Server Install Guide

8.6

Copyright Notice

Contents

System Requirements

Before installing Ivanti Endpoint Security, verify that the targets meets hardware, software, and network requirements.

On servers that do not meet recommended system requirements If your target server does not meet the system requirements, Ivanti Endpoint Security will not perform optimally, or may not install.

Review all hardware, software, and network requirements before proceeding with installation.

Supported Operating Systems

The Ivanti Endpoint Security server is supported on a number of Microsoft Windows operating systems.

Operating System	Edition	Bit version
Microsoft Windows Server 2019	Standard Datacenter	64-bit
Microsoft Windows Server 2016	Standard Datacenter	64-bit
Microsoft Windows Server 2012 R2 [1]	Standard [2] Datacenter [2] Foundation	64-bit
Microsoft Windows Server 2012 [1]	Standard [2] Datacenter [2]	64-bit

1. Initial installation of Ivanti Endpoint Security on this family of operating systems when Core mode is enabled is not supported; a GUI is required. However, following installation, general operation of Ivanti Endpoint Security while Core mode is enabled is supported.
2. The Hyper-V edition of this operating system edition is supported, however, the Microsoft Hyper- V Server 2012 stand-alone edition is not.

Supported Languages and Locales

Ivanti Endpoint Security can be installed on servers only for certain languages and locales. Ensure the target server you are installing on uses one of the listed languages and locales.

Server Supported Locales

Ivanti Endpoint Security is installable on the following locales. The installer is available only in English.

Language	Locale Identifier
English: United States	en-us
English: Australia	en-au
English: Belize	en-bz
English: Canada	en-ca
English: India	en-in
English: Ireland	en-ie
English: Jamaica	en-jm
English: New Zealand	en-nz
English: Philippines	en-ph
English: Singapore	en-sg
English: South Africa	en-az
English: United Kingdom	en-gb
German: Germany	de-de
Spanish: Spain (Modern Sort)	es-es

Server Supported Languages

After installing Ivanti Endpoint Security, the following UI languages are available in your Web browser:

Language	Locale Identifier
English: United States	en-us
French: France	fr-fr
German: Germany	de-de
Spanish: Spain (Modern Sort)	es-es

Hardware Requirements

The Ivanti Endpoint Security server must meet or exceed the specified hardware requirements.

Installing the Ivanti Endpoint Security server on a dedicated server is recommended.

The minimum hardware recommendation is designed for trial environments of 50 endpoints. For a Ivanti Endpoint Security configuration ideal for your environment, see "Recommended Configurations" on page 13.

- 2.0 GHz dual-core processor
- 4 GB RAM
- 50 GB or more hard drive space
  - RAID 1 disk array
  - 7200 RPM drive speed
- 1 Gbps Network Card

Software Requirements

Your Ivanti Endpoint Security server requires other software to operate. Review the listed software requirements to confirm your server has the required software.

Before you begin installation of Ivanti Endpoint Security you must install the following software on your server or another supported location:

Supported Web Browsers and requirements

You need one of several specific Web browsers to use the Ivanti Endpoint Security Web console after installation.

Supported Browser	Supported Versions
Google Chrome	53 and higher
Microsoft Edge	EdgeHTML 14 and higher
Microsoft Internet Explorer	9 and higher
Mozilla Firefox	31 Extended Support Release and higher Support cannot be guaranteed due to the accelerated release cycle of Mozilla Firefox Rapid Release.

Important:

- Microsoft Silverlight 5.0 is also required to use Ivanti Installation Manager.
- Google Chrome and Microsoft Edge are currently incompatible with these Ivanti Endpoint Security features:
    - Patch & Remediation Patch Package Editor
    - Device Control Media Hasher
    - Install Manager

Supported SQL Server versions and requirements

Ivanti Endpoint Security requires an instance of Microsoft SQL Server to store its data. Multiple versions of SQL Server are supported.

Supported Database Servers:

Database	Bit version	Edition
SQL Server 2019	x86/x64	• Express • Standard • Enterprise
SQL Server 2017	x86/x64	• Express • Standard • Enterprise
SQL Server 2016	x86/x64	• Express • Standard • Enterprise
SQL Server 2014 and later	x86/x64	• Express • Standard • Enterprise • Business Intelligence
SQL Server 2012 and later	x86/x64	• Express • Standard • Enterprise

Ivanti recommends using the latest service pack available for your instance of SQL Server.

If installing to a 64-bit server, Ivanti recommends installing using a supported preexisting instance of SQL Server that supports 64-bit architecture.

For evaluation installs, Ivanti Endpoint Security installs an instance of SQL Server 2014 Express SP1, which you can later upgrade to Standard or Enterprise before adding Ivanti Endpoint Security to a production environment. If you are evaluating Ivanti Endpoint Security, and you have no intent of using SQL Server 2014 Express SP1, your evaluation installation of Ivanti Endpoint Security should use your preferred version of SQL Server.

You can install one of the supported database servers instances listed above in the following locations relative to the Ivanti Endpoint Security server:

- On the target Ivanti Endpoint Security server itself, as installed by the Ivanti server installer, which installs an instance of SQL Server 2014 Express SP1 (x64).
- On the target Ivanti server itself, using a preexisting instance of SQL Server.
- On a remote server that the Ivanti server remotely connects to, using a preexisting instance of SQL Server.

Important: When installing Ivanti Endpoint Security using an existing SQL Server instance, the instance collation must be set to one of the following values:

- SQL_Latin1_General_CP1_CI_AS
- Latin1_General_CI_AS

Ivanti Endpoint Security requires additional, supplemental software, but the Ivanti Endpoint Security will install it for you during installation:

.NET Framework Requirements

Ivanti Endpoint Security requires installation of .NET Framework 4.6.7.

.NET Framework Requirements:

Required .NET Framework Version	Operating System Family
Microsoft .NET Framework 4.6.7	Microsoft Windows Server 2019
	Microsoft Windows Server 2016
	Microsoft Windows Server 2012 R2
	Microsoft Windows Server 2012

Ivanti Endpoint Security provides the .NET Framework 4.6.7 installer during installation or upgrade (reboot required). However, pre-requisites must be installed on some Operating Systems prior to this.

IIS Requirements

Before you can install Ivanti Endpoint Security, Microsoft Internet Information Services 7.0 or later must be installed.

Internet Information Services (IIS) Requirements:

Required IIS Version	Operating System Family
Microsoft Internet Information Services 7.0+	Microsoft Windows Server 2019
	Microsoft Windows Server 2016
	Microsoft Windows Server 2012 R2
	Microsoft Windows Server 2012

- Microsoft Silverlight 5.0
- Microsoft Visual C++ 2010 SP1 Redistributable Package (x86 and x64)
- Microsoft Visual C++ 2012 Update 4 Redistributable Package (x86 and x64)

Although Ivanti Endpoint Security installs an instance of SQL Server 2014, (x64), installing an instance yourself is best practice when supporting an enterprise environment.

Network Requirements

Your Ivanti Endpoint Security server needs access to specific websites and network services.

Server Role

Your Ivanti Endpoint Security *should not* be a domain controller.

Firewall Access URLs for replication and agent communication

- https://cdn.securegss.net
- https://cache.patchlinksecure.net
- http://cache.lumension.com
- http://gssnews.lumension.com
- https://download.windowsupdate.com
- https://www.download.windowsupdate.com (For Microsoft content)
- https://go.microsoft.com (For Microsoft content)
- https://ardownload.adobe.com (For Adobe content)
- https://swupdl.adobe.com (For Adobe content)
- https://armdl.adobe.com (For Adobe content)
- https://download.adobe.com (For Adobe content)

Important:

- Refer to Ivanti Community Article 4115 (https://forums.ivanti.com/s/article/Lumension-s-New-Content-Architecture) and Ivanti Community Article 2698 (https://forums.ivanti.com/s/article/Lumension-Global-Subscription-Server-and-GSS-Repository-Information) for additional URLs and IP Addresses which may be required depending upon your configuration and content subscriptions.
- The firewalls on your server may require modification to access these URLs. If your corporate policies do not allow you to make the necessary firewall modifications, please contact Support for a recommended configuration.

Network Discovery Windows Services

Ivanti Endpoint Security uses the server Network Discovery Windows Services to discover other computers and devices on your network and installation. At time of install, the Ivanti Endpoint Security installer prompts you to enable these services:

- DNS Client
- Function Discovery Resource Publication
- SSDP Discovery
- UPnP Device Host

Encryption Protocols

Ivanti Endpoint Security uses Transport Layer Security (TLS) for communication between the Ivanti Endpoint Security Server and the Ivanti Endpoint Security Agent. Ivanti Endpoint Security prompts you to enable this protocol during installation.

Recommended Configurations

Ivanti recommends different hardware and software requirements customized for your Ivanti Endpoint Security network setup.

Server Configuration Considerations

Ivanti Endpoint Security requires two main components to function:

- **Ivanti Endpoint Security Application Server**: This server is responsible for Web site, replication services, and endpoint distribution services.
- **Ivanti Endpoint Security Database Server**: This server is responsible for SQL database and stored procedures.

These servers can be installed on a single server, or on two separate servers.

- **Combined Application and Database Server**: In configurations where the Ivanti Endpoint Security application and database are installed on the same server, the server requires both high processing power and disk speed, as it is performs both application and database functions.

  Combined Ivanti Endpoint Security Application and Database Server

- **Separate Application and Database Servers**: In configurations where the Ivanti Endpoint Security application and database are installed on separate servers, the server requirements are different. Although processing and software requirements on both servers remain the same, the database requires increased HDD specifications, as it executes disk-intensive functions.

  Separated Ivanti Endpoint Security Application and Database Servers

Endpoint Scaling Considerations

Regardless of your Ivanti Endpoint Security application and database configuration, your server (or servers) require increasingly high-end hardware and software to offset increased load from endpoints. Use better hardware in environments with a high endpoint count.

Additional Considerations

- For additional information about the physical memory limits for Windows releases, refer to Memory Limits for Windows Releases (https://msdn.microsoft.com/en-us/library/windows/desktop/ aa366778(v=vs.85).aspx).
- For additional information about moving SQL Server databases, refer to Move System Databases (https://msdn.microsoft.com/en-us/library/ms345408.aspx).
- For additional information about Microsoft's top ten best practices for storage, refer to Storage Top Ten Best Practices (https://technet.microsoft.com/en-us/library/cc966534.aspx).

Combined Ivanti Endpoint Security Application and Database Server

For optimal performance, the hardware and software supporting Ivanti Endpoint Security should be scaled to your endpoint count.

The following table lists the recommended hardware and software for you Ivanti Endpoint Security network.

Installation on a physical server is assumed. If installing to virtual environment, refer to the following article on the Ivanti Community: https://forums.ivanti.com/s/article/Lumension-products-installed-on-virtual-machines.

Endpoint Count		< 50	< 500	< 1,000	< 5,000	< 10,000[1]
Software	Operating System	Windows 2019	Windows 2019	Windows 2019	Windows 2019	Windows 2019
	Operating System Edition	Standard	Standard	Standard	Standard	Standard
	Operating System Architecture	x64	x64	x64	x64	x64
	Database Server	SQL 2019	SQL 2019	SQL 2019	SQL 2019	SQL 2019
	Database Server Edition	Standard[2]	Standard	Standard	Standard	Enterprise
	Database Server Architecture	x64	x64	x64	x64	x64

Endpoint Count		< 50	< 500	< 1,000	< 5,000	< 10,000[1]
Hardware	Core Architecture[3]	2	2	4	8	16
	Core Speed (GHz)	2.0+	2.0+	2.0+	2.0+	2.0+
	RAM (GB)[4]	4	4	8	16	32
	Network (LAN)	1 Gb/s	1 Gb/s	1 Gb/s	1 Gb/s	1 Gb/s
	Disk Array [5]	RAID 1	RAID 1	Multiple RAID	Multiple RAID	Multiple RAID
	# Hard Drives	2	2	4	6	8
	Drive Speed (RPM)	7200	7200	10k/SSD	10k/SSD	15k/SSD
	Hard Drive Volume Breakdown					
	OS/Data	250GB	500GB	N/A	N/A	N/A
	OS	N/A	N/A	RAID 1 - 250GB	RAID 1 - 250GB	RAID 1 - 250GB
	Data	N/A	N/A	RAID 1 - 500GB	RAID 1/ SSD - 1TB	RAID 10/ SSD - 1TB
	Temp DB	N/A	N/A	N/A	RAID 0 - 250GB	SSD - 240GB

1. If you are managing 10000+ endpoints, contact Ivanti Support (https://forums.ivanti.com/s/contactsupport) for a recommended configuration.
2. Evaluation customers should use Express edition with Advanced Services.
3. A Sandy Bridge Xeon+ or AMD equivalent is recommended. On virtualized servers, 2x the assigned cores is recommended.
4. On virtualized servers, 2x RAM is recommended for networks supporting 1000+ endpoints.
5. Due to performance issues, do not use RAID 5 configurations. Replace the disk array with a shared SAN, an enterprise-class SSD, or another enterprise storage solution.
    - 1000 IOPS minimum sustained performance is recommended.
    - A dedicated array or LUN is recommended.

Separated Ivanti Endpoint Security Application and Database Servers

When the Application Server and Database Server are installed on two physical servers, then each servers recommended hardware requirements will increase according to the number of managed endpoints in your network.

Review the following information when the components are installed on separate servers.

Installation on a physical server is assumed. If installing to virtual environment, refer to Ivanti Community Article 2674 (https://forums.ivanti.com/s/article/Lumension-products-installed-on-virtual-machines).

Recommended Application Server Configuration

The following table lists the recommended configuration for the Application Server.

Endpoint Count		< 50	< 500	< 1,000	< 5,000	< 10,000[1]
Software	Operating System	Windows 2019	Windows 2019	Windows 2019	Windows 2019	Windows 2019
	Operating System Edition	Standard	Standard	Standard	Standard	Standard
	Operating System Architecture	x64	x64	x64	x64	x64

Endpoint Count		< 50	< 500	< 1,000	< 5,000	< 10,000[1]
Application Server Hardware	Core Architecture[2]	2	2	4	8	16
	Core Speed (GHz)	2.0+	2.0+	2.0+	2.0+	2.0+
	RAM (GB)[3]	4	4	8	16	16
	Network (LAN)	1 Gb/s	1 Gb/s	1 Gb/s	1 Gb/s	1 Gb/s
	Disk Array[4]	RAID 1	RAID 1	RAID 1/SSD	RAID 1/SSD	RAID 1/SSD
	# Hard Drives	2	2	2	2	2
	Drive Speed (RPM)	7200	7200	10k/SSD	10k/SSD	10k/SSD
	Hard Drive Volume Breakdown					
	OS/Data (GB)	250	500	500	500	500

1. If you are managing 10000+ endpoints, contact Ivanti Support (https://forums.ivanti.com/s/contactsupport) for a recommended configuration.
2. A Sandy Bridge Xeon+ or AMD equivalent is recommended. On virtualized servers, 2x the assigned cores is recommended.
3. On virtualized servers, 2x RAM is recommended for networks supporting 1000+endpoints.
4. Due to performance issues, do not use RAID5 configurations. Replace the disk array with a shared SAN, an enterprise-class SSD, or another enterprise storage solution.
    - 1000 IOPS minimum sustained performance is recommended.
    - A dedicated array or LUN is recommended.

Recommended SQL Server Configuration

The following table lists the recommended configuration for the Database Server.

Endpoint Count		< 50	< 500	< 1,000	< 5,000	< 10,000[1]
Software	Operating System	Windows 2019	Windows 2019	Windows 2019	Windows 2019	Windows 2019
	Operating System Edition	Standard	Standard	Standard	Standard	Standard
	Operating System Architecture	x64	x64	x64	x64	x64
	Database Server	SQL 2019	SQL 2019	SQL 2019	SQL 2019	SQL 2019
	Database Server Architecture	x64	x64	x64	x64	x64
	Database Server Edition	Standard[2]	Standard	Standard	Standard	Enterprise

Endpoint Count		< 50	< 500	< 1,000	< 5,000	< 10,000[1]
SQL Server Hardware	Core Architecture[3]	2	2	4	8	16
	Core Speed (GHz)	2.0+	2.0+	2.0+	2.0+	2.0+
	RAM (GB)[4]	4	4	8	16	32
	Network (LAN)	1 Gb/s	1 Gb/s	1 Gb/s	1 Gb/s	1 Gb/s
	Disk Array [5]	RAID 1	RAID 1	Multiple RAID	Multiple RAID	Multiple RAID
	# Hard Drives	2	2	4	6	8
	Drive Speed (RPM)	7200	7200	10k/SSD	10k/SSD	15k/SSD
	Hard Drive Volume Breakdown					
	OS/Data (GB)	250	500	N/A	N/A	N/A
	OS (GB)	N/A	N/A	RAID 1 - 250	RAID 1 - 250	RAID 1 - 250
	Data	N/A	N/A	RAID 1 - 500GB	RAID 1/ SSD - 1TB	RAID 10/ SSD - 1TB
	Temp DB (GB)	N/A	N/A	N/A	RAID 0 - 250	SSD - 240

1. If you are managing 10000+ endpoints, contact Ivanti Support (https://forums.ivanti.com/s/contactsupport) for a recommended configuration.
2. Evaluation customers should use Express edition with Advanced Services.
3. A Sandy Bridge Xeon+ or AMD equivalent is recommended. On virtualized servers, 2x the assigned cores is recommended.
4. On virtualized servers, 2x RAM is recommended for networks supporting 1000+ endpoints.
5. Due to performance issues, do not use RAID5 configurations. Replace the disk array with a shared SAN, an enterprise-class SSD, or another enterprise storage solution.
    - 1000 IOPS minimum sustained performance is recommended.
    - A dedicated array or LUN is recommended.

Installing Ivanti Endpoint Security

Complete the Ivanti Endpoint Security installation method that is best for your network environment. Before installation, download the latest Ivanti Endpoint Security (Ivanti Endpoint Security) installer. There is an installation procedure for all Ivanti Endpoint Security installation scenarios.

After installation, complete any additional procedures associated with the installation method.

Downloading Ivanti Endpoint Security

When you purchase Ivanti Endpoint Security, you receive no physical media. Rather, you download it from the company Web site.

Download Ivanti Endpoint Security from the Ivanti Endpoint Security Downloads Page.

1. Open your Web browser.
2. Browse to the Ivanti Endpoint Security Downloads Page.
3. Browse to and download the most recent version of the Ivanti Endpoint Security installer to your desired location.

About SQL Server Instance Location

Ivanti Endpoint Security requires an instance of Microsoft SQL Server to store system data values. You can install this SQL Server instance on your target Ivanti Endpoint Security server or a remote server.

Local SQL Server Instance

A SQL Server instance can be installed on the same server as Ivanti Endpoint Security. When using a local SQL Server instance, you can use either a named or default instance of SQL Server that is preexisting, or you can use a new instance of SQL Server (which is set up by the Ivanti Endpoint Security Server installer).

Remote SQL Server Instance

A SQL Server instance can be installed on a different server than Ivanti Endpoint Security, and Ivanti Endpoint Security can then access that remote instance. If you elect to use a remote SQL Server instance, you must direct Ivanti Endpoint Security toward the remote instance during Ivanti Endpoint Security installation. However, before directing Ivanti Endpoint Security to the remote instance, you must configure that instance to accept remote connections. For additional information, refer to Configuring SQL Server to Accept Remote Connections.

Install Ivanti Endpoint Security using a remote SQL Server instance to increase performance.

Defining the Web Client Account and Service Account

Ivanti Endpoint Security requires two user accounts to operate critical components: a Web client account and a service account.

Ivanti recommends creating new local user accounts to use as Web client and service accounts (as defined in the installation procedures). However, you can also use preexisting local or domain accounts. When using preexisting local or domain accounts, certain requirements must be fulfilled. Remember the following rules if you use preexisting user accounts when installing Ivanti Endpoint Security using a remote instance of SQL Server:

- In cross-domain network configurations, accounts from either domain may be used as the Web client and service accounts, but the domains must have a trust relationship.
- Any install in which either the Ivanti Endpoint Security server or the SQL server is in a workgroup must use local accounts as the Web client and service accounts.
- When using local accounts as the Web client and service accounts, there must be a duplicate of each account on each server. For example, if the Ivanti Endpoint Security server hosts an account named `serviceadmin` with a password of `Password.0`, then the SQL server must host an account called `serviceadmin` with a password of `Password.0`.
- When using a domain account for the service accounts it must also belong to the local Administrator group in order to run critical services including Internet Information Services (IIS).

You can use existing user accounts as the Web client account and service account. However, Ivanti recommends creating new accounts specifically for Ivanti Endpoint Security using the installer (if using a remote SQL Server instance, manual creation of identical accounts is required). Creating accounts specifically for the product increases security and automates creation of trust relationships.

Selecting an Installation Method

There are multiple methods of installing the product. When installing, identify the scenario that best suits your network environment, and complete the scenario according to the provided procedures.

- For small network environments that do not require complex instances of SQL Server, complete the basic Ivanti Endpoint Security (Ivanti Endpoint Security) installation. This installation includes an installation of Microsoft SQL Server 2014, Express Edition (x64). This installation method is the simplest Ivanti Endpoint Security method.
    - Installing Using a New SQL Server Instance
- For larger network environments, the Ivanti Endpoint Security installation requires a more sophisticated SQL Server instance that must be installed independently from Ivanti Endpoint Security. This instance of SQL Server, which must be installed before Ivanti Endpoint Security, can be installed on either the target Ivanti Endpoint Security server or a remote server.
    - Installing Using an Existing SQL Server Instance (either locally or remotely)
    - Installing Using a Remote SQL Server Instance (with no local instance)
- In especially large environments, the SQL Server administrator and the Ivanti Endpoint Security administrator may be separate individuals. In this scenario, a special installation procedure is required due to administrator access right limitations.
    - Installing Ivanti Endpoint Security (Separate Ivanti Endpoint Security and SQL Server Admins)

Installing Using a New SQL Server Instance

If SQL Server is not installed on your target server, or if you want to use a new instance instead of an existing one, you can create a new SQL Server 2014, Express Edition (x64) instance during the Ivanti Endpoint Security installation.

Prerequisites:

- You have completed Downloading Ivanti Endpoint Security.
- As applicable to your network environment, you have gathered the information and completed the tasks itemized in the Appendix D: Installation Checklist.

For additional information about using preexisting user accounts to operate critical Ivanti Endpoint Security components, refer to Defining the Web Client Account and Service Account.
If you are installing using a Secure Sockets Layer (SSL), complete the first portion of Appendix B: Configuring Your Server to use SSL

1. Log on to the server on which you want to install Ivanti Endpoint Security using either a local or domain user account with system administrator privileges.
2. Stop or disable any AntiVirus products (such as McAfee, Trend-micro, Symantec, and so on) running on your server.

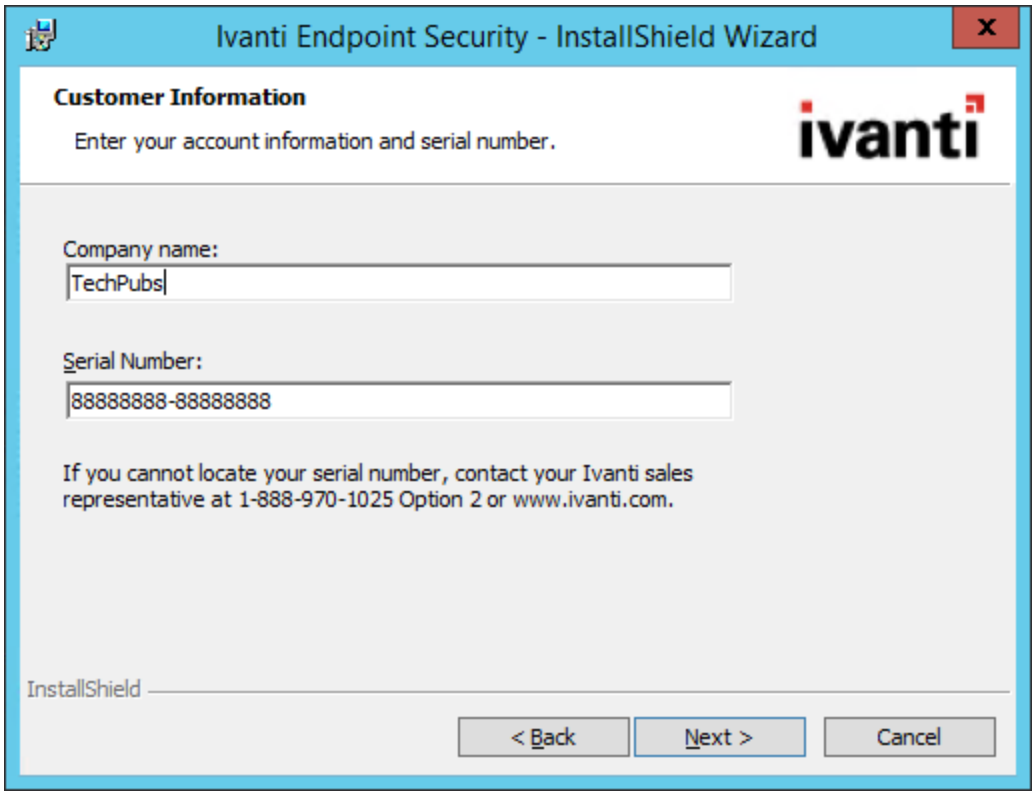
An AntiVirus product can prevent processes from running correctly during the installation. Therefore, to ensure a successful installation, all AntiVirus services must be stopped or disabled prior to running the Ivanti Endpoint Security installer.

3. Double-click the Ivanti Endpoint Security installer at the location defined during the download. The Ivanti Endpoint Security InstallShield Wizard opens and begins extracting files. This process may take several minutes.
4. If prompted, install prerequisites and reboot your server. The installer reopens by itself after the reboot.
5. Click **Next**.
   The License Agreement page opens.

Click **Print** for a hard copy of the license agreement.

6. Review the License Agreement and select the **I accept the terms of the license agreement** option.

7. Click **Next**.



The Customer Information page opens.

8. Type the applicable information in the following fields:

Field	Description
Company Name	Your company name.
Serial Number	Your Ivanti Endpoint Security serial number. Your serial number is two groups of eight alphanumeric characters. Letters are not case sensitive. If you cannot locate your serial number, obtain it by contacting the Ivanti Sales Support (sales@ivanti.com).

Retain your serial number following installation, as it is necessary if a reinstall of the Ivanti Endpoint Security server is needed.

9. Click **Next**.
A new page or dialog opens.

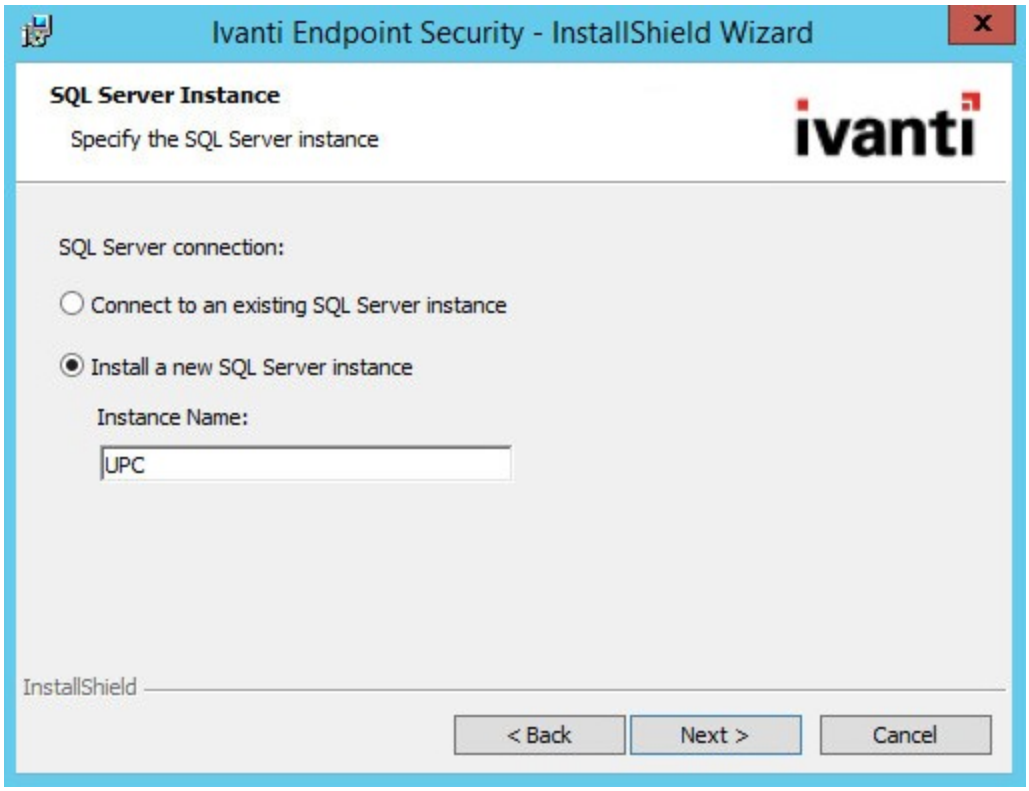
Page/Dialog	Step
If the *Question* dialog opens:	Click **Yes** to start network discovery services. The following services are necessary to use discovery features within Ivanti Endpoint Security: • DNS Client • Function Discovery Resource Location • SSDP Discover • UPnP Device Host
If the *Required IIS Features* page opens:	Your server does not have the required IIS features installed. Click **Install Features** to install the features and proceed. On Windows Server 2008, the default installation of IIS lacks components necessary for Ivanti Endpoint Security. The Ivanti Endpoint Security installer installs the following IIS components if not present: • Static Content • Default Document • HTTP Errors • ASP.NET • .NET Extensibility • ASP • ISAPI Extensions • ISAPI Filters • Basic Authentication • Windows Authentication • Static Content Compression • Dynamic Content Compression
If the *System Requirements* page opens:	Your server does not meet the minimum installation requirements. • If you receive only system requirement warnings, you may proceed with installation by clicking **Next**. Ivanti recommends resolving warnings before proceeding with installation. When installing on a virtual platform you will likely receive a warning about the CPU requirements since the installer is unable to identify the processor in a virtual environment. • If you receive any system requirement *failures*, you must cancel the installation, resolve these failures, and then restart installation. Click **View all Failures/Warnings** for detailed information about prerequisite status deficiencies.

Page/Dialog	Step
If the *Service Accounts* page opens:	Proceed to the next step.

10. Create or define the Web client account and service account that Ivanti Endpoint Security will use.
    These accounts are used to operate components critical to Ivanti Endpoint Security. Select from the following options.

Option	Steps
To create new accounts:	1. Edit the **Web Client Account Username** field. 2. In the **Web Client Account Password** field, type the desired password. 3. In the **Web Client Account Confirm password** field, retype the password. 4. Edit the **Service Account Username** field. 5. In the **Service Account Password** field, type the desired password. 6. In the **Service Account Confirm password** field, retype the password. If you create new Web client account and service account, Ivanti recommends using the default account user names the installation creates; `clientadmin` for the Web client account, and `serviceadmin` for the service account.
To use preexisting accounts:	1. Type the user name associated with the desired account in the **Web Client Account Username** field. 2. Type the password associated with the user name in the **Web Client Account Password** field. 3. Retype the password in the **Web Client Account Confirm password** field. 4. Type the user name associated with the desired account in the **Service Account Username** field. 5. Type the password associated with the service account user name in the **Service Account Password** field. 6. Retype the password in the **Service Account Confirm password** field Ivanti recommends creating new accounts. If using domain accounts, include the domain name as part of the user name (`DOMAIN\Username`). You may only use preexisting accounts if they meet the requirements defined in Defining the Web Client Account and Service Account.

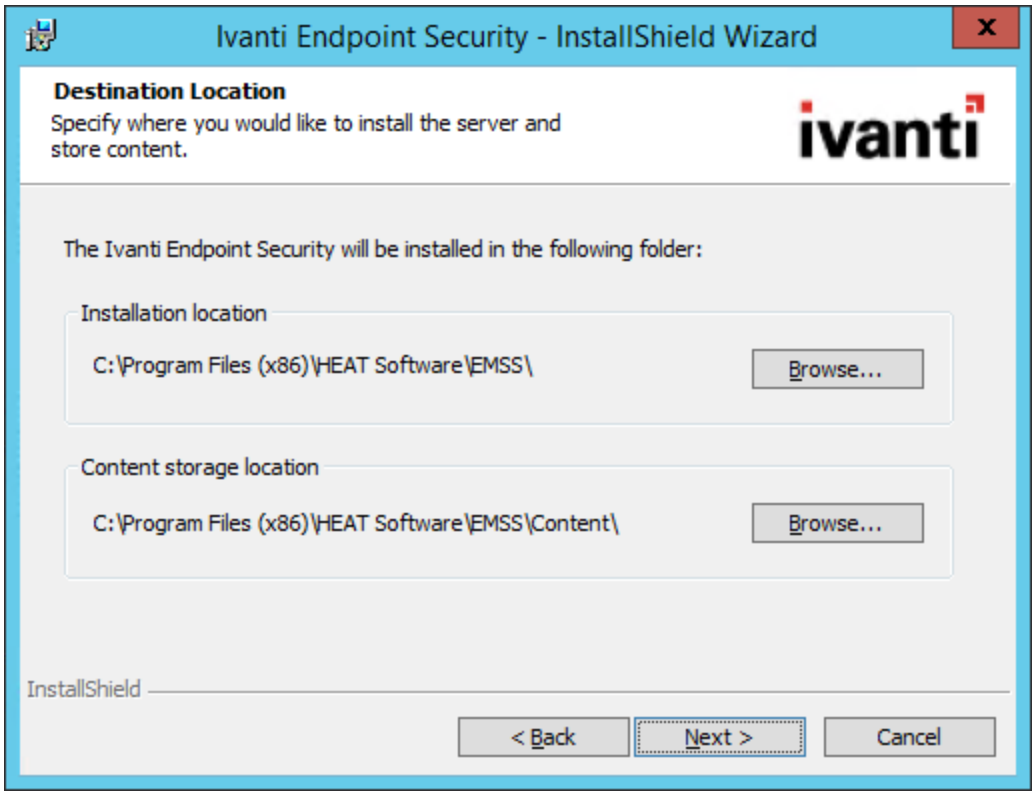
11. Click **Next**.



If required, acknowledge the creation of new accounts by clicking **OK**.
The SQL Server Instance page opens.

12. Select the **Install a new SQL Server instance** option.
13. **[Optional]** Type a new instance name in the **Instance Name** field.

14. Click **Next**.

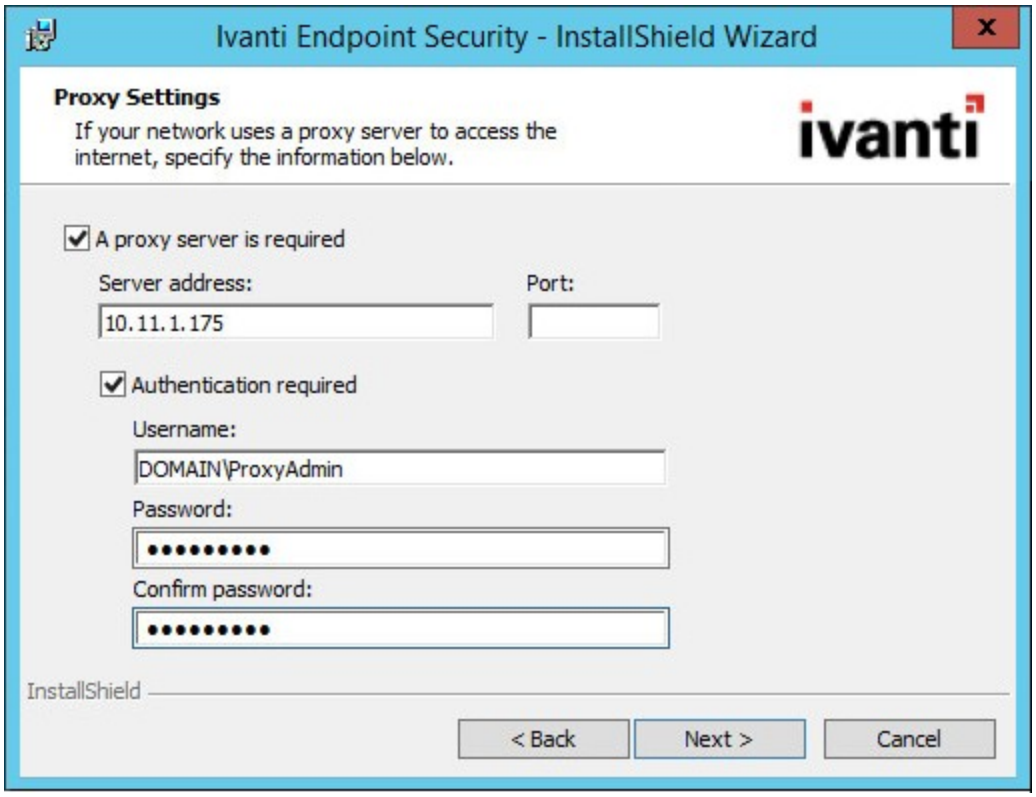


The Destination Location page opens.

15. [Optional] Change the Ivanti Endpoint Security installation location.
    a. Click **Browse**.
    b. Define the desired file path using either the **Look in** lists or the **Folder name** field.
    c. Click **OK**.
    The **Installation Folder** field reflects your changes.
16. [Optional] Change the Ivanti Endpoint Security content storage location.
The content storage location is the location where patches and other content items are downloaded. Ivanti recommends allocating at least 32 GB of storage space to content (plus an additional 10 GB if managing non-Windows endpoints).
    a. Click **Browse**.
    b. Define the desired file path using either the **Look in** lists or the **Folder name** field.
    c. Click **OK**.
    The **Content Storage Folder** field reflects your changes.

17. Click **Next**.
The Proxy Settings page opens.

Refer to the Ivanti Endpoint Security: Requirements Guide for a complete list of proxy types that Ivanti Endpoint Security supports.



If one or both of the storage directories defined on the *Destination Location* page does not contain the recommended available disk space, the *Proxy Settings* page does not immediately open. Rather, a dialog that lets you redefine the storage directories will open. Then after redefining the storage directories, the *Proxy Settings* page will open.

18. If your network uses a proxy server to access the Internet, select the **A proxy server is required** check box and type the applicable information in the following fields.

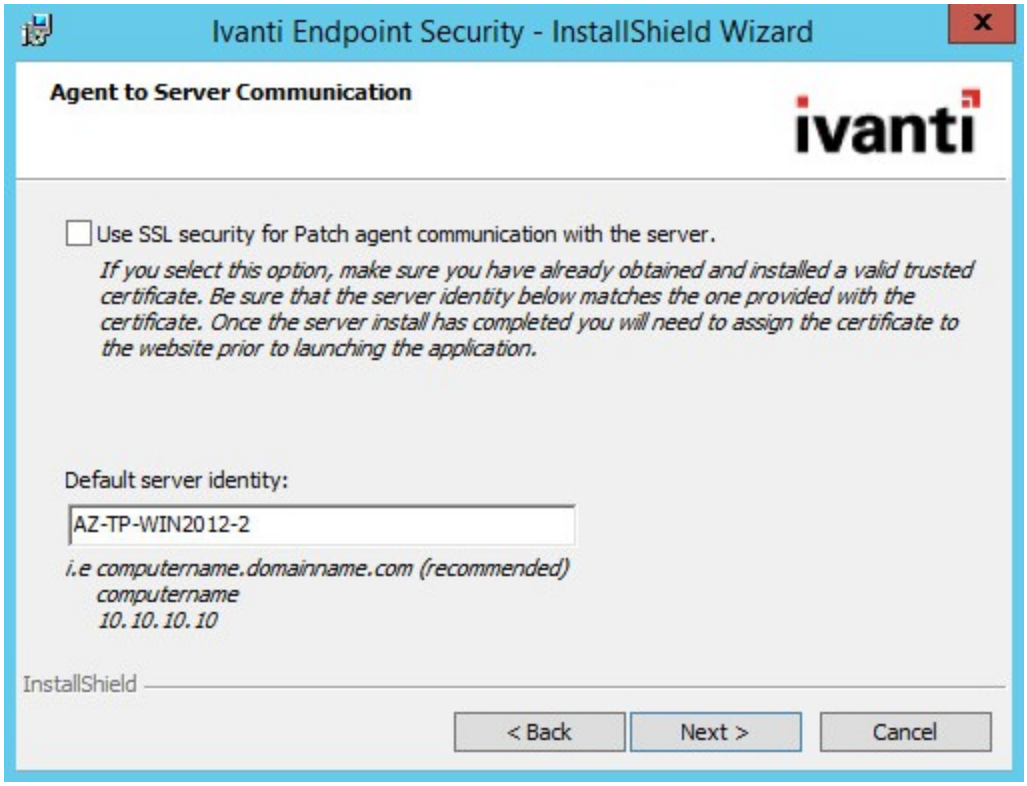
Field	Type
Server Address	The IP address of the applicable proxy server.
Port	The port number used for communication.

You can also configure Ivanti Endpoint Security to use a proxy following installation. Refer to *The Service Tab* in the Ivanti Endpoint Security User Guide for additional information on proxy communication.

19. If your network uses a proxy server to access the Internet, and that proxy requires authentication, select the **Authentication required**check box and type the applicable information in the following fields.

Field	Type
Username	A user name that authenticates with the proxy.
Password	The password associated with the user name.
Confirm Password	The password retyped.

20. Click **Next**.



The Agent to Server Communication page opens.

21. If you are using SSL for server and agent communication, select the **Use SSL security for Patch agent communication with the server** check box.

> You must possess an SSL certificate to implement SSL communication. Implementation of SSL communication during installation is optional. This feature can be implemented following installation.

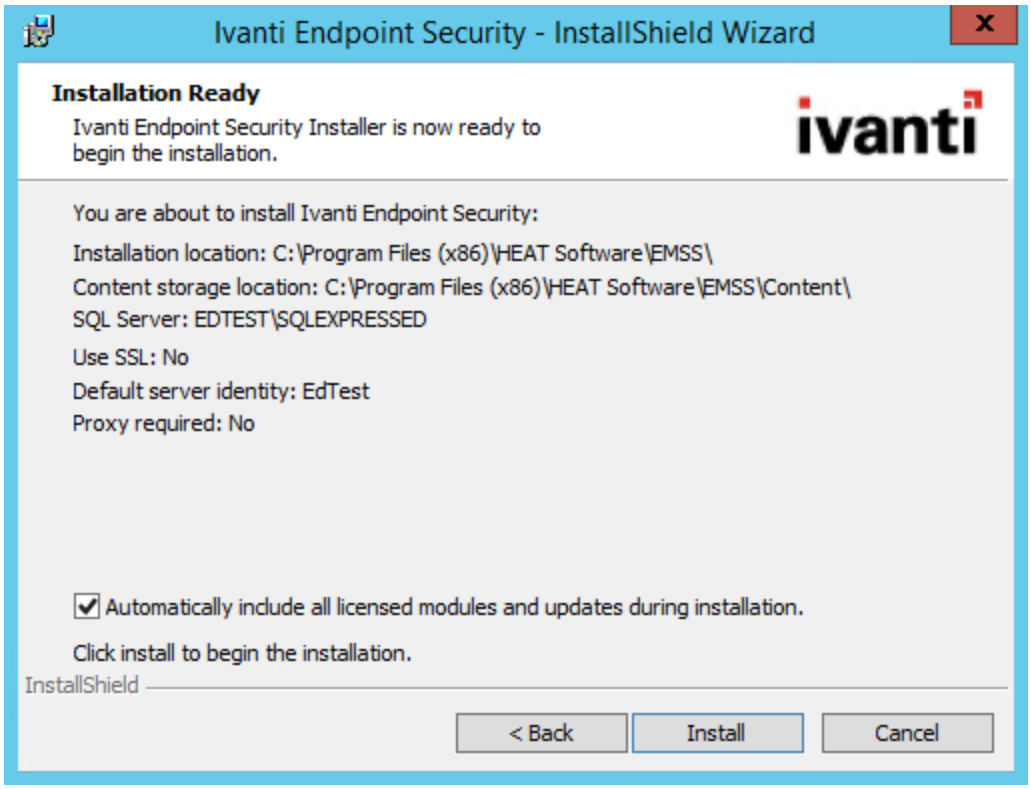
22. In the **Default server identity** field, type the name of your server in one of the following formats:

    - DNS name(`computername.domainname.com`)
    - Computer name(`computername`)
    - IP address(`10.10.10.10`)

    During agent registration, the Ivanti Endpoint Security agents use this name to identify the server.

    > If you are using SSL, the server name that you type in the field must match the server named on your certificate.

23. Click **Next**.



The Installation Ready page opens.

24. [Optional] If you only want to install core components, clear the **Automatically include all licensed modules and updates during installation** check box.

> You may use the Ivanti Installation Manager after the initial installation of Ivanti Endpoint Security to install additional components. For additional information, refer to *Using Ivanti Installation Manager* in the Ivanti Endpoint Security User Guide.

25. Review the installation information and click **Install** to begin the installation of Ivanti Endpoint Security. This process may take severalminutes.

    Important: During installation, do not attempt to access the Ivanti Endpoint Security Web site. Accessing the Web site during installation can cause installation errors.

26. After installation completes, click **Finish**.
27. Acknowledge the notification that appears by clicking **OK**.

    The credentials you use to log in to the Ivanti Endpoint Security Web site for the first time are the credentials that you used when you logged into the server initially.

    Result: Ivanti Endpoint Security is installed and can now be accessed.

After Completing This Task:

Proceed to one of the following procedures based on selections made during installation.

- If your server will use SSL, finish Appendix B: Configuring Your Server to use SSL.
- If your server will not use SSL, proceed to Logging In to Ivanti Endpoint Security.

Installing Using an Existing SQL Server Instance (either locally or remotely)

You can configure your Ivanti Endpoint Security installation to use a SQL Server instance that exists either locally or remotely.

Prerequisites:

- Complete Downloading Ivanti Endpoint Security.
- As applicable to your network environment, you have gathered the information and completed the tasks itemized in the Appendix D: Installation Checklist.
- If you are installing using SSL, complete the first portion of Appendix B: Configuring Your Server to use SSL.
- If you are installing using a remote instance of SQL Server, complete Configuring SQL Server to Accept Remote Connections.

Additionally, if you are installing using a remote instance of SQL Server, and no instances of SQL Server exist locally, complete Installing Using a Remote SQL Server Instance (with no local instance) rather than this procedure.

1. If installing using a remote instance of SQL Server, complete Creating Remote Accounts.

   If using preexisting accounts, you may skip completion of this step.

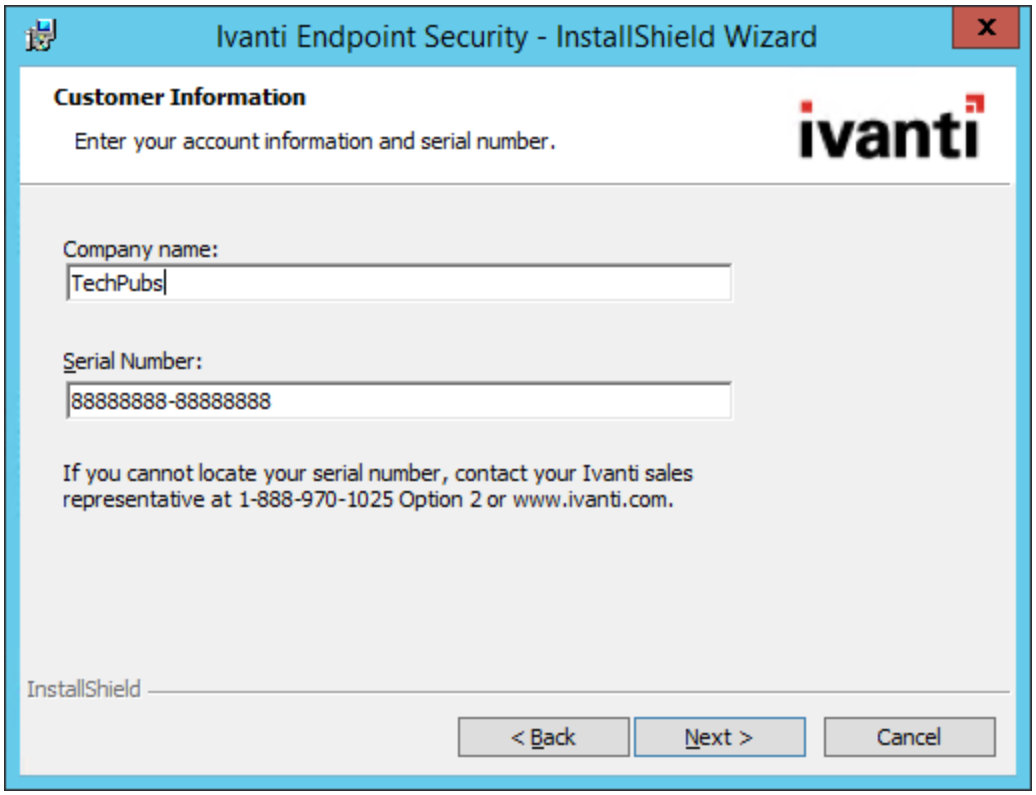
2. Using either a local or domain account with system administrator privileges, log in to the server on which you will install Ivanti Endpoint Security.
3. Stop or disable any AntiVirus products (such as McAfee, Trend-micro, Symantec, and so on) running on your server.

   An AntiVirus product can prevent processes from running correctly during the installation. Therefore, to ensure a successful installation, all AntiVirus services must be stopped or disabled prior to running the Ivanti Endpoint Security installer.

4. Double-click the Ivanti Endpoint Security installer at the location defined during the download. The Ivanti Endpoint Security *InstallShield Wizard* opens and begins extracting files. This process may take several minutes.
5. If prompted, install prerequisites and reboot your server.
   The installer reopens by itself after the reboot.
6. Click **Next**.
   The License Agreement page opens.

   Click **Print** for a hard copy of the license agreement.

7. Review the **License Agreement** and select the **I accept the terms of the license agreement** option.
8. Click **Next**.
   The Customer Information page opens.



9. Type the applicable information in the following fields:

Field	Description
Company Name	Your company name.
Serial Number	Your Ivanti Endpoint Security serial number. Your serial number is two groups of eight alphanumeric characters. Letters are not case sensitive. If you cannot locate your serial number, obtain it by contacting the Ivanti Sales Support (sales@ivanti.com).

Tip: Retain your serial number following installation, as it is necessary if a reinstall of the Ivanti Endpoint Security server is needed.

10. Click **Next**.
    A new page or dialog opens.

Page/Dialog	Step
If the *Question* dialog opens:	Click **Yes** to start network discovery services. The following services are necessary to use discovery features within Ivanti Endpoint Security: • DNS Client • Function Discovery Resource Location • SSDP Discover • UPnP Device Host
If the *Required IIS Features* page opens:	Your server does not have the required IIS features installed. Click **Install Features** to install the features and proceed. On Windows Server 2008, the default installation of IIS lacks components necessary for Ivanti Endpoint Security. The Ivanti Endpoint Security installer installs the following IIS components if not present: • Static Content • Default Document • HTTP Errors • ASP.NET • .NET Extensibility • ASP • ISAPI Extensions • ISAPI Filters • Basic Authentication • Windows Authentication • Static Content Compression • Dynamic Content Compression
If the *System Requirements* page opens:	Your server does not meet the minimum installation requirements. • If you receive only system requirement *warnings*, you may proceed with installation by clicking **Next**. Ivanti recommends resolving warnings before proceeding with installation. When installing on a virtual platform you will likely receive a warning about the CPU requirements since the installer is unable to identify the processor in a virtual environment. • If you receive any system requirement *failures*, you must cancel the installation, resolve these failures, and then restart installation. Click **View all Failures/Warnings** for detailed information about prerequisite status deficiencies.

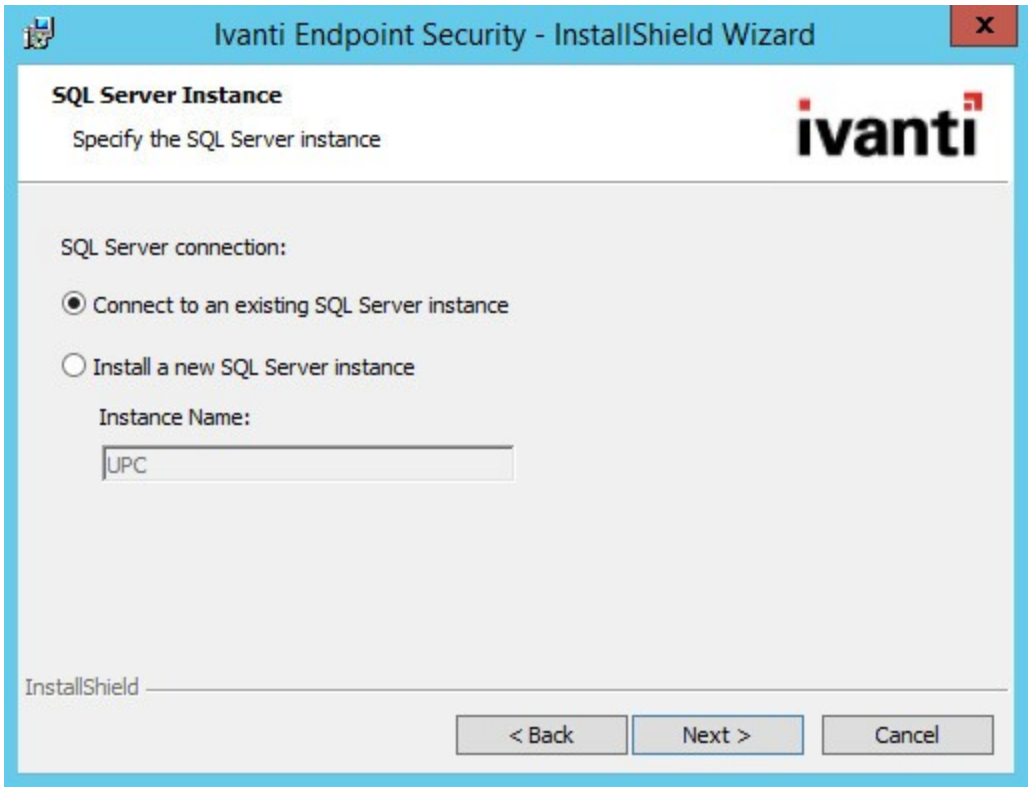
Page/Dialog	Step
If the *Service Accounts* page opens:	Proceed to the next step.

11. Define the Web client account and service account that Ivanti Endpoint Security will use. Define these accounts based on how you are configuring your Ivanti Endpoint Security server.

Option	Steps
If your install will use a local SQL Server instance:	Define the credentials for two new user accounts (which are created by the installer). 1. In the **Web Client Account Username** field, edit the user name. 2. In the **Web Client Account Password** field, type a password. 3. In the **Web Client Account Confirm password** field, retype the password. 4. In the **Service Account Username** field, edit the user name. 5. In the **Service Account Password** field, type a password. 6. In the **Service Account Confirm password** field, retype the password.
If your install will use a remote SQL Server instance:	Define the credentials for the two user accounts created while completing Creating Remote Accounts. 1. In the **Web Client Account Username** field, type the user name of the Web client account on your SQL Server. 2. In the **Web Client Account Password** field, type the password of the Web client account on your SQL Server. 3. In the **Web Client Confirm password** field, retype the password. 4. In the **Service Account Username** field, type the user name of the service account on your SQL Server. 5. In the **Service Account Password** field, type the password of the service account on your SQL Server. 6. In the **Service Account Confirm password** field, retype the password.  **Important:** The Web client account and the service account credentials must be identical on both the SQL Server and the Ivanti Endpoint Security server. If they are not, you cannot access the Ivanti Endpoint Security Web site.

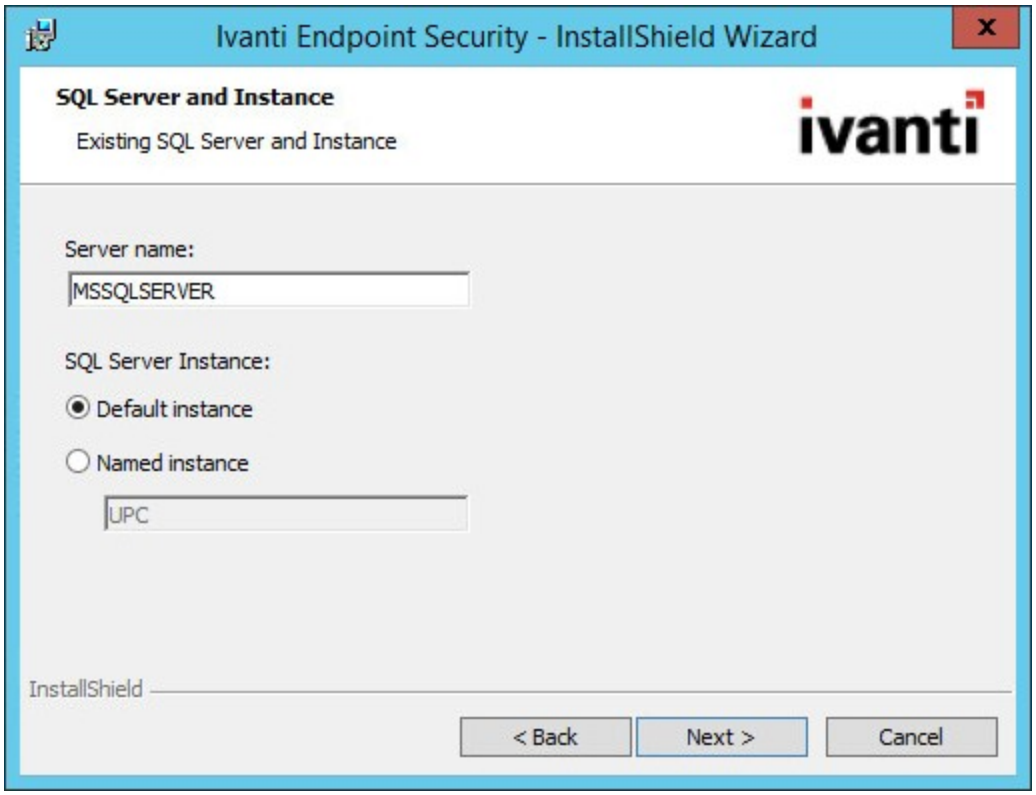
Option	Steps
If your install will use a local or remote SQL Server instance that uses preexisting accounts as the Web Client and Service Accounts:	Define the credentials for the preexisting accounts. 1. Type the user name associated with the desired account in the **Web Client Account Username** field. 2. Type the password associated with the user name in the **Web Client Account Password** field. 3. Retype the password in the **Web Client Account Confirm password** field. 4. Type the user name associated with the desired account in the **Service Account Username** field. 5. Type the password associated with the service account user name in the **Service Account Password** field. 6. Retype the password in the **Service Account Confirm password** field. **Important:** You can use either local or domain accounts. If using domain accounts, include the domain name as part of the user name (`DOMAIN\username`). Additionally, preexisting accounts may only be used if they meet the requirements listed in Defining the Web Client Account and Service Account.

12. Click **Next**.
    If required, acknowledge the creation of new accounts by clicking **OK**.
    The SQL Server Instance page opens.



13. Ensure the **Connect to an existing SQL Server instance** option is selected.

14. Click **Next**.
    The SQL Server and Instance page opens. Use this page to define the SQL Server instance you will use with Ivanti Endpoint Security.



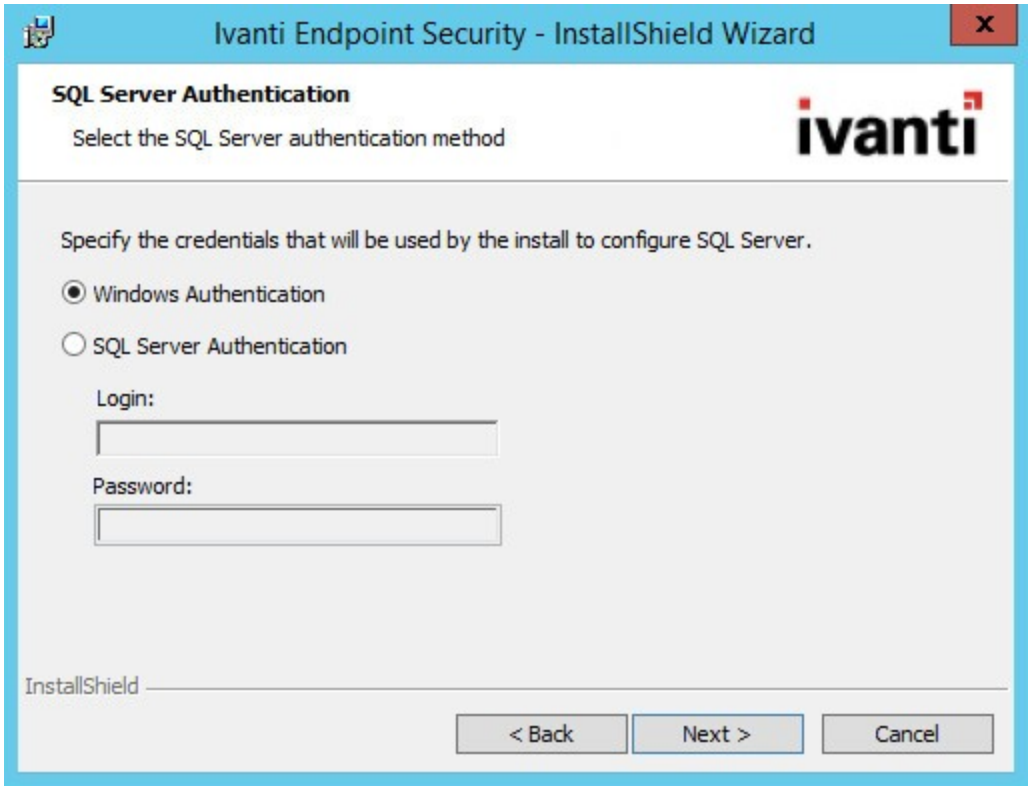
15. Select a **Server Location**.
    Select one of the following options.

Option	Steps
To use a locally installed existing SQL Server instance:	Select the **On this machine (local)** option.
To use a remotely installed existing SQL Server instance:	1. Select the **On another machine (remote)** option. 2. Type the server name (*not* the IP address) in the **Server name** field. If you must define an IP address, either map the IP address to the server name in the hosts file or create an alias using SQL Server Configuration Manager.

16. Select a **SQL Server Instance**.
    Select one of the following options:

Option	Steps
To use a default instance of SQL Server:	Select the **Default instance** option.
To use a named instance of SQL Server:	1. Select the **Named instance** option. 2. If the SQL Server instance is local, select it from the list. If the SQL Server instance is remote, type its name in the field.

17. Click **Next**.
The SQL Server Authentication page opens.



18. Define the credentials that will be used to access the SQL Server instance (based upon its authentication mode).
Select from the following options:

Option	Steps
To use Windows authentication:	Select the **Windows Authentication** option.
To use SQL Server authentication:	1. Select the **SQL Server Authentication** option. 2. Type a user name that will validate with the SQL Server instance in the **Login** field.

Option	Steps
	3. Type the password associated with the user in the **Password** field.

The credentials used to access the SQL Server instance must be assigned the **sysadmin** system role within Microsoft SQL Server Management Studio. If the user account defined is not assigned this role, the *The credentials provided do not have sufficient privileges to continue* dialog opens after clicking **Next**. You need to define a user account and assigned the **sysadmin** system role before you can continue.

If you cannot be assigned this role due to network security policies and procedures that split administrative duties between a Ivanti Endpoint Security administrator and a SQL Server administrator, refer to Installing Ivanti Endpoint Security (Separate Ivanti Endpoint Security and SQL Server Admins).

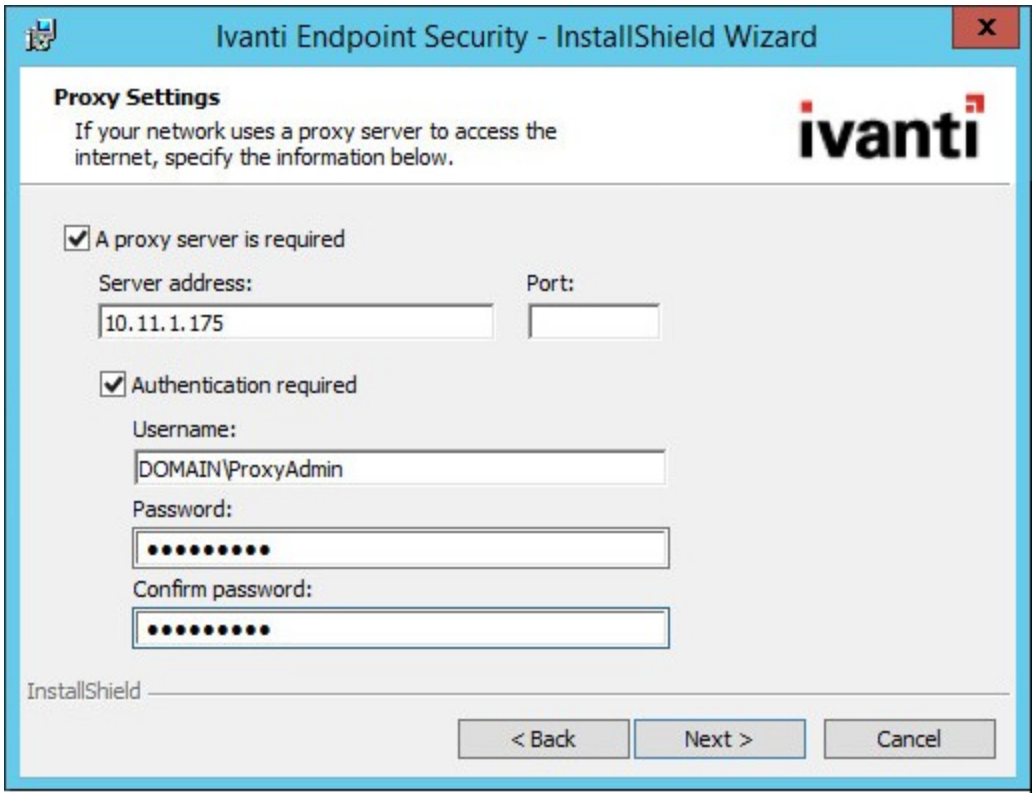
19. Click **Next**.
A new page opens.

Page	Steps
If the *Destination Location* page opens:	Click **Next** and proceed to the next step.
If the *SQL Server Configuration Requirements* page opens:	The pre-installed instance of SQL Server is not configured to work with Ivanti Endpoint Security. • If you only receive SQL Server configuration requirement *informationals or warnings*, click **Next** to continue (the Ivanti Endpoint Security installation will automatically reconfigure SQL Server). Proceed to the next step. • If you receive any SQL Server configuration requirement *failures*, you must cancel the installation, resolve the failures, and then proceed with the installation. Click **View Configuration Detail** for detailed information about SQL Server configuration status requirements.

20. [Optional] Change the Ivanti Endpoint Security installation location.
    a. Click **Browse**.
    b. Define the desired file path using either the **Look in** lists or the **Folder name** field.
    c. Click **OK**.
    The **Installation Folder** field reflects your changes.

21. [Optional] Change the Ivanti Endpoint Security content storage location.
    The content storage location is the location where patches and other content items are downloaded. Ivanti recommends allocating at least 32 GB of storage space to content (plus an additional 10 GB if managing non-Windows endpoints).
    a. Click **Browse**.
    b. Define the desired file path using either the **Look in** lists or the **Folder name** field.
    c. Click **OK**.
    The **Content Storage Location** field reflects your changes.
22. Click **Next**.
    The Proxy Settings page opens.

Refer to the Ivanti Endpoint Security: Requirements Guide for a complete list of proxy types that Ivanti Endpoint Security supports.



If one or both of the storage directories defined on the Destination Location page does not contain the recommended available disk space, the Proxy Settings page does not immediately open. Rather, a dialog that lets you redefine the storage directories opens. Then after redefining the storage directories, the Proxy Settings page opens.

23. If your network uses a proxy server to access the Internet, select the **A proxy server is required** check box and type the applicable information in the following fields.

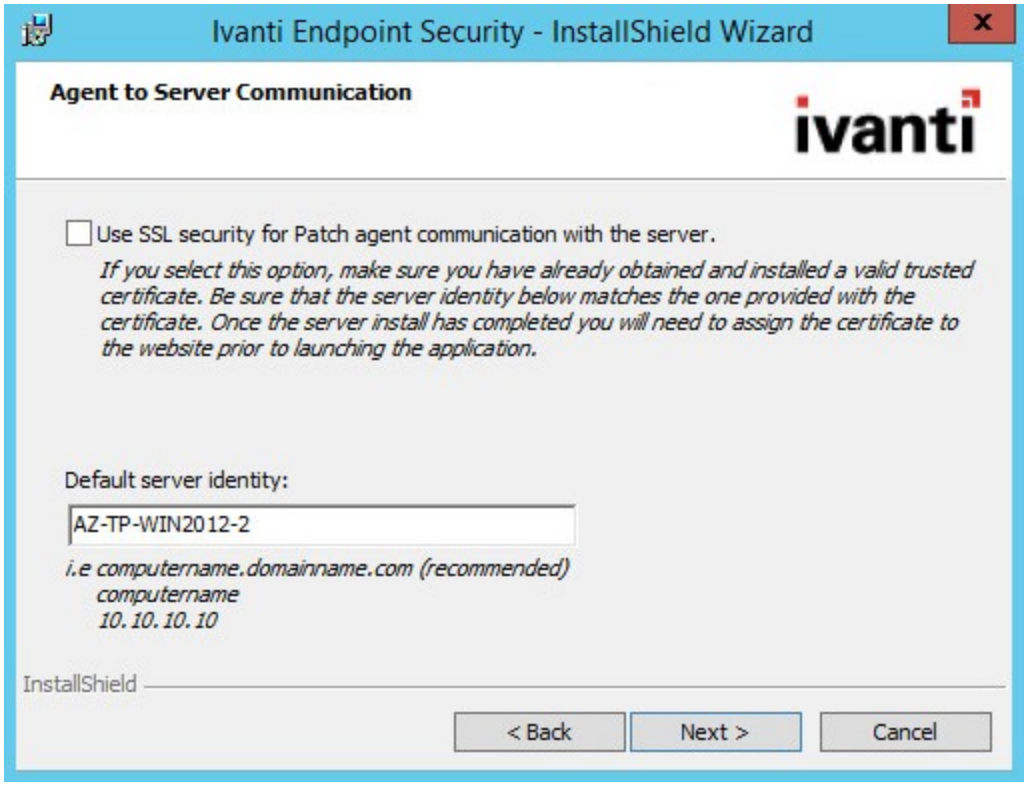
Field	Type
Server Address	The IP address of the applicable proxy server.
Port	The port number used for communication.

You can also configure Ivanti Endpoint Security to use a proxy following installation. Refer to *The Service Tab* in the Ivanti Endpoint Security User Guide for additional information on proxy communication.

24. If your network uses a proxy server to access the Internet, and that proxy requires authentication, select the **Authentication required** check box and type the applicable information in the following fields.

Field	Type
Username	A user name that authenticates with the proxy.
Password	The password associated with the user name.
Confirm Password	The password retyped.

25. Click **Next**.



The Agent to Server Communication page opens.

26. If you are using SSL for server and agent communication, select the **Use SSL security for Patch agent communication with the server** check box.

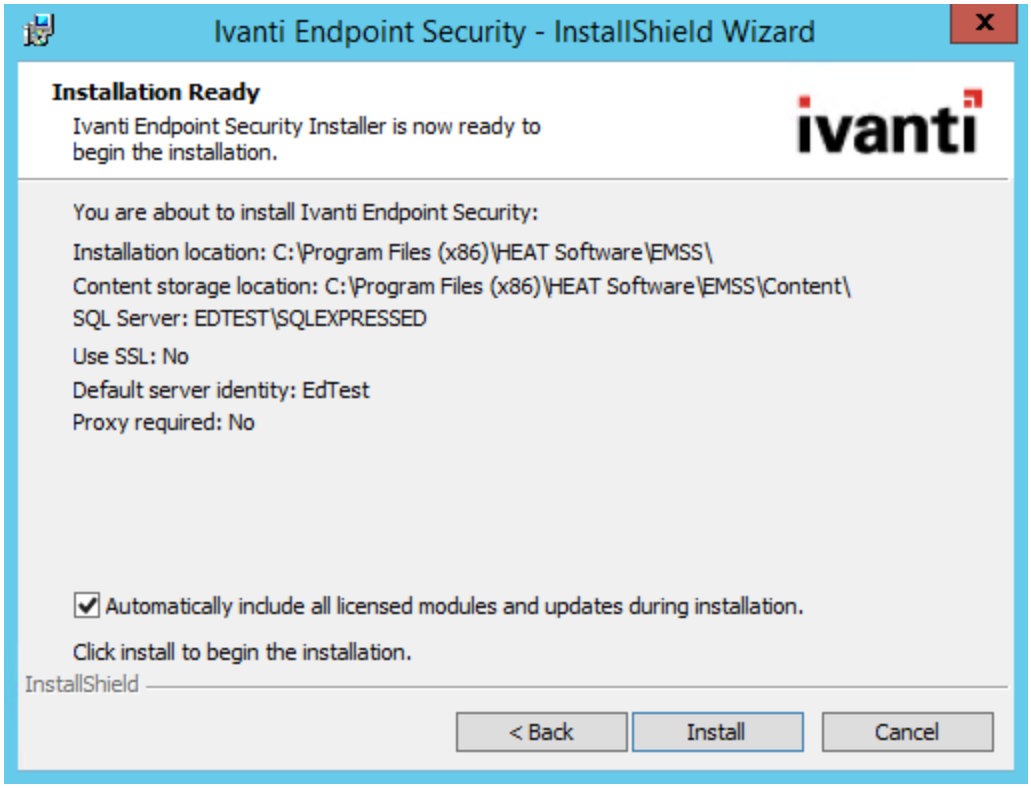
> You must possess an SSL certificate to implement SSL communication. Implementation of SSL communication during installation is optional. This feature can be implemented following installation.

27. In the **Default server identity** field, type the name of your server in one of the following formats:
    - DNS name (`computername.domainname.com`)
    - Computer name (`computername`)
    - IP address (`10.10.10.10`)

    During agent registration, the Ivanti Endpoint Security agents use this name to identify the server.

> If you are using SSL, the server name that you type in the field must match the server named on your certificate.

28. Click **Next**.
    The Installation Ready page opens.



29. [Optional] If you only want to install core components, clear the **Automatically include all licensed modules and updates during installation** check box.

You may use the Ivanti Installation Manager after the initial installation of Ivanti Endpoint Security to install additional components. For additional information, refer to *Using Ivanti Installation Manager* in the Ivanti Endpoint Security User Guide.

30. Review the installation information and click **Install** to begin the installation of Ivanti Endpoint Security. This process may take several minutes.

Important: During installation, do not attempt to access the Ivanti Endpoint Security Web site. Accessing the Web site during installation can cause installation errors.

31. After installation completes, click **Finish**.
32. Acknowledge the notification that appears by clicking **OK**.
    The credentials you use to log in to the Ivanti Endpoint Security Web site for the first time are the credentials that you used when you logged into the server initially.
    Ivanti Endpoint Security is installed and can now be accessed.

After Completing This Task:

Proceed to one of the following procedures based on selections made during installation.

- If your server will use SSL, finish Appendix B: Configuring Your Server to use SSL.
- If your server will not use SSL, proceed to Logging In to Ivanti Endpoint Security.

Installing Using a Remote SQL Server Instance (with no local instance)

Installing Ivanti Endpoint Security using an existing remote SQL Server instance differs slightly when no SQL Server instance exists locally.

Prerequisites:

- Complete Downloading Ivanti Endpoint Security.
- As applicable to your network environment, you have gathered the information and completed the tasks itemized in the Appendix D: Installation Checklist.
- Complete Configuring SQL Server to Accept Remote Connections
- If installing using SSL, complete the first portion of Appendix B: Configuring Your Server to use SSL.

1. Complete Creating Remote Accounts.

   If using preexisting accounts, you may skip completion of this procedure.

2. Using either a local or domain account with system administrator privileges, log in to the server on which you will install Ivanti Endpoint Security.
3. Stop or disable any AntiVirus products (such as McAfee, Trend-micro, Symantec, and so on) running on your server.

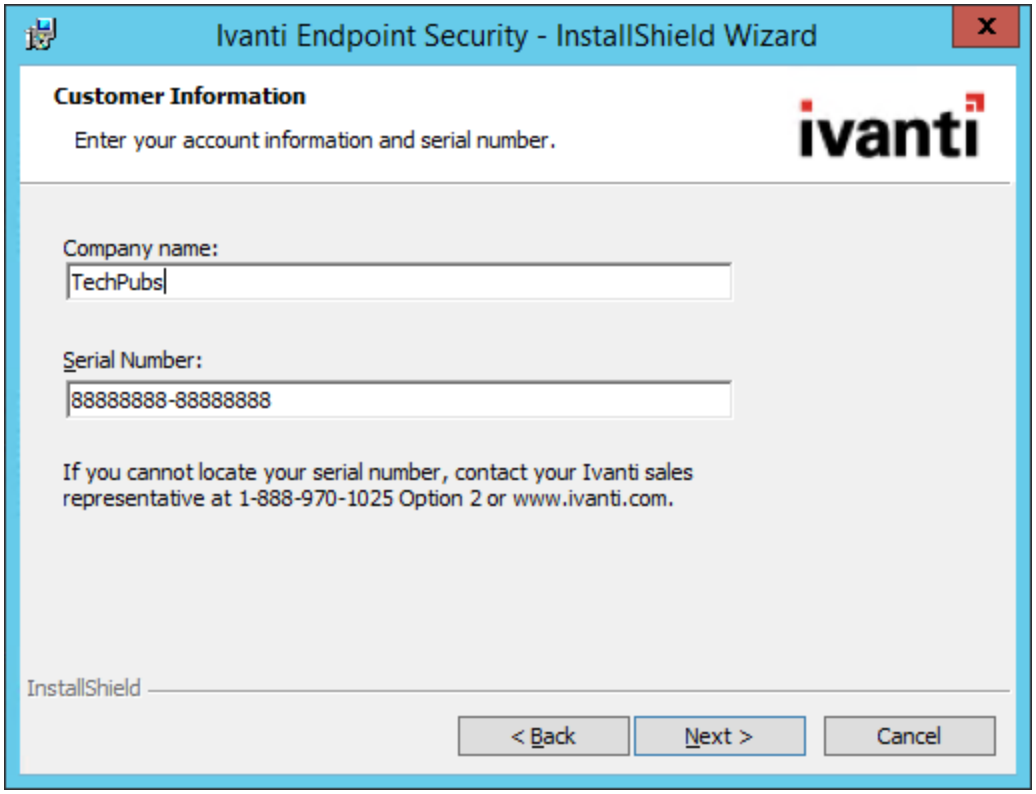
   An AntiVirus product can prevent processes from running correctly during the installation. Therefore, to ensure a successful installation, all AntiVirus services must be stopped or disabled prior to running the Ivanti Endpoint Security installer.

4. Double-click the Ivanti Endpoint Security installer at the location defined during the download.
   The Ivanti Endpoint Security InstallShield Wizard opens and begins extracting files.
   This process may take several minutes.
5. If prompted, install prerequisites and reboot your server.
   The installer reopens by itself after the reboot.
6. Click **Next**.
   The License Agreement page opens.

   Tip: Click **Print** for a hard copy of the license agreement.

7. Review the **License Agreement** and select the **I accept the terms of the license agreement** option.

8. Click **Next**.
   The Customer Information page opens.



9. Type the applicable information in the following fields:

Field	Description
Company Name	Your company name.
Serial Number	Your Ivanti Endpoint Security serial number. Your serial number is two groups of eight alphanumeric characters. Letters are not case sensitive. If you cannot locate your serial number, obtain it by contacting the Ivanti Sales Support (sales@ivanti.com).

Tip: Retain your serial number following installation, as it is necessary if a reinstall of the Ivanti Endpoint Security server is needed.

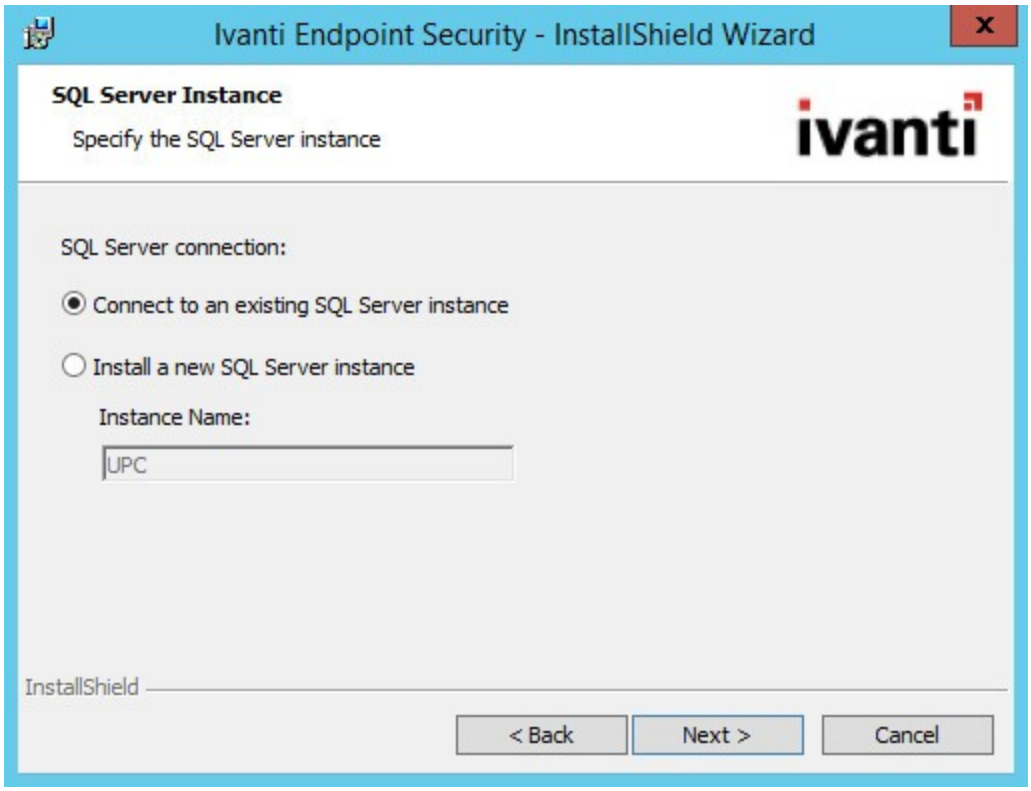
10. Click **Next**.
    A new page or dialog opens.

Page/Dialog	Step
If the Question dialog opens:	Click **Yes** to start network discovery services. The following services are necessary to use discovery features within Ivanti Endpoint Security: • **DNS Client** • **Function Discovery Resource Location** • **SSDP Discover** • **UPnP Device Host**
If the Required IIS Features page opens:	Your server does not have the required IIS features installed. Click Install Features to install the features and proceed. On Windows Server 2008, the default installation of IIS lacks components necessary for Ivanti Endpoint Security. The Ivanti Endpoint Security installer installs the following IIS components if not present: • **Static Content** • **Default Document** • **HTTP Errors** • **ASP.NET** • **.NET Extensibility** • **ASP** • **ISAPI Extensions** • **ISAPI Filters** • **Basic Authentication** • **Windows Authentication** • **Static Content Compression** • **Dynamic Content Compression**
If the System Requirements page opens:	Your server does not meet the minimum installation requirements. • If you receive only system requirement *warnings*, you may proceed with installation by clicking **Next**. Ivanti recommends resolving warnings before proceeding with installation.  When installing on a virtual platform you will likely receive a warning about the CPU requirements since the installer is unable to identify the processor in a virtual environment. • If you receive any system requirement *failures*, you must cancel the installation, resolve these failures, and then restart installation.  Click **View all Failures/Warnings** for detailed information about prerequisite status deficiencies.
If the Service Accounts page opens:	Proceed to the next step.

11. Define the Web client account and service account that your Ivanti Endpoint Security server will use.
    Select from the following options.

Option	Steps
To duplicate the accounts on your SQL Server:	1. In the **Web Client Account Username** field, type the user name of the Web client account on your SQL Server. 2. In the **Web Client Account Password** field, type the password of the Web client account on your SQL Server. 3. In the **Web Client Account Confirm password** field, retype the password. 4. In the **Service Account Username** field, type the user name of the service account on your SQL Server. 5. In the **Service Account Password** field, type the password of the service account on your SQL Server. 6. In the **Service Account Confirm password** field, retype the password. **Important:** The Web client account and the server account credentials must be identical on both the SQL Server and the Ivanti Endpoint Security server. If they are not, you cannot access the Ivanti Endpoint Security Web site.
To use preexisting accounts:	1. Type the user name associated with the desired account in the **Web Client Account Username** field. 2. Type the password associated with the user name in the **Web Client Account Password** field. 3. Retype the password in the **Web Client Account Confirm password** field. 4. Type the user name associated with the desired account in the **Service Account Username** field. 5. Type the password associated with the service account user name in the **Service Account Password** field. 6. Retype the password in the **Service Account Confirm password** field. **Important:** You can use either local or domain accounts. If using domain accounts, include the domain name as part of the user name (`DOMAIN\username`). Additionally, preexisting accounts may only be used if they meet the requirements listed in Defining the Web Client Account and Service Account.

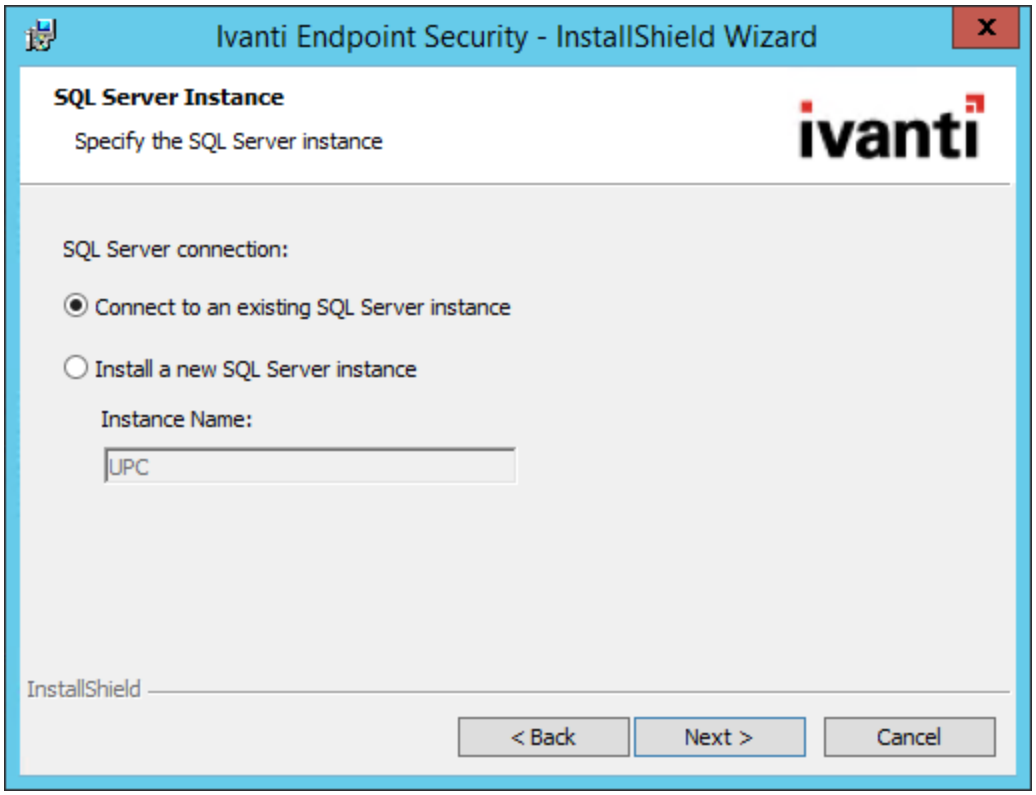
12. Click **Next**.



If required, acknowledge the creation of new accounts by clicking **OK**.
The SQL Server Instance Page opens.

13. Ensure the **Connect to an existing SQL Server instance** option is selected.

14. Click **Next**.



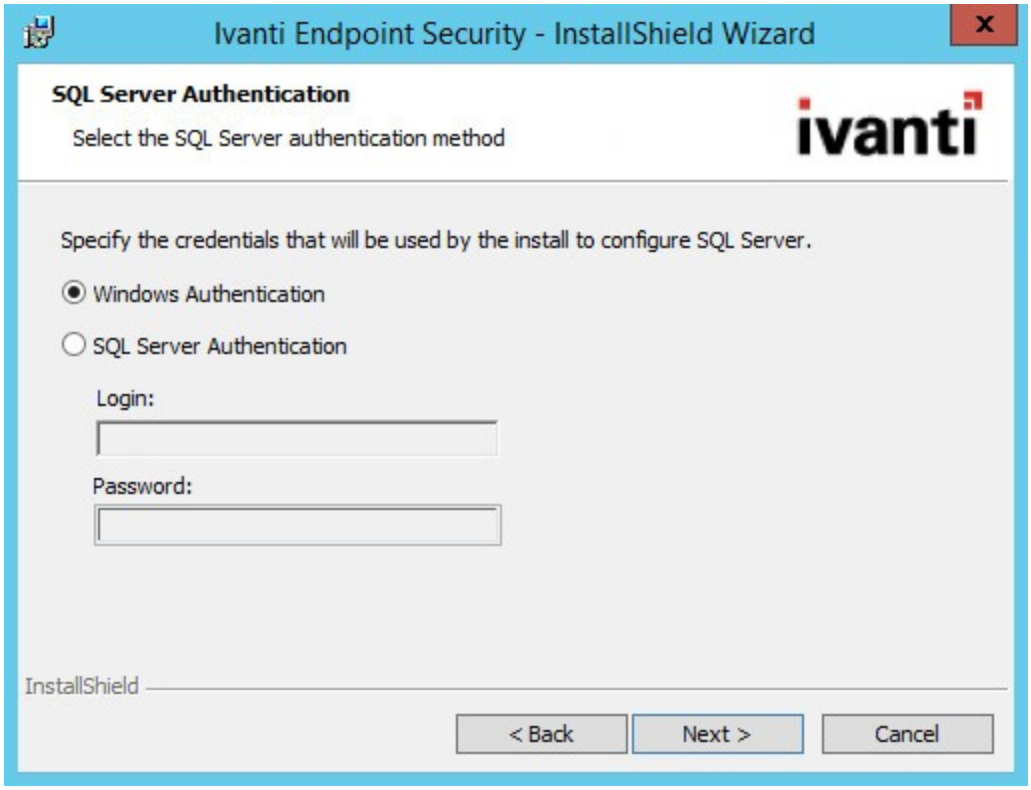
The SQL Server and Instance page opens.

Important: If **Server Location** options are available from this page, you are performing the wrong procedure. Instead, perform Installing Using an Existing SQL Server Instance (either locally or remotely).

15. Type the name (*not* the IP address) of the server hosting the remote SQL Server instance in the **Server name** field.
16. Based on the SQL Server instance you are using, select a **SQL Server Instance** option. Select one of the following options.

Option	Steps
To use a default SQL Server instance:	Select the **Default instance** option.
To use a named SQL Server instance:	1. Select the **Named instance** option. 2. Type the instance name in the **Named instance** field.

17. Click **Next**.
    The SQL Server Authentication page opens.



18. Define the credentials that will be used to access the SQL Server instance (based upon its authentication mode).
    Select from the following options:

Option	Steps
To use Windows authentication:	Select the **Windows Authentication** option.
To use SQL Server authentication:	1. Select the **SQL Server Authentication** option. 2. Type a user name that will validate with the SQL Server instance in the **Login** field. 3. Type the password associated with the user in the Password field.

The credentials used to access the SQL Server instance must be assigned the **sysadmin** system role within Microsoft SQL Server Management Studio. If the user account defined is not assigned this role, the *The credentials provided do not have sufficient privileges to continue* dialog opens after clicking **Next**. You need to define a user account and assigned the **sysadmin** system role before you can continue.

If you cannot be assigned this role due to network security policies and procedures that split administrative duties between a Ivanti Endpoint Security administrator and a SQL Server administrator, refer to Installing Ivanti Endpoint Security (Separate Ivanti Endpoint Security and SQL Server Admins).

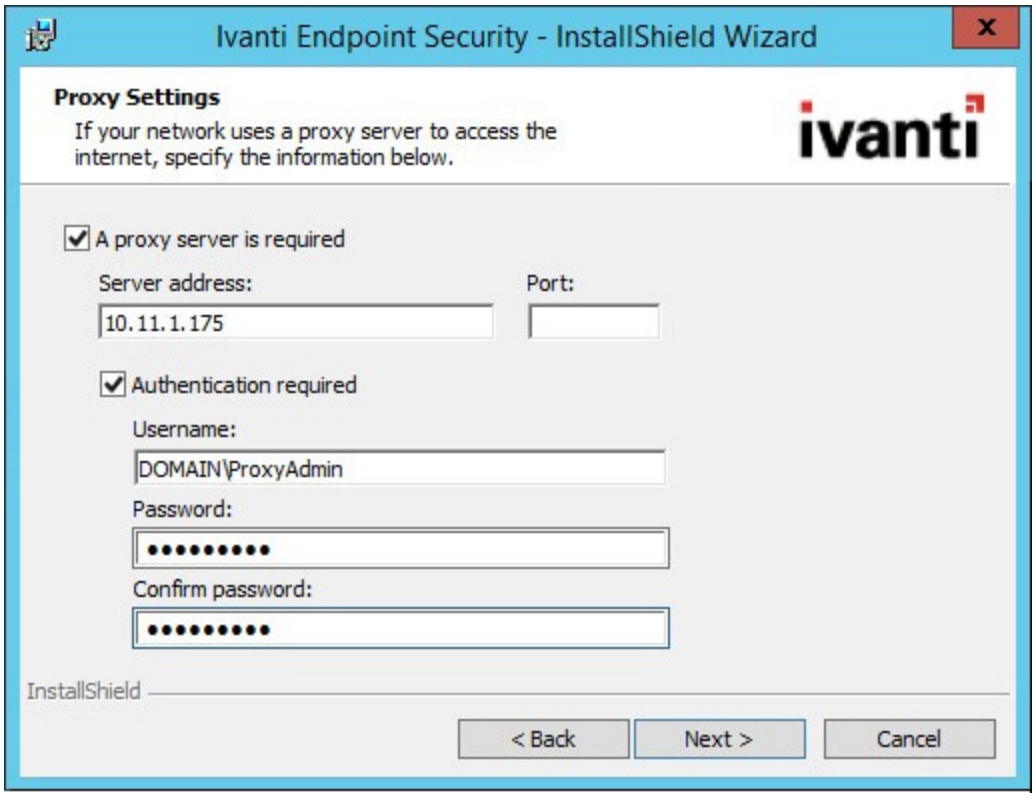
19. Click **Next**.
A new page opens.

Page	Steps
If the Destination Location page opens:	Click **Next** and proceed to the next step.
If the SQL Server Configuration Requirements page opens:	The pre-installed instance of SQL Server is not configured to work with Ivanti Endpoint Security. • If you only receive SQL Server configuration requirement *informationals or warnings*, click **Next** to continue (the Ivanti Endpoint Security installation will automatically reconfigure SQL Server). Proceed to the next step. • If you receive any SQL Server configuration requirement *failures*, you must cancel the installation, resolve the failures, and then proceed with the installation. Click **View Configuration Detail** for detailed information about SQL Server configuration status requirements.

20. [Optional] Change the Ivanti Endpoint Security content storage location.
The content storage location is the location where patches and other content items are downloaded. Ivanti recommends allocating at least 32 GB of storage space to content (plus an additional 10 GB if managing non-Windows endpoints).
    a. Click **Browse**.
    b. Define the desired file path using either the **Look in** lists or the **Folder name** field.
    c. Click **OK**.
    The **Content Storage Location** field reflects your changes.

21. Click **Next**.
The Proxy Settings page opens.

Refer to the Ivanti Endpoint Security: Requirements Guide for a complete list of proxy types that Ivanti Endpoint Security supports.



If one or both of the storage directories defined on the Destination Location page does not contain the recommended available disk space, the Proxy Settings page does not immediately open. Rather, a dialog that lets you redefine the storage directories opens. Then after redefining the storage directories, the Proxy Settings page opens.

22. If your network uses a proxy server to access the Internet, select the **A proxy server is required** check box and type the applicable information in the following fields.

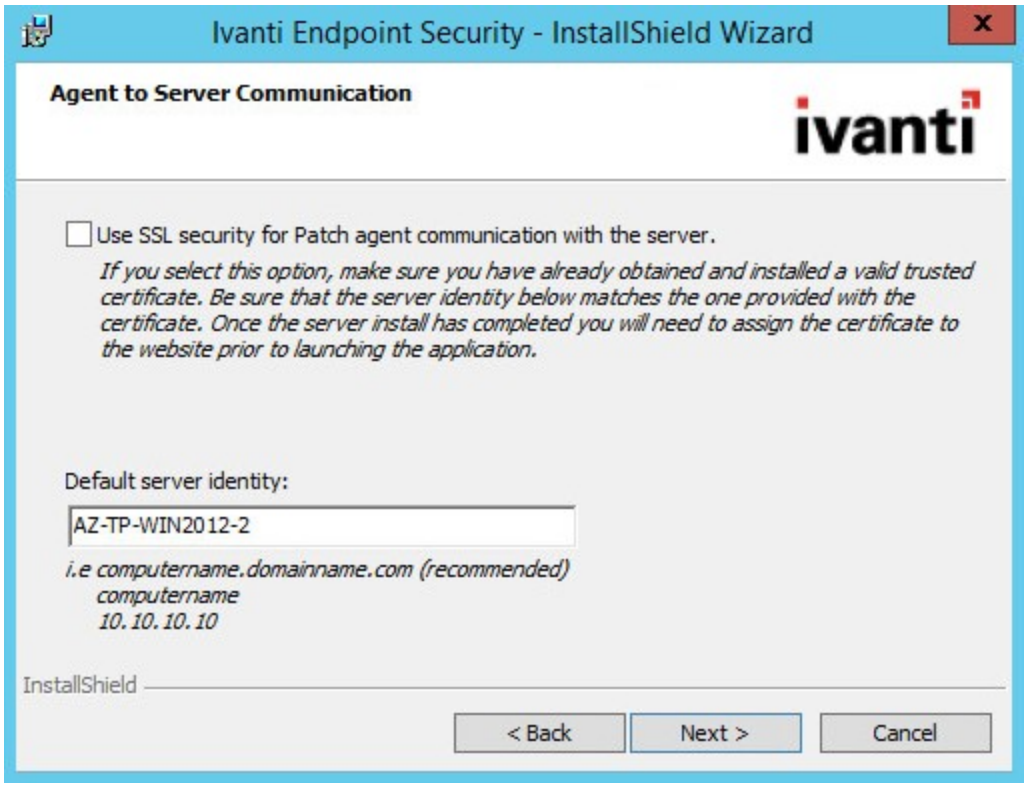
Field	Type
Server Address	The IP address of the applicable proxy server.
Port	The port number used for communication.

You can also configure Ivanti Endpoint Security to use a proxy following installation. Refer to *The Service Tab* in the Ivanti Endpoint Security User Guide for additional information on proxy communication.

23. If your network uses a proxy server to access the Internet, and that proxy requires authentication, select the Authentication required check box and type the applicable information in the following fields.

Field	Type
Username	A user name that authenticates with the proxy.
Password	The password associated with the user name.
Confirm Password	The password retyped.

24. Click **Next**.
The Agent to Server Communication page opens.



25. If you are using SSL for server and agent communication, select the **Use SSL security for Patch agent communication with the server** check box.

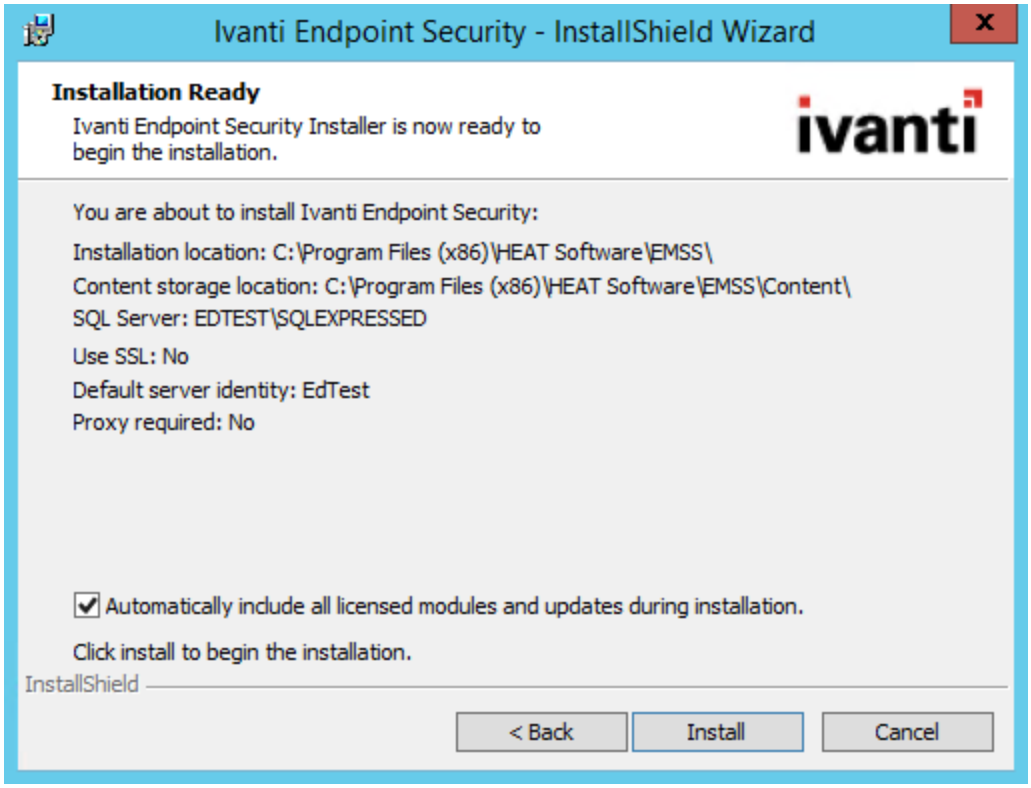
> You must possess an SSL certificate to implement SSL communication. Implementation of SSL communication during installation is optional. This feature can be implemented following installation.

26. In the **Default server identity** field, type the name of your server in one of the following formats:
    - DNS name (`computername.domainname.com`)
    - Computer name (`computername`)
    - IP address (`10.10.10.10`)

    During agent registration, the Ivanti Endpoint Security agents use this name to identify the server.

    > If you are using SSL, the server name that you type in the field must match the server named on your certificate.

27. Click **Next**.
    The Installation Ready page opens.



28. [Optional] If you want to install only core components, clear the **Automatically include all licensed modules and updates during installation** check box.

    > You may use the Ivanti Installation Manager after the initial installation of Ivanti Endpoint Security to install additional components. For additional information, refer to *Using Ivanti Installation Manager* in the Ivanti Endpoint Security User Guide.

29. Review the installation information and click Install to begin the installation of Ivanti Endpoint Security. This process may take several minutes.

    Important: During installation, do not attempt to access the Ivanti Endpoint Security Web site. Accessing the Web site during installation can cause installation errors.

30. After installation completes, click **Finish**.
31. Acknowledge the notification that appears by clicking **OK**.
    The credentials you use to log in to the Ivanti Endpoint Security Web site for the first time are the credentials that you used when you logged into the server initially.
    Ivanti Endpoint Security is installed and can now be accessed.

After Completing This Task:

Proceed to one of the following procedures based on selections made during installation.

- If your server will use SSL, finish Appendix B: Configuring Your Server to use SSL.
- If your server will not use SSL, proceed to Logging In to Ivanti Endpoint Security.

Installing Ivanti Endpoint Security (Separate Ivanti Endpoint Security and SQL Server Admins)

When installing Ivanti Endpoint Security using a remote SQL Server instance in a large network environment, a special installation procedure that splits install duties between the Ivanti Endpoint Security and the SQL Server administrator may be necessary.

When installing Ivanti Endpoint Security (Ivanti Endpoint Security) using a remote SQL Server instance, the user account you use to access the SQL server instance must be assigned the *sysadmin* role within Microsoft SQL Server Management Studio. However, Ivanti recognizes that in larger network environments, the administrator installing Ivanti Endpoint Security may not be able to obtain this role due to IT policies and procedures; only the SQL Server administrator can access the applicable SQL instance.

Therefore, under these circumstances, the network administrator and SQL Server administrator must cooperate to complete Ivanti Endpoint Security installation. To install Ivanti Endpoint Security in this type of environment, the installation is broken in to three separate procedures.

Procedure Portion	Description
"Beginning Installation (Part I)" on the next page	Performed by the Ivanti Endpoint Security administrator on the target Ivanti Endpoint Security server, this procedure begins the product installation. During this procedure, the Ivanti Endpoint Security administrator reviews a licence agreement, defines registration information, defines the remote SQL Server location, and creates a script to modify the SQL Server instance.
"Creating Components on SQL Server (Part II)" on page 65	Performed by the SQL Server administrator on the server hosting the applicable SQL instance, this procedure creates the user accounts necessary to operate Ivanti Endpoint Security and then runs the script created in part I. This script modifies the SQL Server instance to accommodate Ivanti Endpoint Security installation for an administrator without *sysadmin* rights within Microsoft SQL Server.
"Completing Installation (Part III)" on page 68	Performed by the Ivanti Endpoint Security administrator on the target Ivanti Endpoint Security server, this procedure completes Ivanti Endpoint Security installation. This procedure defines where the Ivanti Endpoint Security server and its content will be stored, whether the server will use a proxy server, and whether the server will use SSL.

Beginning Installation (Part I)

The Ivanti Endpoint Security administrator performs the first portion of the install procedure. At the end of this portion, the installer creates a script that is delivered to the SQL Server administrator.

Prerequisites:

- Complete Downloading Ivanti Endpoint Security.
- As applicable to your network environment, you have gathered the information and completed the tasks itemized in the Appendix D: Installation Checklist.
- Complete Configuring SQL Server to Accept Remote Connections.
- If installing using SSL, complete the first portion of Appendix B: Configuring Your Server to use SSL.

This first portion of this installation procedure is performed by the Ivanti Endpoint Security (Ivanti Endpoint Security) administrator on the target Ivanti Endpoint Security server.

1. Using either a local or domain account with system administrator privileges, log in to the server on which you will install Ivanti Endpoint Security.
2. Stop or disable any AntiVirus products (such as McAfee, Trend-micro, Symantec, and so on) running on your server.

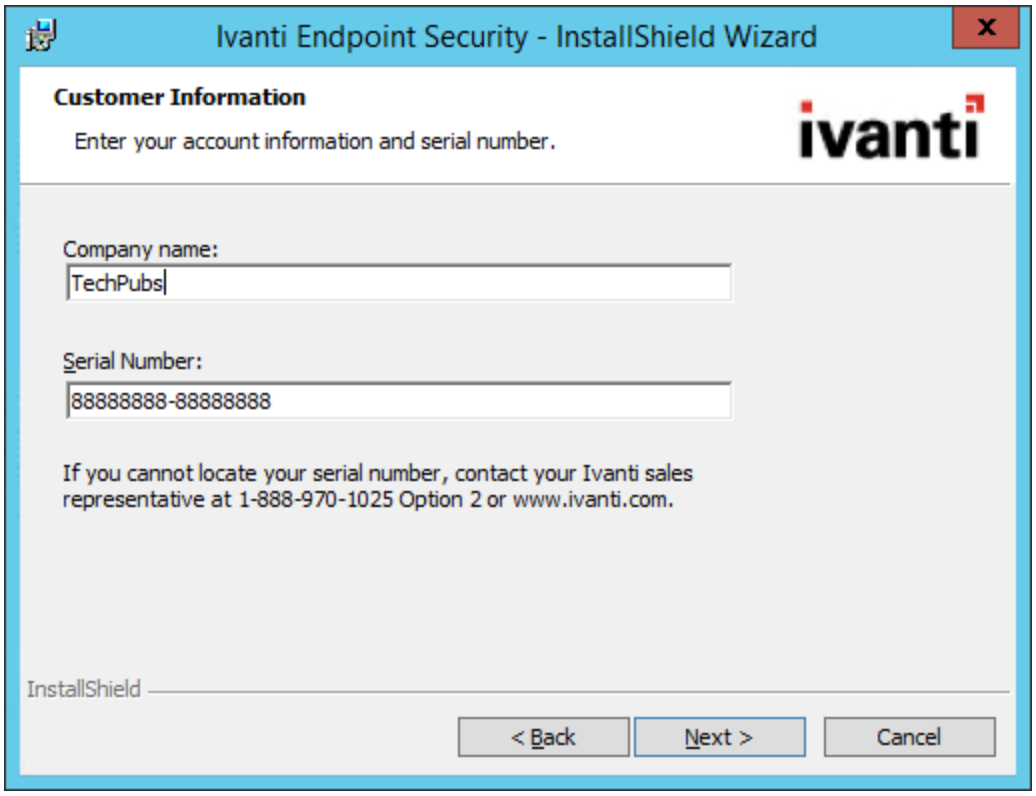
   An AntiVirus product can prevent processes from running correctly during the installation. Therefore, to ensure a successful installation, all AntiVirus services must be stopped or disabled prior to running the Ivanti Endpoint Security installer.

3. Double-click the Ivanti Endpoint Security installer at the location defined during the download. The Ivanti Endpoint Security InstallShield Wizard opens and begins extracting files. This process may take several minutes.
4. If prompted, install prerequisites and reboot your server.
   The installer reopens by itself after the reboot.
5. Click **Next**.
   The License Agreement page opens.

   Tip: Click **Print** for a hard copy of the license agreement.

6. Review the **License Agreement** and select the **I accept the terms of the license agreement** option.

7. Click **Next**.
   The Customer Information page opens.



8. Type the applicable information in the following fields:

Field	Description
Company Name	Your company name.
Serial Number	Your Ivanti Endpoint Security serial number. Your serial number is two groups of eight alphanumeric characters. Letters are not case sensitive. If you cannot locate your serial number, obtain it by contacting the Ivanti Sales Support (sales@ivanti.com).

Tip: Retain your serial number following installation, as it is necessary if a reinstall of the Ivanti Endpoint Security server is needed.

9. Click **Next**.
   A new page or dialog opens.

Page/Dialog	Step
If the Question dialog opens:	Click **Yes** to start network discovery services. The following services are necessary to use discovery features within Ivanti Endpoint Security: • **DNS Client** • **Function Discovery Resource Location** • **SSDP Discover** • **UPnP Device Host**
If the Required IIS Features page opens:	Your server does not have the required IIS features installed. Click **Install Features** to install the features and proceed. On Windows Server 2008, the default installation of IIS lacks components necessary for Ivanti Endpoint Security. The Ivanti Endpoint Security installer installs the following IIS components if not present: • **Static Content** • **Default Document** • **HTTP Errors** • **ASP.NET** • **.NET Extensibility** • **ASP** • **ISAPI Extensions** • **ISAPI Filters** • **Basic Authentication** • **Windows Authentication** • **Static Content Compression** • **Dynamic Content Compression**
If the System Requirements page opens:	Your server does not meet the minimum installation requirements. • If you receive only system requirement *warnings*, you may proceed with installation by clicking **Next**. Ivanti recommends resolving warnings before proceeding with installation. When installing on a virtual platform you will likely receive a warning about the CPU requirements since the installer is unable to identify the processor in a virtual environment. • If you receive any system requirement *failures*, you must cancel the installation, resolve these failures, and then restart installation. Click **View all Failures/Warnings** for detailed information about prerequisite status deficiencies.
If the Service Accounts page opens:	Proceed to the next step.

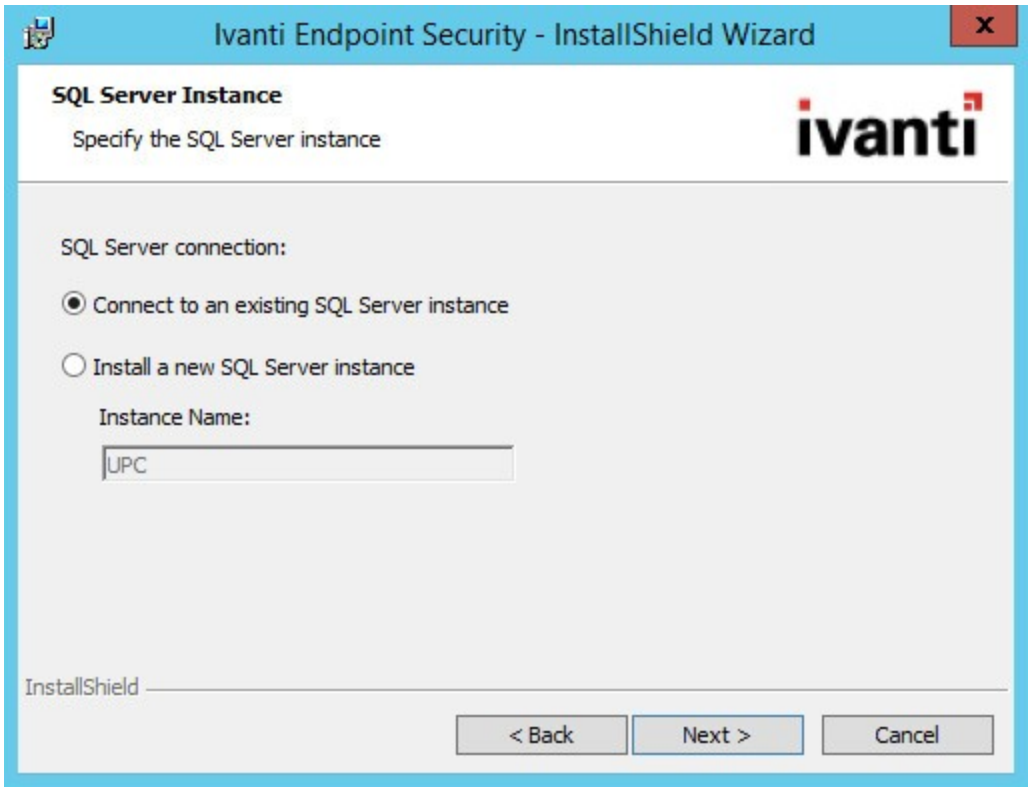
10. Create the Web client account and server accounts that Ivanti Endpoint Security will use.

> **Important:** Preexisting accounts or domain accounts cannot be used for this installation procedure.

    a. [Optional] Edit the **Web Client Account Username** field.
    b. In the **Web Client Account Password** field, type the desired password.
    c. In the **Web Client Account Confirm password** field, retype the password.
    d. [Optional] Edit the **Service Account Username** field.
    e. In the **Service Account Password** field, type the desired password.
    f. In the **Service Account Confirm password** field, retype the password.

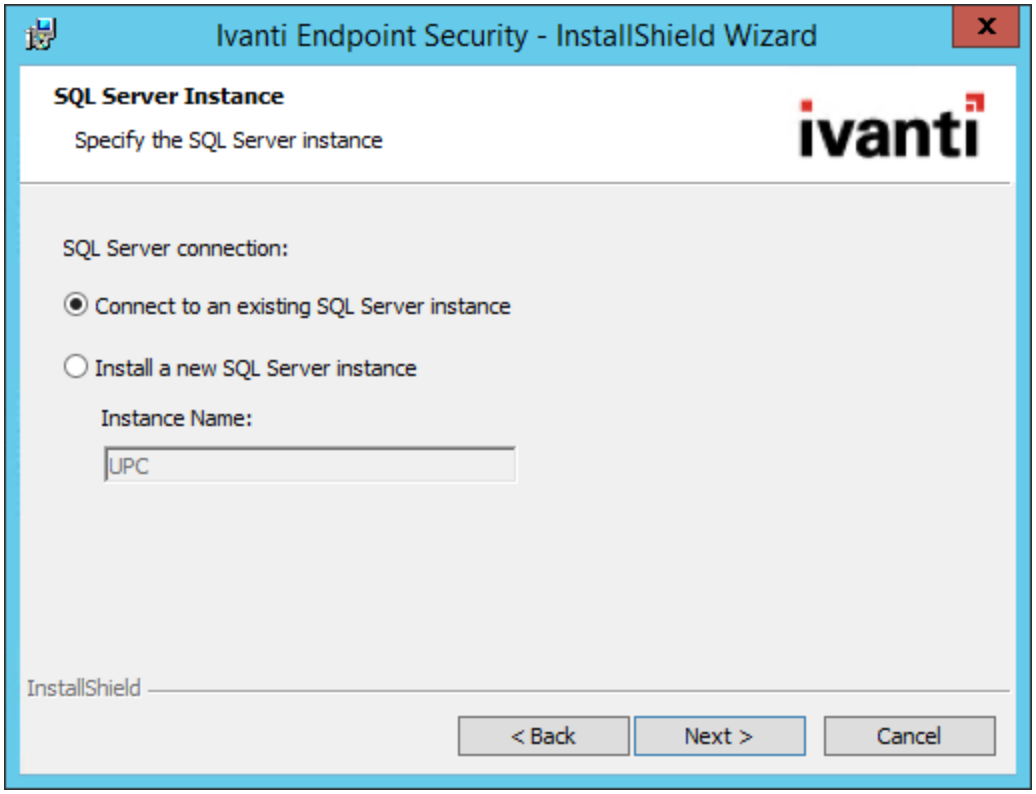
> Ivanti recommends using the default account user names created by the installation.

11. Click **Next**.
If required, acknowledge the creation of new accounts by clicking **OK**.
The SQL Server Instance Page opens.



12. Ensure the **Connect to an existing SQL Server instance** option is selected.

13. Click **Next**.
    The SQL Server and Instance page opens.

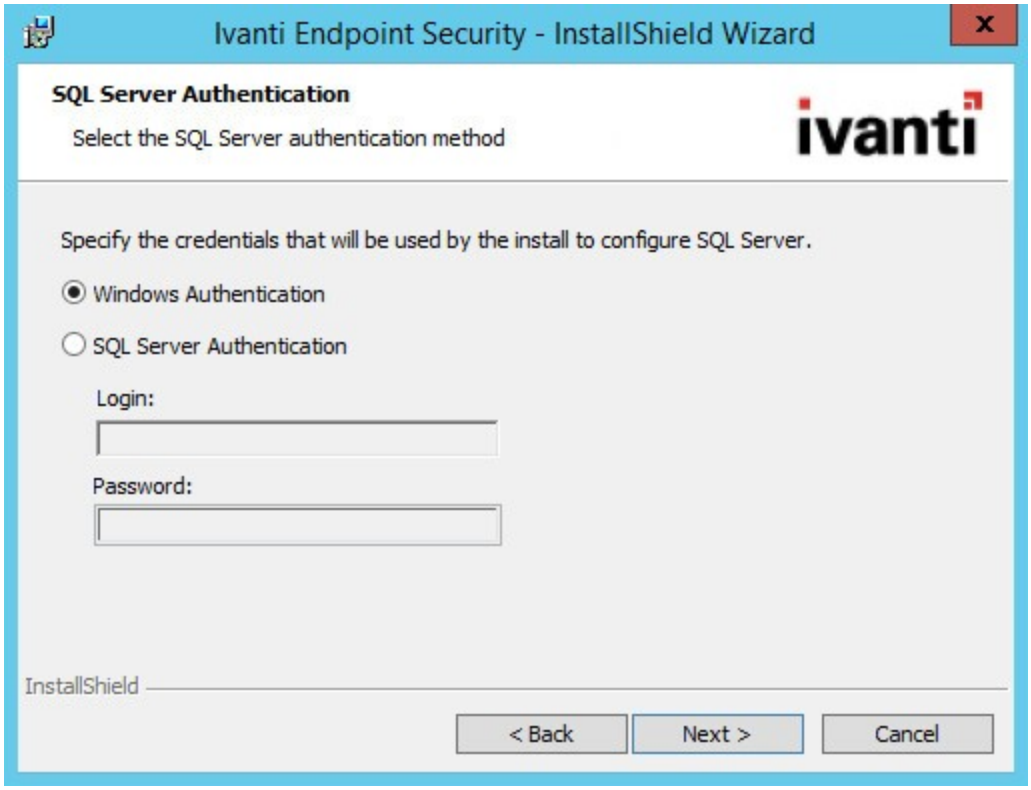


Important: If **Server Location** options are available from this page, you are performing the wrong procedure. Instead, perform Installing Using an Existing SQL Server Instance (either locally or remotely).

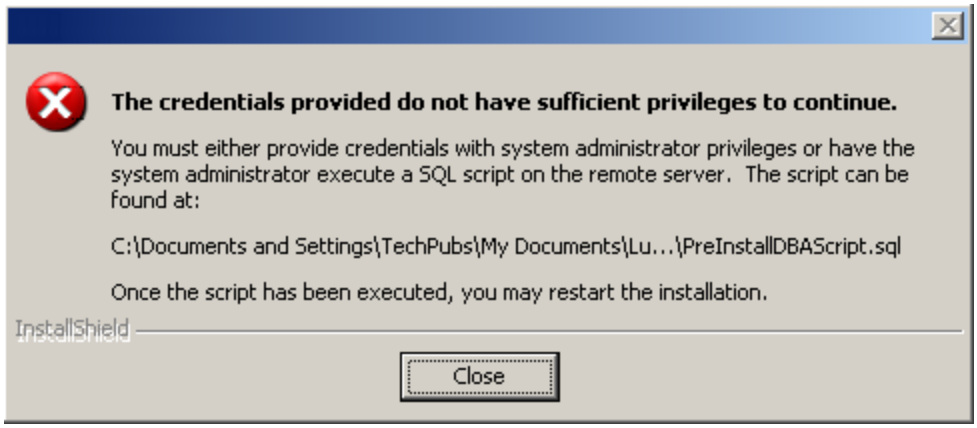
14. Type the name (*not* the IP address) of the server hosting the remote SQL Server instance in the **Server name** field.
15. Based on the SQL Server instance you are using, select a **SQL Server Instance** option.
    Select one of the following options.

Option	Steps
To use a default SQL Server instance:	Select the **Default instance** option.
To use a named SQL Server instance:	1. Select the **Named instance** option. 2. Type the instance name in the **Named instance** field.

16. Click **Next**.
    The SQL Server Authentication page opens.



17. Click **Next**.
    The credentials provided do not have sufficient privileges to continue dialog opens.



18. Note where the script is located and click Close.
19. Leave the installer open on its current page.
    You will continue from this point during the last portion of the procedure.
20. Deliver the script to your SQL Server administrator.

After Completing This Task:

Have your SQL Server administrator complete Creating Components on SQL Server (Part II).

Creating Components on SQL Server (Part II)

The SQL Server administrator performs this portion of the install procedure, which installs components on the SQL Server instance necessary for Ivanti Endpoint Security to function. These components are installed via the script your Ivanti Endpoint Security administrator delivers.

Prerequisites:

- Complete "Configuring SQL Server to Accept Remote Connections" on page 79.
- Complete "Configuring Windows Firewall for SQL Server Instance Access" on page 80.
- Obtain the script created by the Ivanti Endpoint Security (Ivanti Endpoint Security) installation from your network Ivanti Endpoint Security administrator and ensure it is on your SQL Server.
- Review the script to ensure it coincides with your IT department's policies and procedures.

This second portion of the installation procedure is performed by the SQL Server administrator on your existing remote instance of SQL Server.

If you have any questions and/or require additional assistance, contact Ivanti support at https://forums.ivanti.com/s/contactsupport.

1. Log in to your SQL Server using an account with administrative privileges. This account should also be assigned the **sysadmin** server role within Microsoft SQL Server Management Studio.
2. Create three user accounts.

   Important: Preexisting accounts or domain accounts cannot be used for this installation procedure.

   The first account you will create is identical to the user account used to begin the installation of Ivanti Endpoint Security. This account will be granted a login to the Ivanti Endpoint Security databases and assigned the *db_owner* role within Microsoft SQL Server Mangement Studio.

   The second and third accounts created are the Web client account and the service account. These accounts are used to operate components critical to Ivanti Endpoint Security.

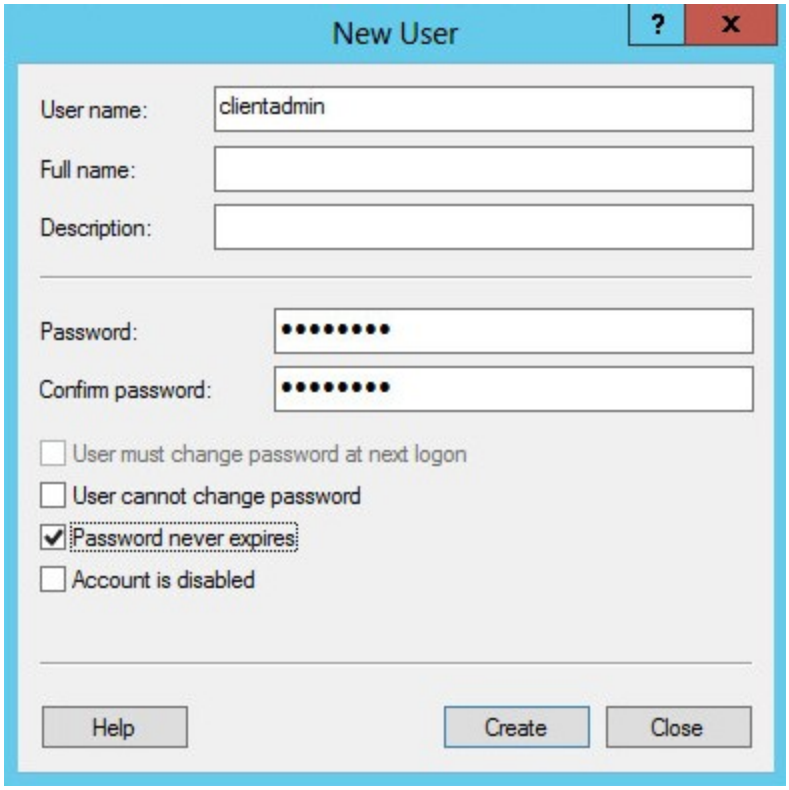
   Important: The credentials for each of these accounts must match their respective accounts on the Ivanti Endpoint Security target server. Consult your network administrator for the credentials for each account. If these accounts are not identical, Ivanti Endpoint Security will not function correctly.

   Complete the following substeps to create the account:

   a. Select **Start > Administrative Tools > Computer Management**.
   The Computer Management dialog opens.

   b. Expand the directory tree structure to **Users (Computer Mangement [local] > System Tools >Local Users and Groups > Users)**.

c. Right-click **Users** and select **New User**.
The New User dialog opens.



d. Create a user account identical to the user account used to begin installation of Ivanti Endpoint Security.
   - In the **User name** field, type the applicable user name.
   - In the **Password** field, type the applicable password.
   - In the **Confirm password** field, retype the password.

   Consult your Ivanti Endpoint Security administrator to obtain these credentials.

e. Clear the **User must change password at next logon** check box.
f. Select the **Password never expires** check box.
g. Click **Create**.
The user account is created.
h. Repeat substeps d though g to create the Web client account.
i. Repeat substeps d though g to create the service account.
j. Click **Close**.

3. Select **Start** > **Run**.
4. In the field, type `cmd`.
5. Click **OK**.
A command prompt opens.

6. From the command prompt, type `sqlcmd -SSERVERNAME\INSTANCENAME -E -ifilepath \PreInstallDBAscript.sql -k1>c:\PreInstallDBAScript_out.txt`

   Remember the following information when entering this command at the prompt:

   - All characters in the command are case sensitive.
   - When typing `SERVERNAME\INSTANCENAME`, the slash and instance name are not necessary if the applicable instance is a default instance.
   - The `-E` command instructs sqlcmd to connect to the SQL Server using a trusted connection.
   - The `-i` command defines where to locate the script to execute. If this command is executed from the directory where `PreInstallDBAScript.sql` is located, then the file path is not necessary; otherwise, the full file path must be defined.
   - The `-k1` command instructs sqlcmd to remove any control characters found in the input file.

   The following databases are created:

   PLUS: Patch Management Database

   PLUS_Staging: Content Replication Database

   SCM: Security Configuration Management Database

   STAT_Guardian: Network Discovery/Agent Deployment Database

   UPCCommon: Endpoint Management Platform Database

   The modifications necessary for your Ivanti Endpoint Security administrator to complete installation of Ivanti Endpoint Security are finished.

After Completing This Task:

Have your Ivanti Endpoint Security administrator complete "Completing Installation (Part III)" on the next page.

Completing Installation (Part III)

The Ivanti Endpoint Security administrator performs this portion of the install procedure, which completes installation of the Ivanti Endpoint Security.

If you have any questions and/or require additional assistance, contact Ivanti support at https://forums.ivanti.com/s/contactsupport.

The final portion of the installation procedure is performed by the Ivanti Endpoint Security (Ivanti Endpoint Security) administrator on your target Ivanti Endpoint Security server.

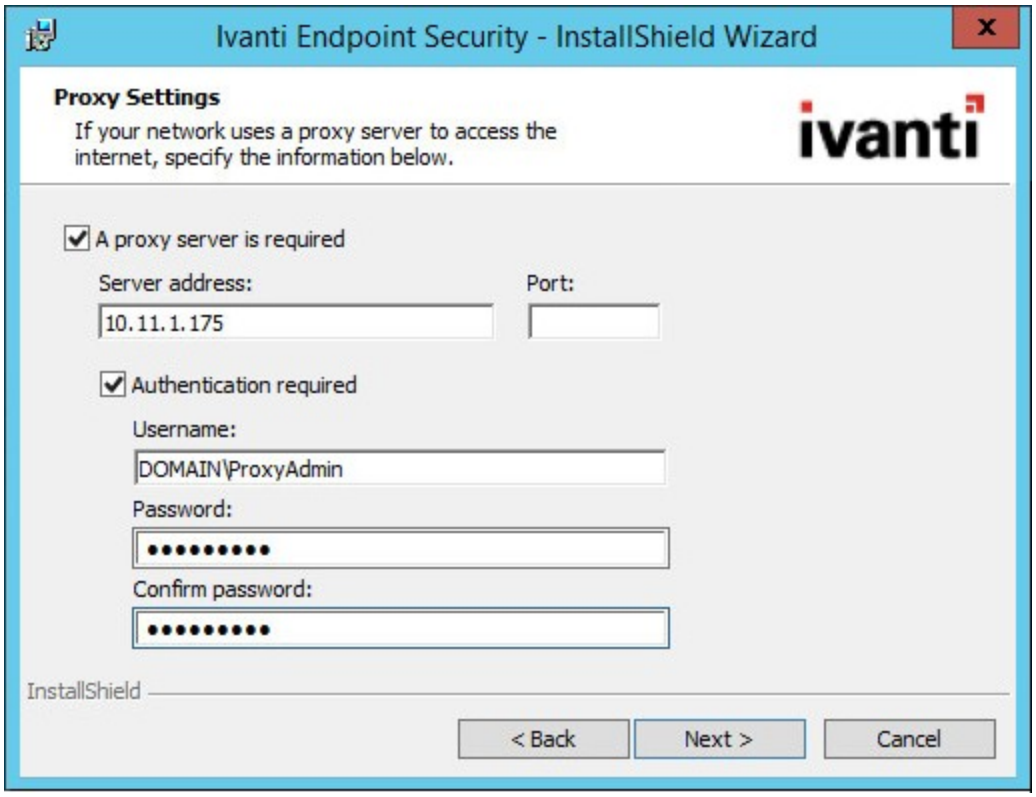
1. Ensure Windows Authentication is selected.
2. Click **Next**.
   A new page opens.

Page	Steps
If the Destination Location page opens:	Click **Next** and proceed to the next step.
If the SQL Server Configuration Requirements page opens:	The pre-installed instance of SQL Server is not configured to work with Ivanti Endpoint Security. • If you only receive SQL Server configuration requirement *informationals* or *warnings*,click **Next** to continue (the Ivanti Endpoint Security installation will automatically reconfigure SQL Server). Proceed to the next step. • If you receive any SQL Server configuration requirement failures, you must cancel the installation, resolve the failures, and then proceed with the installation. Click **View Configuration Detail** for detailed information about SQL Server configuration status requirements.

3. [Optional] Change the Ivanti Endpoint Security installation location.
   a. Click **Browse**.
   b. Define the desired file path using either the **Look in** lists or the **Folder name** field.
   c. Click **OK**.
      The **Installation Folder** field reflects your changes.

4. [Optional] Change the Ivanti Endpoint Security content storage location.
   The content storage location is the location where patches and other content items are downloaded. Ivanti recommends allocating at least 32 GB of storage space to content (plus an additional 10 GB if managing non-Windows endpoints).
   a. Click **Browse**.
   b. Define the desired file path using either the **Look in** lists or the **Folder name** field.
   c. Click **OK**.
      The **Content Storage Location** field reflects your changes.
5. Click **Next**.
   The Proxy Settings page opens.

Refer to the Ivanti Endpoint Security: Requirements Guide (https://help.ivanti.com) for a complete list of proxy types that Ivanti Endpoint Security supports.



If one or both of the storage directories defined on the **Destination Location** page does not contain the recommended available disk space, the **Proxy Settings** page does not immediately open. Rather, a dialog that lets you redefine the storage directories openS. Then after redefining the storage directories, the **Proxy Settings** page opens.

6. If your network uses a proxy server to access the Internet, select the **A proxy server is required** check box and type the applicable information in the following fields.

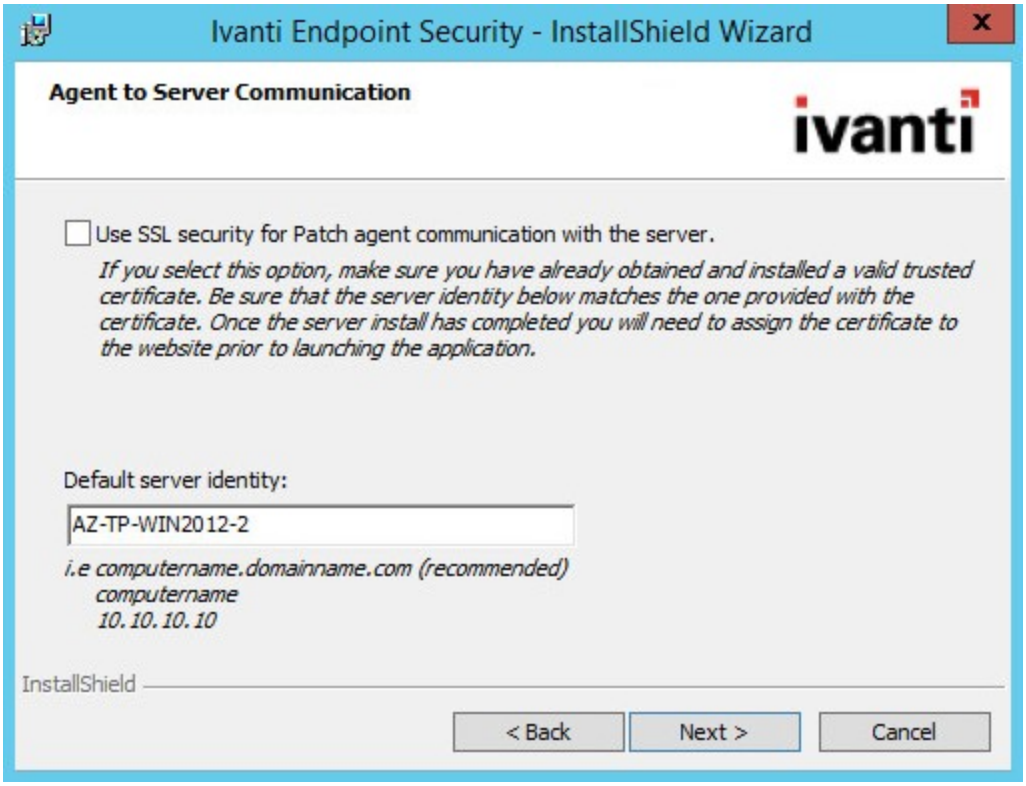
Field	Type
Server Address	The IP address of the applicable proxy server.
Port	The port number used for communication.

You can also configure Ivanti Endpoint Security to use a proxy following installation. Refer to *The Service Tab* in the Ivanti Endpoint Security User Guide (https://help.ivanti.com/) for additional information on proxy communication.

7. If your network uses a proxy server to access the Internet, and that proxy requires authentication, select the **Authentication required** check box and type the applicable information in the following fields.

Field	Type
Username	A user name that authenticates with the proxy.
Password	The password associated with the user name.
Confirm Password	The password retyped.

8. Click **Next**



.

The Agent to Server Communication page opens.

9. If you are using SSL for server and agent communication, select the **Use SSL security for Patch agent communication with the server** check box.

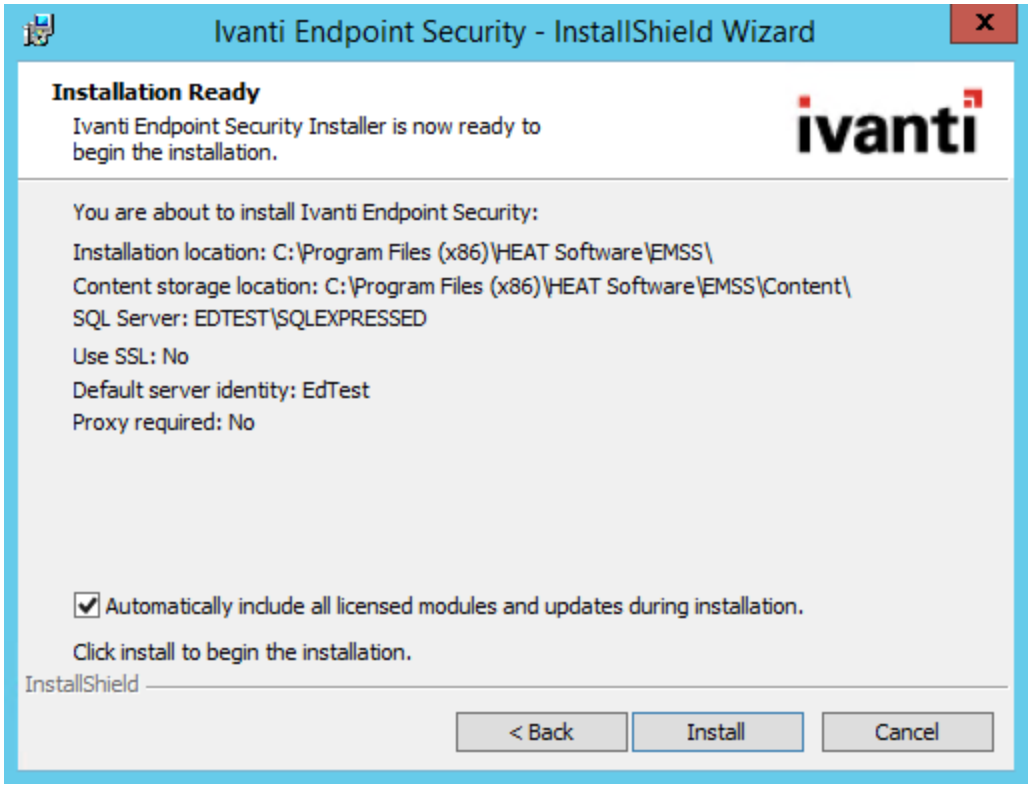
   You must possess an SSL certificate to implement SSL communication. Implementation of SSL communication during installation is optional. This feature can be implemented following installation.

10. In the **Default server identity** field, type the name of your server in one of the following formats:
    - DNS name (`computername.domainname.com`)
    - Computer name (`computername`)
    - IP address (`10.10.10.10`)

    During agent registration, the Ivanti Endpoint Security agents use this name to identify the server.

    If you are using SSL, the server name that you type in the field must match the server named on your certificate.

11. Click **Next**.



    The Installation Ready page opens.

12. [Optional] If you want to install only core components, clear the **Automatically include all licensed modules and updates during installation** check box.

You may use the Ivanti Installation Manager after the initial installation of Ivanti Endpoint Security to install additional components. For additional information, refer to *Using Ivanti Installation Manager* in the *Ivanti Endpoint Security User Guide* (https://help.ivanti.com/).

13. Review the installation information and click **Install** to begin the installation of Ivanti Endpoint Security. This process may take several minutes.

    Important: During installation, do not attempt to access the Ivanti Endpoint Security Web site. Accessing the Web site during installation can cause installation errors.

14. After installation completes, click **Finish**.

    Ivanti Endpoint Security is installed and can now be accessed.

After Completing This Task:

Proceed to one of the following procedures based on selections made during installation.

- If your server will use SSL, finish Appendix B: Configuring Your Server to use SSL.
- If your server will not use SSL, proceed to Logging In to Ivanti Endpoint Security.

Logging In to Ivanti Endpoint Security

After installing Ivanti Endpoint Security, log in to begin configuring the system.

Prerequisites:

One of the following Web browsers:

- Google Chrome
- Mozilla Firefox

You can access the console from any endpoint within your network.

When accessing the Ivanti Endpoint Security console using a Web browser with high security settings enabled, the following message may display:
`Scripting must be enabled to display this application properly.`
In this event, Ivanti recommends adding the Ivanti Endpoint Security Web address as a trusted site in your browser settings to view the Web console.

1. Open your Web browser.
2. In your browser's address bar, type the Ivanti Endpoint Security URL (http[s]://*ServerURL*) and press ENTER.

   You can also use the server IP address.

   A dialog prompting you for credentials opens.
3. Type your user name in the **User name** field.
   When logging in for the first time, type the user name of the Windows user account used to install Ivanti Endpoint Security. You can use additional user names after adding new user profiles to Ivanti Endpoint Security. If logging in using a domain account, type the name in the following format: `DOMAIN\Username`.
4. Type your password in the **Password** field.
5. Click **OK**.
   Ivanti Endpoint Security opens to the Home page and launches the Application Setup Manager.

After Completing This Task:

Complete Setting Up Ivanti Endpoint Security

Setting Up Ivanti Endpoint Security

Following installation and initial log in, the Application Setup Manager dialog opens. This dialog appears only once, the first time you log in to Ivanti Endpoint Security and you use it to configure basic options within the system.

Prerequisites:

- Complete Ivanti Endpoint Security (Ivanti Endpoint Security) installation and open the Web console in your browser.

You cannot reopen this dialog following its completion. However, you can access these settings from various Ivanti Endpoint Security pages.

1. Log in to Ivanti Endpoint Security. For additional information, refer to Logging In to Ivanti Endpoint Security.
   Ivanti Endpoint Security opens and the Application Setup Manager displays. This dialog appears only the first time Ivanti Endpoint Security is opened.
2. Ensure the **Customer Info** tab is selected.
3. Type the applicable information in the following fields:

Field	Description
First name	Your first name.
Last name	Your last name.
Company name	Your company name. The company name specified during installation appears by default but can be edited.

4. Click **Apply**.
5. [Optional] Select the **Languages** tab.
6. [Optional] Select the check boxes associated with the languages you want to receive content in (Patch and Remediation only).
   Each content item available in Ivanti Endpoint Security may be available in multiple versions for different languages.
7. Click **Apply**.
8. Select the **Uninstall Password** tab.
9. Define the global agent uninstall password.
   a. In the **Global uninstall password** field, type the desired password.
   b. In the **Confirm password** field, retype the password.
   This password can be used to manually uninstall Ivanti Endpoint Security agents and should be kept confidential.

Tip: Following installation, you can change the global uninstall password. For additional information on how to change the password outside the **Application Setup Manager**, refer to *Defining the Global Uninstall Password* in the Ivanti Endpoint Security User Guide).

10. Click **Apply**.
11. [Optional] Select the **Email Notifications** tab.
12. [Optional] Define the email information used for email notifications.
    Email notifications are alerts sent by Ivanti Endpoint Security when certain system events occur. Type the applicable information in the following fields.

Field	Description
SMTP Host	The local SMTP mail host name. Ivanti Endpoint Security uses your corporate Internet (SMTP) mail server.
'From' email address	The email address used when the system sends email notifications.
'To' email address	An email address you use to receive system notifications.

    Important: When upgrading Ivanti Endpoint Security via a fresh installation, you must reconfigure your email notifications after installing your licensed server modules. For additional details regarding Email Notifications, refer to *The Email Notifications Page* in the Ivanti Endpoint Security User Guide.
13. Click **Apply**.
14. [Optional] Select the **Install an Agent** tab.
15. [Optional] Select the **Automatically install an agent on the server** check box to install an agent on the server.
    a. Select the check boxes of the applicable modules.
    Selecting these modules activates agent functionality associated with the module.
16. Click **Apply**.
    Your initial settings are applied.
17. Click **Close**.
    Initial configuration is complete. You are now ready to begin monitoring your network with Ivanti Endpoint Security.

Appendix A: Configuring Remote SQL Server Instances

If you elect to install Ivanti Endpoint Security using a remote instance of SQL Server, you must first create two user accounts on the server hosting the instance (provided you are not using preexisting accounts for your installation).

Additionally, you must also configure your instance (and, if in place, its Windows Firewall) to accept remote connections from the server that will host Ivanti Endpoint Security.

Procedures to configure remote instances of SQL Server are provided, as well as a procedure to create the necessary user accounts.

Creating Remote Accounts

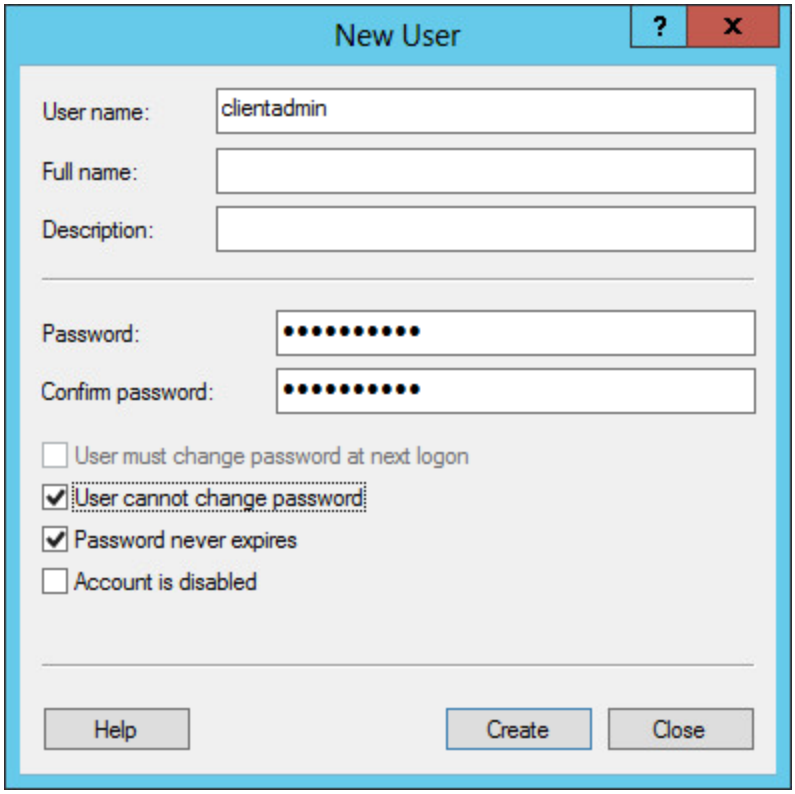
When installing Ivanti Endpoint Security using a remote instance of SQL server, you must first create two user accounts on the server hosting your instance: a Web client account and a service account. Ivanti Endpoint Security uses these accounts to operate components critical to the system. Without these accounts, Ivanti Endpoint Security will be unable to access the remote SQL Server.

Create these accounts on the server hosting your SQL Server instance.

If using domain accounts, these accounts do not have to be created locally. However, any domain account used as the service account must be added to the database server's administrators group. To use a domain account as a service account, complete this task, skipping steps 3-13.

1. Log in to the server hosting your SQL Server instance using either a local or domain user account with system administrator privileges.
   If your SQL Server instance uses mixed mode authentication, ensure that the user account you log in with supports SQL Server login.
2. Open the **Computer Management** dialog.
   a. Open Windows Control Panel.
   b. Open **Administrative Tools**.
   c. Open **Computer Management**.
      The Computer Management dialog opens.
3. Expand the tree to the **Users** folder (**System Tools > Local Users and Groups > Users**).
4. Right-click the **Users** folder.

5. Select **New User**.
   The New User dialog opens.

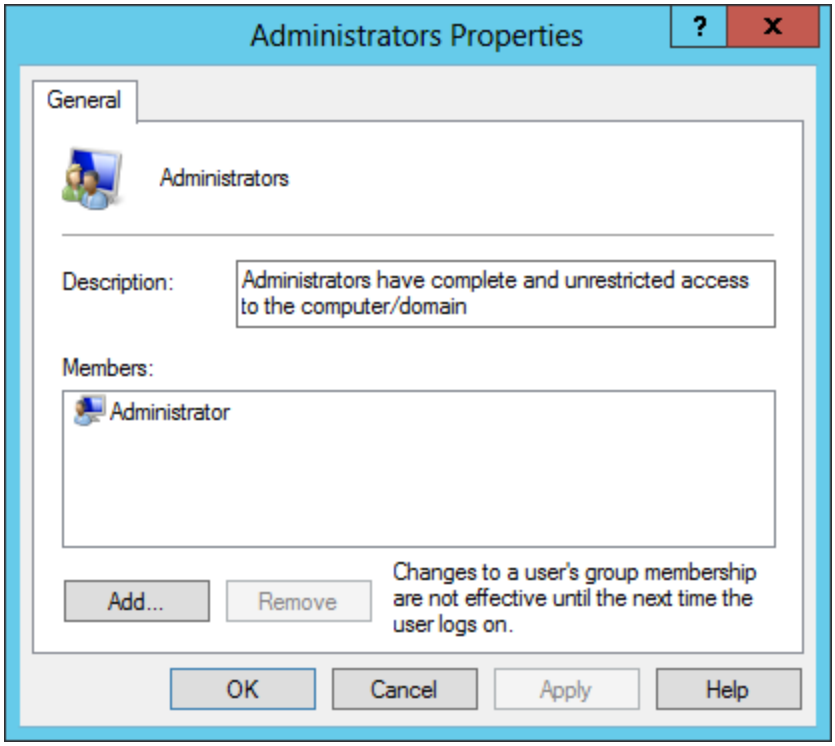


6. In the **User name** field, type the desired Web client account name (or service account name). Ivanti recommends *clientadmin* for the Web client account, and *serviceadmin* for the service account.
7. In the **Password** field, type the desired password.
8. In the **Confirm Password** field, retype the Password.
9. Ensure the **User must change password at next logon** check box is cleared.

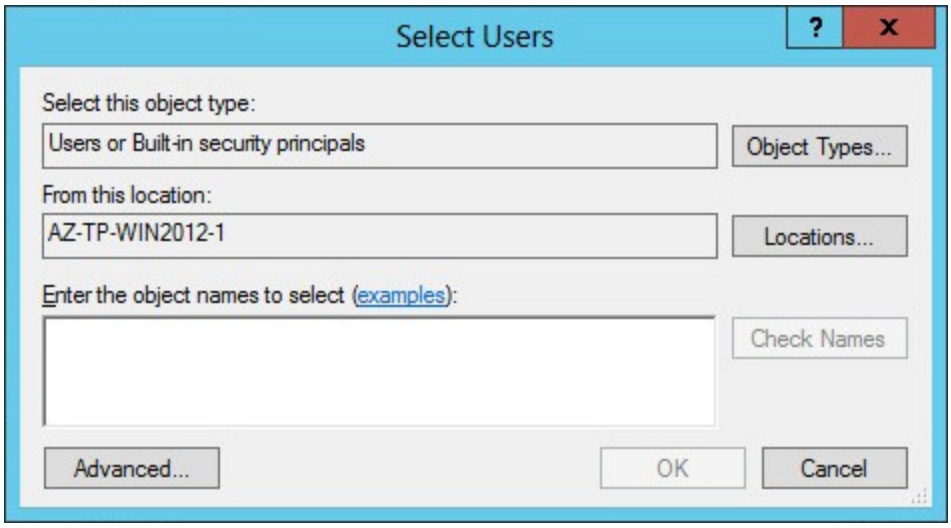
> **Important:** When creating these accounts, failure to clear the **User must change password at next logon** will deny you access to the Ivanti Endpoint Security Web site following installation.

10. Select the **Password never expires** check box.
11. Click **Create**.
    The Web client account is created.
12. Repeat steps 5 through 11 to create the service account.
    The service account is created.
13. Click **Close**.
14. Expand the directory tree structure to the **Groups** folder (**System Tools > Local Users and Groups > Groups**).

15. In the main pane, double-click **Administrators**.
    The Administrators Properties dialog opens.



16. Click **Add**.
    The Select Users dialog opens.



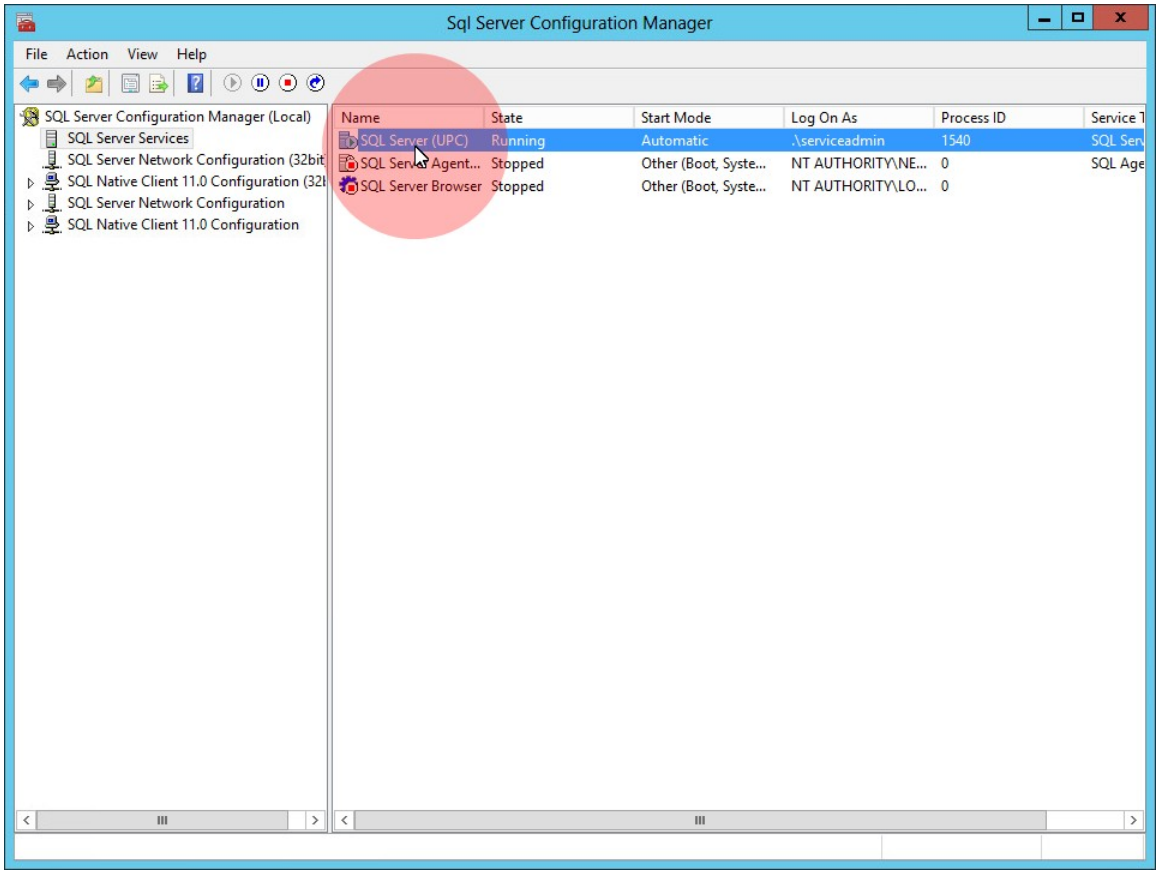
17. In the **Enter the object names to select** field, type your service account name.
18. Click **OK**.
    The service account is added to the Administrators group.
19. Click **OK**.
    The Web client and service accounts are created.

Configuring SQL Server to Accept Remote Connections

When configuring Ivanti Endpoint Security for use with a remote SQL Server instance, you must configure that instance to accept remote connections.

Perform this task on the server hosting the SQL Server instance you want to use with Ivanti Endpoint Security (Ivanti Endpoint Security).

1. Using the **Start** menu or the **Start** screen, open **SQL Server Configuration Manager**.
   SQL Server Configuration Manager opens.



2. Expand the tree to **Protocols for *Ivanti Endpoint SecuritySQLInstanceName***.
   Example: For example, for the default Ivanti Endpoint Security SQL install, select **SQL Server Configuration Mnager (Local)** > **SQL Server Network Configuration** > **Protocols for UPC**.
3. Enable the TCP/IP protocol for your instance.
   a. From the main pane, double-click **TCP/IP**.
   b. Set **Enabled** to **Yes**.
4. Configure the TCP/IP protocol to allow connection from your Ivanti Endpoint Security Server.
   a. From the TCP/IP Properties dialog, select the **IP Addresses** tab.
   b. From an unused **IP** node (*IP1*, *IP2*, or so on), set **Active** to **Yes**.
   c. Set **Enabled** to **Yes**.
   d. Set the **IP Address** to the address of your Ivanti Endpoint Security Server.

e. Click **OK**.
f. Click **OK** to acknowledge that the service needs to be restarted.

5. If installing Ivanti Endpoint Security to a named instance of SQL Server, ensure the SQL Server Browser Service is running.
   a. From the tree, select **SQL Server Services**.
   b. From the main pane, double-click the **SQL Server Browser**.
   c. Ensure the **Service** tab is selected.
   d. Ensure that **Automatic** is selected from the Start Mode list.
   e. Click **OK**.
   f. From the main pane, right-click **SQL Server Browser**.
   g. Select **Restart** (or **Start** if **Restart** is unavailable).
6. From the tree, select **SQL Server Configuration Manager (Local)** > **SQL Server Services**.
7. From the main pane, right-click **SQL Server (Ivanti Endpoint SecuritySQLInstanceName)** and select **Restart**.
   Example: Restart **SQL Server (UPC)**.
8. Close Sql Server Configuration Manager.
   Your SQL Server instance is ready for use with Ivanti Endpoint Security. Proceed with the installation procedure (provided your SQL Server instance is not behind a Windows Firewall).

After Completing This Task:

If your SQL server instance is behind a Windows Firewall, complete Configuring Windows Firewall for SQL Server Instance Access.

Configuring Windows Firewall for SQL Server Instance Access

If you are configuring Ivanti Endpoint Security for use with a remote SQL Server instance, you must configure your SQL Server's Windows Firewall to allow access to Ivanti Endpoint Security (if your SQL Server has Windows Firewall enabled).

Configure your SQL Server firewall according to your SQL server instance version. Complete the steps listed at Configure a Windows Firewall for Database Engine Access (http://msdn.microsoft.com/en-us/library/ms175043.aspx).

You edit your Windows Firewall settings according to your specific server operating system. The procedures available at the provided Microsoft Web sites may differ slightly when you edit your specific settings.

Appendix B: Configuring Your Server to use SSL

During installation of the Ivanti Endpoint Security server, you can configure Ivanti Endpoint Security to use SSL for server to agent communication after obtaining an SSL certificate from a trust provider.

Prerequisites:

- You must obtain a certificate from a root certificate authority.

Obtaining a trusted SSL certificate can take several days. Therefore, Ivanti recommends obtaining an SSL certificate *before* installing Ivanti Endpoint Security. Certificates can be obtained from trust providers such as Verisign Inc. (www.verisign.com) or Entrust (www.entrust.com).

Configuring SSL

Associate your certificate with the Ivanti Endpoint Security (Ivanti Endpoint Security) Web site in your server's Internet Information Services (IIS) Manager.

The first portion of this procedure is performed before installation of Ivanti Endpoint Security, and the second portion is performed following installation of Ivanti Endpoint Security.

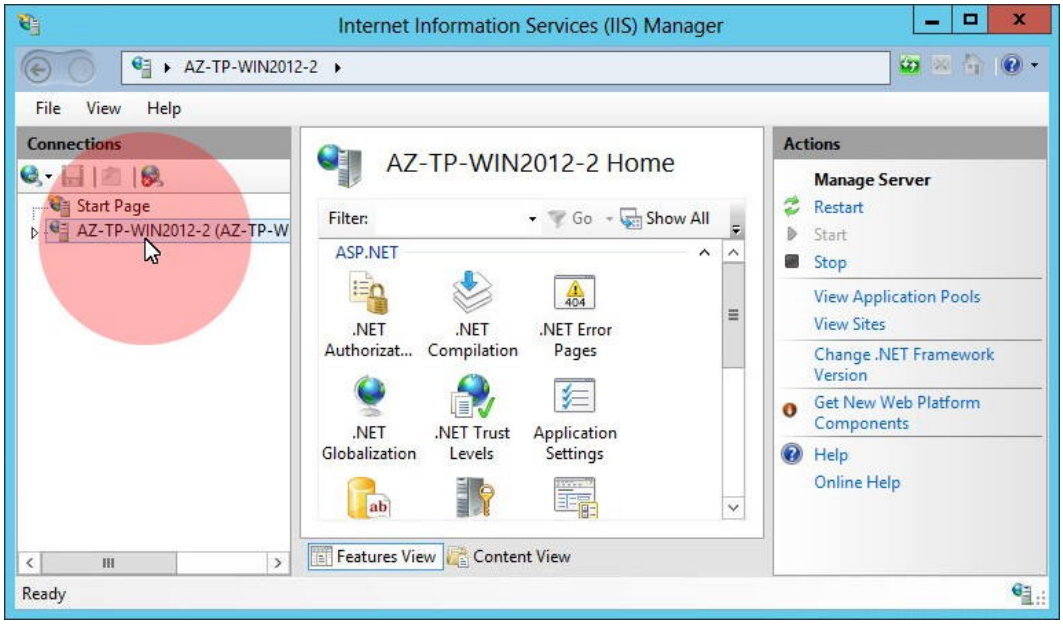
Important: If you are installing Ivanti Endpoint Security on a server that already hosts a Web site, a different procedure must be used for SSL configuration. For additional information, refer to https://forums.ivanti.com/s/article/L-E-M-S-S-One-of-the-IP-Port-combinations-for-site-67-has-already-been-configured-to-be-used-by-another-program for additional guidance.

1. If necessary, import your certificate.

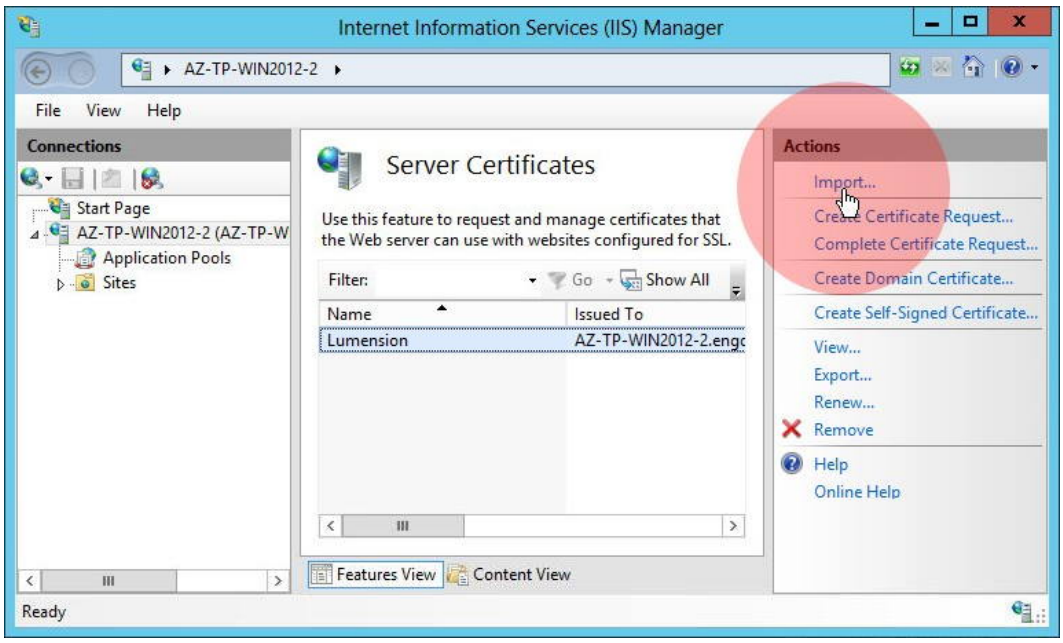
   To import your certificate, complete the following substeps.

   a. Open Internet Information Services (IIS) Manager, which can be found in **Administrative Tools** within **Control Panel**.
   Internet Information Services (IIS) Manager opens.

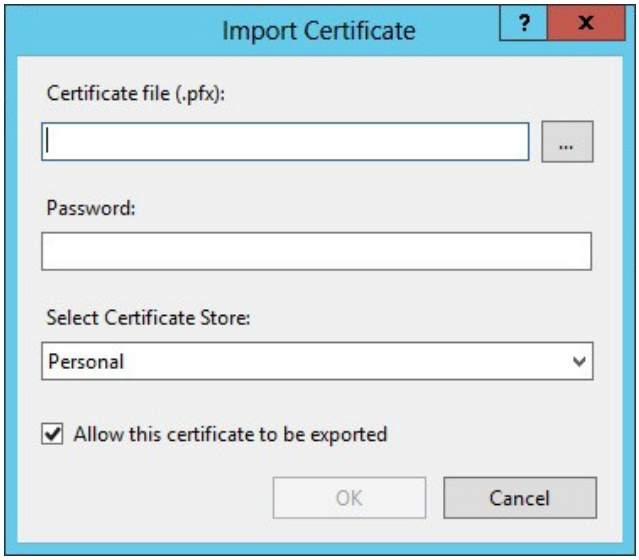
   b. From the tree, select your Ivanti Endpoint Security server.



   c. In the main pane, scroll to the IIS section and double-click **Server Certificates**.
   The Server Certificates page opens.



d. Click the **Import** link.
The **Import Certificate** dialog opens.



e. Click the Elipses button (...), browse to your certificate, and click **Open**.
You may have to edit the **File name type** list to see your certificate.

f. Type the certificate **Password**.

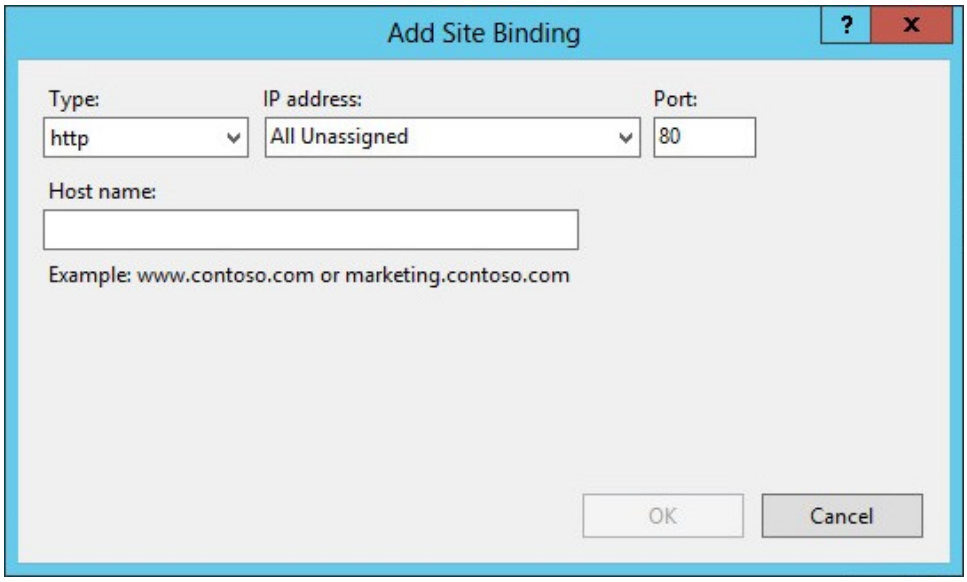
g. Click **OK**.

2. Assign the certificate to the default Web site.
To assign the certificate, complete the following substeps.

a. From the tree, expand to **Default Web Site (*Server Name* > Sites > Default Web Site**).

b. Click the **Bindings** link.
The Site Bindings dialog opens.

c. Click **Add**.
The Add Site Binding dialog opens.



d. From the **Type** list, select **https**.

e. From the **SSL certificate** list, select your certificate.

f. Click **OK**.

g. Click **Close**.

3. Complete one of the Ivanti Endpoint Security installation procedures listed in Selecting an Installation Method.

   While installing Ivanti Endpoint Security, select the **Use SSL security for Patch agent communication with the server** check box.

   Name resolution of the server, endpoints, and the root certificate authority is required to use SSL.

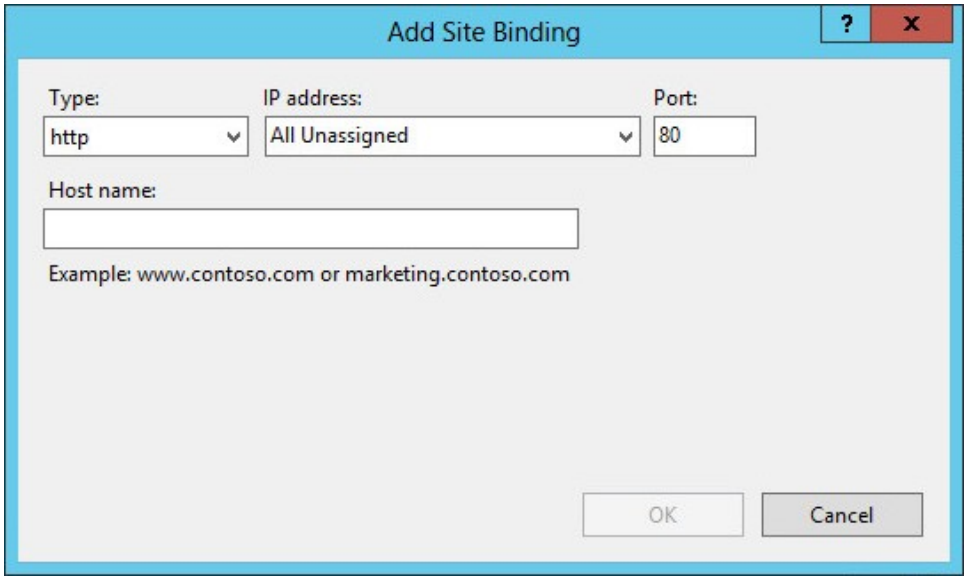
4. Assign the certificate to the Ivanti Endpoint Security Web site.
   Complete the following substeps to assign the certificate.

   a. Open **Internet Information Services (IIS) Manager**, which can be found in **Administrative Tools** within **Control Panel**.
   Internet Information Services (IIS) Manager opens.

   b. From the tree, select **Ivanti** Web site (**Server Name > Sites > Ivanti**).

   c. Click the **Bindings** link.
   The Site Bindings dialog opens.

   d. Click **Add**.
   The Add Site Binding dialog opens.



   e. From the **Type** list, select **https**.

   f. From the **SSL certificate** list, select your certificate.

   g. Click **OK**.

   h. Click **Close**.

5. Configure the Web site to accept only SSL connections.
    1. In the main pane, scroll to the **IIS** section.
    2. Double-click **SSL Settings**.
    3. Select the **Require SSL** check box.
    4. Click **Apply**.
       Your server is now configured for SSL communication.

After Completing This Task:

- Complete Logging In to Ivanti Endpoint Security.
- Complete Setting Up Ivanti Endpoint Security.
- After you have completed setup, edit your global configuration policy set and ensure **Use SSL for agent to server communication** is **True**. For additional information, refer to Secure Your Server With SSL in the Ivanti Endpoint Security User Guide.

Appendix C: Upgrading from Previous Installations

Ivanti routinely releases updates that upgrade previous product installations. Install these new versions to take advantage of new features.

Rather than deleting the previous product installation, you can upgrade the existing installation to the new version. For more information, see the Ivanti Endpoint Security: Upgrade Guide.

Appendix D: Installation Checklist

For your convenience, an installation checklist is provided that itemizes information and tasks.

Server Installation Checklist

This checklist itemizes the information you will need and tasks you will need to complete when installing the Ivanti Endpoint Security server.

Prior to installing Ivanti Endpoint Security (Ivanti Endpoint Security), you must gather and confirm the following information:

☐ Your target server has the required service packs installed for its operating system. For more information, see Supported Operating Systems.

☐ Your target computer meets or exceeds the hardware requirements listed in Combined Ivanti Endpoint Security Application and Database Server.

☐ Your server is *not* a Domain Controller.

☐ Your server has all required software installed:

Software	Requirements
Microsoft SQL Server	"Supported SQL Server versions and requirements" on page 8
Microsoft Internet Information Services	IIS Requirements
Web Browser	Supported Web Browsers and requirements

☐ Ensure the target server uses one of supported locales and browser languages listed in Supported Languages and Locales.

☐ Your Ivanti Endpoint Security server meets network requirements listed in Network Requirements.

☐ If your server is a member of a domain, the default security policies are in effect.

Warning: Avoid changing any Domain Group Policy object (GPO) settings that could overwrite the **Log on as a service** or **Impersonate a client after authentication** settings within the User Rights Assignments area of your local server. Overwriting these settings causes critical SQL Server and Ivanti Endpoint Security settings to be ignored and may result in system failure.

☐ Your server DNS host name is: _____

☐ Your Ivanti Endpoint Security serial number is: _____-_____

☐ Your target system is connected to the Internet.

☐ If you are using SSL, a valid SSL Web certificate has been obtained.

If you are using SSL, you need to obtain a valid Web certificate, from a trust provider such as Verisign Inc. (www.verisign.com) or Entrust (www.entrust.com), prior to installing Ivanti Endpoint Security.

☐ If you are using SSL, you have started the first portion in Appendix B: Configuring Your Server to use SSL (the second portion is completed after installation).

☐ If a proxy server will be used, you know the proxy server's name, IP address, port, user name, and password.

- Name: _____
- IP address: _____ - _____ - _____ - _____
- Port: _____
- Username: _____
- Password: _____

☐ If you are using a preexisting instance of SQL Server, the instance is set to one of the following collation values:

- SQL_Latin1_General_CP1_CI_AS
- Latin1_General_CI_AS

☐ If you are using a preexisting instance of SQL Server, whether local or remote, the operating system of the server hosting the instance is set to an English language locale.

☐ If you are using a remote SQL instance, the instance is configured to accept remote connections. For additional information, refer to Configuring SQL Server to Accept Remote Connections.

☐ If you are using a remote SQL instance, and that instance is behind a firewall, the firewall is configured to allow the Ivanti Endpoint Security server access. For additional information, refer to Configuring Windows Firewall for SQL Server Instance Access.

☐ Your local SMTP mail host name is: _____