Agent Install Guide

8.6

ivanti

Endpoint Security

powered by HEAT

Notices

Version Information

Ivanti Endpoint Security Agent Install Guide - Ivanti Endpoint Security Version 8.6 - Published: Dec 2020

Document Number: 02_017_8.6_171251616

Copyright Information

Table of Contents

Chapter 1

Agent Requirements

In this chapter:

The Ivanti Endpoint Security Agent is supported on a variety of operating systems and platforms. Before installing the agent on an endpoint, ensure that system meets the agent requirements.

Your endpoints must meet the hardware and software requirements for the Ivanti Endpoint Security Agent. The following sections include system requirements that you should verify prior to installing the Ivanti Endpoint Security Agent. The complete list of requirements are listed in the following topics:

- Supported Endpoint Operating Systems on page 7
- Supported Endpoint Browsers on page 11
- Windows Endpoint Requirements on page 11
- Linux, UNIX, or Mac Endpoint Requirements on page 13
- Agent Locales and Internationalization on page 16
- Supported Endpoint Module Operating Systems on page 17

Supported Endpoint Operating Systems

The Ivanti Endpoint Security Agent is supported on most operating systems used in enterprise environments.

The agent is supported on endpoints that contain one of the supported endpoint operating system types:

- Windows Endpoint Operating Systems on page 8
- Mac Endpoint Operating Systems on page 10
- Linux Endpoint Operating Systems on page 10
- UNIX Endpoint Operating Systems on page 10

Windows Endpoint Operating Systems

Ivanti Endpoint Security Agent 8.6 can be installed on most windows platforms.

Supported Windows Operating Systems

Supported Operating Systems	Supported Editions
Windows 10 (32- and 64-bit). For specific Windows 10 version support refer to the following articles: Ivanti Endpoint Security Windows 10 Version Support Matrix Microsoft Support Windows Lifecycle Fact Sheet	• Education • Education N • Enterprise • Enterprise N • Enterprise 2015 Long Term Servicing Branch (LTSB) • Enterprise N 2015 LTSB • Professional • Professional N
Windows 8.1 (32- and 64-bit)	• Enterprise • Enterprise N • Professional[1] • Professional N
Windows Embedded 8.1 (32- and 64-bit)	• Industry Pro • Industry Enterprise

1. This edition is also supported when Windows Media Center is installed.

Supported Windows Server Operating Systems

Supported Operating Systems	Supported Editions
Windows Server 2019 (32- and 64-bit)	• Standard[1] • Datacenter • Essentials
Windows Server 2016 (32- and 64-bit)	• Standard[1] • Datacenter • Essentials
Windows Server 2012 R2 (32- and 64-bit)	• Standard[1] • Datacenter[1] • Foundation • Essentials
Windows Server 2012 (32- and 64-bit)	• Standard[1] • Datacenter[1] • Foundation • Essentials
Windows Storage Server 2012 (32- and 64-bit)	• Standard • Workgroup

1. *Core* mode for this edition is supported.

Mac Endpoint Operating Systems

A different agent, the Linux/Unix/macOS Agent, can be installed on many different versions of Mac operating systems. This version of the agent offers only Patch and Remediation functionality.

For details of the supported macOS operating systems, refer to the Linux/Unix/macOS Agent Release Notes

Linux Endpoint Operating Systems

A different agent, the Linux/Unix/macOS Agent, can be installed on many different versions of Linux. This version of the agent offers only Patch and Remediation functionality.

For details of the supported Linux versions, refer to the Linux/Unix/macOS Agent Release Notes

UNIX Endpoint Operating Systems

A different agent, the Linux/Unix/macOS Agent, can be installed on many different versions of UNIX. This version of the agent offers only Patch and Remediation functionality.

For details of the supported Linux versions, refer to the Linux/Unix/macOS Agent Release Notes

Supported Endpoint Browsers

Ivanti Endpoint Security (Ivanti Endpoint Security) is an Internet application that conforms to standard Web conventions. Ivanti recommends you download the most recent version of the Ivanti Endpoint Security Agent installer using a supported Web browser.

Table 4: Supported Web Browsers

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

Windows Endpoint Requirements

Before installing the Ivanti Endpoint Security (Ivanti Endpoint Security) Agent on a supported Windows endpoint, ensure that it meets the necessary hardware and software requirements.

Processor	800 MHz or higher **Note:** Minimum of 2 CPU cores is recommended for optimal performance during intensive operations like Discover Applicable Updates (DAU) or AntiVirus scans.
Physical RAM	1 GB (minimum) **Note:** Your Ivanti Endpoint Security endpoint may require additional RAM depending on the RAM requirements of other applications installed.
Free Disk Space	1 GB of free space
Network Connection	A 10 Mbps network connection with access to the Ivanti Endpoint Security server.
Antivirus	Ensure any third-party antivirus software on the endpoint computer is disabled prior to Ivanti Endpoint Security Agent installation.

Port Requirements

- Port 80

  This must be open for Ivanti Endpoint Security module downloads.
- Port 443

  This must be open for Ivanti Endpoint Security policy download and general communication.
- Ephemeral ports

  This is used to listen for Notification Manager connection requests (Patch and Remediation) only.

  - Open ports 49152-65535.

Microsoft .NET Framework

Microsoft .NET Framework (is required for Patch and Remediation only). The required version of the .NET Framework changes according to operating system.

Table 5: .NET Framework Version

Operating System	.Net Framework Version
Microsoft Windows 10	4.0+
Microsoft Windows 8.1	4.0+
Microsoft Windows Server 2019	4.0+
Microsoft Windows Server 2016	4.0+
Microsoft Windows Server 2012 R2	4.0+
Microsoft Windows Server 2012	4.0+
Microsoft Windows Storage Server 2012	4.0+

Other Software Requirements

Windows Installer 3.1 or later

Microsoft Visual C++ 2010 Redistributable Package or later

Note: If not installed at time of agent installation, the Microsoft Visual C++ 2010 Redistributable Package is installed during agent installation.

Blank Page

Linux, UNIX, or Mac Endpoint Requirements

Before installing the Ivanti Endpoint Security Agent on a supported Linux, UNIX, or Mac endpoint, ensure that it meets the necessary hardware and software requirements.

Processor	500 MHz processor or higher
Physical RAM	256 MBs or greater **Note:** Your Ivanti Endpoint Security endpoint may require additional RAM depending on the RAM requirements of other applications installed.
Disk Requirements	• Presence of a `/tmp` directory (`/var/tmp` on Oracle Solaris) with 100 MB of free space. • 50 MB of free space for the agent installation directory. • Ivanti Endpoint Security also recommends 100 Mb of unused disk space to download and install content.
Java Libraries	Ensure you have the appropriate Java libraries installed: • **All UNIX endpoints and Mac OS X endpoints prior to version 10.7.3:** Oracle Java Runtime Environment (JRE) 7 or later. • **Mac OS X endpoints versions 10.7.3 and higher:** Oracle Java Development Kit (JDK) 7 or later. • **Linux endpoints:** Oracle JRE 7 or later. **Note:** OpenJDK 7 can be substituted for Oracle Java JRE on the following operating systems: • CentOS Linux • Oracle Enterprise Linux • Red Hat Enterprise Linux • SUSE Linux Enterprise Refer to IcedTea Project (http://openjdk.java.net/projects/icedtea/) for additional information.
Perl	Perl is needed for Linux content. Perl is automatically installed for all open-source Linux operating systems unless uninstalled. **Tip:** To determine if you have perl installed, type `perl -v` on a command line. Refer to Perl Download (http://www.perl.org/get.html) to download.
Network Connection	A 10 Mbps network connection with access to the Ivanti Endpoint Security server.

Antivirus	Ensure any antivirus software installed on the applicable endpoint computer is disabled.
Port Requirements	• Port `80`. This must be open for Ivanti Endpoint Security module downloads. • Port `443`. This must be open for Ivanti Endpoint Security policy download and general communication. • Ports `49152-65535`. These ports are used as listener ports for *check now* commands, which are server-sent requests that agents use to check for tasks. Closing these ports delays agent tasks until they check in themselves.

Agent Locales and Internationalization

The Ivanti Endpoint Security Agent is localized and internationalized for a variety of languages.

The agent has been fully localized and translated for the following locales.

- en-AU: English (Australia)
- en-BZ: English (Belize)
- en-CA: English (Canada)
- en-IN: English (India)
- en-IE: English (Ireland)
- en-JM: English (Jamaica)
- en-NZ: English (New Zealand)
- en-PH: English (Philippines)
- en-SG: English (Singapore)
- en-ZA: English (South Africa)
- en-GB: English (United Kingdom)
- en-US: English (United States)
- fr-FR: French (France)
- de-DE: German (Germany)
- it-IT: Italian (Italy)
- ja-JP: Japanese (Japan)
- nl-NL: Dutch (Netherlands)
- pt-BE: Portuguese (Brazil)
- ru-RU: Russian (Russia)
- es-ES: Spanish (Spain)
- sv-SE: Swedish (Sweden)
- zh-CN / zh-CHS: Chinese (China [Simplified])
- zh-TW / zh-CHT: Chinese (Taiwan [Traditional])

Note: The agent has been internationalized to operate in the following locales. However, the agent UI text has not been translated. English text is displayed.

- da-DA: Danish (Denmark)
- fi-FI: Finnish (Finland)
- ko-KR: Korean (Korea)
- no-NO: Norwegian - Nynorsk (Norway)

Supported Endpoint Module Operating Systems

The modules that you can install vary by operating system and your licensing.

- Windows Endpoint Supported Modules on page 17
- Linux, UNIX, and Mac Supported Modules on page 18

A list of module abbreviations within the tables:

PR	Ivanti Patch and Remediation
LAC	Ivanti Application Control
DC	Ivanti Device Control
AV	Ivanti AntiVirus
PM	Ivanti Power Management
WOL	Ivanti Wake on LAN
SCM	Ivanti Security Configuration Management
RSM	Ivanti Remote Systems Management

Windows Endpoint Supported Modules

The following table lists the modules you can install on endpoints that contain a Windows operating system.

Table 6: Supported Endpoint Windows Operating Systems by Module

Operating System[1]	Modules[2]							
	PR	LAC	DC	AV	PM	WOL	SCM	RSM
Microsoft Windows 10	✓	✓	✓	✓	✓	✓	✓	✓
Microsoft Windows 8.1	✓	✓	✓	✓	✓	✓	✓	✓
Microsoft Windows Server 2019	✓	✓	✓	✓	✓	✓	✓	✓
Microsoft Windows Server 2016	✓	✓	✓	✓	✓	✓	✓	✓

Operating System[1]	Modules[2]							
	PR	LAC	DC	AV	PM	WOL	SCM	RSM
Microsoft Windows Server 2012 R2	✓	✓	✓	✓	✓	✓	✓	✓
Microsoft Windows Server 2012	✓	✓	✓	✓	✓	✓	✓	✓
Microsoft Windows Storage Server 2012	✓	✓	✓	✓	✓	✓	✓	✓

1. Refer to Supported Endpoint Operating Systems on page 21 for a complete list of operating system versions.
2. Refer to Supported Endpoint Module Operating Systems on page 31 for a list of module abbreviation definitions.

Linux, UNIX, and Mac Supported Modules

Ivanti offers a version of the agent for Linux, UNIX, and Mac that provides Patch and Remediation functionality.

Patch Agent for Linux, UNIX, and Mac supports functionality for the Patch and Remediation module and *only* the Patch and Remediation module. All other Ivanti Endpoint Security modules are not supported for these platforms.

Chapter 2

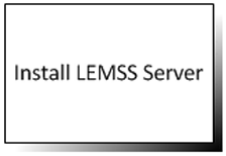
Understanding Agent Installation

In this chapter:

The Ivanti Endpoint Security agent is installed on network endpoints to manage their behavior.

The Ivanti Endpoint Security Agent Workflow

Ivanti Endpoint Security uses a server/client relationship to manage network endpoints. Review this chart to understand the Ivanti Endpoint Security Agent workflow.



Install the Ivanti Endpoint Security (Ivanti Endpoint Security) server and complete an initial replication with the Global Subscription Server. You must have completed a server install prior to installing a Ivanti Endpoint Security Agent.

Note: For server installation information, refer to the Ivanti Endpoint Security: Server Installation Guide (https://help.ivanti.com) .

Prior to installing the agent on an endpoint, determine agent requirements. Refer to Agent Requirements on page 7 for all requirements. For requirements on the endpoint by operating system, refer to:

- Windows Endpoint Requirements on page 11
- Linux, UNIX, or Mac Endpoint Requirements on page 13

Prior to installing the agent on an endpoint, ensure you understand the methods used to install the agent. Refer to Understanding Agent Installation Methods on page 21.

Install the agent. You may install agents on any endpoints that you want to manage. Agent installation is based on administrator need and operating system type. Refer to the following:

- Installing the Agent on Windows on page 23
- Installing the Agent on Linux, UNIX, or Mac on page 67

Following initial installation, the agent and server components begin communicating. The agent downloads the following data from the Ivanti Endpoint Security server:

- Agent policies, which contain information about how the agent should behave.
- Agent packages, which contain files to modify the agent.

The agent uploads the following data to the Ivanti Endpoint Security server:

- Host endpoint operating system information.
- Heartbeats, which are notification messages the agent sends to the server. This message is used continually to notify the server that the agent is available within the network.
- The state of the endpoint and applicable module logs.

After you install the agent on an endpoint, you may access its available controls using the **Agent Control Panel**. Refer to *Using the Ivanti Endpoint Security Agent* in the Ivanti Endpoint Security User Guide (https://help.ivanti.com/) for additional information.

Additionally, if you are licensed for additional Ivanti Endpoint Security modules, you can install these modules on the Ivanti Endpoint Security endpoint that has an agent. Installing modules expands agent functionality.

Note: For more information on modules and module installation, refer to Ivanti Endpoint Security User Guide (https://help.ivanti.com/) .

Understanding Agent Installation Methods

You can install the Ivanti Endpoint Security Agent on your network using a variety of methods.

Network administrators should carefully consider which method to use when installing the agent as each method has its own unique steps. The following table describes each installation method.

Table 7: Installation Methods

Installation Method	Description
Agent Management Job	Benefits in using this method: • Using this method you search for endpoints in your network and then install the agent on network endpoints based on criteria you define. • You complete the Agent Management Job within the Ivanti Endpoint Security Web console using an easy-to-use wizard. • Using this method eases administrative workload, since you do not have to install agents locally on endpoints. • Using this method you may uninstall the agent on network endpoints based on criteria you define. **Important:** This method only supports endpoints that contain a Windows operating system. Refer to the *Command Line* method to install an agent on an endpoint that has a supported Mac, Linux, UNIX, or Mac operating system.
Install Wizard	Benefits in using this method: • This method utilizes an easy-to-use installation wizard to install a single agent on an endpoint. • This installation method is useful if you are unfamiliar with using the command line prompt to install a single agent on a network endpoint. • The agent is installed using an installation wizard and accessed using a graphical user interface via the ***Control Panel***. • The installer for Windows uses the familiar `EXE` file format. • This method supports Windows only.

<table>
<tr><th>Installation Method</th><th>Description</th></tr>
<tr><td>Command Line</td><td>Benefits in using this method:
You may use command line to install the agent.
You may complete silent installs when using a command line parameters. When using silent installs using a command line, the installation of the agent can be run unattended (without user interaction).
This install method supports an endpoint that has one of the following operating systems:
Windows
Linux, UNIX, or Mac</td></tr>
<tr><td>Other Methods</td><td><table><tr><td>Third-Party Software</td><td>In some environments, customers may prefer to use third-party software, such as PsExec, to install the agent.</td></tr><tr><td>Golden Image</td><td>In networks making substantial use of golden images, which are compressed operating system archives that are entirely installed and configured according to an organization's specifications, network administrators may benefit from adding the Ivanti Endpoint Security Agent to their image.</td></tr></table>Attention: These installation methods are not documented in this guide. For additional information on these installation methods, contact Support..</td></tr>
</table>

Note: Supported operating systems listed in this topic are generalized for each operating system. Before installing the agent on an endpoint, ensure its operating system is supported by referring to Supported Endpoint Operating Systems on page 7.

Chapter 3

Installing the Agent on Windows

In this chapter:

There are various methods when installing the Ivanti Endpoint Security Agent on a Windows endpoint.

Windows Installation Methods

To install the Ivanti Endpoint Security Agent on a Windows platform you can utilize various methods.

- An Agent Management Job. This method supports installing an agent on endpoints that have a Windows operating system using the Ivanti Endpoint Security Web console. For additional information, refer to Installing Agents by Agent Management Job on page 35.
- You may use a command line to install an agent on Windows endpoints. For additional information, refer to Silently Installing the Agent by Command Line for Windows on page 57.
- You may use the Ivanti Endpoint Security installer. This method uses an easy-to-use installation wizard that allows you to install a single agent on an endpoint. For additional information, refer to Manually Installing the Agent for Windows on page 63.

For a description of the benefits of each install method, refer to Understanding Agent Installation Methods on page 21.

Agent Management Job for Windows

The Ivanti Endpoint Security Web console utilizes the Agent Management Job method to install agents on Windows endpoints. This method uses an easy-to-use wizard to discover endpoints within your network and then install the agent.

This method only supports endpoints that use the Windows operating system.

Each Agent Management Job consists of two parts; endpoint detection and agent management itself.

Detection	The initial portion of an Agent Management Job detects endpoints and their operating systems in a network. This is done by scanning the network. Access to the endpoints is based on credentials used during job configuration.
Management	During agent management, the agent is installed (or uninstalled) based on information found during scanning. The Agent Management Job determines which type of agent to install on applicable endpoints. Agent installation occurs silently on the endpoint; endpoint users are unaware of the installation.

After installing Ivanti Endpoint Security (Ivanti Endpoint Security) on a server, you must perform additional configuration on the endpoint and server prior to an Ivanti Endpoint Security Agent Management Job.

Refer to Agent Management Job Checklist on page 24 for a description of the configuration needs on the endpoint and server prior to an Agent Management Job.

Agent Management Job Checklist

This checklist itemizes the information and tasks an administrator needs to perform prior to an Agent Management Job.

Prior to configuring your network to successfully use Agent Management Jobs, confirm the following information:

Tasks Performed on the Endpoint

- ☐ Verify your target endpoints meets or exceeds the requirements defined in the Windows Endpoint Requirements on page 11.
- ☐ Verify that your target endpoints are all supported Windows endpoints. You cannot complete an Agent Management Job on Linux, UNIX, or Mac endpoints. Refer to the list of Windows operating systems in the Supported Endpoint Operating Systems on page 7.
- ☐ Ensure any antivirus software installed on target endpoints is disabled.
- ☐ Verify that your target endpoints have applicable ports open. Refer to Port and ICMP Requirements for an Agent Management Job on page 25.
- ☐ Configure your target endpoints to accept an Agent Management Job. Target endpoints must be configured to allow the Agent Management Job access to the endpoint. This includes verifying that the C$ and ADMIN$ network shares are enabled, Refer to Configuring Windows Endpoints on page 26.

Tasks Performed on the Server

- ☐ Verify that your Ivanti Endpoint Security server can utilize the Discovery Scanning process needed in by the Agent Management Job. Refer to Configuring the Ivanti Endpoint Security Server for Discovery Scanning on page 34.

- ☐ Gather credentials for the endpoints. A user name and password that authenticates with Windows-based endpoints is required during configuration of the Agent Management Job. Type the user name in a local format (UserName) or a domain format (DOMAIN\UserName).
- ☐ Gather proxy information if your agents will be required to use a proxy to access your Ivanti Endpoint Security server. The proxy information is required during configuration of the Agent Management Job that is using a proxy server.

Note: A Squid proxy server will only properly resolve using a fully qualified domain name.

Refer to Ivanti Community Article 59102 for additional information on a Squid proxy server configuration.

Once you have completed the tasks in the list you may begin installing or uninstalling the Ivanti Endpoint Security Agent using an Agent Management Job. For information on this install method, refer to Installing Agents by Agent Management Job on page 35.

Port and ICMP Requirements for an Agent Management Job

Certain ports are required on the endpoint during the installation process of the Agent Management Job. Firewall configuration changes may be required to access applicable ports.

Note: If your firewall policies cannot allow needed port access, contact Ivanti Support (https://community.ivanti.com/community/contact-support) for a recommended configuration.

On the endpoint, open the ports listed in the following table.

Table 8: Required Ports

Required Ports	Direction	Description
• 445/TCP • 139/TCP • 135/UDP • 137/UDP	Inbound	Ivanti Endpoint Security uses these ports to access the endpoint during the installation of the Agent Management Job. After the Agent Management Job completes, you can close these ports. **Tip:** In addition, the Discovery Scan Job also use these ports to discover information about the endpoint.
• 443/TCP • 80/TCP	Outbound	Following agent installation, the Ivanti Endpoint Security Agent uses these ports to register and communicate with the Ivanti Endpoint Security server. After the Agent Management Job completes, you need to leave these ports open.

Both the Discovery Scan Job and the Agent Management Job requires the endpoint to accept ping requests from the Ivanti Endpoint Security server. Ping operates by sending Internet Control Message Protocol (ICMP) echo request packets to the target host and waiting for an ICMP response. Therefore,

you need an exception within your endpoint firewall for inbound Internet Control Message Protocol (ICMP) echo request.

Refer to Enable or disable Internet Control Message Protocol requests for ICF (http://technet.microsoft.com/en-us/library/cc738771(v=ws.10).aspx) for additional information.

Configuring Windows Endpoints

Prior to using an Agent Management Job to install agents on your Windows endpoints, you must first configure your endpoints.

Prerequisites:

Prior to configuring, review the following requirements:

- You can perform these steps on endpoints with the following operating systems:
  - Windows 10
  - Windows 8.1
  - Windows 7
  - Windows Server 2019
  - Windows Server 2016
  - Windows Server 2012 R2
  - Windows Server 2012
  - Windows Server 2008 R2
- You have gathered and confirmed the information and tasks in the Agent Management Job checklist. Refer to Agent Management Job Checklist on page 24 for a description.
- Verify your Windows endpoint meets the defined hardware and software requirements. Refer to Agent Requirements on page 7 for a complete list of agent requirements.

Note: If your organization uses a third-party firewall:

- Do not complete the steps for creating Windows Firewall exceptions. Your third-party firewall makes them unnecessary.
- However, you must create exceptions for Ivanti Endpoint Security within you third-party firewall. For additional information, refer to Port and ICMP Requirements for an Agent Management Job on page 25.

1. Start applicable Windows services.

   Tip: There are specific Windows services that are necessary for successful Agent Management Job completion.

   a) Open **Administrative Tools**.
   b) Double-click **Services**.

      Step Result: The ***Services*** dialog opens.

c) Ensure the necessary Windows services are started for an Agent Management Job.

The following list itemizes the services that must be started for Agent Management Job completion.

- **DCOM Server Process Launcher**
- **Remote Procedure Call (RPC)**
- **Server**
- **Windows Firewall**
- **Windows Management Instrumentation**

Note: In environments that use a third-party firewall, ensure the Windows Firewall service is instead *disabled*.

d) If all of the listed services required for your configuration purposes have a **Server status** of **Started**, continue to the next step. If any of the listed services for your configuration purposes are not started, complete the following:

1. Right-click the applicable service and select **Properties**.
2. Ensure **Startup type** list is set to **Automatic**. If edits are necessary, click **Apply** after selecting **Automatic** from the list.
3. Click **Start**.
4. Click **OK**.
5. If necessary, repeat the previous steps for each unstarted service.

e) Close the ***Services*** dialog and the ***Administrative Tools*** dialog.

Step Result: The applicable Windows services for a successful Agent Management Job are started.

2. Configure **Sharing and Discovery** settings.

Tip: The discovery setting allows the endpoint to be seen by the Ivanti Endpoint Security server, while the file sharing setting allows the Ivanti Endpoint Security server to install the agent during agent management. These settings are necessary for a successful Agent Management Job.

a) From ***Control Panel***, click **Network and Internet**.

Step Result: ***Control Panel*** opens to the **Network and Internet** options.

b) Click **Network and Sharing Center**.

Step Result: ***Control Panel*** opens to the ***Network and Sharing Center***.

c) Ensure **Network discovery** is enabled.

Enabling this setting makes the endpoint publicly known within the network.

Tip: Ivanti Endpoint Security uses the information shared by this setting to return more detailed information about the endpoint during discovery scanning.

Based on the endpoint operating system, complete the applicable steps.

Operating System	Step
• Windows 8.1 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 • Windows Server 2019	**1.** Click **Change advanced sharing settings**. **2.** Expand one of the following network locations: • **Private** • **Guest or Public** • **Domain** **3.** Scroll to **Network discovery**. **4.** Ensure **Turn on network discovery** option is selected. **5.** Ensure **Turn on automatic setup of network connected devices** option is cleared. **6.** If necessary, click **Save Changes**. **7.** Repeat these steps for each profile section.

d) Ensure **File sharing** is enabled.

Based on the endpoint operating system, complete the applicable steps.

Operating System	Step
• Windows 8.1 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 • Windows Server 2019	**1.** Click **Change advanced sharing settings**. **2.** Expand one of the following sections: • **Private** • **Guest or Public** • **Domain** **3.** Scroll to **File and printer**. **4.** Ensure **Turn on file and printer sharing** option is selected. **5.** If necessary, click **Save Changes**. **6.** Repeat these steps for each profile section.

e) Close ***Network and Sharing Center***.

Step Result: ***Network and Sharing Center*** closes.

Step Result: The **Sharing and Discovery** settings is configured for the Agent Management Job.

3. Ensure Windows Firewall is configured to allow exceptions.

Tip: A Windows Firewall that does not allow exceptions will block pings and other agent management processes necessary for a successful Agent Management Job.

a) Open a run prompt using the **Start Menu** or **Start Screen**.

Step Result: The ***Run*** prompt opens.

b) Type `gpedit.msc` in the **Open** field and press `ENTER`.

Step Result: The ***Local Group Policy Editor*** opens.

c) Expand the local computer policy tree to **Computer Configuration** > **Administrative Templates** > **Network** > **Network Connections** > **Windows Firewall** > **Domain Profiles**. Ensure **Domain Profiles** folder is selected.

Step Result: The ***Domain Profile*** windows opens.

d) Ensure the following settings (and their subsettings) are configured for the **Domain Profile**.

Name	Step
Windows Firewall: Do not allow exceptions	1. Right-click and select **Edit** to open the setting dialog. 2. Ensure **Disabled** option is selected. 3. Click **OK**.
Windows Firewall: Allow inbound file and printer sharing exception	1. Right-click and select **Edit** to open the setting dialog. 2. Ensure **Enabled** option is selected. 3. Define an IP range in the **Allow unsolicited incoming messages from** field. **Note:** Ivanti recommends defining this field using your Ivanti Endpoint Security Server IP address. This input is not validated. To define a range, you may use the following syntax: • `*` (any IP address) • `10.3.2.0/24` (specific Class C subnet) • `localsubnet` (for local subnetwork access only) 4. Click **OK**.
Windows Firewall: Allow ICMP exceptions	1. Right-click and select **Edit** to open the setting dialog. 2. Ensure **Enabled** option is selected. 3. Click **OK**.

Name	Step
Windows Firewall: Allow inbound remote administration exception	1. Right-click and select **Edit** to open the setting dialog. 2. Ensure **Enabled** option is selected. 3. Define an IP range in the **Allow unsolicited incoming messages from** field. **Note:** Ivanti recommends defining this field using your Ivanti Endpoint Security Server IP address. This input is not validated. To define a range, you may use the following syntax: • `*` (any IP address) • `10.3.2.0/24` (specific Class C subnet) • `localsubnet` (for local subnetwork access only) 4. Click **OK**.

e) Expand the local computer policy tree to **Computer Configuration** > **Administrative Templates** > **Network** > **Network Connections** > **Windows Firewall** > **Domain Profiles**. Ensure **Standard Profiles** folder is selected.

Step Result: The ***Standard Profile*** windows opens.

f) Ensure the following settings (and their subsettings) are configured for the **Standard Profile**.

Tip: These settings will mimic the **Domain Profile**.

Name	Step
Windows Firewall: Do not allow exceptions	1. Right-click and select **Edit** to open the setting dialog. 2. Ensure **Disabled** option is selected. 3. Click **OK**.

Name	Step
Windows Firewall: Allow inbound file and printer sharing exception	1. Right-click and select **Edit** to open the setting dialog. 2. Ensure **Enabled** option is selected. 3. Define an IP range in the **Allow unsolicited incoming messages from** field. **Note:** Ivanti recommends defining this field using your Ivanti Endpoint Security Server IP address. This input is not validated. To define a range, you may use the following syntax: • `*` (any IP address) • `10.3.2.0/24` (specific Class C subnet) • `localsubnet` (for local subnetwork access only) 4. Click **OK**.
Windows Firewall: Allow ICMP exceptions	1. Right-click and select **Edit** to open the setting dialog. 2. Ensure **Enabled** option is selected. 3. Click **OK**.
Windows Firewall: Allow inbound remote administration exception	1. Right-click and select **Edit** to open the setting dialog. 2. Ensure **Enabled** option is selected. 3. Define an IP range in the **Allow unsolicited incoming messages from** field. **Note:** Ivanti recommends defining this field using your Ivanti Endpoint Security Server IP address. This input is not validated. To define a range, you may use the following syntax: • `*` (any IP address) • `10.3.2.0/24` (specific Class C subnet) • `localsubnet` (for local subnetwork access only) 4. Click **OK**.

g) Close the ***Local Group Policy Editior*** (or the ***Group Policy Object Editor***).

Step Result:

Note: The creation of Windows Firewall exceptions opens the following ports, which are required for job completion:

- 445/TCP
- 139/TCP
- 135/UDP
- 137/UDP

Step Result: The Windows Firewall is configured to allow exceptions for an Agent Management Job.

4. Complete the configuration of your endpoint by verifying that the C$ and ADMIN$ network shares are enabled.

Tip: The C$ and ADMIN$ network shares are necessary for remote management. This is necessary for a successful Agent Management Job completion.

a) Open ***Windows Control Panel***.

b) From the ***Command Prompt***, type `net share` and press `ENTER`.

Step Result: The endpoint network shares are listed.

c) Ensure that the following shares are listed in the `Share name` column.

- `C$`
- `ADMIN$`

Note: If these shares are not listed, complete the following steps to enable them. If one of the necessary shares is enabled but not the other, only enable the share that needs to be enabled.

d) From the ***Command Prompt***, type the necessary commands to enable the required network shares.

Example: Complete the following:

- To enable the C$ share, type `NET SHARE C$=C` and press `ENTER`.
- To enable the ADMIN$ share, type `NET SHARE ADMIN$` and press `ENTER`.

Step Result: You have enabled the required share(s). All enabled shares remain active until the system reboots.

e) Close the ***Command Prompt*** window.

Step Result: The ***Command Prompt*** closes.

Step Result: You have completed the configuration of your endpoint for an Agent Management Job by verifying that the C$ and ADMIN$ network shares are enabled.

Result: You have completed all necessary configuration steps.

After Completing This Task:
Refer to Agent Management Job Checklist on page 24 prior beginning the Agent Management Job.

Configuring the Ivanti Endpoint Security Server for Discovery Scanning

The Ivanti Endpoint Security server must be configured to accept session security encryption so that you may run the Agent Management Job on your managed endpoints.

Prerequisites:

- Ivanti Endpoint Security (Ivanti Endpoint Security) is installed and initial replication has been completed. For details regarding installing Ivanti Endpoint Security, refer to the Ivanti Endpoint Security: Server Installation Guide (https://help.ivanti.com) .

On the server the authentication package for the local security authority has values defined in the server registry. You need to authenticate that the server has the correct security encryption value in order to run the Agent Management Job on endpoints within your network.

1. Log in to the Ivanti Endpoint Security server using an account with System Administrator privileges.
2. Open the ***Registry Editor***.
   a) From the **Start Menu** or **Start Screen**, open a **Run** prompt.
   b) Type `regedit.exe` and press `ENTER`.

   Step Result: The ***Registry Editor*** window opens.
3. Expand the registry tree to `HKEY_LOCAL_MACHINE\SYSTEM\Currentcontrolset\Control\Lsa`.
4. Ensure the value for the `LmCompatibilityLevel` registry value is set to `3`.
   a) Ensure Lsa is selected in the registry tree.
   b) In the right-window area, select the `LmCompatibilityLevel` binary value.
   c) Right-click on the `LmCompatibilityLevel` binary value select **Modify**.

   Step Result: The ***Edit Binary*** dialog opens.

d) Ensure `3` is visible in the **Value data** field. If not present, then change the value to `3`.

Note: Under most network conditions, a setting of 3 (Send NTLM 2 response only) is sufficient. However, in some networks, this key may require a different value. To determine which value to use, refer to How to Enable NTLM 2 Authentication (http://support.microsoft.com/kb/239869).

Result: The Ivanti Endpoint Security server is configured to utilize discovery scanning.

After Completing This Task:
If you are configuring the server for scanning in preparation for an Agent Management Job, ensure you have complete the tasks needed for an Agent Management Job. For more information, see Agent Management Job Checklist on page 24.

Installing Agents by Agent Management Job

You may install agents on network endpoints remotely using an Agent Management Job.

Prerequisites:

- Ivanti Endpoint Security (Ivanti Endpoint Security) is installed and initial replication has been completed. For details regarding installing Ivanti Endpoint Security, refer to the Ivanti Endpoint Security: Server Installation Guide (https://help.ivanti.com) .
- Ensure that your endpoint meets the minimum requirements for agent installation. For additional information, refer to Agent Requirements on page 7.

Note: You cannot complete an Agent Management Job on Linux, UNIX, or Mac endpoints.

- You have gathered and confirmed the information and tasks in the Agent Management Job checklist. Refer to Agent Management Job Checklist on page 24 for a description.

Configuration using an Agent Management Job is similar to configuration using the Discovery Scan Job. Configuration occurs using the ***Install Agents Wizard***.

1. Log in to Ivanti Endpoint Security.
   For additional information, refer to Ivanti Endpoint Security User Guide (https://help.ivanti.com/) .
2. Begin configuration of the ***Install Agent Wizard***.
   Complete one of the following steps to begin configuration.

Context	Steps
To open the Wizard without targets predefined:	Select **Discover** > **Assets and Install Agents**.

Context	Steps
To open the Wizard with target predefined:	1. Select **Manage** > **Endpoints**. 2. Select the endpoints you want to install the agent on. 3. From the toolbar, select **Manage Agents** > **Install Agents**.

Step Result: The wizard opens to the ***Job Name and Scheduling*** page.

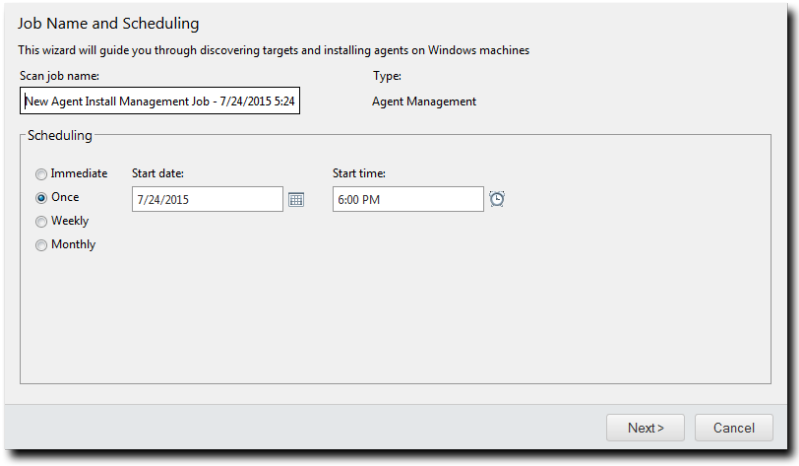


Figure 1: Job Name and Scheduling Page

3. [Optional] Type a new name in the **Scan job name** field.

Note: By default, a new Agent Management Job for installation is named `New Agent Install Management Job`, followed by the server's date and time.

4. Schedule the job.

   Use one of the following methods.

Tip: During job scheduling, you can use the following shortcuts:

- Click the **Calender** icon to select a **Start date**. Selecting a date automatically fills the **Start date** field.
- Click the **Clock** icon to select a **Start time**. Selecting a time automatically fills the **Start time** field.

Method	Steps
To schedule an immediate job:	Select the **Immediate** option.

Method	Steps
To schedule a one-time job:	**1.** Ensure the **Once** option is selected. **2.** Define a start date by typing a date in the **Start date** field. **Note:** Type the date in a `mm/dd/yyyy` format. **3.** Define a start time by typing a time in the **Start time** field. **Note:** Type the time in `hh:mm` format followed by `AM` or `PM` (if necessary). This field supports both 12- and 24-hour time. **Tip:** Scheduling a one-time job for a past date and time will launch the job immediately.
To schedule a recurring weekly job:	**1.** Select the **Weekly** option. **2.** Define a start date by typing a date in the **Start date** field. **Note:** Type the date in a `mm/dd/yyyy` format. **3.** Define a start time by typing a time in the **Start time** field. **Note:** Type the time in `hh:mm` format followed by `AM` or `PM` (if necessary). This field supports both 12- and 24-hour time. **4.** Define the day of the week the job runs by selecting a day from the **Run every week on the following day** list.
To schedule a recurring monthly job:	**1.** Select the **Monthly** option. **2.** Define a start date by typing a date in the **Start date** field. **Note:** Type the date in a `mm/dd/yyyy` format. **3.** Define a start time by typing a time in the **Start time** field. **Note:** Type the time in `hh:mm` format followed by `AM` or `PM` (if necessary). This field supports both 12- and 24-hour time. **4.** Define the day of the month the job runs by typing a day in the **Run every month on the following day** field.

Tip: One-time and recurring jobs scheduled for the last day of a 31-day month are automatically rescheduled for the last day of shorter months.

5. Click **Next**.

   Step Result: The ***Targets*** page opens.

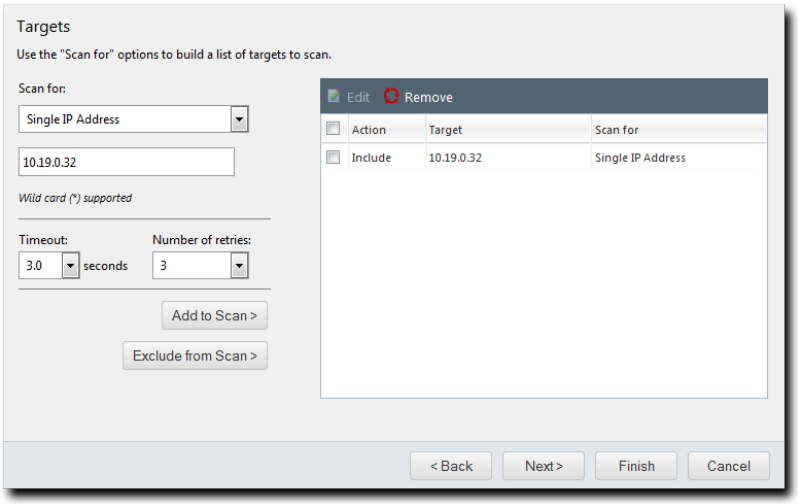


Figure 2: Targets Page

6. Define targets (endpoints) for the job to locate.

   Select one or more of the following discovery methods to build a list of targets to scan.

Method	Steps
To define targets using a single IP address:	1. From the **Scan for** list, select **Single IP Address**. 2. Type an IP address in the empty field. Wildcards are supported. **Note:** For additional information refer to Defining Targets Using Wildcards on page 51. 3. Select an item in the **Timeout** list. **Note:** The **Timeout** list item defines the number of seconds per attempt before a scan fails due to inactivity for a particular target. Under most network conditions, the **Timeout** list item does not require editing. 4. Edit the **Number of retries** list. **Note:** The Number of retries list defines the number of times a scan retries on that target if the scan times out.

Method	Steps
To define targets using an IP range:	1. From the **Scan for** list, select **IP Range**. 2. In the first empty field, type the beginning of IP range. **Note:** Wildcards are supported. For additional information refer to Defining Targets Using Wildcards on page 51. 3. In the second empty field, type the ending of the IP range. 4. Select an item in the **Timeout** list. **Note:** The **Timeout** list defines the number of seconds per attempt before a scan fails due to inactivity for that particular target. Under most network conditions, the **Timeout** list item does not require editing. 5. Select an item in the **Number of retries** list. **Note:** The **Number of retries** item defines the number of times a scan retries on that target if the scan times out.
To define targets using a computer name:	1. From the **Scan for** list, select **Computer name**. 2. In the empty field, type an endpoint name in one of the following formats: `computername` or `domain\computername`.
To define targets using network neighborhood:	1. From the **Scan for** list, select **Network Neighborhood**. 2. From the second list, select the desired network neighborhood.

Method	Steps
To define targets using active directory:	**1.** From the **Scan for** list, select **Active Directory**. **2.** In the **Fully-qualified domain name** field, type the DNS domain name of the domain controller you want to scan. **Note:** For example, if your domain controller DNS name is *box.domain.company.local*, you would type *domain.company.local* in this field. **3.** Optionally, in the **Organizational Unit** field, type the active directory organizational unit string from specific to broad, separating each string with front slashes (such as `Techpubs/Engineering/Corporate`). **Note:** The omission of this field returns job results containing the full contents of *all* the active directory organizational units. View the following figure for an example of how to enter data using **Active Directory**. **4.** In the **Domain controller** field, type the domain controller IP address. **5.** In the **Username** field, type a user name that authenticates with the domain controller. **Note:** Type the user name in one of the following format: `domainname\username` or `username`. **6.** In the **Password** field, type the password associated with the user name.

Method	Steps
To define targets using an imported file:	1. From the **Scan for** list, select **Import file**. 2. Click **Browse**. 3. Browse to the file you want to use for target discovery. **Note:** The following file types are supported: `.txt` and `.csv`. 4. Click **Open**. **Note:** Refer to Defining Targets Within an Imported File on page 52 for additional information on file types.

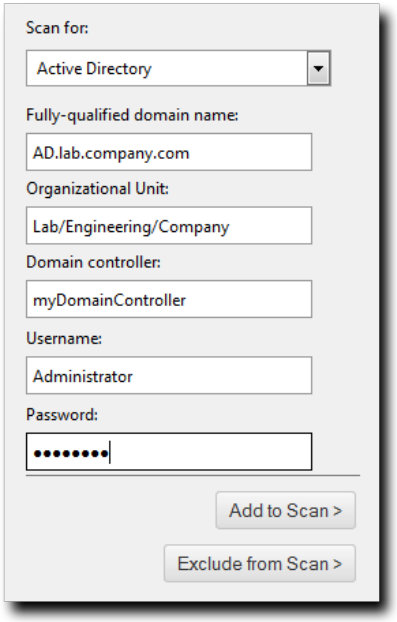


Figure 3: Active Directory Input Example

7. Add targets to the wizard list. This list indicates whether defined targets are included in or excluded from the job.

   Use one of the following methods.

Note: You must include at least one target for **Next** to become available. You can also delete targets from the list by selecting the applicable check boxes and clicking **Remove**.

Method	Steps
To include defined targets in the job:	Click **Add to Scan**.

Method	Steps
To exclude defined targets from the job:	Click **Exclude from Scan**.

Tip: Repeat this step to add additional targets to the list.

8. [Optional] Edit the **Targets** list.
   - To remove targets from the list, select the list item(s) and click **Remove**.
   - To edit targets on the list, select the list item(s) and click **Edit**.
     For additional information on editing, refer to Editing Targets on page 47.
9. Click **Next**.

   Step Result: The ***Scan Options*** page opens.

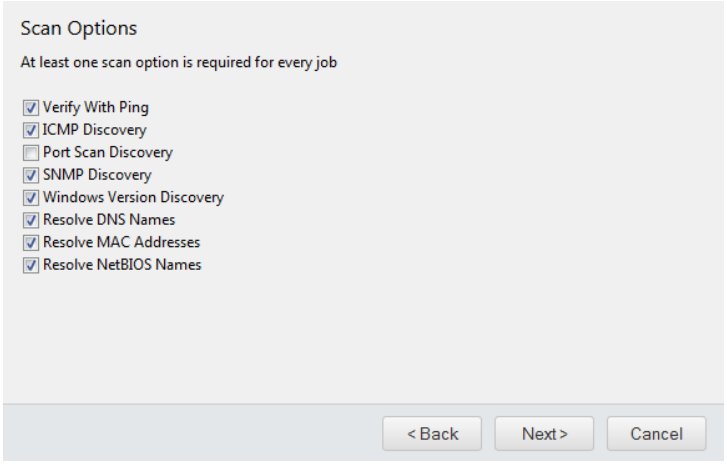


Figure 4: Scan Options Page

10. Select or clear the desired **Scan Options**.

The following table defines each **Scan Option**.

Option	Description
Verify With Ping	Jobs using this option send ping requests to all network endpoints targeted for discovery. Endpoints that respond to the request are flagged for scanning; unresponsive endpoints are skipped. Endpoints unresponsive to **Verify With Ping** are not scanned by other selected discovery options. **Note:** Anti-virus software and host firewalls may block **Verify With Ping**. If necessary, adjust any antivirus and firewall configurations to permit ping requests.
ICMP Discovery	Jobs using this option request a series of echoes, information, and address masks from endpoints. Endpoint responses are then compared to a list of known ICMP fingerprints to identify endpoint operating systems. **Note: ICMP Discovery** is ineffective on endpoints configured to ignore ICMP requests. For best results identifying Windows operating systems, use this option in conjunction with **Windows Version Discovery**.
Port Scan Discovery	Jobs using this option perform a limited scan on endpoint FTP, Telnet, SSH, SMTP, and HTTP ports. Based on the application banners found in these ports, endpoint operating systems are generically identified. **Note:** For best results in identifying Windows operating systems, use this option in conjunction with **Windows Version Discovery**.
SNMP Discovery	Jobs using this option request system properties for SNMP devices (routers, printers, and so on) from the management information base. Following credential authentication, SNMP devices are identified. **Note:** Without authenticated credentials, SNMP devices ignore **SNMP Discovery** requests. In this event, one of two outcomes occur: the SNMP device is misidentified as a UNIX endpoint or the SNMP device is not detected. Jobs with no SNMP credentials use the *public* credential by default.

Option	Description
Windows Version Discovery	Jobs using this option identify an endpoint's specific version of Windows following generic operating system identification during **ICMP** or **Port Scan Discovery**. **Note:** Correct operating system identification is contingent upon authenticated credentials. This option must be used in conjunction with either **ICMP** or **Port Scan Discovery**.
Resolve DNS Names	Jobs using this option acquire the endpoint DNS name through a local DNS server query. These names are displayed in job results for easy endpoint identification.
Resolve MAC Addresses	Jobs using this option acquire endpoint MAC addresses through endpoint queries. These addresses are displayed in job results for easy endpoint identification. **Note:** Monitor network inventory reports to prevent MAC address spoofing that may alter the **Resolve MAC Addresses** results.
Resolve NetBIOS Names	Jobs using this option acquire endpoint NetBIOS names through WINS NetBIOS mapping. These names are displayed in job results for easy endpoint identification.

11. Click **Next**.

Step Result: The ***Agent Options*** page opens.

12. Select the desired **Agent Options**.

These options control which version of the agent is installed on Windows-based endpoints.

a) Select an agent version from the **Agent version** list.

Note: The agent versions available for selection are defined by the **Agent Version Options**, which you can edit from the ***Options*** page ***Agents*** tab within the Ivanti Endpoint Security Web console. For additional information, refer to *Agent Versions* in the Ivanti Endpoint Security User Guide (https://help.ivanti.com/) .

b) Select the modules you want to install with the agent.

Select the check boxes associated with the modules you want to install.

c) [Optional] Select the **Overwrite existing agents** check box.
This option reinstalls the agent on endpoints.

Attention: Selecting this option will cause data loss when an endpoint's Ivanti Endpoint Security Agent is overwritten. However, you may select **Agent Versions** on the ***Manage Endpoints*** page to upgrade agents without losing data. Refer to Upgrading the Agent Using the Endpoints Page on page 79 for details.

13. Click **Next**.

Note: If a dialog opens that notifies you that an endpoint reboot is required following agent installation, click **Continue** to dismiss the dialog.

Step Result: The ***Credentials*** page opens.

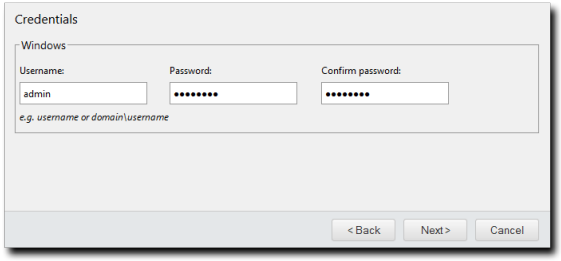


Figure 5: Credentials Page

14. Define **Windows** credentials for the target.
Type the applicable information in the following fields.

Note: When configuring an Agent Management Job, you must define valid Windows credentials.

Field	Description
Username	A user name that authenticates with Windows-based endpoints. Type the user name in a local format (`UserName`) or a domain format (`DOMAIN\UserName`). **Note:** When configuring Agent Management Jobs, Ivanti recommends using the built-in Administrator account.
Password	The password associated with the **Username**.
Confirm password	The **Password** retyped.

15. Click **Next**.

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

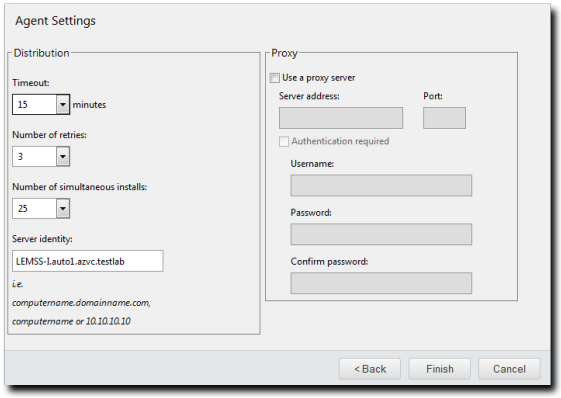


Figure 6: Agent Settings Page

16. Define the **Distribution** options.

The following table describes each list their available values.

List	Description
Timeout (list)	Defines the number of minutes before the Agent Management Job terminates an install attempt due to a non-responsive agent installation or removal (0-30).
Number of retries (list)	Defines the number of attempts an agent installation or removal will retry if the initial attempt fails (1-10).
Number of simultaneous installs (list)	Defines the maximum number of agents that can installed or removed simultaneously during the job (1-25). A value of `1` indicates that serial installs or removals should occur.

17. Define the Ivanti Endpoint Security server that the agent will report to using the **Server Identity** field.

Define the **Server identity** using one of the following formats.

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

Tip: The wizard fills this field with the server computername by default.

18. If the target endpoints will communicate with the Ivanti Endpoint Security server through a proxy server following initial agent installation, select the **Use a proxy server** check box and define the following fields.

Note: In many network environments, although a proxy is used for Internet access, a proxy bypass is used for all access within the corporate network. Therefore, only enter proxy information if your agents will be required to use a proxy to access your Ivanti Endpoint Security server.

Field	Description
Server address	The applicable proxy IP address.
Port	The applicable proxy port number used to communicate.

19. If the target endpoints will use a proxy for agent to server communication, and that proxy requires authentication, select the **Authentication required** check box and define the following fields.

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

20. Click **Finish**.

Result: The ***Install Agents Wizard*** closes. Depending on how you configured the job, it moves to either the ***Scheduled*** tab or ***Active*** tab on the ***Job Results*** page. The job will run at the applicable time, installing agents on the defined targets, and move to ***Completed*** tab when finished.

Note: After the Agent Management Job completes, install agent modules. For additional information, refer to *Managing Endpoint Modules* in Ivanti Endpoint Security User Guide (https://help.ivanti.com/) .

Editing Targets

While configuring jobs, you can edit items included in the **Targets** list in the ***Install Agents Wizard***.

Edit **Target** list items from the ***Targets*** page of the wizard.

1. From the **Targets** list, select the check box associated with the item you want to edit.

   Step Result: The **Edit** button becomes active.

2. Click **Edit**.

   Step Result: The ***Edit Targets*** dialog opens.

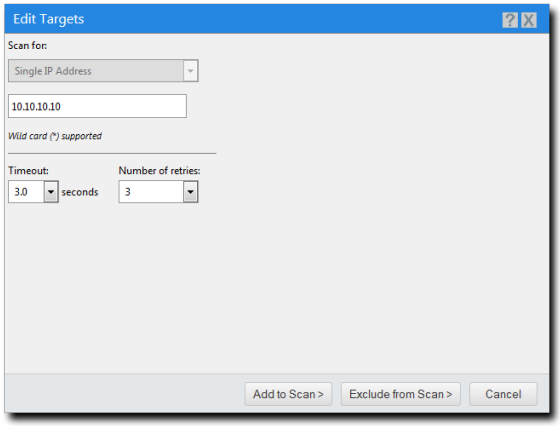


Figure 7: Edit Targets Dialog

3. Based on the type of discovery method, edit the item.

Discovery Method	Steps
Single IP Address	1. Type a new IP address in the field. Wildcards are supported. For additional information, refer to Defining Targets Using Wildcards on page 51. 2. If necessary, edit the **Timeout** list. The **Timeout** list defines the number of seconds before a scan fails due to inactivity. Under most network conditions, the **Timeout** field does not require editing. 3. If necessary, edit the **Number of retries** list. The **Number of retries** list defines the number of times a discover assets scan retries if the scan times out.

Discovery Method	Steps
IP Range	1. In the field, type the beginning of IP range. Wildcards are supported. For additional information, refer to Defining Targets Using Wildcards on page 51. 2. In the field, type the ending of the IP range. 3. If necessary, edit the **Timeout** list. The **Timeout** list defines the number of seconds before a scan fails due to inactivity. Under most network conditions, the **Timeout** field does not require editing. 4. If necessary, edit the **Number of retries** list. The **Number of retries** list defines the number of times a discover assets scan retries if the scan times out.
Computer Name	In the empty field, type a new endpoint name in one of the following formats: `endpointname` or `domain\endpointname`.
Network Neighborhood	From list, select the desired network neighborhood.

Discovery Method	Steps
Active Directory	1. In the **Fully-qualified domain name** field, type the DNS domain name of the domain controller you want to scan. For example, if your domain controller's DNS name was *box.domain.company.local*, you would type *domain.company.local* in this field. 2. Optionally, in the **Organizational Unit** field, type the active directory organizational unit string from specific to broad, separating each string with front slashes (such as `Techpubs/Engineering/Corporate`). The omission of this field returns job results containing the full contents of *all* the active directory organizational units. View the following figure for an example of how to enter data using **Active Directory**. 3. In the **Domain controller** field, type the domain controller's IP address. 4. In the **Username** field, type user name that will authenticate with the domain controller. Type the user name in one of the following format: `domainname\username` or `username`. 5. In the **Password** field, type the password associated with the user name.

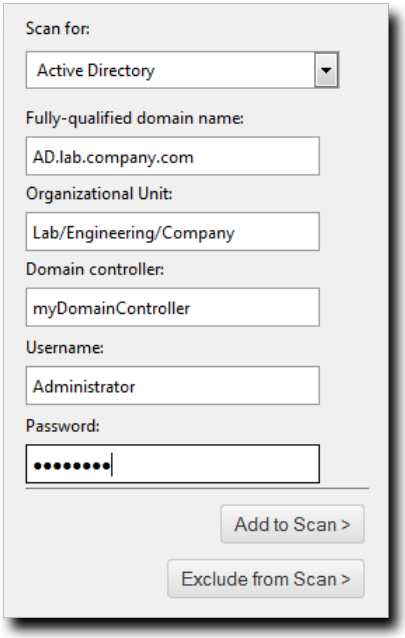


Figure 8: Active Directory Input Example

4. Add targets to the wizard list. This list indicates whether defined targets are included in or excluded from the job.

   Use one of the following methods.

Method	Steps
To include defined targets in the job:	Click **Add to Scan**.
To exclude defined targets from the job:	Click **Exclude from Scan**.

5. Review the **Targets** list.

Result: The **Targets** list reflects your changes.

Defining Targets Using Wildcards

When configuring a Discovery Scan Job or Agent Management Job, you can define scan targets using *wildcard* IP addresses. Wildcards are characters that can be used to substitute for any other character or characters in a string. In otherwords, you can use wildcards to scan for numerous IP address instead of just one. Use wildcards to scan specific IP address ranges.

The following table lists examples of how to define targets using wildcards.

Table 9: Wildcard Examples

Discovery Method	Step	Example	Targets Defined
To define wildcard IP addresses:	Type a wildcard IP address using commas (,). Type a wildcard IP address using dashes (-). Type a wildcard IP address using asterisks (*).	10.1.1.2,9 10.1.1.2-5 10.1.1.*	10.1.1.2 and 10.1.1.9 10.1.1.2, 10.1.1.3, 10.1.1.4, and 10.1.1.5 10.1.1.0 through 10.1.1.255
To define wildcard IP addresses using dashes in various octets:	Type a wildcard IP address using dashes, placing the dashes where applicable. You can use dashes in any octet.	10.2-4.5.9	10.2.5.9, 10.3.5.9, 10.4.5.9

Discovery Method	Step	Example	Targets Defined
To define wildcard IP addresses using asterisks in various octets:	Type a wildcard IP address using asterisks, placing the asterisks where applicable. You can use asterisks in any octet.	*.6.65.92 10.25.*.*	1.6.65.92 through 255.6.65.92 10.25.0.0 through 10.25.255.255
To define wildcard IP addresses using commas in various octets:	Type a wildcard IP address using commas, placing the commas where applicable. You can use commas in any octet.	10,12,19.2.5.9	10.2.5.9, 12.2.5.9, 19.2.5.9
To define wildcard IP addresses using a combination of wildcard characters:	Type a wildcard IP address using dashes, commas, and asterisks.	10-13.*.12.2,4,7 10.2-4.5,23.*	10, 11, 12, 13.0-255.12.2, 4, 7 10.2, 3, 4.5, 23.0-255

Defining Targets Within an Imported File

Using imported files, you can define job targets using a combination of single IP addresses, wildcard IP addresses, IP ranges, DNS names, NetBIOS names, and so on. To create a file containing targets, open a text editor that allows you to create `.txt` or `.csv` (like Notepad). This topic also explains how to use wildcards for any job type.

Using the ***Install Agents Wizard*** within an Agent Management Job you may define targets using an imported file.

The following table lists the methods you can use to define discovery methods within an importable file type, and then follows those methods with examples. Use one method per line.

Table 10: Basic Use

Discovery Method	Step	Example	Targets Defined
To define single IP addresses:	Type a single address.	10.1.1.2	10.1.1.2

Discovery Method	Step	Example	Targets Defined
To define wildcard IP addresses:	Type a wildcard IP address using commas (,). Type a wildcard IP address using dashes (-). Type a wildcard IP address using asterisks (*).	10.1.1.2,9 10.1.1.2-5 10.1.1.*	10.1.1.2 and 10.1.1.9 10.1.1.2, 10.1.1.3, 10.1.1.4, and 10.1.1.5 10.1.1.0 through 10.1.1.255
To define IP ranges:	Type two IP addresses separated by a greater-than sign (>). Type two IP addresses separated by a dash (-).	10.1.1.2 > 10.1.1.9 10.1.1.2 - 10.1.1.9	10.1.1.2 through 10.1.1.9 10.1.1.2 through 10.1.1.9
To define DNS names:	Type a DNS host name for an endpoint.	DNS.dom.com	The defined DNS name.
To define NetBIOS names:	Type a NetBIOS name for an endpoint.	NetBIOSname	The defined NetBIOS name.

Table 11: Advanced Use

Discovery Method	Steps	Examples	Targets Defined
To define wildcard IP addresses using dashes in various octets:	Type a wildcard IP address using dashes, placing the dashes where applicable. You can use dashes in the first, second, and last octet.	10.2-4.5.9	10.2.5.9, 10.3.5.9, 10.4.5.9
To define wildcard IP addresses using asterisks in various octets:	Type a wildcard IP address using asterisks, placing the asterisks where applicable. You can use asterisks in any octet.	*.6.65.92 10.25.*.*	1.6.65.92 through 255.6.65.92 10.35.0.0 through 10.35.255.255
To define wildcard IP addresses using commas in various octets:	Type a wildcard IP address using commas, placing the commas where applicable. You can use commas in first, second, and last octet.	10,12,19.2.5.9	10.2.5.9, 12.2.5.9, 19.2.5.9

Discovery Method	Steps	Examples	Targets Defined
To define wildcard IP addresses using a combination of wildcard characters:	Type a wildcard IP address using dashes, commas, and asterisks. You can use the dash and comma wildcards in the first, second, and lost octets. The asterick can be used in all octets.	10-13.*.12.2,4,7 10.2-4.5,23.*	10, 11, 12, 13.0-255.12.2, 4, 7 10.2, 3, 4.5, 23.0-255

Command Line for Windows

You can use the command line to install an agent on a Windows endpoint.

An advantage in using a command line is silent installation. When using silent installation, you can enter all the information necessary prior to the silent installation and then the installation itself runs unattended (without user interaction).

Command Line Workflow for Windows

Review this chart to understand the Ivanti Endpoint Security Agent workflow for a command line installation on a Windows endpoint.

Determine agent requirements. Refer to Agent Requirements on page 7 for a complete list of hardware and software requirements for the agent.

Download the agent installer on Windows endpoints. Refer to Downloading the Installer on page 55.

Silently install the agent using a command line on any Windows endpoints. Refer to Silently Installing the Agent by Command Line for Windows on page 57.

Following initial installation, the agent and server components begin communicating. Additionally, if you are licensed for additional modules, you can install these modules on any endpoint that has the Ivanti Endpoint Security Agent.

Note: For more information on modules and module installation, refer to Ivanti Endpoint Security User Guide (https://help.ivanti.com/) .

Downloading the Installer

Download the agent installer from your Ivanti Endpoint Security server by using the Web console.

To download the installer, log in to the target endpoint, and then download the installer.

1. Log on to the target endpoint as the local administrator (or a member of the Local Administrators group).
2. Log in to Ivanti Endpoint Security (Ivanti Endpoint Security) server console as user with administrator privileges.

   For additional information on log in, refer to the Ivanti Endpoint Security User Guide (https://help.ivanti.com/) .

   Step Result: The Ivanti Endpoint Security ***Home*** page opens.

3. Select **Tools** > **Download Agent Installer**.

   Step Result: The ***Download Agent Installers*** dialog opens.

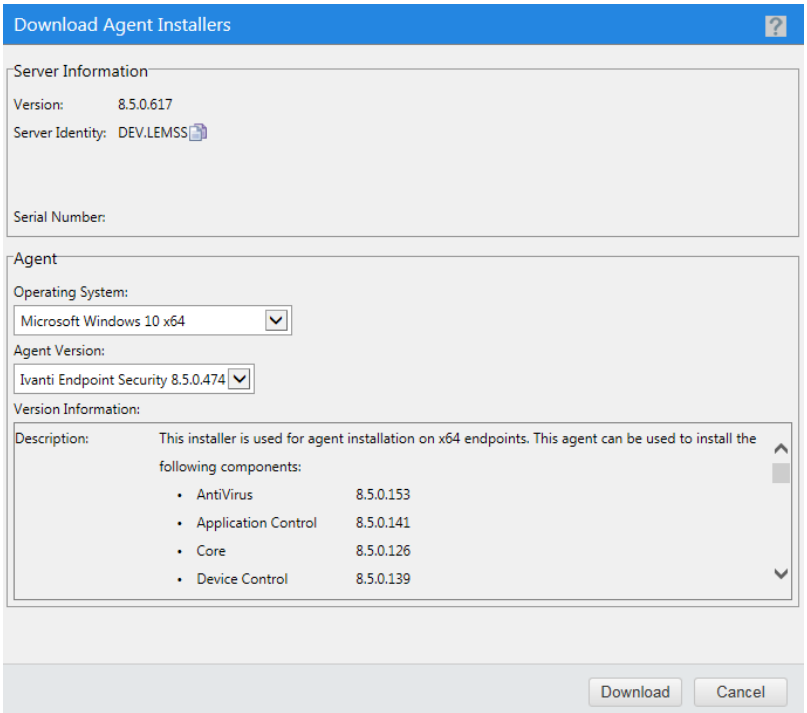


Figure 9: Download Agent Installers Dialog

> **Tip:** The icon allows you to copy information to your clipboard.

4. Select your endpoint's operating system from the **Operating System** drop-down list.
5. Select the version of the agent that you want to install from the **Agent Version** drop-down list.

> **Note:** The agent versions available for selection are defined by the **Agent Version Options**, which you can edit from the ***Options*** page ***Agents*** tab within the Ivanti Endpoint Security Web console. For additional information, refer to *Configuring the Agents Tab* in the Ivanti Endpoint Security User Guide (https://help.ivanti.com/) .

6. Click **Download**.

   Step Result: A dialog opens, prompting you to define a download location.

> **Tip:** The ***Download Agent Installers*** dialog remains open during the installer download.

7. Using the dialog controls, define a download location and begin the download.

8. After the download completes, close the dialog.

Tip: You may click **Cancel** to close the ***Download Agent Installers*** dialog or leave open while installing the agent. The dialog contains Ivanti Endpoint Security server and agent information.

Result: You have successfully downloaded the Ivanti Endpoint Security Agent installer.

Silently Installing the Agent by Command Line for Windows

Complete a silent install of the agent using a command line. When configured using command line parameters, the installation of the agent can be run unattended.

Prerequisites:

- Ivanti Endpoint Security (Ivanti Endpoint Security) is installed and initial replication has been completed. For details regarding installing Ivanti Endpoint Security, refer to the Ivanti Endpoint Security: Server Installation Guide (https://help.ivanti.com) .
- Ensure that your endpoint meets the minimum requirements for agent installation. For additional information, refer to Agent Requirements on page 7.
- Ensure any antivirus software installed on the computer is disabled.
- Ensure you are logged on with an administrative user account.
- Download the Windows agent installer. Refer to Downloading the Installer on page 55.

After downloading the agent installer for Windows, you can begin a silent install from the Windows ***Command Prompt***. In addition to setting the Ivanti Endpoint Security URL (or IP), you can define a proxy for agent-to-server communication and auto-assign groups during silent installation.

1. Using the **Start Menu** or **Start Screen**, open a **Command Prompt**.

   Step Result: The ***Command Prompt*** opens.

2. Change directories to the root directory.

   Type `cd\` and press `ENTER`.

   Step Result: The directory is changed to the root directory.

3. Change directories to the location where you downloaded the installer.

   Type `cd <Your\Download\Directory>` and press `ENTER`.

   Step Result: The directory changes to the directory where you downloaded the installer.

4. Install the agent by typing the install command followed by parameters.

Note: If you downloaded the 64-bit installer, replace `lmsetup.exe` with `lmsetupx64.exe` when typing install commands.

Example parameters:

Example:
```
lmsetup.exe install SERVERIPADDRESS="<xxx.xxx.xxx.xxx>"
```

(required parameters)

Example:

```
lmsetup.exe install SERVERIPADDRESS="<xxx.xxx.xxx.xxx>"
 PROXYADDRESS="<xxx.xxx.xxx.xxx>" PROXYPORT="<xx>" PROXYUSERNAME="<ProxyUser>"
 PROXYPASSWORD="<ProxyUserPassword>" MODULELIST="<Module>|<Module2>"
 GROUPLIST="<Group>|<Group2>"
```

(all parameters)

Note: When installing the Ivanti Endpoint Security agent from a command line, you can add a number of parameters to modify how the agent is installed on the endpoint. Read the following table for detailed instructions about how to use each parameter. Remember the following information when using these parameters:

- Parameters do not have to be entered in a specific order.
- The only required parameter is SERVERIPADDRESS.
- The parameter name may be capitalized or lowercase, or mixed.
- Surround variables with double quotes. Words wrapped in carrots are variables relative to your environment. For example when defining the SERVERIPADDRESS parameter, you might type `SERVERIPADDRESS="10.19.0.133"`
- With the exception of password variables, variables are not case sensitive.

Table 12: Description of Installation Parameters

Parameter	Description
SERVERIPADDRESS	The IP address of your Ivanti Endpoint Security server. Example: `SERVERIPADDRESS="<xxx.xxx.xxx.xxx>"` **Note:** This can also be a local name or fully qualified domain name of your Ivanti Endpoint Security server. A fully qualified domain name is recommended over local.
PROXYADDRESS	The IP address for your proxy server. Example: `PROXYADDRESS="<xxx.xxx.xxx.xxx>"` **Note:** This can also be a local name or fully qualified domain name of your Ivanti Endpoint Security server. A fully qualified domain name recommended over local. A Squid proxy server will only properly resolve using a fully qualified domain name. Refer to Ivanti Community Article 59102 for additional information on a Squid proxy server configuration.
PROXYPORT	The port your proxy server is using for communication. Example: `PROXYPORT="<xx>"`

Parameter	Description
PROXYUSERNAME	Login user for an authenticated proxy. Example: `PROXYUSERNAME="<ProxyUserName>"`
PROXYPASSWORD	Login password for an authenticated proxy. Example: `PROXYPASSWORD="<ProxyUserPassword>"` **Tip:** The password will be encrypted and saved on the endpoint.

GROUPLIST	This parameter adds the target endpoint to existing Ivanti Endpoint Security groups during agent installation. The following list includes information about using this parameter.
	• You can only use this parameter to add endpoints to existing groups. This parameter cannot create new groups.
	• When using this parameter, you can add the endpoint to two or more groups. To add the endpoint to multiple groups, type a pipe symbol `|` between two group names. Do not type spaces between the group names and the pipe(s).
	Example (single group): `GROUPLIST="<Group>"`
	Example (multiple groups): `GROUPLIST="<Group>|<Group2>|<Group3>"`
	• When using this parameter, you can use either the group name or the distinguished name.
	  • If two or more groups exist that share the same name, using the group name will add the endpoint to all groups using the name.
	  • If two or more groups exist that share the same name, using the distinguished name will add the endpoint to a specific group.
	  Example (distinguished name use): `GROUPLIST="OU=<Group>,OU=Custom Groups,OU=My Groups"`
	• To view your group names and distinguished names, view the ***Groups*** page ***Group Membership*** view in the Ivanti Endpoint Security Web console.

Parameter	Description
MODULELIST	This parameter installs Ivanti Endpoint Security endpoint modules along with the Ivanti Endpoint Security Agent during installation. The following list includes information about using this parameter. • You can use this parameter to add endpoint modules you are licensed for. • When using this parameter, you can add two or more modules. For multiple modules, type a pipe symbol | between two module names. Do not type spaces between the modules names and the pipe(s). Example: `MODULELIST="<Module>|<Module2>|<Module3>"` The following list includes the MODULELIST parameter for each Ivanti Endpoint Security module: • `VulnerabilityManagement` (Patch and Remediation) • `ApplicationControl` (Application Control) • `Antivirus` (AntiVirus) • `PowerMgmt` (Power Management) • `DeviceControl` (Device Control)
INSTALLDIR	This parameter defines the directory where the Ivanti Endpoint Security agent will be installed. Example: `INSTALLDIR="C:\<Your>\<Install>\<Directory>"` **Note:** Omitting this parameter installs the agent to the default directory of `C:\Program Files\HEAT\EMSSAgent`. Only ASCII characters are allowed in the folder name.

Install of the Agent for Windows Manually

Ivanti Endpoint Security Agents can be installed on a single Windows endpoint using the agent installer.

You can log in to the Ivanti Endpoint Security Web console, download the agent, and then run the agent installer.

Tip: If you are unfamiliar with the command prompt, you may prefer this agent installation method to install the agent.

Manual Install Workflow for Windows

A simple method to install the Ivanti Endpoint Security agent on an endpoint is manually installing the agent on a Windows endpoint. The Ivanti Endpoint Security agent installer features a straightforward wizard that can be used to install the agent on a single endpoint.

Determine agent requirements. Refer to Agent Requirements on page 7 for a complete list of hardware and software requirements for the agent.

Download the agent installer on a Windows endpoint. Downloading the Installer on page 61.

Install the agent. You may install agents on Windows endpoints that you want to manage. Agent installation is based on administrator need and operating system type. Refer to Manually Installing the Agent for Windows on page 63.

Following initial installation, the agent and server components begin communicating. Additionally, if you are licensed for additional modules, you can install these modules on any endpoint that has the Ivanti Endpoint Security Agent.

Note: For more information on modules and module installation, refer to Ivanti Endpoint Security User Guide (https://help.ivanti.com/) .

Downloading the Installer

Download the agent installer from your Ivanti Endpoint Security server by using the Web console.

To download the installer, log in to the target endpoint, and then download the installer.

1. Log on to the target endpoint as the local administrator (or a member of the Local Administrators group).
2. Log in to Ivanti Endpoint Security (Ivanti Endpoint Security) server console as user with administrator privileges.

   For additional information on log in, refer to the Ivanti Endpoint Security User Guide (https://help.ivanti.com/) .

   Step Result: The Ivanti Endpoint Security ***Home*** page opens.

3. Select **Tools** > **Download Agent Installer**.

   Step Result: The ***Download Agent Installers*** dialog opens.

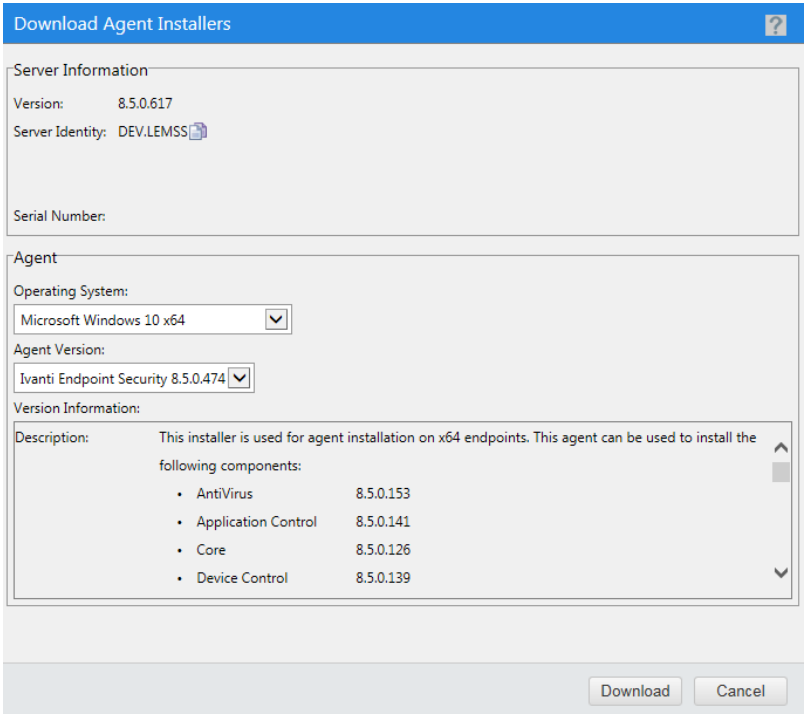


Figure 10: Download Agent Installers Dialog

> **Tip:** The icon allows you to copy information to your clipboard.

4. Select your endpoint's operating system from the **Operating System** drop-down list.
5. Select the version of the agent that you want to install from the **Agent Version** drop-down list.

> **Note:** The agent versions available for selection are defined by the **Agent Version Options**, which you can edit from the ***Options*** page ***Agents*** tab within the Ivanti Endpoint Security Web console. For additional information, refer to *Configuring the Agents Tab* in the Ivanti Endpoint Security User Guide (https://help.ivanti.com/) .

6. Click **Download**.

   Step Result: A dialog opens, prompting you to define a download location.

> **Tip:** The ***Download Agent Installers*** dialog remains open during the installer download.

7. Using the dialog controls, define a download location and begin the download.

8. After the download completes, close the dialog.

Tip: You may click **Cancel** to close the ***Download Agent Installers*** dialog or leave open while installing the agent. The dialog contains Ivanti Endpoint Security server and agent information.

Result: You have successfully downloaded the Ivanti Endpoint Security Agent installer.

Manually Installing the Agent for Windows

Endpoints running Windows communicate with the Ivanti Endpoint Security server using the Ivanti Endpoint Security Agent.

Prerequisites:

- Ivanti Endpoint Security (Ivanti Endpoint Security) is installed and initial replication has been completed. For details regarding installing Ivanti Endpoint Security, refer to the Ivanti Endpoint Security: Server Installation Guide (https://help.ivanti.com) .
- Ensure that your endpoint meets the minimum requirements for agent installation. For additional information, refer to Agent Requirements on page 7.
- Ensure any antivirus software installed on the computer is disabled.
- Download the appropriate installer for your operating system. See Downloading the Installer on page 61 for more information.
- Ensure you are logged on with an administrative user account.

After downloading the agent installer for Windows, you can begin an install using the ***Agent Setup Wizard***.

1. From the download location, open the ***Agent Setup Wizard***.
   - On 32-bit endpoints, double-click **lmsetup.exe**.
   - On 64-bit endpoints, double-click **lmsetupx64.exe**.
2. Review the **License agreement** and select the **I accept the terms in the License agreement** option.

Tip: Click **Print** to perform the following actions:

- Open a text file of the license agreement.
- Open a ***Print*** dialog.

3. Click **Next**.

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

4. [Optional] Change the Ivanti Endpoint Security agent installation location.

   Tip: Only ASCII characters are allowed in the folder name.

   a) Click **Browse**.

      Step Result: The ***Browse for Folder*** dialog opens.

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

      Step Result: The ***Browse for Folder*** dialog closes and the ***Destination folder*** page reflects the new location.

5. Click **Next**.

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

6. Type the appropriate server address information in the **Server identity** field.

Server Definition Option	Step
To define the server with an IP address:	Type *xxx.xxx.xxx.xxx*
To define the server with a server name:	Type *ServerName*
To define the server using a fully qualified domain name:	Type *ServerName.DomainName.com*

7. [Optional] If the agent will communicate with the Ivanti Endpoint Security server through a proxy server, select the **A proxy server is required** check box and complete the following steps.

   Note: In many network environments, although a proxy is used for Internet access, a proxy bypass is used for all access within the corporate network. Therefore, only enter proxy information if your agents will be required to use a proxy to access your Ivanti Endpoint Security server. Proxy information is not validated. A Squid proxy server will only properly resolve using a fully qualified domain name.

   Refer to Ivanti Community Article 59102 for additional information on a Squid proxy server configuration.

   a) Type the proxy IP address or host name in the **Proxy server address** field.
   b) Type the port number that the proxy uses in the **Port number** field.
   c) [Optional] If the proxy server requires authentication, complete the following steps:

      1. Select the **Authentication is required** check box.
      2. Type the user name in the **Username** field.
      3. Type a new password for the proxy in the **Password** field.

4. Re-type the proxy password for the proxy in the **Confirm Password** field.

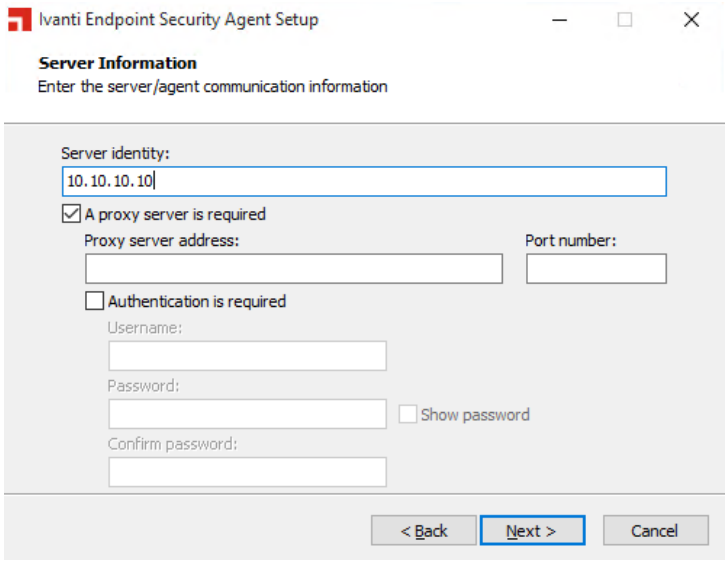


Figure 11: Server Information Page With Proxy Fields Enabled

Tip: Select the **Show password** check box to display the password text.

8. Click **Next**.

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

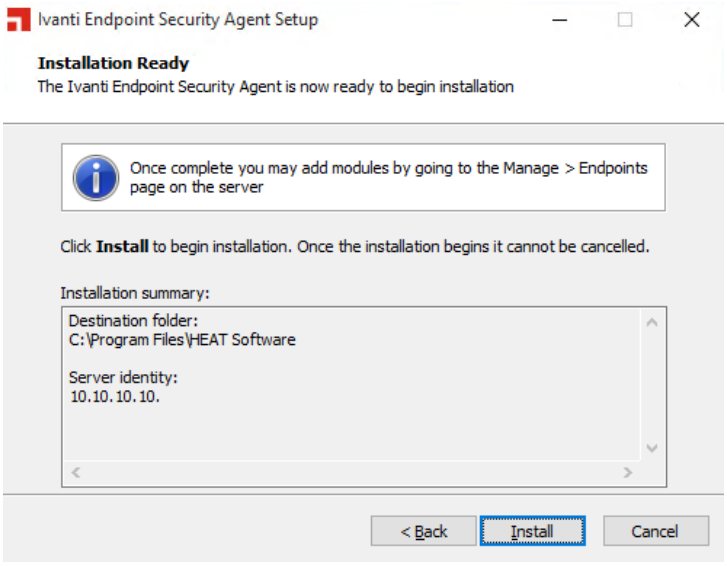


Figure 12: Installation Ready Page

9. Review the installation information and click **Install** to install the agent.

   Note: Once installation begins it cannot be cancelled.

   Step Result: The agent is installed and the ***Installation Complete*** page displays.

   Tip: Click **Open setup log** to open `lmsetup.log` in your text editor.

10. Click **Close** to exit the wizard.

Chapter 4

Installing the Agent on Linux, UNIX, or Mac

In this chapter:

Use the *Command Line* method when installing the Ivanti Endpoint Security Agent on a Linux, UNIX, or Mac endpoints.

Note: To install an agent on Linux, UNIX, or Mac you are restricted to the command line method. For a description of the command line method, refer to Understanding Agent Installation Methods on page 21.

Linux and UNIX Installation Method

A command line is the only method that can be used to install the Ivanti Endpoint Security Agent on Linux, UNIX, or Mac platform.

Install the Ivanti Endpoint Security (Ivanti Endpoint Security) Agent on an endpoint that contains a Linux, UNIX, or Mac operating system using one of the following;

- Use an install parameter in a command line. For additional information, refer to: Installing the Agent by Command Line for Linux, UNIX, or Mac on page 71.
- Use a silent install parameter in a command line. Refer to Silent Install by Command Line for Linux, UNIX, or Mac on page 73.

Note: For a description of agent install methods, refer to Understanding Agent Installation Methods on page 21.

Installing Java Runtime Environment

Prior to installing the Ivanti Endpoint Security Agent, you must have Java Runtime Environment (JRE) 7 or higher.

Verify you are running Java Runtime Environment (JRE) 7 or later on your target endpoint.

1. Log in to the target endpoint using the root user account.
2. Open the ***Terminal*** window.

3. Type `java -version` and press `ENTER`.

   Step Result: The ***Terminal*** window displays the installed version of the Java Runtime Environment (JRE).

4. Use the output in the ***Terminal*** window to verify that the `java version` is `7` or later.
   - If your `java version` is `7` or later, your target endpoint is ready for Ivanti Endpoint Security Agent installation.
   - If your `java version` is earlier than `7`, you must update the Java Runtime Environment. Proceed to the next step.

5. If Java isn't already installed, download and install the latest version of the Java Runtime Environment (JRE).
   a) Open your Web browser and go to Java Web site for the latest version.
   b) Download and install the version of Java Runtime Environment (JRE) that is applicable to your target environment.

   Tip: The Java Web site contains instructions to complete the install of Java Runtime Environment (JRE) for each applicable operating system.

Result: The latest version of Java Runtime Environment (JRE) is installed on your target endpoint.

After Completing This Task:
Complete agent installation by following one of these procedures:

- Installing the Agent by Command Line for Linux, UNIX, or Mac on page 71
- Silent Install by Command Line for Linux, UNIX, or Mac on page 73

Command Line Workflow for Linux, UNIX, or Mac

Review this chart to understand the Ivanti Endpoint Security Agent workflow for command line installation on a Linux, UNIX, or Mac endpoint.

Note: An advantage in using a command line is silent installation. When using silent installation, you can enter all the information necessary prior to the silent installation and then the installation itself runs unattended (without user interaction).

Determine agent requirements. Refer to Agent Requirements on page 7 for a complete list of hardware and software requirements for the agent.

Ensure that Java Runtime Environment 7 or higher is installed on the Linux or UNIX endpoint. Refer to Installing Java Runtime Environment on page 67.

Download the agent installer on a Linux, UNIX, or Mac endpoint. Refer to Downloading the Installer on page 69.

Install the agent. You may install agents on any Linux, UNIX, or Mac endpoints that you want to manage. Agent installation may be done using either:

- A command line. Refer to Installing the Agent by Command Line for Linux, UNIX, or Mac on page 71.
- A silent install parameter in a command line. Refer to Silent Install by Command Line for Linux, UNIX, or Mac on page 73.

Following initial installation, the agent and server components begin communicating. Additionally, if you are licensed for additional modules, you can install these modules on any endpoint that has the Ivanti Endpoint Security Agent.

Note: For more information on modules and module installation, refer to Ivanti Endpoint Security User Guide (https://help.ivanti.com/) .

Downloading the Installer

Download the agent installer from your Ivanti Endpoint Security server by using the Web console.

1. Log on to the target endpoint as the local administrator (or a member of the Local Administrators group).
2. Log in to Ivanti Endpoint Security (Ivanti Endpoint Security) server console as user with administrator privileges.

   For additional information on log in, refer to the Ivanti Endpoint Security User Guide (https://help.ivanti.com/) .

   Step Result: The Ivanti Endpoint Security ***Home*** page opens.

3. Select **Tools** > **Download Agent Installer**.

   Step Result: The ***Download Agent Installers*** dialog opens.

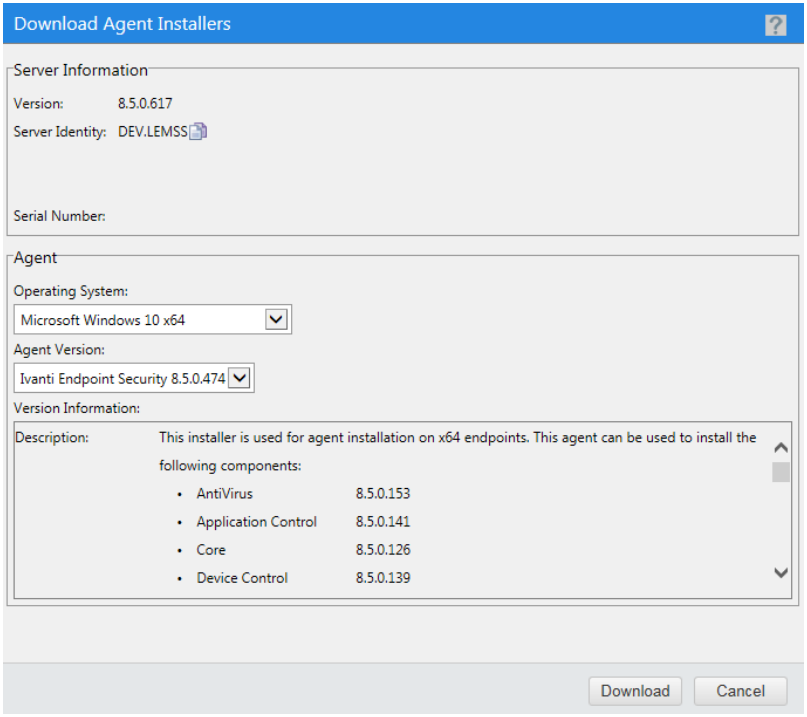


Figure 13: Download Agent Installers Dialog

> **Tip:** The icon allows you to copy information to your clipboard.

4. Select your endpoint's operating system from the **Operating System** drop-down list.
5. Select the version of the agent that you want to install from the **Agent Version** drop-down list.

> **Note:** The agent versions available for selection are controlled by defining the **Agent Versions** option within Ivanti Endpoint Security. For additional information, refer to *Configuring the Agents Tab* in the Ivanti Endpoint Security User Guide (https://help.ivanti.com/) .

6. Click **Download**.

   Step Result: A dialog opens, prompting you to define a download location.

> **Tip:** The ***Download Agent Installer*** dialog remains open during the installer download.

7. Using the dialog controls, define a download location and begin the download.

8. After the download completes, close the ***Download Agent Installers*** dialog by clicking **Cancel**.

Tip: Leave the dialog open while installing the agent to have easy access to Ivanti Endpoint Security server information used during the installation procedure.

Result: You have successfully downloaded the Ivanti Endpoint Security Agent installer.

Installing the Agent by Command Line for Linux, UNIX, or Mac

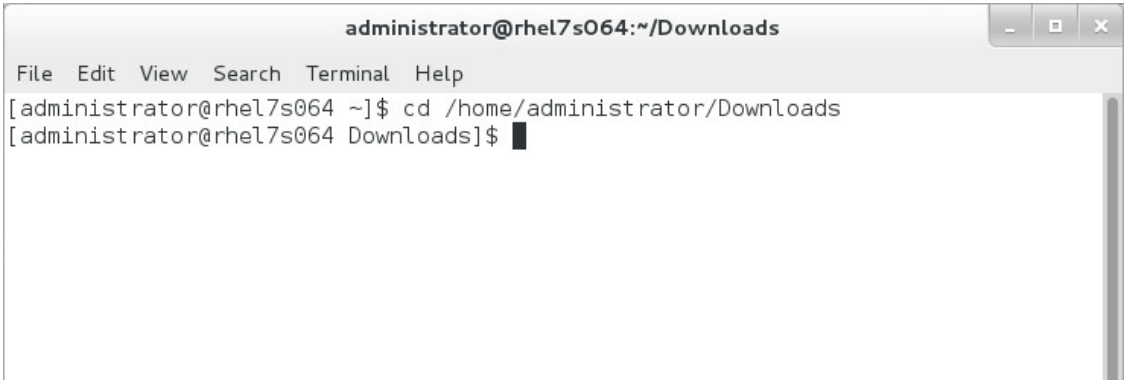
Complete the agent install using a command line.

Prerequisites:

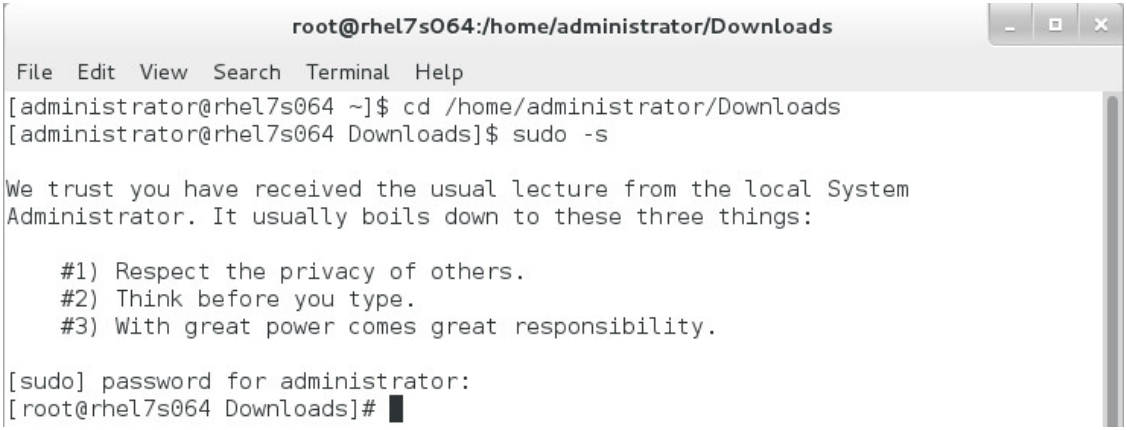
- Review Linux, UNIX, or Mac Endpoint Requirements on page 13.
- Complete Downloading the Installer on page 69.

Complete the following steps to install the agent using a command line.

1. Browse to the location that you downloaded UnixPatchAgent.tar.
2. Extract UnixPatchAgent.tar to any location.
3. Open ***Terminal*** and change the directory to the location of the extracted UnixPatchAgent, which you should have downloaded from the Ivanti Endpoint Security Server.



4. Elevate your command line privileges to superuser.



5. Begin installation by typing `./install` and press **ENTER**.
6. When prompted, define a Patch Agent install location.
   - Press **ENTER** to accept the default location.
   - Type your own location and press **ENTER** to choose a custom path.
7. Enter your Ivanti Endpoint Security Server URL.
   - To use a server name, type `http(s)://`*`servername`* and press **ENTER**.
   - To use an IP address, type `http(s)://`*`IP address`* (`http://10.10.10.10` for example) and press ENTER.
8. Type your Ivanti Endpoint Security serial number and press **ENTER**.

   Tip: You can view the serial number from the ***Home*** page of the Ivanti Endpoint Security Web console.

9. If your enterprise uses FastPath servers (also known as caching proxies) to speed up content deployment, enter FastPath server information.

   Note:
   - If you don't use FastPath servers, press **ENTER** to default to `N`, and continue to the next step.
   - This prompt isn't used to define a firewall proxy.

   a) Type `y` and press **ENTER**.

b) Enter your proxy server URL and press **ENTER**.

- To use a server name, type `http(s)://servername` and press **ENTER**.
- To use an IP address, type `http(s)://IP address` (`http://10.10.10.10` for example) and press ENTER.

Note: A Squid proxy server will only properly resolve using a fully qualified domain name. Refer to Ivanti Community Article 59102 for additional information on a Squid proxy server configuration.

c) If your proxy requires authentication, enter a username and password that authenticate with the proxy. If the proxy doesn't require authentication, just press **ENTER** to continue.

10. If you want the endpoint to add itself to existing Ivanti Endpoint Security groups during registration, complete the following substeps. If not, simply press **ENTER** and continue to the next step.

a) Type `y` and press **ENTER**.

b) Type the groups that you want the endpoint to register with, using the syntax rules that follow. Press `ENTER` when you're done.

Example: *GroupName1|GroupName2|GroupName3*

Syntax rules:

- Separate each group using a pipe (|). If only adding the endpoint to a single group, omit the pipe.
- If you want to add the group to multiple groups, and those groups share the same short name, used the group distinguished name instead.

Tip: You can view group names and distinguished group names within the Group Membership view in the Ivanti Endpoint Security console.

11. If you want to define a nice value for the UnixPatchAgent.tar, type a value (-20 through 20) and press **ENTER**. If you don't want to define a nice value, just leave the prompt empty and press **ENTER**.

Result: The agent is installed. When the process is complete, you can close terminal.

Silent Install by Command Line for Linux, UNIX, or Mac

Complete a silent install using a command line. When configured using command line parameters, the installation of the agent can be run unattended.

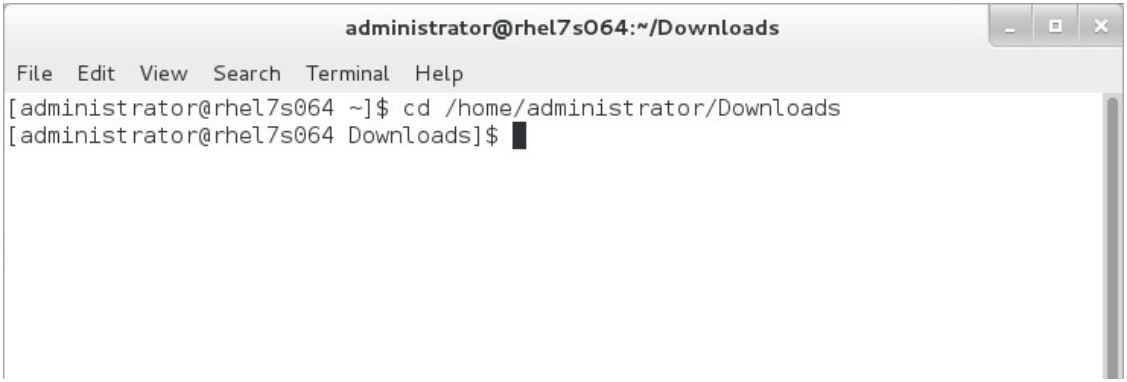
Prerequisites:

- Review Linux, UNIX, or Mac Endpoint Requirements on page 13.
- Complete Downloading the Installer on page 69.

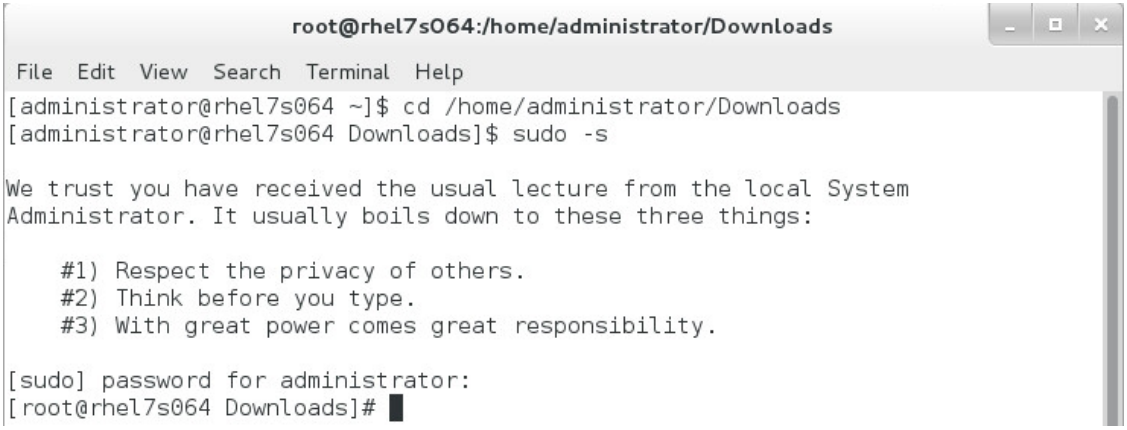
Complete the following steps from your Linux, UNIX, or Mac endpoints.

1. Browse to the location that you downloaded UnixPatchAgent.tar.

2. Extract UnixPatchAgent.tar to any location.
3. Open ***Terminal*** and change the directory to the location of the extracted UnixPatchAgent, which you should have downloaded from the Ivanti Endpoint Security Server.



4. Elevate your command line privileges to superuser.



5. Begin the install by typing the install command followed by the parameters needed to install the agent in your environment.
   - To perform a silent install with a proxy, type the following syntax and press ENTER:

     ```
     ./install -silent -d "/usr/local" -p "http://<MyServer>" -sno "<xxxxxxxx>-<xxxxxxxx>" -proxy
      "http://<MyProxy>" -port <xx> -g "<GroupName>|<GroupName2>"
     ```

   - To perform a silent install without a proxy, type the following syntax and press ENTER:

     ```
     ./install -silent -d "/usr/local" -p "http://<MyServer>" -sno "<xxxxxxxx>-<xxxxxxxx>" -g
      "<GroupName>|<GroupName2>"
     ```

   When installing the Patch Agent from command line, you can add a number of parameters to modify how the agent is installed on the endpoint. The following table lists all available command

line parameters. Read the following table for detailed instruction about how to use each parameter. Remember the following information when using these parameters:

- Parameters do not have to be entered in a specific order.
- Words surrounded in carrots are variables relative to your environment. When defining these parameters, omit the carrots and replace the variable with information relevant in your environment. For example when defining the -p, you might type `-p "http://10.19.0.133"`
- With the exception of password variables, variables are not case sensitive.

Table 13: Parameter Descriptions

Parameter	Description
-silent	Performs installation silently. Example: `-silent`
-d	The install directory. Ivanti recommends using `/usr/local` for most Linux endpoints. Example: `-d "install/directory"`
-p	The URL (or IP) of your Ivanti Endpoint Security server. Examples: • `-p "http://MyServer"` • `-p "http://xxx.xxx.xxx.xxx"`
-sno	The serial number of your Ivanti Endpoint Security. Example: `-sno "xxxxxxxx-xxxxxxxx"`
-proxy	The URL (or IP) of your proxy. Examples: • `-proxy "http://MyServer"` • `-proxy "http://xxx.xxx.xxx.xxx"` **Note:** A Squid proxy server will only properly resolve using a fully qualified domain name. Refer to Ivanti Community Article 59102 for additional information on a Squid proxy server configuration.
-port	The proxy port. Example: `-port "xx"`

Parameter	Description

-g	This parameter adds the target endpoint to existing Ivanti Endpoint Security groups during agent installation. The following list includes information about using this parameter.
	• You can only use this parameter to add endpoints to existing groups. This parameter cannot create new groups.
	• When using this parameter, you can add the endpoint to two or more groups. To add the endpoint to multiple groups, type a pipe between two group names. Do not type spaces between the group names and the pipe(s).
	  • Example (single group): `-g "<Group>"`
	  • Example (multiple groups): `-g "<Group>|<Group2>|<Group3>"`
	• When using this parameter, you can use either the group name or the distinguished name.
	  • If two or more groups exist that share the same name, using the group name will add the endpoint to all groups using the name.
	  • If two or more groups exist that share the same name, using the distinguished name will add the endpoint to a specific group.
	  Example (distinguished name use): `-g "OU=<Group>,OU=Custom Groups,OU=My Groups"`
	Tip: You can view group names and distinguished names from the ***Group Membership*** view within the ***Groups*** page in the Ivanti Endpoint Security Web console.

Result: The agent is installed.

Appendix
A

Upgrading Agents

In this appendix:

- Agent Upgrade on Windows
- Agent Upgrade on Linux, UNIX or Mac

For users upgrading older Ivanti Endpoint Security Agents to the most recent version, there are several options for updating your Ivanti Endpoint Security Agent. The methods available for upgrading vary based on the endpoint's operating system.

Agent Upgrade on Windows

You can use the Ivanti Endpoint Security Web console to upgrade your Ivanti Endpoint Security Agents automatically.

For more information, see Upgrading Agents From the Web Console on page 77.

Note: You may overwrite your Ivanti Endpoint Security Agent on an endpoint. You can overwrite using an Agent Management Job if needed. Using this method will cause data loss when an endpoint's Ivanti Endpoint Security Agent is overwritten. Refer to Installing Agents by Agent Management Job on page 35 for instruction.

Upgrading Agents From the Web Console

You may use the Ivanti Endpoint Security Web console to upgrade your Windows endpoints to the newest agent version.

Window agents can be upgraded from the **Endpoints** page. The following tasks are needed to execute an automatic upgrade of existing network agents.

- Ensure that your agent options are configured so that the latest Ivanti Endpoint Security Agent is available for installation. For additional information, refer to Defining Installable Agent Versions on page 78.
- Select the endpoints you want to upgrade and complete the agent upgrade. For additional information, refer to Upgrading the Agent Using the Endpoints Page on page 79.

Defining Installable Agent Versions
Use the Ivanti Endpoint Security Web console to define that the latest version of the Ivanti Endpoint Security Agent is available for agent installation.

Prerequisites:

Ensure Ivanti Endpoint Security replicates with the Global Subscription Service. This will make certain you have the latest agent version available. Refer to *Replication* in the Ivanti Endpoint Security User Guide (https://help.ivanti.com/) for additional information.

Define the **Agent Versions** from within the Ivanti Endpoint Security (Ivanti Endpoint Security) Web console.

1. Log in to the Ivanti Endpoint Security Web console.
   For additional information, refer to the *Logging in to Ivanti Endpoint Security* in the Ivanti Endpoint Security User Guide (https://help.ivanti.com/) .
2. Select **Tools** > **Options**.
   Step Result: The ***Options*** page opens.
3. Select the ***Agents*** tab.
   Step Result: The ***Agents*** tab opens.
4. Define the **Agent Version**.
   a) Locate the **Agent Versions** area.
   b) Select **Newest available** in the **Windows Vista and newer agent versions** field.

   Tip: The **Newest available** option determines that only the latest agent is available for endpoints. However, you can alternatively select **Ivanti Endpoint Security<*AgentVersion*>+** when selecting an agent version. This selection makes available all agent versions released after the selected version.
5. Click **Save**.

Result: Your agent version selection is saved.

After Completing This Task:
Complete the agent upgrade. For additional information, refer to Upgrading the Agent Using the Endpoints Page on page 79.

Upgrading the Agent Using the Endpoints Page

You may upgrade your Windows agent by using the Ivanti Endpoint Security Web console.

Prerequisites:

- You have a Ivanti Endpoint Security Agent installed on an endpoint containing a supported Windows operating system. Refer to Supported Endpoint Operating Systems on page 7 for a list of supported operating systems.
- Complete Defining Installable Agent Versions on page 78.
- The agent status for the endpoint is `Online`.

Upgrade your Windows agents from the ***Endpoints*** page of the Ivanti Endpoint Security (Ivanti Endpoint Security) Web console.

1. Log in to the Ivanti Endpoint Security Web console.
2. Select **Manage** > **Endpoints**.

   Step Result: The ***Endpoints*** page opens to the **All** tab.
3. From the page list, select the endpoints that you want to upgrade to the latest agent version.
4. Click **Agent Versions**.

   Step Result: The ***Manage Agent Versions*** dialog opens.
5. From the **Select One** list, select the most recent agent version and click **Apply to All Agents**.

   Tip: You may want to test the upgrade on a few endpoints before upgrading your entire network. Do so, by selecting endpoints to test and then select the latest agent version for the endpoints from the **Agent Version** list.
6. Click **OK**.

   Step Result: The agent begins upgrading and the ***Manage Agent Versions*** dialog closes.

   Note: The upgrade process may take several minutes. You may only upgrade an endpoint again once the first upgrade has completed.

Result: The agent is upgraded on all selected endpoints.

Agent Upgrade on Linux, UNIX or Mac

You can upgrade the Ivanti Endpoint Security Agent on a Linux, UNIX, or Mac platform using one of the following methods:

- You can upgrade using a deployment. Refer to Upgrading Agents by Deployment for Linux, UNIX, or Mac on page 80 for additional information.

  Note: For Patch and Remediation users, Ivanti recommends upgrading the agent for Linux, UNIX, or Mac using a deployment, as the patch downloads, installs, and configures the upgrade on your endpoints automatically.

- You can upgrade using a command line. Refer to Upgrading Agents by Command Line for Linux, UNIX, or Mac on page 82 for additional information.

Upgrading Agents by Deployment for Linux, UNIX, or Mac

From your Ivanti Endpoint Security Web console, you can use the ***Deployment Wizard*** to deploy the Patch Agent Upgrade to your Linux, UNIX, or Mac endpoints. The patch downloads, installs, and configures the upgrade automatically.

1. Log in to the Ivanti Endpoint Security Web console.
2. From the navigation menu, select **Review** > **Vulnerabilities** > **All.**

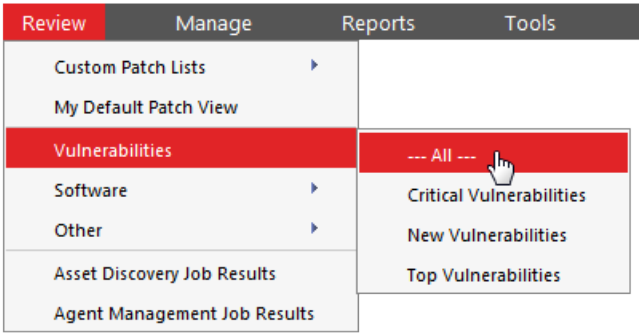


Figure 14: Navigation Menu

3. Enter `Patch Agent Upgrade` in the **Name or CVE_ID** field and click **Update View** to search for the patch agent.

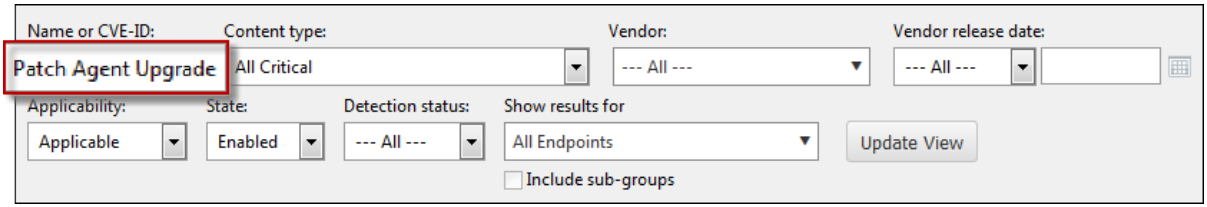


Figure 15: Search Input Example

Step Result: A list of matching packages displays.

4. Select **C – Ivanti Patch Agent Upgrade for LinuxUnixMac from 7.0+ to 8.3032 (See Notes)**.

Note: Do not select the patch titled **C – Ivanti Patch Agent for LinuxUnixMac from 7.0+ to 8.3032 (Manual Install) (See Notes)**. This patch requires manual installation and does not upgrade your endpoints automatically.

5. Click **Deploy**.

Step Result: The ***Deployment Wizard*** opens.

6. Click **Next**.
7. Select the Linux, UNIX, and Mac endpoints you want to upgrade.
8. Click **Next**.

Step Result: A list of available packages displays.

9. The **C – Ivanti Patch Agent Upgrade for LinuxUnixMac from 7.0+ to 8.3032 (See Notes)** patch is preselected in the list. Click **Next**.
10. Accept the terms and conditions of the end user license agreement and click **Next**.
11. Continue through the rest of the wizard. Click **Finish** to finalize the deployment of the package you selected.

Step Result: The agent is upgraded.

Upgrading Agents by Command Line for Linux, UNIX, or Mac

Upgrading the agent manually by command line uninstalls the existing Ivanti Endpoint Security Agent running on Linux, UNIX, or Mac endpoints and installs the most recent version of the agent. The agent upgrade retains all existing agent data.

Prerequisites:

- You have an Ivanti Endpoint Security Agent installed on a Linux, UNIX, or Mac supported operating system. Refer to Supported Endpoint Operating Systems on page 7 for a list of supported operating systems.
- You are logged on to the endpoint using a root user account.

Perform these steps on a Linux, UNIX, or Mac endpoint.

1. Download the most recent version of the agent that is applicable to your target endpoint. Refer to Downloading the Installer on page 69 for more information.
2. Upgrade the agent using one of the following methods:
   - You may upgrade by command line. Refer to Upgrading the Agent by Command Line for Linux, UNIX, or Mac on page 82 for more information.
   - You may use a silent upgrade by command line. Refer to Silent Upgrade by Command Line for Linux, UNIX, or Mac on page 83 for more information.

   Step Result: The agent is upgraded.

Result: After the upgrade completes, you may use the new agent.

Upgrading the Agent by Command Line for Linux, UNIX, or Mac

Complete the agent upgrade using a command line.

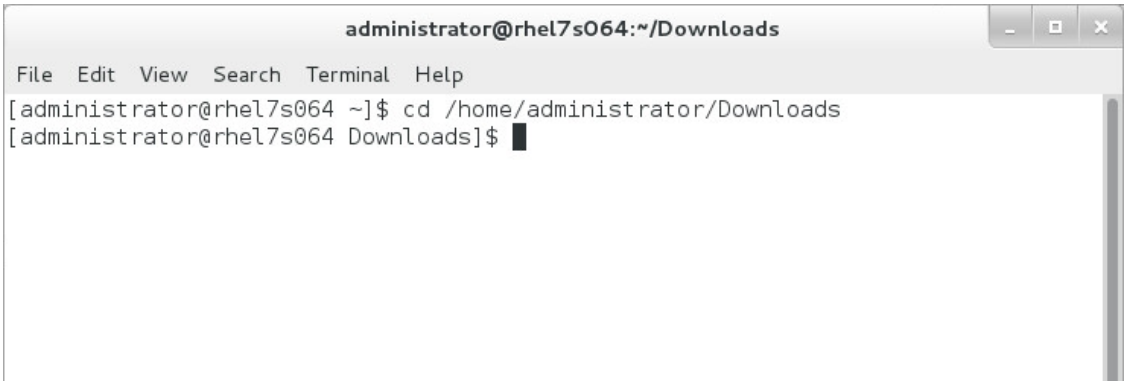
Prerequisites:

- Review Linux, UNIX, or Mac Endpoint Requirements on page 13.
- Complete Downloading the Installer on page 69.

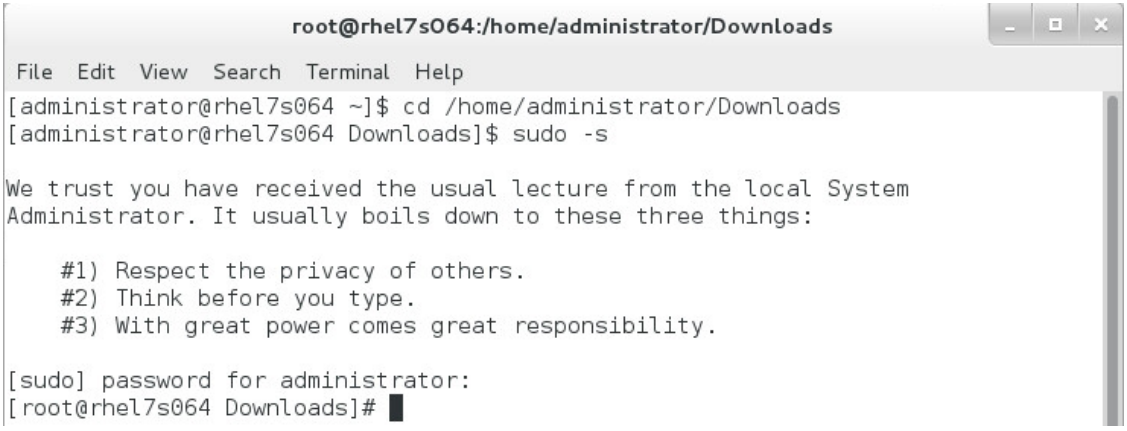
Complete the following steps to upgrade the agent using a command line.

1. Browse to the location that you downloaded UnixPatchAgent.tar.
2. Extract UnixPatchAgent.tar to any location.

3. Open ***Terminal*** and change the directory to the location of the extracted UnixPatchAgent, which you should have downloaded from the Ivanti Endpoint Security Server.



4. Elevate your command line privileges to superuser.



5. Begin the upgrade by typing `./install -reinstall` and press **ENTER**.

Result: The agent is upgraded. When the process is complete, you can close the terminal.

Silent Upgrade by Command Line for Linux, UNIX, or Mac
Complete a silent upgrade using a command line. When configured using command line parameters, the upgrade of the agent can be run unattended.

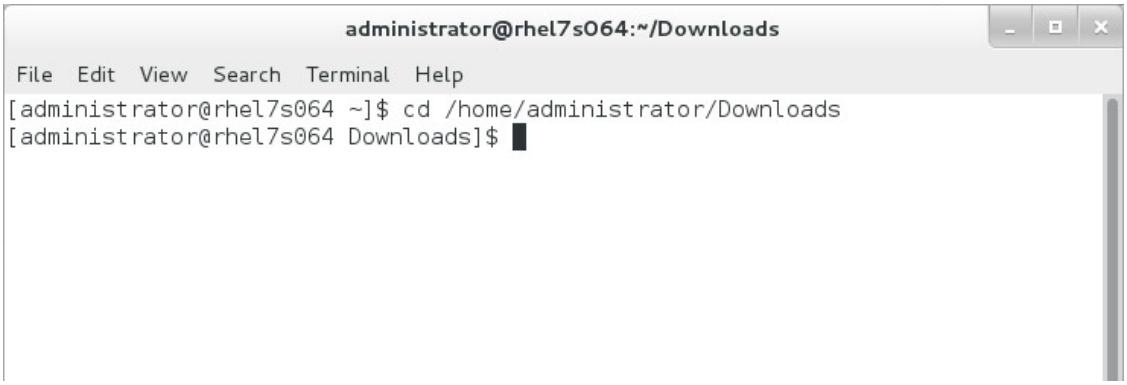
Prerequisites:

- Review Linux, UNIX, or Mac Endpoint Requirements on page 13.
- Complete Downloading the Installer on page 69.

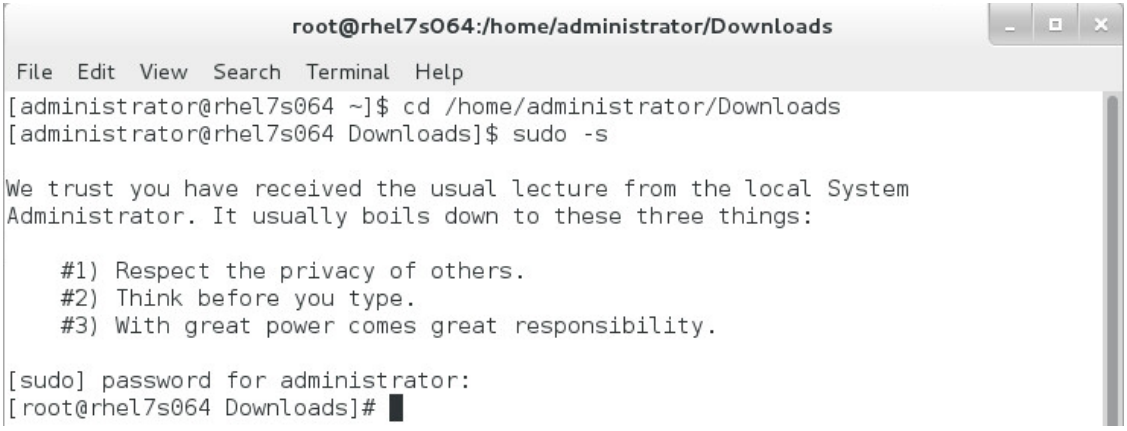
Complete the following steps from your Linux, UNIX, or Mac endpoints.

1. Browse to the location that you downloaded UnixPatchAgent.tar.
2. Extract UnixPatchAgent.tar to any location.

3. Open ***Terminal*** and change the directory to the location of the extracted UnixPatchAgent, which you should have downloaded from the Ivanti Endpoint Security Server.



4. Elevate your command line privileges to superuser.



5. Begin the upgrade by typing the install command, followed by the reinstall command, followed by the parameters needed to install the new agent in your environment.
   - To perform a silent install with a proxy, type the following syntax and press ENTER:

     ```
     ./install -reinstall -silent -d "/usr/local" -p "http://<MyServer>" -sno
      "<xxxxxxxx>-<xxxxxxxx>" -proxy "http://<MyProxy>" -port <xx> -g "<GroupName>|<GroupName2>"
     ```

   - To perform a silent install without a proxy, type the following syntax and press ENTER:

     ```
     ./install -reinstall -silent -d "/usr/local" -p "http://<MyServer>" -sno
      "<xxxxxxxx>-<xxxxxxxx>" -g "<GroupName>|<GroupName2>"
     ```

Result: The agent is upgraded. When the process is complete, you can close the terminal.

Appendix B

Uninstalling Agents

In this appendix:

You can uninstall the Ivanti Endpoint Security Agent using several methods. The methods available for uninstall vary based on the endpoint's operating system.

Agent Uninstall on Windows

To uninstall the Ivanti Endpoint Security Agent on a Windows platform you can utilize the following methods:

- For uninstalling the agent using an Agent Management Job, refer to Uninstalling the Agent by Agent Management Job on page 85.
- For uninstalling using Windows Control Panel, refer to Uninstalling the Agent on Windows on page 96.
- For uninstall using a command prompt, refer to Uninstalling the Agent by Command Line on page 98

Uninstalling the Agent by Agent Management Job

You can remotely uninstall an agent from Windows endpoints using an Agent Management Job. An Agent Management Job allows you to uninstall the agent from the Ivanti Endpoint Security Web console.

Prerequisites:

- You completed the configuration needs for an Agent Management Job. Refer to Agent Management Job Checklist on page 24 for a description.
- Verify that your target endpoint that you installed an agent on is a Windows endpoint. Mac, Linux, and UNIX endpoints cannot have agents uninstalled using an Agent Management Job.
- The agent status for the endpoint is `Online`.

You complete the Agent Management Job within the Ivanti Endpoint Security Web console using an easy-to-use wizard. Configuration occurs in the ***Uninstall Agents Wizard***.

Note: Configuration of the Agent Management Job is similar to configuration of a Discovery Scan Job.

1. Begin configuration of the ***Uninstall Agent Wizard***.
   Complete one of the following sets of steps to begin configuration.

Context	Steps
To open the Wizard without targets predefined:	Select **Discover** > **Assets and Uninstall Agents**.
To open the Wizard with target predefined:	1. Select **Manage** > **Endpoints**. 2. Select the endpoints you want to uninstall agents from. 3. From the toolbar, select **Manage Agents** > **Uninstall Agents**.

   Step Result: The wizard opens to the ***Job Name and Scheduling*** page.

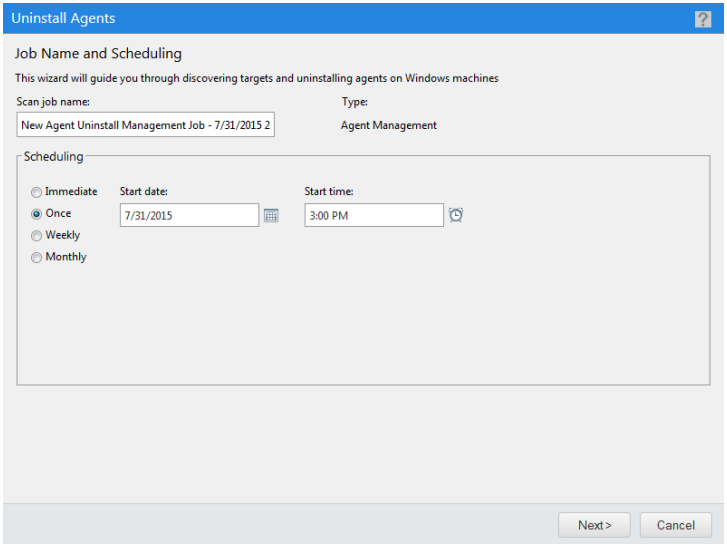


Figure 16: Job Name and Scheduling Page

2. [Optional] Type a new name in the **Scan job name** field.

Note: By default, a new Agent Management Job for uninstallation is named `New Agent Uninstall Management Job`, followed by the server's date and time, which is formatted according to your browser's locale setting.

3. Schedule the job.

   Use one of the following methods.

Tip: During job scheduling, you can use the following shortcuts:

- Click the **Calender** icon to select a **Start date**. Selecting a date automatically fills the **Start date** field.
- Click the **Clock** icon to select a **Start time**. Selecting a time automatically fills the **Start time** field.

Method	Steps
To schedule an immediate job:	Select the **Immediate** option.
To schedule a one-time job:	1. Ensure the **Once** option is selected. 2. Define a start date by typing a date in the **Start date** field. **Note:** Type the date in a `mm/dd/yyyy` format. 3. Define a start time by typing a time in the **Start time** field. **Note:** Type the time in `hh:mm` format followed by `AM` or `PM` (if necessary). This field supports both 12- and 24-hour time. **Tip:** Scheduling a one-time job for a past date and time will launch the job immediately.
To schedule a recurring weekly job:	1. Select the **Weekly** option. 2. Define a start date by typing a date in the **Start date** field. **Note:** Type the date in a `mm/dd/yyyy` format. 3. Define a start time by typing a time in the **Start time** field. **Note:** Type the time in `hh:mm` format followed by `AM` or `PM` (if necessary). This field supports both 12- and 24-hour time. 4. Define the day of the week the job runs by selecting a day from the **Run every week on the following day** list.

Method	Steps
To schedule a recurring monthly job:	**1.** Select the **Monthly** option. **2.** Define a start date by typing a date in the **Start date** field. **Note:** Type the date in a `mm/dd/yyyy` format. **3.** Define a start time by typing a time in the **Start time** field. **Note:** Type the time in `hh:mm` format followed by `AM` or `PM` (if necessary). This field supports both 12- and 24-hour time. **4.** Define the day of the month the job runs by typing a day in the **Run every month on the following day** field.

Tip: One-time and recurring jobs scheduled for the last day of a 31-day month are automatically rescheduled for the last day of shorter months.

4. Click **Next**.

Step Result: The ***Targets*** page opens.

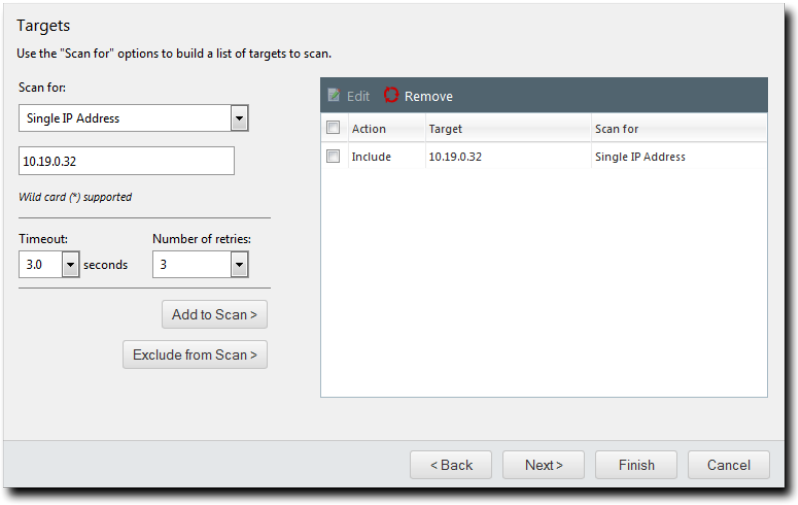


Figure 17: Targets Page

5. Define targets (endpoints) for the job to locate.
   Use one or more of the following discovery methods.

Method	Steps
To define targets using a single IP address:	1. From the **Scan for** list, select **Single IP Address**. 2. Type an IP address in the empty field. **Note:** Wildcards are supported. For additional information, refer to Defining Targets Using Wildcards on page 51. 3. Edit the **Timeout** list. **Note:** The **Timeout** list defines the number of seconds before a scan fails due to inactivity for a particular target. Under most network conditions, the **Timeout** field does not require editing. 4. Edit the **Number of retries** list. **Note:** The **Number of retries** list defines the number of times a scan retries on that target if the scan times out.
To define targets using an IP range:	1. From the **Scan for** list, select **IP Range**. 2. In the first empty field, type the beginning of IP range. **Note:** Wildcards are supported. For additional information, refer to Defining Targets Using Wildcards on page 51. 3. In the second empty field, type the ending of the IP range. 4. Edit the **Timeout** list. **Note:** The **Timeout** list defines the number of seconds before a scan fails due to inactivity for that particular target. Under most network conditions, the **Timeout** field does not require editing. 5. Edit the **Number of retries** list. **Note:** The **Number of retries** list defines the number of times a scan retries on that target if the scan times out.
To define targets using a computer name:	1. From the **Scan for** list, select **Computer name**. 2. In the empty field, type an endpoint name. **Note:** Use one of the following formats: `endpointname` or `domain\endpointname`.

Method	Steps
To define targets using network neighborhood:	1. From the **Scan for** list, select **Network Neighborhood**. 2. From the second list, select the desired network neighborhood.
To define targets using active directory:	1. From the **Scan for** list, select **Active Directory**. 2. In the **Fully-qualified domain name** field, type the DNS domain name of the domain controller you want to scan. **Note:** For example, if your domain controller DNS name is *box.domain.company.local*, you would type *domain.company.local* in this field. 3. Optionally, in the **Organizational Unit** field, type the active directory organizational unit string from specific to broad, separating each string with front slashes (such as `Techpubs/Engineering/Corporate`). **Note:** The omission of this field returns job results containing the full contents of *all* the active directory organizational units. View the following figure for an example of how to enter data using **Active Directory**. 4. In the **Domain controller** field, type the domain controller IP address. 5. In the **Username** field, type a user name that authenticates with the domain controller. **Note:** Type the user name in one of the following format: `domainname\username` or `username`. 6. In the **Password** field, type the password associated with the user name.

Method	Steps
To define targets using an imported file:	1. From the **Scan for** list, select **Import file**. 2. Click **Browse**. 3. Browse to the file you want to use for target discovery. **Note:** The following file types are supported: `.txt` and `.csv`. 4. Click **Open**.

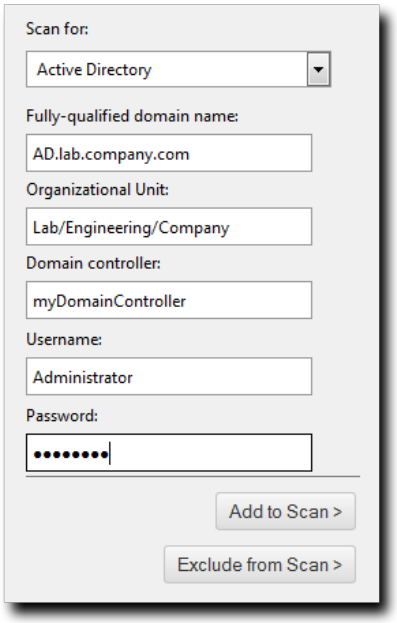


Figure 18: Active Directory Input Example

6. Add targets to the wizard list. This list indicates whether defined targets are included in or excluded from the job.

   Use one of the following methods.

Note: You must include at least one target for **Next** to become available. You can also delete targets from the list by selecting the applicable check boxes and clicking **Remove**.

Method	Steps
To include defined targets in the job:	Click **Add to Scan**.

Method	Steps
To exclude defined targets from the job:	Click **Exclude from Scan**.

Tip: Repeat this step to add additional targets to the list.

7. [Optional] Edit the **Targets** list.
   - To remove targets from the list, select the list item(s) and click **Remove**.
   - To edit targets on the list, select the list item(s) and click **Edit**.

     For additional information on editing, refer to *Editing Targets* in the Ivanti Endpoint Security User Guide (https://help.ivanti.com/) .
8. Click **Next**.

   Step Result: The ***Options*** page opens.

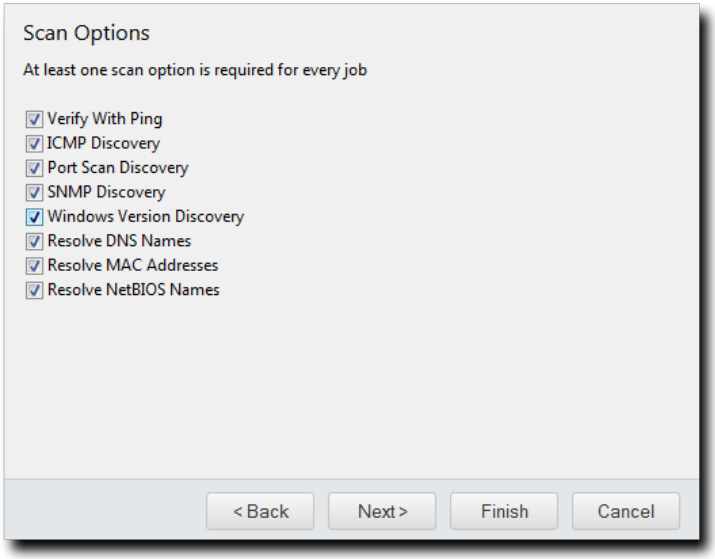


Figure 19: Options Page

9. Select or clear the desired **Scan Options**.
   The following table defines each **Scan Option**.

Option	Description
Verify With Ping	Jobs using this option send ping requests to all network endpoints targeted for discovery. Endpoints that respond to the request are flagged for scanning; unresponsive endpoints are skipped. Endpoints unresponsive to **Verify With Ping** are not scanned by other selected discovery options. **Note:** Anti-virus software and host firewalls may block **Verify With Ping**. If necessary, adjust any antivirus and firewall configurations to permit ping requests.
ICMP Discovery	Jobs using this option request a series of echoes, information, and address masks from endpoints. Endpoint responses are then compared to a list of known ICMP fingerprints to identify endpoint operating systems. **Note: ICMP Discovery** is ineffective on endpoints configured to ignore ICMP requests. For best results identifying Windows operating systems, use this option in conjunction with **Windows Version Discovery**.
Port Scan Discovery	Jobs using this option perform a limited scan on endpoint FTP, Telnet, SSH, SMTP, and HTTP ports. Based on the application banners found in these ports, endpoint operating systems are generically identified. **Note:** For best results in identifying Windows operating systems, use this option in conjunction with **Windows Version Discovery**.
SNMP Discovery	Jobs using this option request system properties for SNMP devices (routers, printers, and so on) from the management information base. Following credential authentication, SNMP devices are identified. **Note:** Without authenticated credentials, SNMP devices ignore **SNMP Discovery** requests. In this event, one of two outcomes occur: the SNMP device is misidentified as a UNIX endpoint or the SNMP device is not detected. Jobs with no SNMP credentials use the *public* credential by default.

Option	Description
Windows Version Discovery	Jobs using this option identify an endpoint's specific version of Windows following generic operating system identification during **ICMP** or **Port Scan Discovery**. **Note:** Correct operating system identification is contingent upon authenticated credentials. This option must be used in conjunction with either **ICMP** or **Port Scan Discovery**.
Resolve DNS Names	Jobs using this option acquire the endpoint DNS name through a local DNS server query. These names are displayed in job results for easy endpoint identification.
Resolve MAC Addresses	Jobs using this option acquire endpoint MAC addresses through endpoint queries. These addresses are displayed in job results for easy endpoint identification. **Note:** Monitor network inventory reports to prevent MAC address spoofing that may alter the **Resolve MAC Addresses** results.
Resolve NetBIOS Names	Jobs using this option acquire endpoint NetBIOS names through WINS NetBIOS mapping. These names are displayed in job results for easy endpoint identification.

10. Click **Next**.

Step Result: The ***Credentials*** page opens.

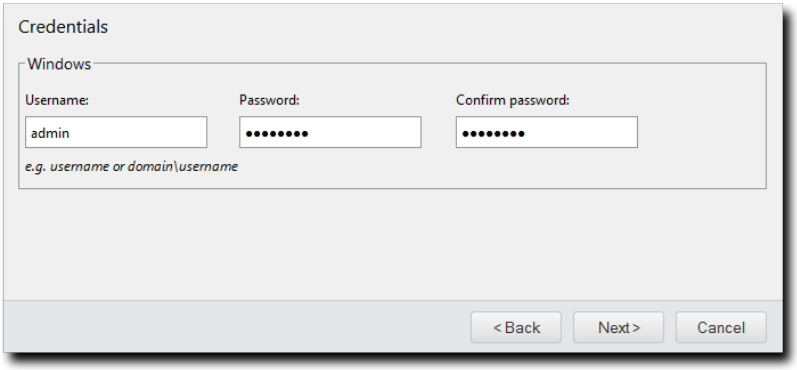


Figure 20: Credentials Page

11. Define **Windows** credentials for the target.

Type the applicable information in the following fields.

Note: When configuring an Agent Management Job, you must define valid Windows credentials.

Field	Description
Username	A user name that authenticates with Windows-based endpoints. Type the user name in a local format (*UserName*) or a domain format (*DOMAIN\UserName*). **Note:** When configuring Agent Management Jobs, Ivanti recommends using the built-in Administrator account.
Password	The password associated with the **Username**.
Confirm password	The **Password** retyped.

12. Click **Next**.

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

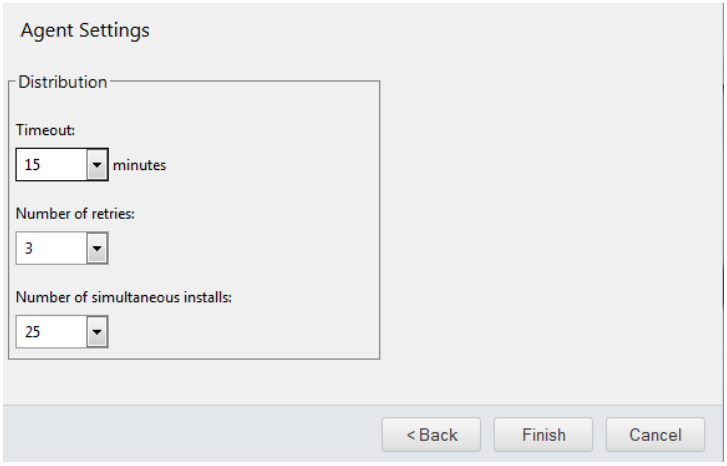


Figure 21: Agent Settings Page

13. Define the **Distribution** options.

The following table describes each list their available values.

List	Description
Timeout (list)	Defines the number of minutes before the Agent Management Job terminates an install attempt due to a non-responsive agent installation or removal (0-30).

List	Description
Number of retries (list)	Defines the number of attempts an agent installation or removal will retry if the initial attempt fails (1-10).
Number of simultaneous installs (list)	Defines the maximum number of agents that can installed or removed simultaneously during the job (1-25). A value of `1` indicates that serial installs or removals should occur.

14. Click **Finish**.

Result: The ***Uninstall Agents Wizard*** closes. Depending on how you configured the job, it moves to either the ***Scheduled*** tab or ***Active*** tab on the ***Job Results*** page. The job will run at the applicable time, uninstalling agents on the defined targets, and move to the ***Completed*** tab when finished.

Uninstalling the Agent on Windows

You can uninstall Ivanti Endpoint Security Agent on a Windows endpoint manually using the ***Agent Setup Wizard***.

Prerequisites:

- You have a Ivanti Endpoint Security Agent installed on an endpoint containing a supported Windows operating system. Refer to Supported Endpoint Operating Systems on page 7 for a list of supported operating systems.
- Ensure you are logged on with an administrative user account.

To uninstall the agent, perform the following procedure on an endpoint with a supported Windows operating system.

1. Open **Add or Remove Programs**.
2. Uninstall the **Ivanti Endpoint Security Agent**.

Tip: You can also uninstall the agent by downloading and opening the ***Agent Setup Wizard***. For additional information about obtaining this wizard, refer to Downloading the Installer on page 61.

Step Result: The ***Agent Setup Wizard*** opens to the ***Authorization Required to Upgrade or Uninstall*** page.

Note: The ***Authorization Required to Upgrade or Uninstall*** page does not open when the **Agent Uninstall Protection** policy is set to `Off` for the endpoint. For additional information on agent uninstall protection, refer to *Editing an Agent Policy Set* in the Ivanti Endpoint Security User Guide (https://help.ivanti.com/) .

If this page does not open, proceed to 4 on page 97.

3. Type the global uninstall password or the agent uninstall password for the endpoint in the **Global or agent uninstall password** field and click **Next**.

Note: Ivanti *does not* recommend providing end users with the global uninstall password in uninstall scenarios. The **Global uninstall password** should be used by the Ivanti Endpoint Security Administrator only.

Tip: Use the Ivanti Endpoint Security Web console to find these passwords.

- View an endpoint uninstall password from its ***Endpoint Details*** page.
- View the global uninstall password from the ***Agent Policy Sets*** page by editing the **Global System Policy**.

Step Result: The ***Previous Agent Installation Detected*** page opens.

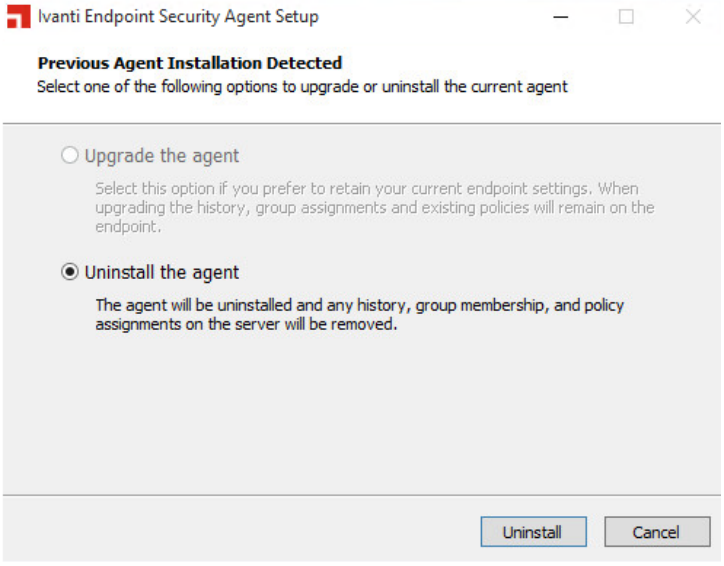


Figure 22: Previous Agent Installation Detected Page

4. Select the **Uninstall the agent** option and click **Uninstall**.

Step Result: The uninstall begins. Upon completion the ***Uninstall Complete*** page opens.

Note: If the Microsoft Visual C++ 2010 Redistributable package or later was installed during agent install, it is not removed during agent uninstall.

5. Complete the uninstall.
   - If no further steps are needed, click **Close**.
   - If you are prompted to reboot your endpoint, click **Restart Now**.

Result: The agent is uninstalled.

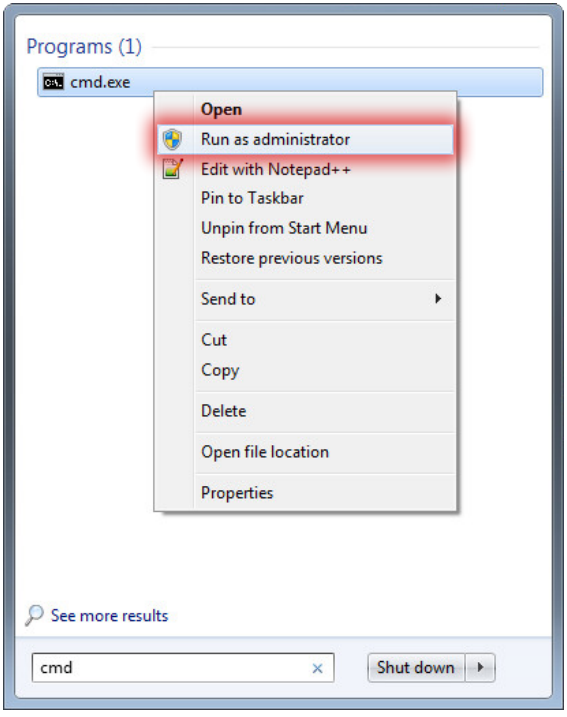
> **Tip:** If desired, you may reinstall the agent. Refer to Understanding Agent Installation Methods on page 21 for additional information.

Uninstalling the Agent by Command Line

Instead of using the ***Agent Install Wizard***, you can open a prompt and uninstall the agent with a command.

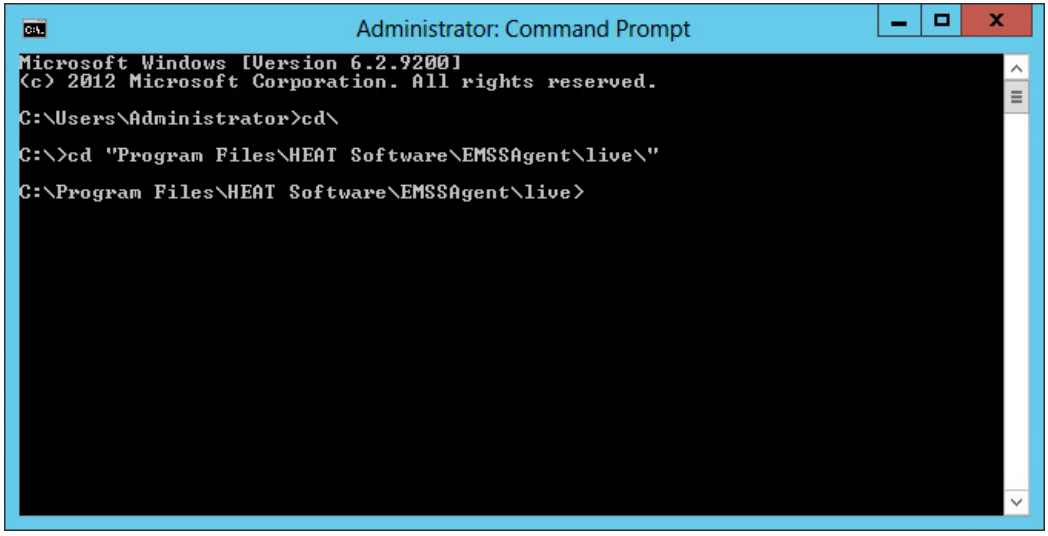
1. From the endpoint where you'll be uninstalling the Ivanti Endpoint Security Agent, open a command prompt as administrator.

   Open the **Start Menu** or **Start Screen** and search for **cmd**. Right-click it and select **Run as administrator**.

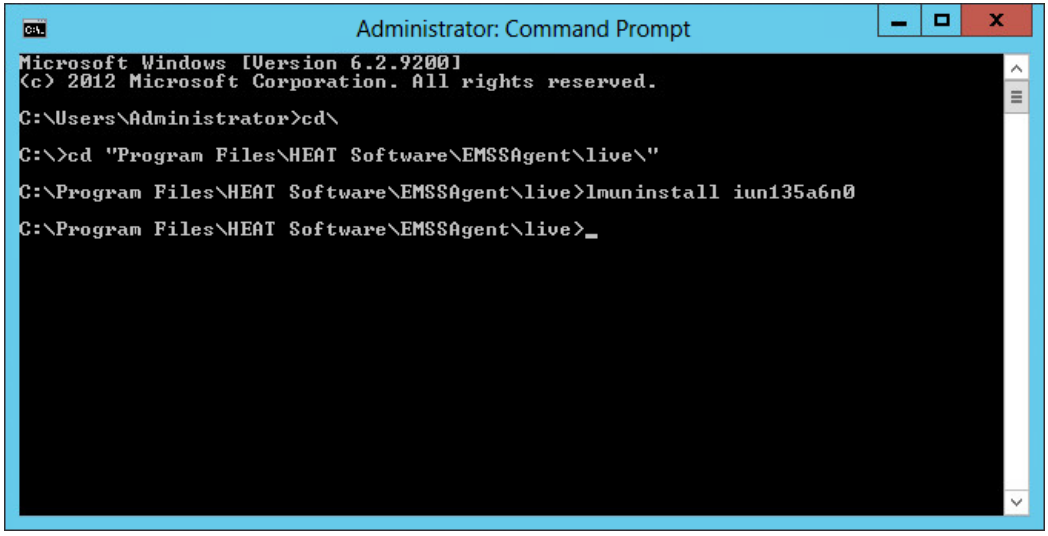


2. Change to the Ivanti Endpoint Security Agent live directory.

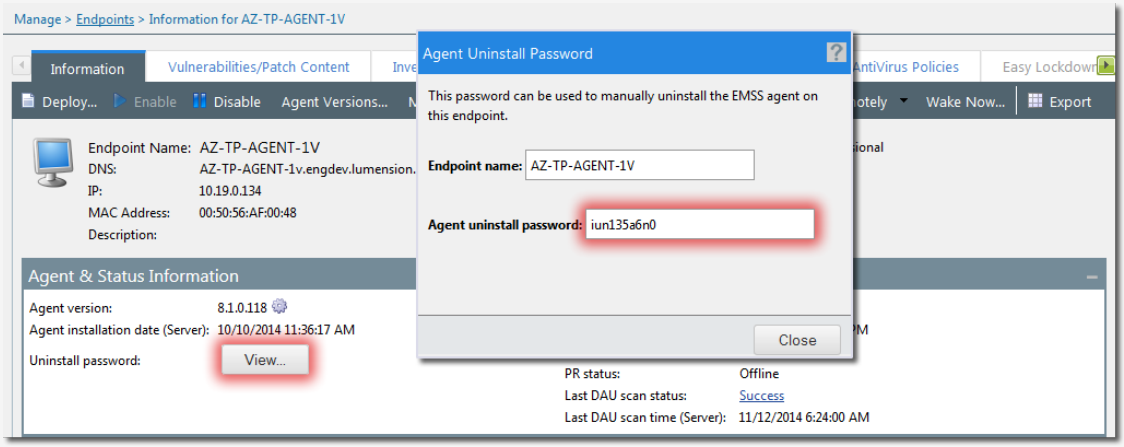
   It's usually located at **%Program Files%\HEAT Software\EMSSAgent\live**, but it may be in a different place if you installed it in a custom location.



3. Remove the agent by entering the uninstall command along with the agent's uninstall password: `lmuninstall %agentUninstallPassword%`.



Tip: You can find the uninstall password by navigating to the agent's ***Endpoint Details*** page in the Ivanti Endpoint Security console.



Step Result: The agent uninstall begins (but there won't be anything on screen that indicates this action is occurring.)

Result:
- The agent uninstall completes when you can type text in the command prompt again.
- The agent listing is also removed from the Ivanti Endpoint Security console.

Agent Uninstall on Linux, UNIX, or Mac

You can use a command line to uninstall the Ivanti Endpoint Security Agent on a Linux, UNIX, or Mac platform.

You may uninstall the Ivanti Endpoint Security (Ivanti Endpoint Security) Agent on an endpoint that contains a Linux, UNIX, or Mac operating system. Refer to Uninstalling the Agent for Mac, Linux, or UNIX on page 100.

Uninstalling the Agent for Mac, Linux, or UNIX

Uninstall of Mac, Linux, or UNIX agents can only be completed by command line.

Prerequisites:

- You have a Ivanti Endpoint Security Agent installed on an your endpoint that contains either a Mac, Linux, or UNIX operating system. Refer to Supported Endpoint Operating Systems on page 7 for a list of supported operating systems.
- Ensure you are logged on to the endpoint using a root user account.

To uninstall the agent, perform the following procedure on an endpoint with a Mac, Linux, or UNIX operating system.

1. Open ***Terminal***.

   Note: How you open ***Terminal*** varies by operating system.

   Step Result: ***Terminal*** opens.

2. Change directory to the agent installation directory. The following table lists the default installation directory for various operating systems.

Operating System	Command
Mac	`/private/var/patchagent`
Linux	`/usr/local/patchagent`
UNIX	`/export/home/patchagent`

   Note: If you installed the agent to a directory other than the default directory, navigate to that directory.

3. Type `./uninstall` at the command prompt and press `ENTER`.

   Step Result: The agent is uninstalled.

4. Change directory to the parent directory of the installation directory. Type the command for your operating system below and press `ENTER`.

Operating System	Command
Mac	`cd /private/var/`
Linux	`cd /usr/local/`
UNIX	`cd /export/home/`

   Note: If you installed the agent to a directory other than the default directory, navigate to the parent directory of the agent installation directory.

5. Type `rm -rf patchagent` and press `ENTER`.

Result: The agent installation directory is deleted.

Tip: If desired, you may reinstall the agent using the Command Line method. Refer to Understanding Agent Installation Methods on page 21 for additional information.