Notices

Version Information
Ivanti Endpoint Security Server Install Guide; - Ivanti Endpoint Security Version 8.5 Update 2 - Published: Apr 2018
Document Number: 02_202_8.5 Update 2_171251546

Copyright Information
This document contains the confidential information and/or proprietary property of Ivanti, Inc. and its affiliates (referred to collectively as “Ivanti”), and may not be disclosed or copied without prior written consent of Ivanti.

Ivanti retains the right to make changes to this document or related product specifications and descriptions, at any time, without notice. Ivanti makes no warranty for the use of this document and assumes no responsibility for any errors that can appear in the document nor does it make a commitment to update the information contained herein.

For the most current product information, please visit www.ivanti.com.

Copyright© 2018, Ivanti. All rights reserved.
Ivanti and its logos are registered trademarks or trademarks of Ivanti, Inc. and its affiliates in the United States and/or other countries. Other brands and names may be claimed as the property of others.

Protected by patents, see https://www.ivanti.com/patents.
# Table of Contents

## System Requirements
- Supported Operating Systems ................................................................. 7
- Supported Languages and Locales ............................................................... 8
- Software Requirements
  - Web Browser Requirements ................................................................. 9
  - SQL Server Requirements ................................................................. 10
  - IIS Requirements .............................................................................. 11
  - .NET Framework Requirements ...................................................... 12
- Hardware Requirements ............................................................................. 13
- Network Requirements ............................................................................. 14
- Recommended Configurations
  - Combined Ivanti Endpoint Security Application and Database Server .... 15
  - Separated Ivanti Endpoint Security Application and Database Servers ... 16

## Chapter 2: Installing Ivanti Endpoint Security
- Downloading Ivanti Endpoint Security ...................................................... 21
- About SQL Server Instance Location ......................................................... 22
- Defining the Web Client Account and Service Account ......................... 22
- Selecting an Installation Method .............................................................. 23
- Installing Using a New SQL Server Instance .......................................... 24
- Installing Using an Existing SQL Server Instance (Either Locally or Remotely) ... 25
- Installing Using a Remote SQL Server Instance (with no Local Instance) .... 26
- Installing Ivanti Endpoint Security (Separate Ivanti Endpoint Security and SQL Server Admins) ......................................................... 61
  - Beginning Installation (Part I) .............................................................. 62
  - Creating Components on SQL Server (Part II) ..................................... 69
  - Completing Installation (Part III) ......................................................... 71
- Logging In to Ivanti Endpoint Security ...................................................... 76
- Setting Up Ivanti Endpoint Security ......................................................... 77

## Appendix A: Configuring Remote SQL Server Instances
- Creating Remote Accounts ....................................................................... 81
- Configuring SQL Server to Accept Remote Connections ........................ 84
- Configuring Windows Firewall for SQL Server Instance Access ............... 86

## Appendix B: Configuring Your Server to use SSL
- Configuring SSL ....................................................................................... 87

## Appendix C: Upgrading from Previous Installations
- .................................................................................................................. 93

## Appendix D: Installation Checklist
- Server Installation Checklist ....................................................................... 95
System Requirements

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

On servers that do not meet recommended 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.

Table 1: Supported Operating Systems

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Edition</th>
<th>Data Width</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Windows Server 2016</td>
<td>Standard</td>
<td>64-bit</td>
</tr>
<tr>
<td></td>
<td>Datacenter</td>
<td></td>
</tr>
<tr>
<td>Microsoft Windows Server 2012 R2</td>
<td>Standard&lt;sup&gt;2&lt;/sup&gt;</td>
<td>64-bit</td>
</tr>
<tr>
<td></td>
<td>Datacenter&lt;sup&gt;2&lt;/sup&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Foundation</td>
<td></td>
</tr>
<tr>
<td>Microsoft Windows Server 2012</td>
<td>Standard&lt;sup&gt;2&lt;/sup&gt;</td>
<td>64-bit</td>
</tr>
<tr>
<td></td>
<td>Datacenter&lt;sup&gt;2&lt;/sup&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Foundation</td>
<td></td>
</tr>
<tr>
<td>Microsoft Windows Server 2008 R2</td>
<td>Standard&lt;sup&gt;2&lt;/sup&gt;</td>
<td>64-bit</td>
</tr>
<tr>
<td></td>
<td>Enterprise&lt;sup&gt;2&lt;/sup&gt;</td>
<td></td>
</tr>
<tr>
<td>Microsoft Windows Server 2008 SP</td>
<td>Web</td>
<td>64-bit&lt;sup&gt;4&lt;/sup&gt;</td>
</tr>
<tr>
<td>2 SP1</td>
<td>Standard</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enterprise</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Web</td>
<td></td>
</tr>
</tbody>
</table>
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. For more information on enabling and disabling Core mode on Windows 2012 and 2012 R2 servers, see Ivanti Community Article 59234 (Converting Windows Server 2012 from a Server with a GUI mode to Core mode).

2. The Hyper-V edition of this operating system edition is supported, however, the Microsoft Hyper-V Server 2012 stand-alone edition is not.

3. The Datacenter and Core editions of this operating system family are not supported.

4. New installations of Ivanti Endpoint Security are only supported on the 64-bit version of this operating system. However, if upgrading to 8.5 Update 2 from a prior supported version of Ivanti Endpoint Security, the 32-bit version of this operating system is still supported.

### Supported Languages and Locales

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

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

Table 2: Server Supported Locales

<table>
<thead>
<tr>
<th>Language</th>
<th>Locale Identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>English: United States</td>
<td>en-us</td>
</tr>
<tr>
<td>English: Australia</td>
<td>en-au</td>
</tr>
<tr>
<td>English: Belize</td>
<td>en-bz</td>
</tr>
<tr>
<td>English: Canada</td>
<td>en-ca</td>
</tr>
<tr>
<td>English: India</td>
<td>en-in</td>
</tr>
<tr>
<td>English: Ireland</td>
<td>en-ie</td>
</tr>
<tr>
<td>English: Jamaica</td>
<td>en-jm</td>
</tr>
<tr>
<td>English: New Zealand</td>
<td>en-nz</td>
</tr>
<tr>
<td>English: Philippines</td>
<td>en-ph</td>
</tr>
<tr>
<td>English: Singapore</td>
<td>en-sg</td>
</tr>
<tr>
<td>English: South Africa</td>
<td>en-az</td>
</tr>
<tr>
<td>English: United Kingdom</td>
<td>en-gb</td>
</tr>
<tr>
<td>German: Germany</td>
<td>de-de</td>
</tr>
<tr>
<td>Spanish: Spain (Modern Sort)</td>
<td>es-es</td>
</tr>
</tbody>
</table>
After installing Ivanti Endpoint Security, you can use a translated UI by selecting one of the following languages in your Web browser.

Table 3: Server Supported Languages

<table>
<thead>
<tr>
<th>Language</th>
<th>Language Identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>English: United States</td>
<td>en-us</td>
</tr>
<tr>
<td>French: France</td>
<td>fr-fr</td>
</tr>
<tr>
<td>German: Germany</td>
<td>de-de</td>
</tr>
<tr>
<td>Spanish: Spain (Modern Sort)</td>
<td>es-es</td>
</tr>
</tbody>
</table>

**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:

<table>
<thead>
<tr>
<th>Software</th>
<th>Documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported Web Browsers</td>
<td>Web Browser Requirements on page 10</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Software</th>
<th>Documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft SQL Server</td>
<td>SQL Server Requirements on page 11</td>
</tr>
<tr>
<td>Microsoft .NET Framework</td>
<td>.NET Framework Requirements on page 13</td>
</tr>
<tr>
<td>Microsoft Windows Installer</td>
<td>IIS Requirements on page 12</td>
</tr>
<tr>
<td>Microsoft Silverlight 5.0</td>
<td>.NET Framework Requirements on page 13</td>
</tr>
<tr>
<td>Microsoft Visual C++ 2010 SP1 Redistributable</td>
<td></td>
</tr>
<tr>
<td>Package (x86 and x64)</td>
<td></td>
</tr>
<tr>
<td>Microsoft Visual C++ 2012 Update 4 Redistributable Package (x86 and x64)</td>
<td></td>
</tr>
</tbody>
</table>

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

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

Table 4: Supported Web Browsers

<table>
<thead>
<tr>
<th>Supported Browser</th>
<th>Supported Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google Chrome</td>
<td>53 and higher</td>
</tr>
<tr>
<td>Microsoft Edge</td>
<td>EdgeHTML 14 and higher</td>
</tr>
<tr>
<td>Microsoft Internet Explorer</td>
<td>9 and higher</td>
</tr>
<tr>
<td>Mozilla Firefox</td>
<td>31 Extended Support Release and higher</td>
</tr>
<tr>
<td></td>
<td>Support cannot be guaranteed due to the accelerated release cycle of Mozilla Firefox Rapid Release.</td>
</tr>
</tbody>
</table>

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
**SQL Server Requirements**

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

Table 5: Supported Database Servers

<table>
<thead>
<tr>
<th>Database</th>
<th>Data Width</th>
<th>Edition</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQL Server 2016</td>
<td>x86/x64</td>
<td>• Express</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Standard</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Enterprise</td>
</tr>
<tr>
<td>SQL Server 2014 SP1</td>
<td>x86/x64</td>
<td>• Express</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Standard</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Enterprise</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Business Intelligence</td>
</tr>
<tr>
<td>SQL Server 2014</td>
<td>x86/x64</td>
<td>• Express</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Standard</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Enterprise</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Business Intelligence</td>
</tr>
<tr>
<td>SQL Server 2012 and later</td>
<td>x86/x64</td>
<td>• Express</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Standard</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Enterprise</td>
</tr>
<tr>
<td>SQL Server 2008 R2 SP1 and later</td>
<td>x86/x64</td>
<td>• Express</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Standard</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Enterprise</td>
</tr>
<tr>
<td>SQL Server 2008 SP2 and later</td>
<td>x86/x64</td>
<td>• Express</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Standard</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Enterprise</td>
</tr>
</tbody>
</table>

**Note:**

- 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.

Table 6: Supported Database Instance Install Locations

<table>
<thead>
<tr>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>• On the target Ivanti Endpoint Security server itself, as installed by</td>
</tr>
<tr>
<td>the Ivanti server installer, which installs an instance of SQL Server</td>
</tr>
<tr>
<td>2014 Express SP1 (x64).</td>
</tr>
<tr>
<td>• On the target Ivanti server itself, using a preexisting instance of SQL</td>
</tr>
<tr>
<td>Server.</td>
</tr>
<tr>
<td>• On a remote server that the Ivanti server remotely connects to, using</td>
</tr>
<tr>
<td>a preexisting instance of SQL Server.</td>
</tr>
</tbody>
</table>

**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

**IIS Requirements**

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

Table 7: Internet Information Services (IIS) Requirements

<table>
<thead>
<tr>
<th>Required IIS Version</th>
<th>Operating System Family</th>
<th>Microsoft Documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Internet Information Services 7.0+</td>
<td>Microsoft Windows Server 2012 R2</td>
<td><a href="http://www.iis.net/learn/install/installing-iis-85/installing-iis-85-on-windows-server-2012-r2">http://www.iis.net/learn/install/installing-iis-85/installing-iis-85-on-windows-server-2012-r2</a></td>
</tr>
</tbody>
</table>
.NET Framework Requirements


Table 8: .NET Framework Requirements

<table>
<thead>
<tr>
<th>Required .NET Framework Version</th>
<th>Operating System Family</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Microsoft .NET Framework 4.6.</td>
<td>• Microsoft Windows Server 2008 R2 SP1</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Windows Server 2008 SP2</td>
</tr>
<tr>
<td><strong>Note:</strong> Ivanti Endpoint Security provides the .NET Framework 4.6 installer during installation or upgrade (reboot required). However, pre-requisites must be installed on some Operating Systems prior to this.</td>
<td>• Microsoft Windows Server 2012</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Windows Server 2012 R2</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Windows Server 2016</td>
</tr>
</tbody>
</table>

Hardware Requirements

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

**Note:**

• 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 15.

• 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
# Network Requirements

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

<table>
<thead>
<tr>
<th>Network Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Server Role:</strong> Your Ivanti Endpoint Security <em>should not</em> be a domain controller.</td>
</tr>
<tr>
<td><strong>Firewall Access URLs for replication and agent communication:</strong></td>
</tr>
<tr>
<td>- <a href="https://cdn.securegss.net">https://cdn.securegss.net</a></td>
</tr>
<tr>
<td>- <a href="http://cache.patchlinksecure.net">http://cache.patchlinksecure.net</a></td>
</tr>
<tr>
<td>- <a href="http://cache.lumension.com">http://cache.lumension.com</a></td>
</tr>
<tr>
<td>- <a href="http://gssnews.lumension.com">http://gssnews.lumension.com</a></td>
</tr>
<tr>
<td>- <a href="https://leicapi-lemss.lumension.com">https://leicapi-lemss.lumension.com</a></td>
</tr>
<tr>
<td>- <a href="http://download.windowsupdate.com">http://download.windowsupdate.com</a></td>
</tr>
<tr>
<td>- <a href="http://www.download.windowsupdate.com">http://www.download.windowsupdate.com</a> (For Microsoft content)</td>
</tr>
<tr>
<td>- <a href="http://go.microsoft.com">http://go.microsoft.com</a> (For Microsoft content)</td>
</tr>
<tr>
<td>- <a href="http://ardownload.adobe.com">http://ardownload.adobe.com</a> (For Adobe content)</td>
</tr>
<tr>
<td>- <a href="http://swupdl.adobe.com">http://swupdl.adobe.com</a> (For Adobe content)</td>
</tr>
<tr>
<td>- <a href="http://armdl.adobe.com">http://armdl.adobe.com</a> (For Adobe content)</td>
</tr>
<tr>
<td>- <a href="http://download.adobe.com">http://download.adobe.com</a> (For Adobe content)</td>
</tr>
</tbody>
</table>

**Important:**

- Refer to Ivanti Community Article 51165 (*New Content Architecture*) and Ivanti Community Article 58310 (*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.

<table>
<thead>
<tr>
<th>Network Discovery Windows Services:</th>
</tr>
</thead>
<tbody>
<tr>
<td>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:</td>
</tr>
<tr>
<td>- DNS Client</td>
</tr>
<tr>
<td>- Function Discovery Resource Publication</td>
</tr>
<tr>
<td>- SSDP Discovery</td>
</tr>
<tr>
<td>- UPnP Device Host</td>
</tr>
</tbody>
</table>
**Network Requirement**

**Encryption Protocols:** Ivanti Endpoint Security uses Transport Layer Security for communication between the Ivanti Endpoint Security Server and the Ivanti Endpoint Security Agent: TLS 1.0, 1.1, and 1.2. Ivanti Endpoint Security prompts you to enable these protocols 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 performs both application and database functions.
  
  Combined Ivanti Endpoint Security Application and Database Server on page 16

- **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 on page 17

**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


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 your Ivanti Endpoint Security network.

Note: Installation on a physical server is assumed. If installing to virtual environment, refer to Ivanti Community Article 58253 (Lumension products installed on virtual machines).

<table>
<thead>
<tr>
<th>Endpoint Count</th>
<th>&lt; 50</th>
<th>&lt; 500</th>
<th>&lt; 1,000</th>
<th>&lt; 5,000</th>
<th>&lt; 10,000</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operating System Architecture</td>
<td>x64</td>
<td>x64</td>
<td>x64</td>
<td>x64</td>
<td>x64</td>
</tr>
<tr>
<td>Database Server Architecture</td>
<td>x64</td>
<td>x64</td>
<td>x64</td>
<td>x64</td>
<td>x64</td>
</tr>
<tr>
<td>Hardware</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Core Architecture</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>16</td>
</tr>
<tr>
<td>Core Speed (GHz)</td>
<td>2.0+</td>
<td>2.0+</td>
<td>2.0+</td>
<td>2.0+</td>
<td>2.0+</td>
</tr>
<tr>
<td>RAM (GB)</td>
<td>4</td>
<td>4</td>
<td>8</td>
<td>16</td>
<td>32</td>
</tr>
<tr>
<td>Network (LAN)</td>
<td>1 Gb/s</td>
<td>1 Gb/s</td>
<td>1 Gb/s</td>
<td>1 Gb/s</td>
<td>1 Gb/s</td>
</tr>
<tr>
<td>Disk Array</td>
<td>RAID 1</td>
<td>RAID 1</td>
<td>Multiple RAID</td>
<td>Multiple RAID</td>
<td>Multiple RAID</td>
</tr>
<tr>
<td># Hard Drives</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>6</td>
<td>8</td>
</tr>
</tbody>
</table>
Separated Ivanti Endpoint Security Application and Database Servers

When the Application Server and Database Server are installed on two physical servers, then each server’s 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.

**Note:** Installation on a physical server is assumed. If installing to virtual environment, refer to Ivanti Community Article 58253 (Lumension products installed on virtual machines).

### Recommended Application Server Configuration

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

<table>
<thead>
<tr>
<th>Endpoint Count</th>
<th>&lt; 50</th>
<th>&lt; 500</th>
<th>&lt; 1,000</th>
<th>&lt; 5,000</th>
<th>&lt; 10,000¹</th>
</tr>
</thead>
</table>

---

1. If you are managing more than 10000+ endpoints, contact Ivanti Support ([https://community.ivanti.com/community/contact-support](https://community.ivanti.com/community/contact-support)) 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.
### Recommended SQL Server Configuration

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

<table>
<thead>
<tr>
<th>Endpoint Count</th>
<th>&lt; 50</th>
<th>&lt; 500</th>
<th>&lt; 1,000</th>
<th>&lt; 5,000</th>
<th>&lt; 10,000¹</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operating System Architecture</td>
<td>x64</td>
<td>x64</td>
<td>x64</td>
<td>x64</td>
<td>x64</td>
</tr>
</tbody>
</table>

---

1. If you are managing 10000+ endpoints, contact Ivanti Support ([https://community.ivanti.com/community/contact-support](https://community.ivanti.com/community/contact-support)) 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 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.
### System Requirements

<table>
<thead>
<tr>
<th>Endpoint Count</th>
<th>&lt; 50</th>
<th>&lt; 500</th>
<th>&lt; 1,000</th>
<th>&lt; 5,000</th>
<th>&lt; 10,000¹</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Server Architecture</td>
<td>x64</td>
<td>x64</td>
<td>x64</td>
<td>x64</td>
<td>x64</td>
</tr>
<tr>
<td>SQL Server Hardware</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Core Architecture³</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>16</td>
</tr>
<tr>
<td>Core Speed (GHz)</td>
<td>2.0+</td>
<td>2.0+</td>
<td>2.0+</td>
<td>2.0+</td>
<td>2.0+</td>
</tr>
<tr>
<td>RAM (GB)⁴</td>
<td>4</td>
<td>4</td>
<td>8</td>
<td>16</td>
<td>32</td>
</tr>
<tr>
<td>Network (LAN)</td>
<td>1 Gb/s</td>
<td>1 Gb/s</td>
<td>1 Gb/s</td>
<td>1 Gb/s</td>
<td>1 Gb/s</td>
</tr>
<tr>
<td>Disk Array⁵</td>
<td>RAID 1</td>
<td>RAID 1</td>
<td>Multiple RAID</td>
<td>Multiple RAID</td>
<td>Multiple RAID</td>
</tr>
<tr>
<td># Hard Drives</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>6</td>
<td>8</td>
</tr>
<tr>
<td>Drive Speed (RPM)</td>
<td>7200</td>
<td>7200</td>
<td>10k/SSD</td>
<td>10k/SSD</td>
<td>15k/SSD</td>
</tr>
</tbody>
</table>

#### Hard Drive Volume Breakdown

<table>
<thead>
<tr>
<th></th>
<th>OS/Data (GB)</th>
<th>OS (GB)</th>
<th>Data</th>
<th>Temp DB (GB)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>250</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>OS/Data (GB)</td>
<td>500</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>OS (GB)</td>
<td>N/A</td>
<td>RAID 1 - 250</td>
<td>RAID 1 - 250</td>
<td>RAID 1 - 250</td>
</tr>
<tr>
<td>Data</td>
<td>N/A</td>
<td>RAID 1 - 500GB</td>
<td>RAID 1/SSD - 1TB</td>
<td>RAID 10/SSD - 1TB</td>
</tr>
<tr>
<td>Temp DB (GB)</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>RAID 0 - 250</td>
</tr>
</tbody>
</table>

---

¹ If you are managing 10000+ endpoints, contact Ivanti Support (https://community.ivanti.com/community/contact-support) 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.
Chapter

2

Installing Ivanti Endpoint Security

In this chapter:

• Downloading Ivanti Endpoint Security
• About SQL Server Instance Location
• Defining the Web Client Account and Service Account
• Selecting an Installation Method
• Installing Using a New SQL Server Instance
• Installing Using an Existing SQL Server Instance (Either Locally or Remotely)
• Installing Using a Remote SQL Server Instance (with no Local Instance)
• Installing Ivanti Endpoint Security (Separate Ivanti Endpoint Security and SQL Server Admins)
• Logging In to Ivanti Endpoint Security
• Setting Up 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.


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

**After Completing This Task:**
Complete the installation procedure applicable to your network environment. For additional information, refer to *Selecting an Installation Method* on page 23.

### 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* on page 84. |

**Tip:** 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).

**Note:** 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** on page 24

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)** on page 34
- **Installing Using a Remote SQL Server Instance (with no Local Instance)** on page 48

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)** on page 61

**Attention:** Complete **Downloading Ivanti Endpoint Security** on page 21 before beginning an installation procedure.
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 on page 21.
- As applicable to your network environment, you have gathered the information and completed the tasks itemized in the Server Installation Checklist on page 95.

Note: 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 on page 22.

If you are installing using a Secure Sockets Layer (SSL), complete the first portion of Configuring SSL on page 87.

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.

   Note: 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.

   Step Result: 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.

   Step Result: 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.

**Step Result:** The Customer Information page opens.

![Customer Information Page](image)

Figure 1: Customer Information Page

8. Type the applicable information in the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company Name</td>
<td>Your company name.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>Your Ivanti Endpoint Security serial number.</td>
</tr>
</tbody>
</table>

**Note:** 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](mailto: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.

<table>
<thead>
<tr>
<th>Page/Dialog</th>
<th>Step</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>If the Question dialog opens:</strong></td>
<td>Click <strong>Yes</strong> to start network discovery services. The following services are necessary to use discovery features within Ivanti Endpoint Security:</td>
</tr>
<tr>
<td></td>
<td>• DNS Client</td>
</tr>
<tr>
<td></td>
<td>• Function Discovery Resource Location</td>
</tr>
<tr>
<td></td>
<td>• SSDP Discover</td>
</tr>
<tr>
<td></td>
<td>• UPnP Device Host</td>
</tr>
<tr>
<td><strong>If the Required IIS Features page opens:</strong></td>
<td>Your server does not have the required IIS features installed. Click <strong>Install Features</strong> to install the features and proceed.</td>
</tr>
</tbody>
</table>

**Note:** 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
### Page/Dialog | Step
--- | ---
**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.  
  **Note:** 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.  
  **Tip:** 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 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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Steps</th>
</tr>
</thead>
</table>
| **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.  
  **Note:** 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. |
<table>
<thead>
<tr>
<th>Option</th>
<th>Steps</th>
</tr>
</thead>
</table>
| 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  
**Note:** 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 on page 22. |
11. Click Next.
If required, acknowledge the creation of new accounts by clicking OK.

**Step Result:** The *SQL Server Instance* page opens.

![SQL Server Instance Page](image)

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.

**Step Result:** The *Destination Location* page opens.

![Destination Location Page](image)


   a) Click **Browse**.
   b) Define the desired file path using either the **Look in** lists or the **Folder name** field.
   c) Click **OK**.

   **Step Result:** The **Installation Folder** field reflects your changes.


   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**.

   **Step Result:** The **Content Storage Location** field reflects your changes.
17. Click Next.

**Step Result:** The *Proxy Settings* page opens.

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

---

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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Address</td>
<td>The IP address of the applicable proxy server.</td>
</tr>
</tbody>
</table>
Ivanti Endpoint Security

### Field | Type
--- | ---
Port | The port number used for communication.

**Note:** 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.

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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>A user name that authenticates with the proxy.</td>
</tr>
<tr>
<td>Password</td>
<td>The password associated with the user name.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>The password retyped.</td>
</tr>
</tbody>
</table>

20. Click **Next**.

**Step Result:** The *Agent to Server Communication* page opens.

![Agent to Server Communication Page](image)

Figure 5: Agent to Server Communication Page
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.

**Note:** 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.

**Note:** 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**.

**Step Result:** The **Installation Ready** page opens.

![Installation Ready Page](image)

Figure 6: Installation Ready Page
24. [Optional] If you only want to install core components, clear the **Automatically include all licensed modules and updates during installation** check box.

**Note:** 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/).

25. 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.

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 Configuring SSL on page 87.
- If your server will not use SSL, proceed to Logging In to Ivanti Endpoint Security on page 76.

---

**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:**

- As applicable to your network environment, you have gathered the information and completed the tasks itemized in the Server Installation Checklist on page 95.
- If you are installing using SSL, complete the first portion of Configuring SSL on page 87
- If you are installing using a remote instance of SQL Server, complete Configuring SQL Server to Accept Remote Connections on page 84

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) on page 48 rather than this procedure.
1. If installing using a remote instance of SQL Server, complete Creating Remote Accounts on page 81.

   **Note:** 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.

   **Note:** 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.

   **Step Result:** 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.

   **Step Result:** 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**.

**Step Result:** The **Customer Information** page opens.

![Customer Information Page](image)

Figure 7: Customer Information Page

9. Type the applicable information in the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Company Name</strong></td>
<td>Your company name.</td>
</tr>
<tr>
<td><strong>Serial Number</strong></td>
<td>Your Ivanti Endpoint Security serial number.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>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 <strong>Ivanti Sales Support</strong> (<a href="mailto:sales@ivanti.com">sales@ivanti.com</a>).</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Page/Dialog</th>
<th>Step</th>
</tr>
</thead>
</table>
| **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.  
**Note:** 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.

  **Note:** 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.

  **Tip:** 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 Ivanti Endpoint Security will use. Define these accounts based on how you are configuring your Ivanti Endpoint Security server.

<table>
<thead>
<tr>
<th>Option</th>
<th>Steps</th>
</tr>
</thead>
</table>
| 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. |
<table>
<thead>
<tr>
<th>Option</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>If your install will use a remote SQL Server instance:</strong></td>
<td>Define the credentials for the two user accounts created while completing Creating Remote Accounts on page 81.</td>
</tr>
<tr>
<td></td>
<td>1. In the <strong>Web Client Account Username</strong> field, type the user name of the Web client account on your SQL Server.</td>
</tr>
<tr>
<td></td>
<td>2. In the <strong>Web Client Account Password</strong> field, type the password of the Web client account on your SQL Server.</td>
</tr>
<tr>
<td></td>
<td>3. In the <strong>Web Client Confirm password</strong> field, retype the password.</td>
</tr>
<tr>
<td></td>
<td>4. In the <strong>Service Account Username</strong> field, type the user name of the service account on your SQL Server.</td>
</tr>
<tr>
<td></td>
<td>5. In the <strong>Service Account Password</strong> field, type the password of the service account on your SQL Server.</td>
</tr>
<tr>
<td></td>
<td>6. In the <strong>Service Account Confirm password field</strong>, retype the password.</td>
</tr>
<tr>
<td></td>
<td><strong>Important:</strong> 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.</td>
</tr>
<tr>
<td><strong>If your install will use a local or remote SQL Server instance that uses preexisting accounts as the Web Client and Service Accounts:</strong></td>
<td>Define the credentials for the preexisting accounts.</td>
</tr>
<tr>
<td></td>
<td>1. Type the user name associated with the desired account in the <strong>Web Client Account Username</strong> field.</td>
</tr>
<tr>
<td></td>
<td>2. Type the password associated with the user name in the <strong>Web Client Account Password</strong> field.</td>
</tr>
<tr>
<td></td>
<td>3. Retype the password in the <strong>Web Client Account Confirm password</strong> field.</td>
</tr>
<tr>
<td></td>
<td>4. Type the user name associated with the desired account in the <strong>Service Account Username</strong> field.</td>
</tr>
<tr>
<td></td>
<td>5. Type the password associated with the service account user name in the <strong>Service Account Password</strong> field.</td>
</tr>
<tr>
<td></td>
<td>6. Retype the password in the <strong>Service Account Confirm password</strong> field.</td>
</tr>
<tr>
<td></td>
<td><strong>Important:</strong> 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 on page 22.</td>
</tr>
</tbody>
</table>
12. Click **Next**.
   If required, acknowledge the creation of new accounts by clicking **OK**.

**Step Result:** The *SQL Server Instance* page opens.

![SQL Server Instance Page](image)

**Figure 8:** SQL Server Instance Page

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

**Step Result:** The *SQL Server and Instance* page opens. Use this page to define the SQL Server instance you will use with Ivanti Endpoint Security.

![SQL Server and Instance Page](image)

Figure 9: SQL Server and Instance Page

15. Select a **Server Location**.

Select one of the following options.

<table>
<thead>
<tr>
<th>Option</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>To use a locally installed existing SQL Server instance:</td>
<td>Select the <strong>On this machine (local)</strong> option.</td>
</tr>
</tbody>
</table>
| 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. |

**Note:** 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:

<table>
<thead>
<tr>
<th>Option</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>To use a default instance of SQL Server:</td>
<td>Select the <strong>Default instance</strong> option.</td>
</tr>
<tr>
<td>To use a named instance of SQL Server:</td>
<td>1. Select the <strong>Named instance</strong> option.</td>
</tr>
<tr>
<td></td>
<td>2. If the SQL Server instance is local, select it from the list. If</td>
</tr>
<tr>
<td></td>
<td>the SQL Server instance is remote, type its name in the field.</td>
</tr>
</tbody>
</table>

17. Click **Next**.

   **Step Result:** The **SQL Server Authentication** page opens.

![SQL Server Authentication Page](image)

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>To use Windows authentication:</td>
<td>Select the <strong>Windows Authentication</strong> option.</td>
</tr>
</tbody>
</table>
Option | Steps
--- | ---
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.

**Note:** 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 assign 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)* on page 61.

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

<table>
<thead>
<tr>
<th>Page</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>If the <strong>Destination Location</strong> page opens:</td>
<td>Click <strong>Next</strong> and proceed to the next step.</td>
</tr>
</tbody>
</table>
| 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.  
**Tip:** Click **View Configuration Detail** for detailed information about SQL Server configuration status requirements. |

a) Click **Browse**.  
b) Define the desired file path using either the **Look in** lists or the **Folder name** field.
c) Click **OK**.

**Step Result:** 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**.

   **Step Result:** The *Content Storage Location* field reflects your changes.
22. Click Next.

**Step Result:** The *Proxy Settings* page opens.

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

![Proxy Settings Page]

**Figure 11: Proxy Settings Page**

**Note:** 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.

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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Address</td>
<td>The IP address of the applicable proxy server.</td>
</tr>
</tbody>
</table>
### Field | Type
--- | ---
Port | The port number used for communication.

**Note:** 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.

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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>A user name that authenticates with the proxy.</td>
</tr>
<tr>
<td>Password</td>
<td>The password associated with the user name.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>The password retyped.</td>
</tr>
</tbody>
</table>

25. Click **Next**.

**Step Result:** The **Agent to Server Communication** page opens.

![Agent to Server Communication Page](image)

Figure 12: Agent to Server Communication Page
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.

**Note:** 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.

**Note:** 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**.

**Step Result:** The **Installation Ready** page opens.

![Installation Ready Page](image)

Figure 13: Installation Ready Page
29. [Optional] If you only want to install core components, clear the **Automatically include all licensed modules and updates during installation** check box.

**Note:** 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/).

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.

**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 Configuring SSL on page 87.
- If your server will not use SSL, proceed to Logging In to Ivanti Endpoint Security on page 76.

### 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:**

- As applicable to your network environment, you have gathered the information and completed the tasks itemized in the Server Installation Checklist on page 95.
- Complete Configuring SQL Server to Accept Remote Connections on page 84
- If installing using SSL, complete the first portion of Configuring SSL on page 87.


   **Note:** 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.

**Note:** 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.

**Step Result:** 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**.

   **Step Result:** 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**.

   **Step Result:** The **Customer Information** page opens.

Figure 14: Customer Information Page
9. Type the applicable information in the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company Name</td>
<td>Your company name.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>Your Ivanti Endpoint Security serial number.</td>
</tr>
</tbody>
</table>

**Note:** 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](mailto: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.

<table>
<thead>
<tr>
<th>Page/Dialog</th>
<th>Step</th>
</tr>
</thead>
<tbody>
<tr>
<td>If the Question dialog opens:</td>
<td>Click <strong>Yes</strong> to start network discovery services. The following services are necessary to use discovery features within Ivanti Endpoint Security:</td>
</tr>
<tr>
<td></td>
<td>• DNS Client</td>
</tr>
<tr>
<td></td>
<td>• Function Discovery Resource Location</td>
</tr>
<tr>
<td></td>
<td>• SSDP Discover</td>
</tr>
<tr>
<td></td>
<td>• UPnP Device Host</td>
</tr>
<tr>
<td>Page/Dialog</td>
<td>Step</td>
</tr>
<tr>
<td>------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>If the <em>Required IIS Features</em> page opens:</td>
<td>Your server does not have the required IIS features installed. Click <strong>Install Features</strong> to install the features and proceed.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> 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:</td>
</tr>
<tr>
<td></td>
<td>• Static Content</td>
</tr>
<tr>
<td></td>
<td>• Default Document</td>
</tr>
<tr>
<td></td>
<td>• HTTP Errors</td>
</tr>
<tr>
<td></td>
<td>• ASP.NET</td>
</tr>
<tr>
<td></td>
<td>• .NET Extensibility</td>
</tr>
<tr>
<td></td>
<td>• ASP</td>
</tr>
<tr>
<td></td>
<td>• ISAPI Extensions</td>
</tr>
<tr>
<td></td>
<td>• ISAPI Filters</td>
</tr>
<tr>
<td></td>
<td>• Basic Authentication</td>
</tr>
<tr>
<td></td>
<td>• Windows Authentication</td>
</tr>
<tr>
<td></td>
<td>• Static Content Compression</td>
</tr>
<tr>
<td></td>
<td>• Dynamic Content Compression</td>
</tr>
<tr>
<td>If the <em>System Requirements</em> page opens:</td>
<td>Your server does not meet the minimum installation requirements.</td>
</tr>
<tr>
<td></td>
<td>• If you receive only system requirement <strong>warnings</strong>, you may proceed with installation by clicking <strong>Next</strong>. Ivanti recommends resolving warnings before proceeding with installation.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> 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.</td>
</tr>
<tr>
<td></td>
<td>• If you receive any system requirement <strong>failures</strong>, you must cancel the installation, resolve these failures, and then restart installation.</td>
</tr>
<tr>
<td></td>
<td><strong>Tip:</strong> Click <strong>View all Failures/Warnings</strong> for detailed information about prerequisite status deficiencies.</td>
</tr>
<tr>
<td>If the <em>Service Accounts</em> page opens:</td>
<td>Proceed to the next step.</td>
</tr>
</tbody>
</table>
11. Define the Web client account and service account that your Ivanti Endpoint Security server will use. Select from the following options.

<table>
<thead>
<tr>
<th>Option</th>
<th>Steps</th>
</tr>
</thead>
</table>
| **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** on page 22. |                                                                                                                                                                                                                                                                                                                                 |
12. Click **Next**.

If required, acknowledge the creation of new accounts by clicking **OK**.

**Step Result:** The **SQL Server Instance** Page opens.

![SQL Server Instance Page](image.png)

Figure 15: SQL Server Instance Page

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

Step Result: The SQL Server and Instance page opens.

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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>To use a default SQL Server instance:</td>
<td>Select the Default instance option.</td>
</tr>
<tr>
<td>To use a named SQL Server instance:</td>
<td>1. Select the Named instance option.</td>
</tr>
<tr>
<td></td>
<td>2. Type the instance name in the Named instance field.</td>
</tr>
</tbody>
</table>
17. Click **Next**.

**Step Result:** The *SQL Server Authentication* page opens.

![SQL Server Authentication Page](image)

**Figure 17: SQL Server Authentication Page**

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

Select from the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>To use Windows authentication:</td>
<td>Select the <em>Windows Authentication</em> option.</td>
</tr>
</tbody>
</table>
Option | Steps
--- | ---
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.

**Note:** 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)* on page 61.

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

<table>
<thead>
<tr>
<th>Page</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>If the <strong>Destination Location</strong> page opens:</td>
<td>Click <strong>Next</strong> and proceed to the next step.</td>
</tr>
</tbody>
</table>
| 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.  
**Tip:** 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**.

**Step Result:** The **Content Storage Location** field reflects your changes.

21. Click **Next**.

**Step Result:** The **Proxy Settings** page opens.

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

Figure 18: Proxy Settings Page

**Note:** 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.
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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Address</td>
<td>The IP address of the applicable proxy server.</td>
</tr>
<tr>
<td>Port</td>
<td>The port number used for communication.</td>
</tr>
</tbody>
</table>

**Note:** 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.

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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>A user name that authenticates with the proxy.</td>
</tr>
<tr>
<td>Password</td>
<td>The password associated with the user name.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>The password retyped.</td>
</tr>
</tbody>
</table>
24. Click **Next**.

**Step Result:** The *Agent to Server Communication* page opens.

![Agent to Server Communication Page](image)

Figure 19: Agent to Server Communication Page

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.

**Note:** 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 (*computename.domainname.com*)
- Computer name (*computename*)
- IP address (*10.10.10.10*)

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

**Note:** 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.

**Step Result:** The *Installation Ready* page opens.

![Installation Ready Page](image)

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

**Note:** 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/).

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.

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 Configuring SSL on page 87.
- If your server will not use SSL, proceed to Logging In to Ivanti Endpoint Security on page 76.

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.

Table 9: Install Procedure

<table>
<thead>
<tr>
<th>Procedure Portion</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Beginning Installation (Part I)</strong> on page 62</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Creating Components on SQL Server (Part II)</strong> on page 69</td>
<td>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.</td>
</tr>
</tbody>
</table>
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:

- As applicable to your network environment, you have gathered the information and completed the tasks itemized in the Server Installation Checklist on page 95.
- Complete Configuring SQL Server to Accept Remote Connections on page 84
- If installing using SSL, complete the first portion of Configuring SSL on page 87.

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.

   **Note:** 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.

   **Step Result:** 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**.

   **Step Result:** 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.

**Step Result:** The *Customer Information* page opens.

![Customer Information Page](image)

Figure 21: Customer Information Page

8. Type the applicable information in the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company Name</td>
<td>Your company name.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>Your Ivanti Endpoint Security serial number.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> 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 <em>Ivanti Sales Support</em> (<a href="mailto:sales@ivanti.com">sales@ivanti.com</a>).</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Page/Dialog</th>
<th>Step</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>If the Question dialog opens:</strong></td>
<td>Click <strong>Yes</strong> to start network discovery services. The following services are necessary to use discovery features within Ivanti Endpoint Security:</td>
</tr>
<tr>
<td></td>
<td>• DNS Client</td>
</tr>
<tr>
<td></td>
<td>• Function Discovery Resource Location</td>
</tr>
<tr>
<td></td>
<td>• SSDP Discover</td>
</tr>
<tr>
<td></td>
<td>• UPnP Device Host</td>
</tr>
<tr>
<td><strong>If the Required IIS Features page opens:</strong></td>
<td>Your server does not have the required IIS features installed. Click <strong>Install Features</strong> to install the features and proceed.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> 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:</td>
</tr>
<tr>
<td></td>
<td>• Static Content</td>
</tr>
<tr>
<td></td>
<td>• Default Document</td>
</tr>
<tr>
<td></td>
<td>• HTTP Errors</td>
</tr>
<tr>
<td></td>
<td>• ASP.NET</td>
</tr>
<tr>
<td></td>
<td>• .NET Extensibility</td>
</tr>
<tr>
<td></td>
<td>• ASP</td>
</tr>
<tr>
<td></td>
<td>• ISAPI Extensions</td>
</tr>
<tr>
<td></td>
<td>• ISAPI Filters</td>
</tr>
<tr>
<td></td>
<td>• Basic Authentication</td>
</tr>
<tr>
<td></td>
<td>• Windows Authentication</td>
</tr>
<tr>
<td></td>
<td>• Static Content Compression</td>
</tr>
<tr>
<td></td>
<td>• Dynamic Content Compression</td>
</tr>
</tbody>
</table>
### 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.

**Note:** 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.

**Tip:** 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.

- [Optional] Edit the **Web Client Account Username** field.
- In the **Web Client Account Password** field, type the desired password.
- In the **Web Client Account Confirm password** field, retype the password.
- [Optional] Edit the **Service Account Username** field.
- In the **Service Account Password** field, type the desired password.
- In the **Service Account Confirm password** field, retype the password.

**Note:** Ivanti recommends using the default account user names the installation creates.
11. Click **Next**.
   If required, acknowledge the creation of new accounts by clicking **OK**.
   
   **Step Result:** The **SQL Server Instance** Page opens.

![Figure 22: SQL Server Instance Page](image)

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

**Step Result:** The *SQL Server and Instance* page opens.

![Image of SQL Server and Instance Page](image)

Figure 23: SQL Server and Instance Page (No Local Options)

**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) on page 34.

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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>To use a default SQL Server instance:</td>
<td>Select the <strong>Default instance</strong> option.</td>
</tr>
<tr>
<td>To use a named SQL Server instance:</td>
<td>1. Select the <strong>Named instance</strong> option.</td>
</tr>
<tr>
<td></td>
<td>2. Type the instance name in the <strong>Named instance</strong> field.</td>
</tr>
</tbody>
</table>
16. Click Next.

**Step Result:** The *SQL Server Authentication* page opens.

![SQL Server Authentication Page](image)

Figure 24: SQL Server Authentication Page

17. Click Next.

**Step Result:** *The credentials provided do not have sufficient privileges to continue* dialog opens.

![Insufficient Credentials Dialog](image)

Figure 25: Insufficient Credentials Dialog

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)* on page 69.

**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 84.
- Complete *Configuring Windows Firewall for SQL Server Instance Access* on page 86.
- 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.

**Tip:** If you have any questions and/or require additional assistance, contact Ivanti support at https://community.ivanti.com/community/contact-support.

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 Management 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**.

**Step Result:** 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.

**Step Result:** The New User dialog opens.

![New User Dialog](image)

**Figure 26: New User Dialog**

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.

**Note:** 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**.

**Step Result:** 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**.

4. In the field, type cmd.

5. Click OK.

   **Step Result:** A command prompt opens.

6. From the command prompt, type `sqlcmd -S SERVERNAME\INSTANCENAME -E -i filepath \PreInstallDBAscript.sql -k1>c:\PreInstallDBAscript_out.txt`.

   **Note:** 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.

**Result:** The following databases are created:

<table>
<thead>
<tr>
<th>Database</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PLUS</td>
<td>Patch Management Database</td>
</tr>
<tr>
<td>PLUS_Staging</td>
<td>Content Replication Database</td>
</tr>
<tr>
<td>SCM</td>
<td>Security Configuration Management Database</td>
</tr>
<tr>
<td>STAT_Guardian</td>
<td>Network Discovery/Agent Deployment Database</td>
</tr>
<tr>
<td>UPCCommon</td>
<td>Endpoint Management Platform Database</td>
</tr>
</tbody>
</table>

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 page 71.

**Completing Installation (Part III)**

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

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.

**Tip:** If you have any questions and/or require additional assistance, contact Ivanti support at [https://community.ivanti.com/community/contact-support](https://community.ivanti.com/community/contact-support).

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

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

   a) Click Browse.
   b) Define the desired file path using either the Look in lists or the Folder name field.
   c) Click OK.
   **Step Result:** The Installation Folder field reflects your changes.

   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.
   **Step Result:** The Content Storage Location field reflects your changes.
5. Click **Next**.

**Step Result:** The *Proxy Settings* page opens.

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

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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Server Address</strong></td>
<td>The IP address of the applicable proxy server.</td>
</tr>
</tbody>
</table>
# Ivanti Endpoint Security

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>The port number used for communication.</td>
</tr>
</tbody>
</table>

**Note:** 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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>A user name that authenticates with the proxy.</td>
</tr>
<tr>
<td>Password</td>
<td>The password associated with the user name.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>The password retyped.</td>
</tr>
</tbody>
</table>

8. Click **Next**.

**Step Result:** The **Agent to Server Communication** page opens.

![Agent to Server Communication Page](image)

Figure 28: Agent to Server Communication Page
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.

   **Note:** 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 (computename.domainname.com)
    - Computer name (computename)
    - IP address (10.10.10.10)

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

   **Note:** 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**.

   **Step Result:** The *Installation Ready* page opens.

   ![Installation Ready Page](image)

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

**Note:** 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**.

**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 *Configuring SSL* on page 87.
- If your server will not use SSL, proceed to *Logging In to Ivanti Endpoint Security* on page 76.

---

**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.

**Note:** 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.

   **Tip:** You can also use the server IP address.

   **Step Result:** 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**.

   **Result:** Ivanti Endpoint Security opens to the **Home** page and launches the **Application Setup Manager**.

---

**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** on page 76.

   **Step Result:** Ivanti Endpoint Security opens and the **Application Setup Manager** displays. This dialog only appears 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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>First name</td>
<td>Your first name.</td>
</tr>
<tr>
<td>Last name</td>
<td>Your last name.</td>
</tr>
<tr>
<td>Company name</td>
<td>Your company name. The company name specified during installation appears by default but can be edited.</td>
</tr>
</tbody>
</table>

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 (https://help.ivanti.com/).

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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP Host</td>
<td>The local SMTP mail host name. Ivanti Endpoint Security uses your corporate Internet (SMTP) mail server.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>‘From’ email address</td>
<td>The email address used when the system sends email notifications.</td>
</tr>
<tr>
<td>‘To’ email address</td>
<td>An email address you use to receive system notifications.</td>
</tr>
</tbody>
</table>

**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*](https://help.ivanti.com/).

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**.

   **Step Result:** Your initial settings are applied.

17. Click **Close**.

   **Result:** Initial configuration is complete. You are now ready to begin monitoring your network with Ivanti Endpoint Security.
Appendix A

Configuring Remote SQL Server Instances

In this appendix:
• Creating Remote Accounts
• Configuring SQL Server to Accept Remote Connections
• Configuring Windows Firewall for SQL Server Instance Access

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.

Note: 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**.

**Step Result:** 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**.

**Step Result:** The **New User** dialog opens.

![New User Dialog](image)

**Figure 30: New User Dialog**

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**.

**Step Result:** The Web client account is created.
12. Repeat steps 5 through 11 to create the service account.

   **Step Result:** 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**.

   **Step Result:** The **Administrators Properties** dialog opens.

![Administrators Properties Dialog](image)

Figure 31: Administrators Properties Dialog
16. Click Add.

**Step Result:** The *Select Users* dialog opens.

![Select Users Dialog](image)

17. In the **Enter the object names to select** dialog, type your service account name.

18. Click **OK**.

**Step Result:** The service account is added to the *Administrators* group.

19. Click **OK**.

**Result:** 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.

   **Step Result:** SQL Server Configuration Manager opens.

   ![Image of SQL Server Configuration Manager]

   **Figure 33: SQL Server Configuration Manager**

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 Manager (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**.

**Result:** 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 on page 86.

---

### 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).


**Note:** 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

In this appendix:
• Configuring 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.

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

For security purposes, you can configure the Ivanti Endpoint Security server and agent to use SSL communication. To use SSL, assign your certificate to the Ivanti Endpoint Security Web site.

Prerequisites:
You must obtain a certificate from a root certificate authority.

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

Note: 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 Ivanti Community Article 53859 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.

   Step Result: Internet Information Services (IIS) Manager opens.
b) From the tree, select your Ivanti Endpoint Security server.

Figure 34: Internet Information Services (IIS) Manager

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

**Step Result:** The **Server Certificates** page opens.

Figure 35: Server Certificates Page
d) Click the **Import** link.

**Step Result:** The **Import Certificate** dialog opens.

![Import Certificate Dialog](image)

Figure 36: Import Certificate Dialog

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.

**Step Result:** The **Site Bindings** dialog opens.
c) Click **Add**.

**Step Result:** The *Add Site Binding* dialog opens.

![Figure 37: Add Site Binding Dialog](image)

- **Type** list, select **https**.
- From the **SSL certificate** list, select your certificate.
- Click **OK**.
- Click **Close**.

3. Complete one of the following Ivanti Endpoint Security installation procedures listed in Selecting an Installation Method on page 23.

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

   **Note:** 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**.

      **Step Result:** *Internet Information Services (IIS) Manager* opens.

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

   c) Click the **Bindings** link.

      **Step Result:** The *Site Bindings* dialog opens.
d) Click Add.

**Step Result:** The Add Site Binding dialog opens.

![Add Site Binding Dialog](image)

Figure 38: Add Site Binding Dialog

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.
   a) In the main pane, scroll to the **IIS** section.
   b) Double-click **SSL Settings**.
   c) Select the **Require SSL** check box.
   d) Click **Apply**.

**Result:** Your server is now configured for SSL communication.

---

**After Completing This Task:**

- Complete **Logging In to Ivanti Endpoint Security** on page 76.
- Complete **Setting Up Ivanti Endpoint Security** on page 77.
- After you have completed setup, edit your global configuration policy set and ensure **Use SSL for agent to server communication** to **True**. For additional information, refer to **Secure Your Server With SSL** in the [Ivanti Endpoint Security User Guide](https://help.ivanti.com/).
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 (https://help.ivanti.com).
Appendix D

Installation Checklist

In this appendix: For your convenience, an installation checklist is provided that itemizes information and tasks.

- Server Installation Checklist

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:

☐ You target server has the required service packs installed for its operating system. For more information, see Supported Operating Systems on page 7.

☐ Your target computer meets or exceeds the hardware requirements listed in Combined Ivanti Endpoint Security Application and Database Server on page 16.

☐ Your server is not a Domain Controller.

☐ Your server has all required software installed:

<table>
<thead>
<tr>
<th>Software</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft SQL Server</td>
<td>SQL Server Requirements on page 11</td>
</tr>
<tr>
<td>Microsoft Internet Information Services</td>
<td>IIS Requirements on page 12</td>
</tr>
<tr>
<td>Web Browser</td>
<td>Web Browser Requirements on page 10</td>
</tr>
</tbody>
</table>

☐ Ensure the target server uses one of supported locales and browser languages listed in Supported Languages and Locales on page 8.

☐ Your Ivanti Endpoint Security server meets network requirements listed in Network Requirements on page 14.
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.

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

If you are using SSL, you have started the first portion of Configuring SSL on page 87 (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: ________________
- User name: ______________
- 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 remote SQL instance, the instance is configured to accept remote connections. For additional information, refer to Configuring SQL Server to Accept Remote Connections on page 84.

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 on page 86.

Your local SMTP mail host name is: ________________________________