see the installation status.

# View the Installation Logs

The following table contains the installation log locations. Other logs exist in the installation destination folder.

*Table 3: <caption>*

| Function | Log Location and Name |
|---|---|
| Server Installation Log | %windir%\AdaptivaSetupLogs\Server\AdaptivaServerSetup.log |
| Client Installation Log | %windir%\AdaptivaSetupLogs\Client\AdaptivaClientSetup.log |

# Product Licensing and Server Activation

If you added your license key at the start of the Server installation, your product is licensed and ready to use. Use the Admin Portal to manage your Patch estate, including license details.