# Ivanti Content Wizard 8.6

## User Guide

ivanti | Endpoint Security

powered by HEAT

# Notices

**Version Information**

Ivanti Content Wizard User Guide - Ivanti Content Wizard Version 8.6 - Published: Dec 2020 Document Number: 02_007_8.6_171421134

**Copyright Information**

# Table of Contents

# Chapter 1

## Ivanti Content Wizard Overview

**In this chapter:**

The Ivanti Content Wizard enables you to build custom patches to maintain software within your organization.

Along with the Ivanti Endpoint Security, the Ivanti Content Wizard provides a comprehensive solution for patching and maintaining a company network, and comes with a subscription of pre-built patches delivered over a secure Internet connection.

Content Wizard allows you to perform the following tasks:

- Import patches
- Export patches
- Create and edit custom patches

**Note:** You cannot edit any published Ivanti patches.

## Understanding Patch Structure

The structure of a Ivanti patch allows the ability to create one patch and apply it to many different operating systems and software versions. This allows for the creation of different packages and signatures capable of identifying the presence of patch files within a device.

The typical structure of a patch is represented below. As shown in the diagram, you can have more than one signature for each patch. Each signature can have multiple fingerprints and pre-requisites. However, you can only have one package assigned per signature.

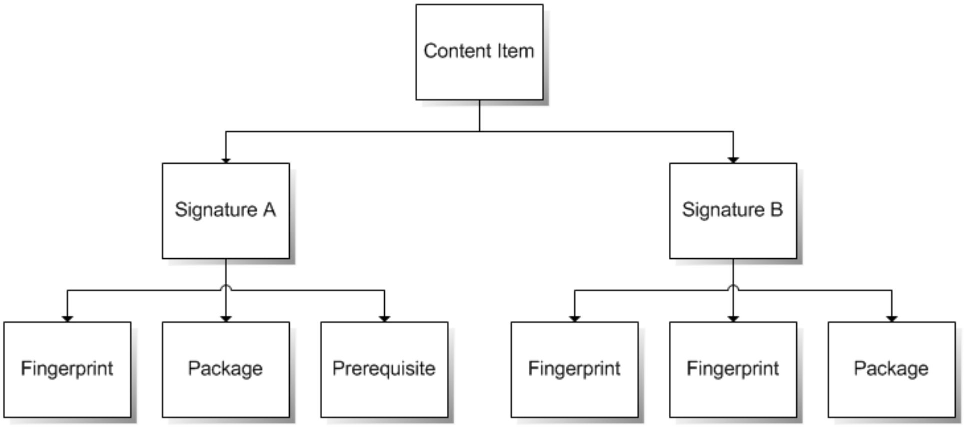


Figure 1: Patch Structure

The various components of a patch are:

| Patch Component | Description |
|---|---|
| **Patch** | A patch is the container for the entire object. All properties set for the patch are viewed from the ***Vulnerabilities*** page of the Ivanti Endpoint Security. Each patch can have more than one signature. |
| **Signature** | A signature recognizes a specific combination of installed software in an operating system. Patches usually contain multiple signatures to compensate for variances within applications. Frequently, a patch requires different executables, dynamic-link libraries, and switches in order to run or detect the patch within different operating systems. |
| **Fingerprint** | A fingerprint can represent a unique file, folder, registry key, or other data value somewhere within a system. Each signature can contain one or more fingerprints which detects if a patch is present in the system. |

| Patch Component | Description |
|---|---|
| **Pre-requisite** | A pre-requisite is a signature belonging to another patch with its own fingerprints. Adding a pre-requisite to a signature requires the pre-requisite is met before analyzing the signature for the current patch. If that signature's pre-requisite is met, the agent analyzes the fingerprints of the current signature, otherwise they are ignored and the patch is not be applied to the device. |
| **Package** | A package contains the actual files used to update or install software on the system. Each package contains the script commands for installing the package files or running the executable that installs the patch. |

Chapter

2

# Installing the Ivanti Content Wizard

**In this chapter:**

- Minimum Hardware Requirements
- Supported Environments
- Other Requirements
- Verifying Your Ivanti Content Wizard License
- Installing the Ivanti Content Wizard Server
- Installing the Ivanti Content Wizard Client

The Ivanti Content Wizard consists of both a server and client component. Both components must be installed before you can use the Ivanti Content Wizard.

Prior to installing either of the Ivanti Content Wizard components, you must install the Ivanti Endpoint Security (Endpoint Security) server. For details regarding the installation of Endpoint Security, refer to the Ivanti Endpoint Security: Server Installation Guide (https://www.ivanti.com/support/product-documentation).

To install the Ivanti Content Wizard server component, refer to Installing the Ivanti Content Wizard Server on page 16.

To install the Ivanti Content Wizard client component, refer to Installing the Ivanti Content Wizard Client on page 19.

**Note:** As there were no changes to the Ivanti Content Wizard associated with Ivanti Endpoint Security 8.6, the Content Wizard has not been updated and the Content Wizard 8.5 Update 3 version is compatible with Ivanti Endpoint Security 8.6

**Warning:** If you have Ivanti Content Wizard 7.2 or earlier installed, you must uninstall it before running the Ivanti Content Wizard 8.5 Update 3 installer.

## Minimum Hardware Requirements

To successfully install the Ivanti Content Wizard, your computer must meet or exceed the specified hardware requirements.

### Server Requirements

- Ivanti Endpoint Security
- Patch and Remediation module for Ivanti Endpoint Security
- Microsoft .NET Framework 3.5 (this specific version of .NET Framework is required.)

### Client Requirements

- 1.4 GHz Processor (or higher)
- 1 GB RAM
- 20 MB of free disk space for installation
- 5 GB of free disk space after installation
- Microsoft .NET Framework 4.0 (or higher)

## Supported Environments

The Ivanti Content Wizard can only be installed on supported operating systems and within supported environments.

### Server Components

The Ivanti Content Wizard server component is supported on Ivanti Endpoint Security 8.0+ servers:

**Note:** Regardless of the Endpoint Security server version, the Patch and Remediation module is also required.

### Client Components

The Ivanti Content Wizard client component is supported on the following operating systems:

- Microsoft Windows 8.1 (x86/x64)
- Microsoft Windows 10 (x86/x64)
- Microsoft Windows Server 2012 (x64)
- Microsoft Windows Server 2012 R2 (x64)
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019

## Other Requirements

The Ivanti Content Wizard requires the following additional requirements.

- The Patch and Remediation module be installed. The Patch and Remediation module is used to deploy created package content built using the Ivanti Content Wizard. Refer to Ivanti Endpoint Security: Patch and Remediation User Guide (https://www.ivanti.com/support/product-documentation) for installation instructions.
- The computer where you are installing the Content Wizard server component must use English (United States) as the language parameter setting.
- Each computer that hosts the Ivanti Content Wizard client component requires .NET Framework 4.0 or higher installed.

## Verifying Your Ivanti Content Wizard License

Verify that your Ivanti Content Wizard license is valid before installing the Ivanti Content Wizard server component.

1. Log into the Endpoint Security server console as a user with administrator privileges.
2. Select **Tools** > **Subscription Updates**.

   **Step Result:** The ***Subscription Updates*** page opens.

3. Click **Update Now**.

   **Step Result:** The ***Subscription Service*** page shows that both **Vulnerabilities / Content** and **Licenses** has completed successfully.

4. Select **Help** > **Product Licensing**.

   **Step Result:** The ***Product Licensing*** page opens.

5. Click **Validate**.

   **Step Result:** A dialog opens, asking you to acknowledge the validation initiation.

6. Click **OK**.

   **Step Result:** The job begins. Completion may take several minutes.

7. Click the **Rotating Chevron** (>) to expand the Content Wizard list item.
8. Verify the **Product Information** section shows Content Wizard with an expiration date that has not expired.

   **Important:** If you do not have a valid Content Wizard license, discontinue installation and contact Ivanti Sales Support (sales@lumension.com).

## Installing the Ivanti Content Wizard Server

The Ivanti Content Wizard server component is installed on the Ivanti Endpoint Security server. The server component is installed before the client component.

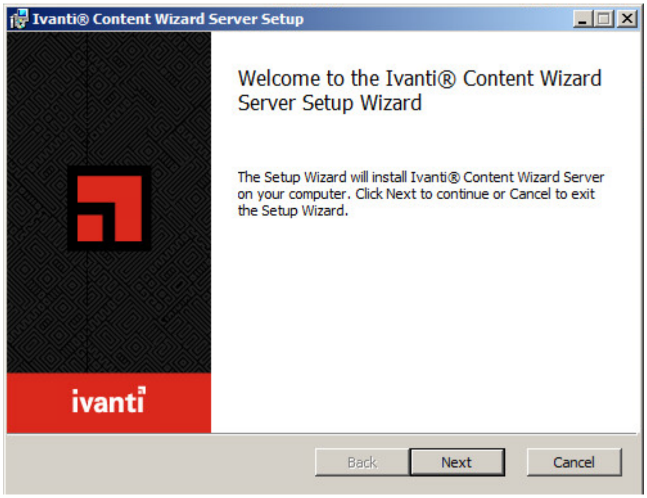
**Prerequisites:**

- Verify that you satisfy the minimum hardware. For more information, see Minimum Hardware Requirements on page 13.
- Verify that your operating system is supported. For more information, see Supported Environments on page 14.
- Install the Ivanti Endpoint Security (Endpoint Security) server and verify that you can connect to it.
- The Ivanti Content Wizard (Content Wizard) requires that the Patch and Remediation module be installed.
- Administrative rights on the Endpoint Security server where you are installing the Content Wizard server component.
- Verify the computer where you are installing the Content Wizard server component is configured with English (United States) as the language parameter.
- You must be licensed for the Content Wizard. Refer to Verifying Your Ivanti Content Wizard License on page 15.
- Download the most current version of the Content Wizard installer from the Ivanti Customer Portal (https://www.ivanti.com/support/product-documentation/).

1. Browse to the location where you downloaded the most current version of the Content Wizard installer and open the `HCWServer.msi`.

2. Open the installation file.

   **Step Result:** The ***Ivanti Content Wizard Server Setup Wizard*** opens.



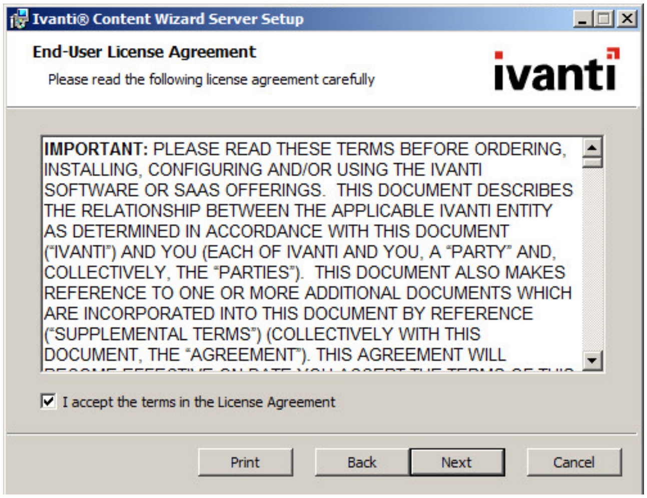
Welcome to the Ivanti® Content Wizard Server Setup Wizard

The Setup Wizard will install Ivanti® Content Wizard Server on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

Figure 2: Ivanti Content Wizard Server Setup Wizard

3. Click **Next**.

   **Step Result:** The ***License Agreement*** page opens.



**End-User License Agreement**

Please read the following license agreement carefully

**IMPORTANT:** PLEASE READ THESE TERMS BEFORE ORDERING, INSTALLING, CONFIGURING AND/OR USING THE IVANTI SOFTWARE OR SAAS OFFERINGS. THIS DOCUMENT DESCRIBES THE RELATIONSHIP BETWEEN THE APPLICABLE IVANTI ENTITY AS DETERMINED IN ACCORDANCE WITH THIS DOCUMENT ("IVANTI") AND YOU (EACH OF IVANTI AND YOU, A "PARTY" AND, COLLECTIVELY, THE "PARTIES"). THIS DOCUMENT ALSO MAKES REFERENCE TO ONE OR MORE ADDITIONAL DOCUMENTS WHICH ARE INCORPORATED INTO THIS DOCUMENT BY REFERENCE ("SUPPLEMENTAL TERMS") (COLLECTIVELY WITH THIS DOCUMENT, THE "AGREEMENT"). THIS AGREEMENT WILL

☑ I accept the terms in the License Agreement

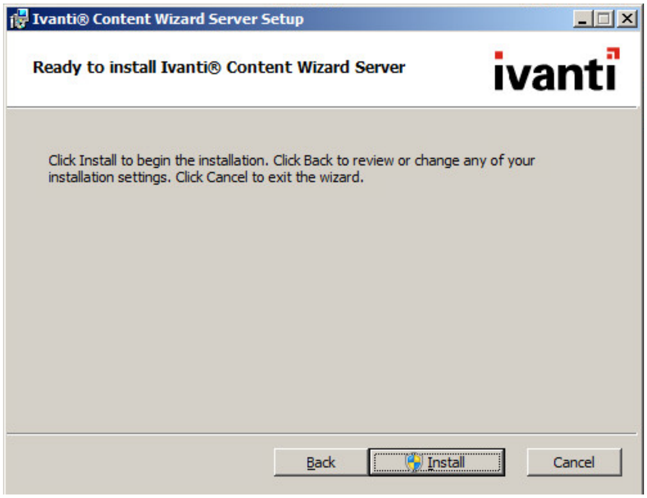
Figure 3: License Agreement Page

4. Accept the terms of the license agreement if you wish to proceed with the installation process.

   a) Select **I accept the terms in the License Agreement**.

b) Click **Next**.

**Step Result:** The ***Ready to install*** page opens.



Ivanti® Content Wizard Server Setup
Ready to install Ivanti® Content Wizard Server
ivanti
Back
Install
Cancel

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

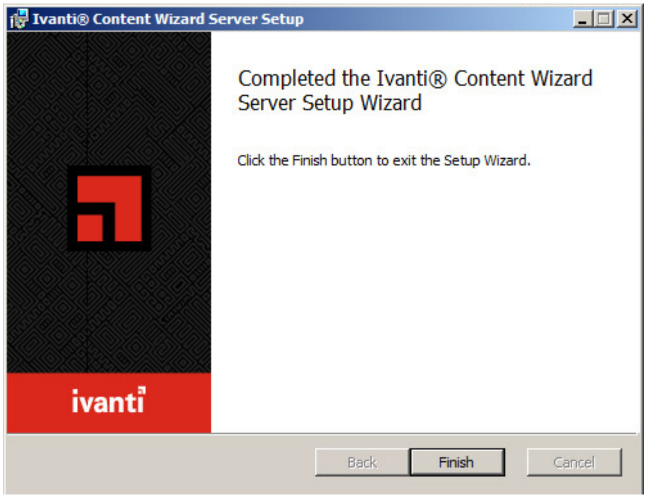
Figure 4: Ready to Install Ivanti Content Wizard Server Page

**5.** Click **Install**.

**Step Result:** The ***Ivanti Content Wizard Server*** page opens and the **Status** bar shows the installation progress.

**6.** When installation completes, click **Next**.

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



Completed the Ivanti® Content Wizard Server Setup Wizard

Click the Finish button to exit the Setup Wizard.

Figure 5: Installation Complete Page

7. Click **Finish**.

   **Step Result:** The ***Ivanti Content Wizard Server Setup Wizard*** closes.

**Result:** The Ivanti Content Wizard server component is installed.

**After Completing This Task:**
Install the Ivanti Content Wizard client component. Refer to Installing the Ivanti Content Wizard Client on page 19.

## Installing the Ivanti Content Wizard Client

The Ivanti Content Wizard client component can be installed on multiple computers. The Ivanti Content Wizard client component connects to the Ivanti Endpoint Security server through the Ivanti Content Wizard server component.

**Prerequisites:**

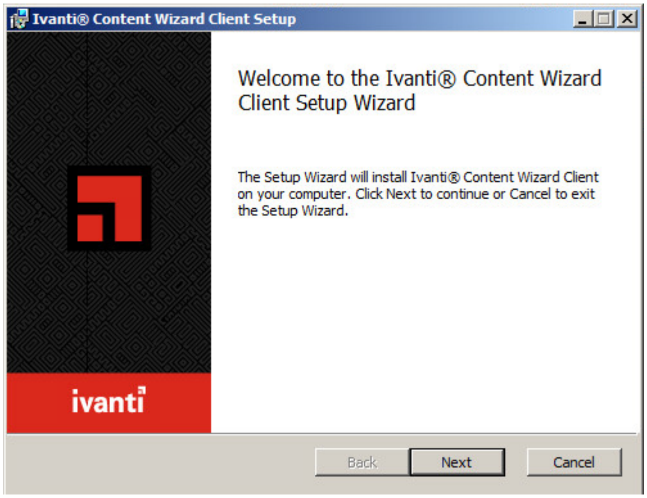
- Verify that you satisfy the minimum hardware and software requirements. For more information, see Minimum Hardware Requirements on page 13.
- The the Ivanti Content Wizard server component has been installed. For more information, see Installing the Ivanti Content Wizard Server on page 16.
- Have a user account with administrative rights on the target computer where you are going to install the Content Wizard client.
- Verify your target computer has .NET Framework 3.5 or higher installed.
- Download the most current version of the Content Wizard installer from the Ivanti Customer Portal (https://www.ivanti.com/support/product-documentation/).

1. Open the `HCWClient.msi`.

   a) Browse to the location where you downloaded the most current version of the Content Wizard installer.

b) Double-click the `HCWClient.msi` file.

**Step Result:** The ***Ivanti Content Wizard Client Setup Wizard*** opens.



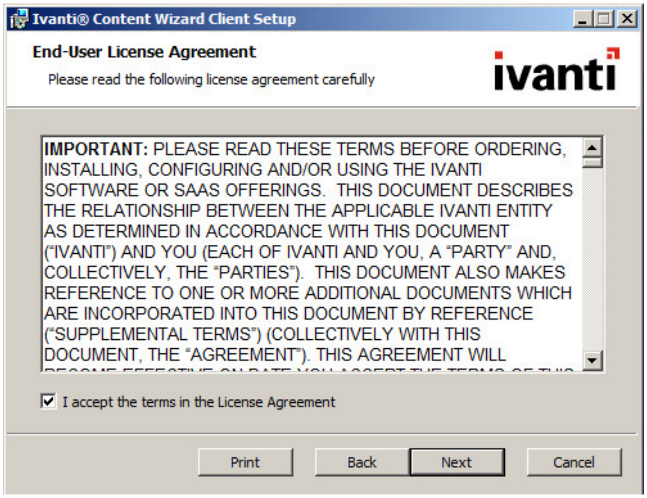
Welcome to the Ivanti® Content Wizard Client Setup Wizard

The Setup Wizard will install Ivanti® Content Wizard Client on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

Figure 6: Ivanti Content Wizard Client Setup Wizard

2. Click **Next**.

   **Step Result:** The ***End-User License Agreement*** page opens.



End-User License Agreement

Please read the following license agreement carefully

**IMPORTANT:** PLEASE READ THESE TERMS BEFORE ORDERING, INSTALLING, CONFIGURING AND/OR USING THE IVANTI SOFTWARE OR SAAS OFFERINGS. THIS DOCUMENT DESCRIBES THE RELATIONSHIP BETWEEN THE APPLICABLE IVANTI ENTITY AS DETERMINED IN ACCORDANCE WITH THIS DOCUMENT ("IVANTI") AND YOU (EACH OF IVANTI AND YOU, A "PARTY" AND, COLLECTIVELY, THE "PARTIES"). THIS DOCUMENT ALSO MAKES REFERENCE TO ONE OR MORE ADDITIONAL DOCUMENTS WHICH ARE INCORPORATED INTO THIS DOCUMENT BY REFERENCE ("SUPPLEMENTAL TERMS") (COLLECTIVELY WITH THIS DOCUMENT, THE "AGREEMENT"). THIS AGREEMENT WILL

☑ I accept the terms in the License Agreement

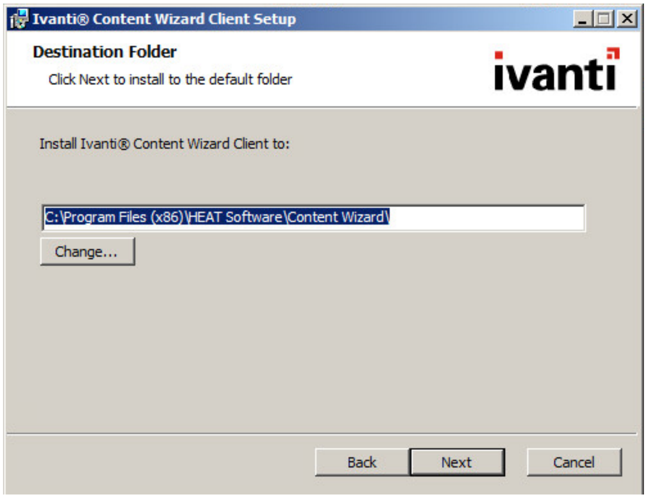
Figure 7: End-User License Agreement Page

3. Accept the terms of the license agreement if you wish to proceed with the installation process.

   a) Select **I accept the terms in the License Agreement**.

b) Click **Next**.

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



Ivanti® Content Wizard Client Setup
Destination Folder
Click Next to install to the default folder
ivanti
Back
Next
Cancel
Change...

Install Ivanti® Content Wizard Client to:

C:\Program Files (x86)\HEAT Software\Content Wizard\

Figure 8: Destination Folder Page

**4.** [Optional] To select a different installation location.

By default, the Content Wizard client is installed to the `C:\Program Files\HEAT Software\Content Wizard\` folder destination.

a) Click **Change**.

**Step Result:** The ***Change destination folder*** page opens.

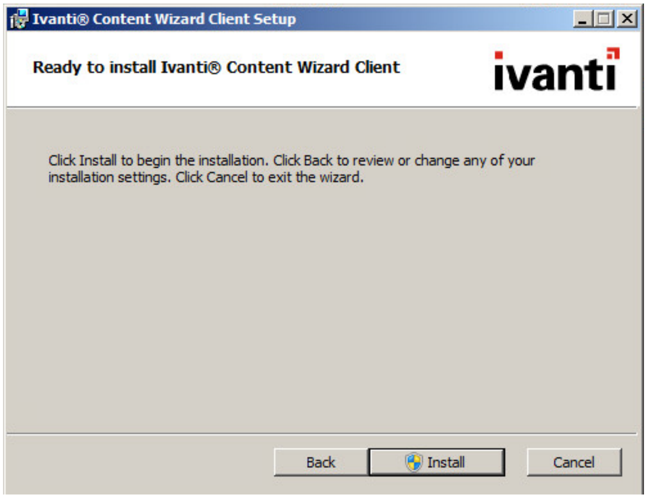
b) Define the desired path by using the **Look in** list or the **Folder name** field.

c) Click **OK**.

**Step Result:** You are redirected to the ***Destination Folder*** page and the **Install Ivanti Content Wizard Client to** field reflects your changes.

5. Click **Next**.

   **Step Result:** The ***Ready to install Ivanti Content Wizard Client*** page opens.



Ivanti® Content Wizard Client Setup

Ready to install Ivanti® Content Wizard Client

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

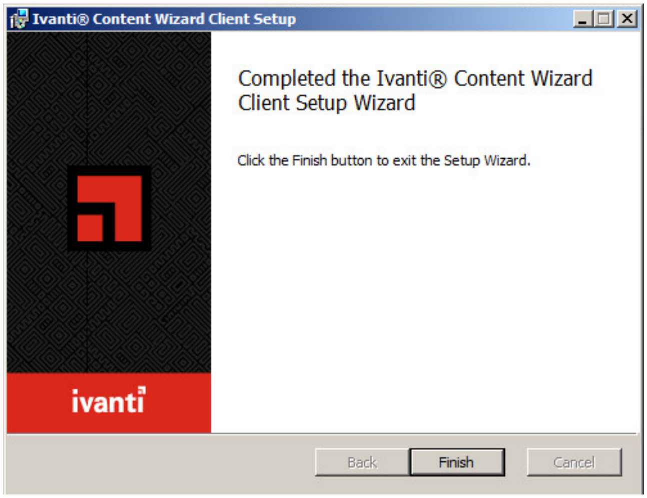
Figure 9: Ready to Install Ivanti Content Wizard Client Page

6. Click **Install**.

   **Step Result:** The ***Installing Ivanti Content Wizard Client*** page opens and the **Status** bar shows the installation progress.

7. When installation completes, click **Next**.

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



Ivanti® Content Wizard Client Setup

Completed the Ivanti® Content Wizard Client Setup Wizard

Click the Finish button to exit the Setup Wizard.

Figure 10: Installation Complete Page

8. Click **Finish**.

   **Step Result:** The ***Ivanti Content Wizard Client Setup Wizard*** closes.

**Result:** The Ivanti Content Wizard client component is installed at the selected location on the computer.

Chapter

3

# Using the Ivanti Content Wizard

**In this chapter:**

- Connecting to the Ivanti Endpoint Security Server
- The Navigation Menu

The Ivanti Content Wizard allows you to create and edit patches for your own network as well as import and export patches between different networks.

Before you can begin using the Ivanti Content Wizard, you must connect it to the selected Ivanti Endpoint Security server.

## Connecting to the Ivanti Endpoint Security Server

You must connect to the Ivanti Endpoint Security (Endpoint Security) server before you can use the Ivanti Content Wizard.

### Role Based Access

If any role possesses either the **Manage Content** or **Manage Packages** right or both, then the users in that role can access the Ivanti Endpoint Security using the Ivanti Content Wizard.

Users are profiles people can use to access the Ivanti Endpoint Security (Endpoint Security). Roles, which are assigned to users, determine the users access rights within Endpoint Security. You may create new roles and users to delegate Endpoint Security duties to appropriate colleagues. For more information, refer to the *Creating New Users and Roles* in the Ivanti Endpoint Security User Guide (https://www.ivanti.com/support/product-documentation).

## Starting the Ivanti Content Wizard

You can access the Ivanti Content Wizard (Content Wizard) from the Windows **Start** menu or by clicking the desktop icon for the application. Once you start the application, you can choose which Ivanti Endpoint Security you want to connect to.

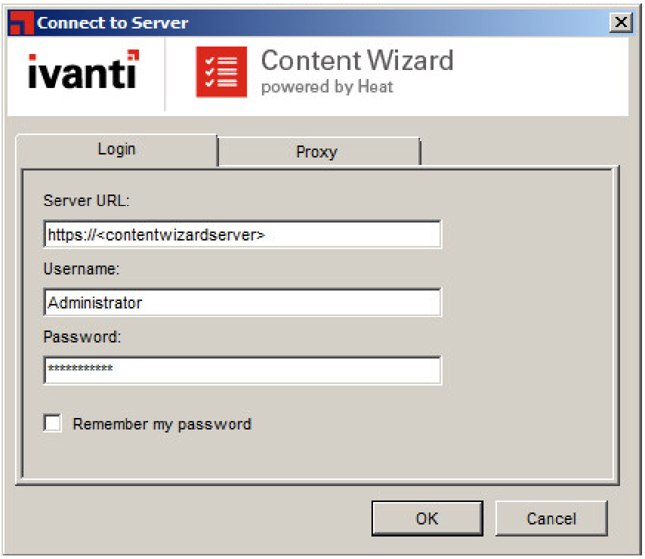
**Prerequisites:**

Prior to starting the Content Wizard, ensure that:

- The Content Wizard Server has been installed successfully. For more information, refer to Installing the Ivanti Content Wizard Server on page 16.
- The Content Wizard Client has been installed successfully. For more information, refer to Installing the Ivanti Content Wizard Client on page 19.
- The user has valid credentials to connect to the Ivanti Endpoint Security (Endpoint Security) server. For more information, refer to Role Based Access on page 25.
- If you are using a proxy to connect to the Endpoint Security server, configure the Content Wizard proxy settings. For more information, refer to Using a Proxy to Connect to the Ivanti Endpoint Security Server on page 27.

1. Select **Start** > **Programs** > **Ivanti** > **Ivanti Content Wizard**.

   **Step Result:** The ***Connect to Server*** dialog opens. By default, the ***Login*** tab displays.



Server URL:
https://<contentwizardserver>

Username:
Administrator

Password:
***********

☐ Remember my password

Figure 11: Connect to Server Dialog

2. Type the URL of the Endpoint Security server in the **Server URL** field.

   **Example:** Type the URL in one of the following formats:

   - For standard servers, type `http://ServerAddress/`.
   - For secure servers, type `https://ServerAddress/`.

3. Type the username for your account on the Endpoint Security server in the **Username** field.
4. Type the password for your account in the **Password** field.

   **Tip:**

   - The **Server URL** and **Username** are cached after logging in for the first time.
   - Select **Remember my password** to cache the password.

5. Click **OK**.

   **Important:** If you are using a proxy to connect to the Endpoint Security server, configure the Content Wizard proxy settings prior to log in. For more information, refer to Using a Proxy to Connect to the Ivanti Endpoint Security Server on page 27.

**Result:** The Ivanti Content Wizard is connected to the selected server.

- By default, Ivanti Content Wizard opens to the ***Open Patch*** dialog.
- If you have cleared the Show Open Dialog at Startup option, Ivanti Content Wizard, opens to its main console. Disable this option by selecting **View** > **Options**.

## Using a Proxy to Connect to the Ivanti Endpoint Security Server

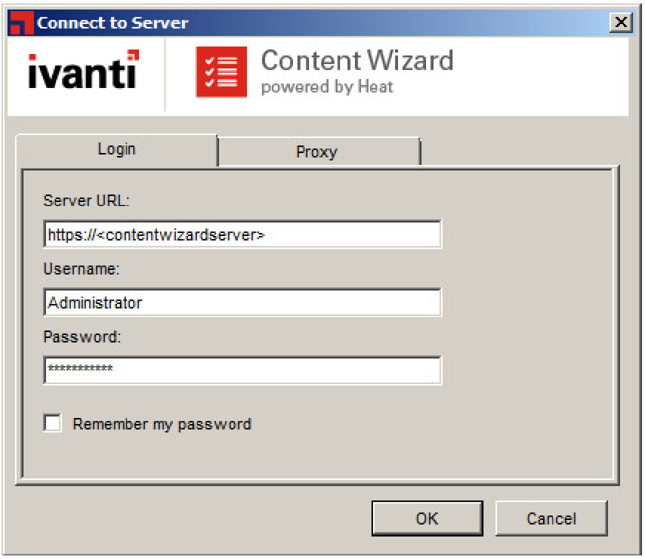
The Ivanti Content Wizard (Content Wizard) allows you to connect to the Ivanti Endpoint Security (Endpoint Security) through a proxy. You need to configure proxy settings in the Ivanti Endpoint Security server before connecting to the Endpoint Security server by proxy.

**Prerequisites:**

Configure proxy settings on the Ivanti Endpoint Security server. For more information, refer to Ivanti Endpoint Security User Guide (https://www.ivanti.com/support/product-documentation).

1. Select **Start** > **Ivanti Content Wizard**.

   **Step Result:** The ***Connect to Server*** dialog opens.



Connect to Server

Login | Proxy

Server URL: https://<contentwizardserver>

Username: Administrator

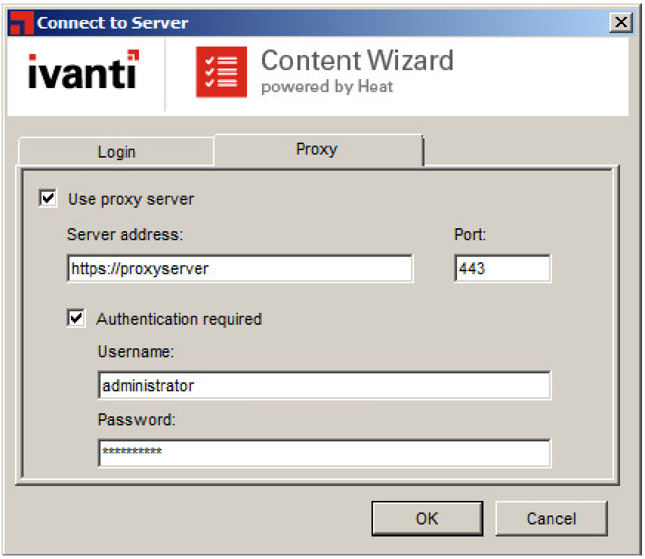
Password: ***********

□ Remember my password

Figure 12: Connect to Server Dialog

2. Click **Proxy**.

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



Connect to Server

Login | Proxy

☑ Use proxy server

Server address: https://proxyserver

Port: 443

☑ Authentication required

Username: administrator

Password: **********

Figure 13: Proxy Dialog

3. Select the **Use proxy server** check box.

   **Step Result:** The ***Proxy*** dialog fields become active.

4. Type the server address in the **Server address** field.
5. Type the proxy port number in the **Port** field.
6. If your network uses a proxy server, and that proxy server requires authentication, select the **Authentication required** check box and complete the following substeps:

   a) Type the user name that authenticates the proxy in the **Username** field.
   b) Type the password associated with the user name in the **Password** field.

   > **Tip:** Use the same authentication details as those specified for the Ivanti Endpoint Security Server proxy. On subsequent connection attempts, proxy information from the first connection attempt will be retained.

7. Click **OK**.

**Result:** The Ivanti Content Wizard connects to the Endpoint Security through the specified proxy.

- By default, Ivanti Content Wizard opens to the ***Open Patch*** dialog.
- If you have cleared the Show Open Dialog at Startup option, Ivanti Content Wizard, opens to its main console. Disable this option by selecting **View** > **Options**.

## Exiting the Ivanti Content Wizard

Exit the Ivanti Content Wizard after you are finished using the application to prevent any unauthorized usage of the Ivanti Content Wizard.

Select **File** > **Exit** from the main menu.

**Step Result:** The Ivanti Content Wizard closes.

> **Note:** If you have an unsaved patch, a dialog appears asking if you want to save your changes prior to exiting the Ivanti Content Wizard.

**Result:** The Ivanti Content Wizard closes on the target computer.

## The Navigation Menu

This menu appears on all Ivanti Content Wizard pages. Use this menu to navigate through the application.

This menu organizes product features based on functionality. When you select a menu item, a new window, page, or dialog opens. You can access all features of the system from this menu.

Table 1: Navigation Menu

| Menu | Menu Item | Function |
|---|---|---|
| **File** | **New** | Opens the ***Patch Properties*** page. Refer to Creating and Editing Patch Properties on page 36 for additional information. The keyboard shortcut is CTRL+N. |
| | **Open...** | Opens the ***Open Patch*** page. Refer to Finding a Patch on page 143 for additional information. The keyboard shortcut is CTRL+O. |
| | **Delete...** | Opens the ***Delete Patch*** page. Refer to Deleting Obsolete Patches on page 146 for additional information. The keyboard shortcut is CTRL+L. |
| | **Save** | Saves the patch. The keyboard shortcut is CTRL+S. |
| | **Save Copy** | Saves a copy of the patch. Refer to Saving a Copy of a Patch on page 147 for additional information. |
| | **Export Wizard** | Opens the ***Export Patches*** dialog. Refer to Exporting Patches Using the Export Wizard on page 153 for additional information. The keyboard shortcut is CTRLl+E. |
| | **Import Wizard** | Opens the ***Import Patches*** dialog. Refer to Importing Patches Using the Import Wizard on page 150 for additional information. The keyboard shortcut is CTRLl+I. |
| | **Exit** | Closes the Ivanti Content Wizard. |
| **View** | **Status Bar** | Displays the status bar. |
| | **Options...** | Opens the ***Options*** page. This page displays tabs used for logging and update information. |
| | **Vendor Management** | Opens the ***Vendor Management*** page. Refer to Adding a New Vendor on page 39 for additional information.. |

| Menu | Menu Item | Function |
|---|---|---|
| | **Dependencies** | Opens the ***Dependency Viewer*** page. This page allows you to view package properties and also display the current ***Patch Properties*** page information in a text editor pop-up window. |
| | **Print View** | Displays current ***Patch Properties*** page information in a text editor pop-up window. |
| | **Refresh** | Refreshes the current ***Patch Properties*** page. The keyboard shortcut is F5. |
| **Tools** | **New Patch Wizard** | Opens the ***New Patch Wizard*** dialog. Refer to The New Patch Wizard on page 161 for additional information. |
| | **Uninstall Wizard** | Opens the ***Uninstall Wizard*** dialog. Refer to The Uninstall Wizard on page 168 for additional information. |
| | **Power Management Wizard** | Opens the ***Power Management Wizard*** dialog. Refer to The Power Management Wizard on page 172 for additional information. |
| | **Policy Wizard** | Opens the ***Policy Wizard*** dialog. Refer to The Policy Wizard on page 176 for additional information. |
| | **Windows Firewall Wizard** | Opens the ***Windows Firewall Wizard*** dialog. Refer to The Windows Firewall Wizard on page 184 for additional information. |
| | **Community Subscribe** | Opens the ***Community Subscribe Wizard*** dialog. Refer to The Community Subscribe Wizard on page 206 for additional information. |
| | **Community Publish** | Opens the ***Community Publish Wizard*** dialog. Refer to The Community Publish Wizard on page 209 for additional information. |
| **Help** | **Help Topics** | Opens the ***Help*** page. Help provides product feature explanations, step-by-step procedures, and reference material. The keyboard shortcut is F1. |
| | **About** | Opens the ***About*** dialog. |

Chapter

4

# Defining Patch Properties

**In this chapter:**

A patch consists of a patch definition and how it is detected. It also contains the necessary signatures and fingerprints required to determine if the patch is applicable to a given endpoint, and also whether it has been installed.

The Ivanti Content Wizard allows you to create patches for endpoints hosting a Windows operating system using the ***Patch Creation Wizard***. For more information, refer to Using the New Patch Wizard on page 162.

If you want to create patches for non-Windows operating systems, refer to Creating a Linux Patch on page 137.

## Understanding Patch Severity Levels

Patch severity indicates how urgent it is to deploy that patch to a system.

The **Impact** field in the ***Patch Properties*** window lets you determine the severity of a patch. The following patch severity levels are available for assignment.

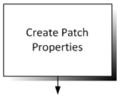
| Severity Level | Description |
|---|---|
| **Critical** | Ivanti Software or the product manufacturer has determined that this patch is critical and should be installed as soon as possible. Most of the recent security updates fall in to this category. The patches for this category are automatically downloaded and stored on your Ivanti Patch and Remediation server. |
| **Critical - 01** | Ivanti Software or the product manufacturer has determined that this patch is critical and should be installed as soon as possible. This patch is older than 30 days and has not been superseded. |
| **Critical - 05** | Ivanti Software or the product manufacturer has determined that this patch is critical and should be installed as soon as possible. These patches have been superceded. |

| Severity Level | Description |
|---|---|
| **Critical - Intl** | An international patch, where Ivanti Software or the product manufacturer has determined that this patch is critical and should be installed as soon as possible. Most of the recent international security updates fall in to this category. After 30 days international patches in this category will be moved to Critical - 01. |
| **Service packs** | Collections of software fixes and enhancements that apply to installed software. |
| **Software installers** | Installers for third party software. |
| **Updates** | Non-critical updates to installed software. |
| **Detection Only** | These security content items contain signatures that are common to multiple vulnerabilities. They contain no associated patches and are only used in the detection process. |
| **Informational** | These security content items detect a condition that Ivanti Software or the product manufacturer has determined as informational. If the report has an associated package, you may want to install it at your discretion. |
| **Policies** | These security content items apply security policies to an endpoint. |
| **Recommended** | Ivanti Software or the product manufacturer has determined that these security content items, while not critical or security related is useful and should be applied to maintain the health of your computers. |
| **Task** | These security content items contain tasks which administrators may use to run various detection or deployment tasks across their network. |
| **Virus Removal** | This security content items contain packages which administrators may use to run various virus detections across their network. Anti-Virus tools and updates are included in this category. |

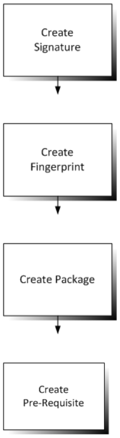
## Building a Patch

Patch creation involves many stages. The process includes creating the initial properties and completing the signature details.

The process of creating a patch is as follows:



Create the initial properties of the patch. This includes the name, vendor selection, impact determination, status, and the description to be viewed within the Ivanti Endpoint Security.



Create and define the signature. It recognizes specific combinations of installed software in an operating system. Patches usually contain multiple signatures to compensate for variances within applications.

Create and define the fingerprint. A fingerprint can represent a unique file, folder, registry key, or other data value somewhere within a system. Each signature can contain one or more fingerprints, which detects if a patch is present in the system.

Create and define the package. Each package contains the script commands to install the package files or run the executable that installs the patch. Every signature can have only one package associated with it.

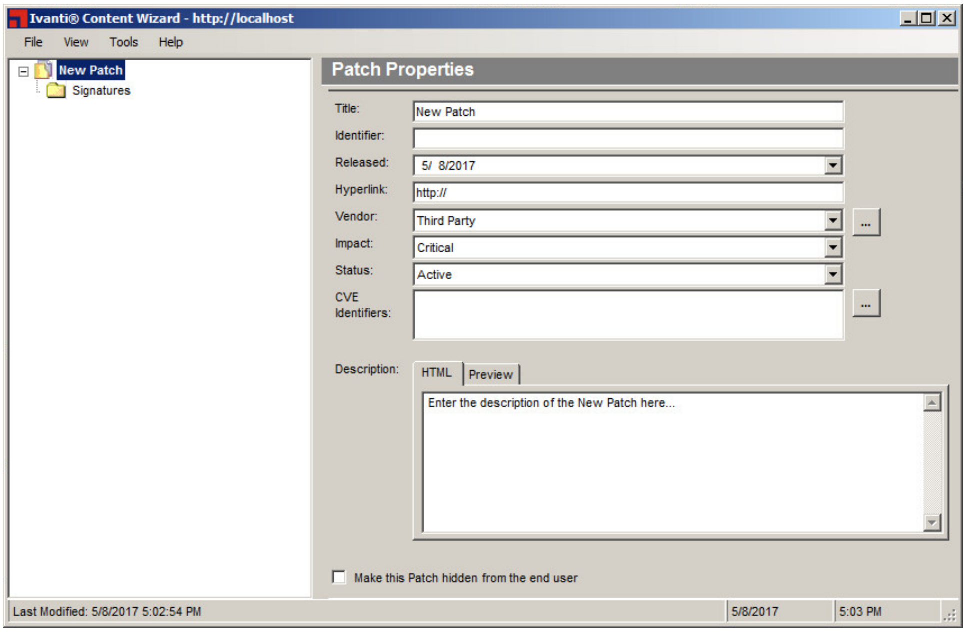
Create and define the pre-requisite. Adding pre-requisites to a signature requires the pre-requisite be met before analyzing the signature.

## The Patch Properties Page

The ***Patch Properties*** page allows you to view and edit the properties and fields associated with the selected patch.

To preview the patch description from within the Ivanti Content Wizard, click the ***Preview*** tab.

**Tip:** When creating a patch, provide as much information about the patch as possible.



Title: New Patch

Identifier:

Released: 5/ 8/2017

Hyperlink: http://

Vendor: Third Party

Impact: Critical

Status: Active

CVE Identifiers:

Description: Enter the description of the New Patch here...

☐ Make this Patch hidden from the end user

Last Modified: 5/8/2017 5:02:54 PM 5/8/2017 5:03 PM

Figure 14: Patch Properties Page

The following list describes the ***Patch Properties*** page fields and properties:

| Field Name | Description |
|---|---|
| **Title** | Contains the name of the patch. The patch requires a title to display properly in your Ivanti Endpoint Security (Endpoint Security) server. |
| **Identifier** | Contains the vendor specific number or identifier value that uniquely correlates with the patch. |
| **Released** | Contains the date when the vendor released the patch. When creating a new patch, this field is set to the current date by default. This date should be changed to correspond with the date the patch was released by the vendor. |
| **Hyperlink** | Contains an optional link to more information. If a URL is entered in this field, the **More Information** link in the ***Vulnerabilities*** page within the Endpoint Security is visible. |
| **Vendor** | Contains the name of the company that released the patch. The drop-down list allows you to select from a list of vendors that are already in the database. |
| **Impact** | Indicates the level of severity for the patch. The various severity levels are listed in Understanding Patch Severity Levels on page 33. |
| **Status** | Defines the status of the patch. If set to **Active**, Endpoint Security users will be able to view this patch in the ***Patches*** page. If set to **Beta**, only Endpoint Security websites set for Beta use will be able to view the patch. |
| **CVE Identifiers** | Allows for the patch to be defined and classified using the Common Vulnerabilities and Exposures standard. See http://cve.mitre.org for more information. |
| **Description** | Contains a text description of the patch. The information is displayed in the ***Patches*** page of the Endpoint Security server as well. |
| **Make Patch Hidden** | Determines if the patch is hidden from the end user when deployed. The check box is cleared by default. |

## Creating and Editing Patch Properties

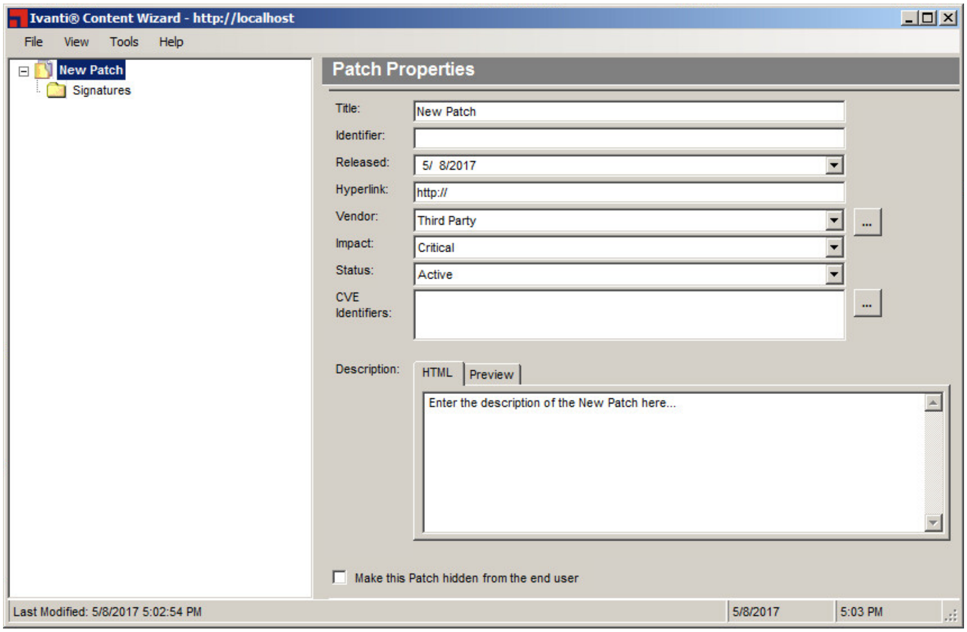
Creating patch properties is part of the process that creates a new patch and saves it to the Ivanti Endpoint Security. Once a patch is created, you can subsequently edit its properties using the ***Patch Properties*** page.

1. Start the Ivanti Content Wizard.

2. If the ***Open Patch*** page opens, click **Cancel**.

   If it doesn't, proceed to the next step.

   **Step Result:** The ***Patch Properties*** page opens.



Title: New Patch

Identifier:

Released: 5/ 8/2017

Hyperlink: http://

Vendor: Third Party

Impact: Critical

Status: Active

CVE Identifiers:

Description: Enter the description of the New Patch here...

☐ Make this Patch hidden from the end user

Last Modified: 5/8/2017 5:02:54 PM | 5/8/2017 | 5:03 PM

Figure 15: Patch Properties Page

> **Note:** For more information on the various properties and fields in the ***Patch Properties*** page, refer to The Patch Properties Page on page 35.

3. Type a unique name for the patch in the **Title** field.

   The default title is **New Patch**.

4. Type a unique identifier for the patch in the **Identifier** field.

   You may determine the identifier or you may choose to use one supplied by the vendor.

5. Type the release date for the patch in the **Released** field.

   By default, the current date is specified. You can use the vendor's date if necessary.

6. Type the vendor's URL in the **Hyperlink** field.

7. Select a vendor from the **Vendor** drop-down list.

   Vendors must be added before they can show up as an item in the **Vendor** drop-down list. For more information, see Adding a New Vendor on page 39.

8. Select an impact from the drop-down list in the **Impact** field.

   To understand the various impact options available, refer to Understanding Patch Severity Levels on page 33.

9. Select an applicable patch status from the drop-down list in the **Status** field:

   - **Active**
   - **Beta**
   - **Pending**

   To understand the various status options and their meaning, refer to The Patch Properties Page on page 35.

10. [Optional] Select CVE Identifiers.

    a) Click the **CVE Identifiers** button.

       **Step Result:** The ***CVE Identifiers*** dialog opens.

    b) Select **File** > **Add**.

       **Step Result:** The ***Add CVE Code*** dialog opens and lists the available CVE Identifiers.

    c) Double-click on the CVE Identifier that is applicable to your needs.

       **Step Result:** The ***Add CVE Code*** dialog closes and the item is added to the ***CVE Identifiers*** dialog.

    d) Click **Save**.

       **Step Result:** The ***CVE Identifiers*** dialog closes and the item is added to **CVE Identifiers** field.

    e) [Optional] Repeat steps a, b, c and d to add additional CVE Identifiers.

11. Type a description in the **Description** field.

    This description will be visible in the ***Patches*** page of the Ivanti Endpoint Security.

12. [Optional] Select the **Make this Patch hidden from the end user** check box.

13. Select **File** > **Save**.

    **Note:** If you save the patch without adding a package, you are asked if you want to save without adding a package. Click **Yes** to proceed.

**Result:** The patch properties are saved for the new patch.

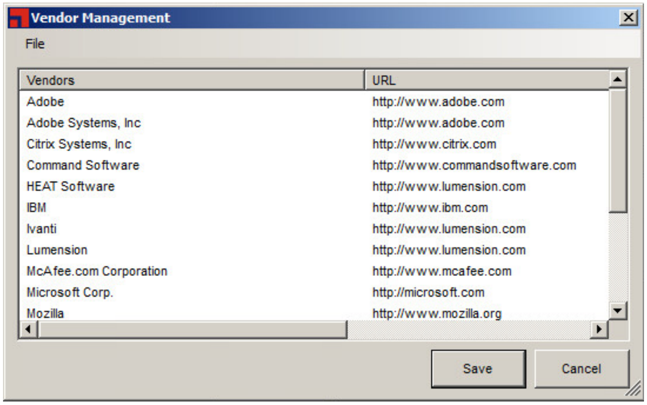
**After Completing This Task:**
After creating the patch properties, continue with the other steps involved in patch creation such as adding a signature, fingerprint, and so on. The various steps are detailed in Creating a Linux Patch on page 137.

## Adding a New Vendor

If the vendor you want is not in the existing list, you can add it from the ***Vendor Management*** window.

1. Select **View** > **Vendor Management**.

   **Step Result:** The ***Vendor Management*** page opens.



| Vendors | URL |
|---|---|
| Adobe | http://www.adobe.com |
| Adobe Systems, Inc | http://www.adobe.com |
| Citrix Systems, Inc | http://www.citrix.com |
| Command Software | http://www.commandsoftware.com |
| HEAT Software | http://www.lumension.com |
| IBM | http://www.ibm.com |
| Ivanti | http://www.lumension.com |
| Lumension | http://www.lumension.com |
| McAfee.com Corporation | http://www.mcafee.com |
| Microsoft Corp. | http://microsoft.com |
| Mozilla | http://www.mozilla.org |

Figure 16: Vendor Management Page

2. Select **File** > **New Vendor**.

   **Step Result:** The ***Add Vendor*** dialog opens.

3. Type the name of the vendor in the **Vendor Name** field.
4. Type the URL of the vendor in the **Vendor URL** field.
5. Click **OK**.

   **Step Result:** The ***Add Vendor*** window closes and the new vendor appears in the ***Vendor Management*** window.

6. Click **Save**.

   **Step Result:** The ***Vendor Management*** page closes.

**Result:** The new vendor is added to the vendor list.

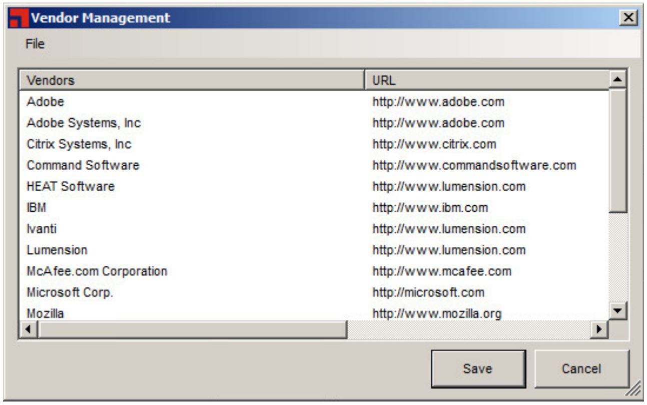
## Editing a Vendor

Changes to vendor information may require you to edit the details of a vendor in your vendor list. You can edit details for a vendor from the ***Vendor Management*** window.

**Note:** You can only edit vendor details for a vendor that you have added previously to the vendor list. Existing vendors cannot be edited.

1. Select **View** > **Vendor Management**.

   **Step Result:** The ***Vendor Management*** page opens.



| Vendors | URL |
|---|---|
| Adobe | http://www.adobe.com |
| Adobe Systems, Inc | http://www.adobe.com |
| Citrix Systems, Inc | http://www.citrix.com |
| Command Software | http://www.commandsoftware.com |
| HEAT Software | http://www.lumension.com |
| IBM | http://www.ibm.com |
| Ivanti | http://www.lumension.com |
| Lumension | http://www.lumension.com |
| McAfee.com Corporation | http://www.mcafee.com |
| Microsoft Corp. | http://microsoft.com |
| Mozilla | http://www.mozilla.org |

Figure 17: Vendor Management Page

2. Select **File** > **Edit Vendor**.

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

3. Modify the name of the vendor in the **Vendor Name** field, if needed.
4. Modify the vendor's URL in the **Vendor URL** field, if needed.
5. Click **OK**.

   **Step Result:** The ***Edit Vendor*** window closes.

6. Click **Save**.

   **Step Result:** The ***Vendor Management*** page closes.

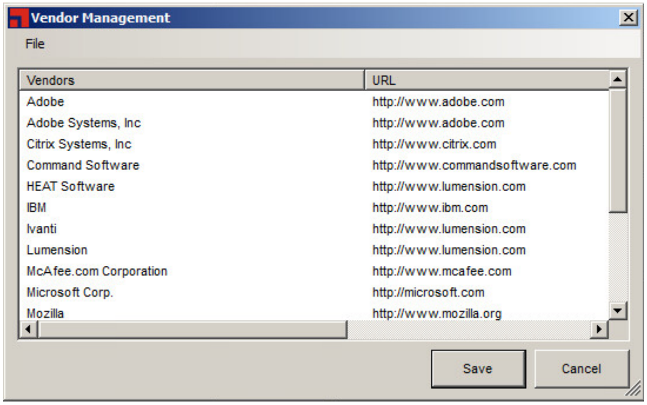
**Result:** The changes to the vendor's details are saved.

## Deleting a Vendor

You can delete a vendor that you have previously added to the vendor list.

1. Select **View** > **Vendor Management**.

   **Step Result:** The ***Vendor Management*** page opens.



| Vendors | URL |
|---|---|
| Adobe | http://www.adobe.com |
| Adobe Systems, Inc | http://www.adobe.com |
| Citrix Systems, Inc | http://www.citrix.com |
| Command Software | http://www.commandsoftware.com |
| HEAT Software | http://www.lumension.com |
| IBM | http://www.ibm.com |
| Ivanti | http://www.lumension.com |
| Lumension | http://www.lumension.com |
| McAfee.com Corporation | http://www.mcafee.com |
| Microsoft Corp. | http://microsoft.com |
| Mozilla | http://www.mozilla.org |

Figure 18: Vendor Management Page

2. Select the vendor you want to remove from the list.
3. Select **File** > **Delete Vendor**.

   **Step Result:** The vendor is removed from the ***Vendor Management*** page.

4. Click **Save**.

   **Step Result:** The ***Vendor Management*** page closes.

**Result:** The selected vendor is deleted from the vendor list.

# Chapter 5

# Working with Signatures

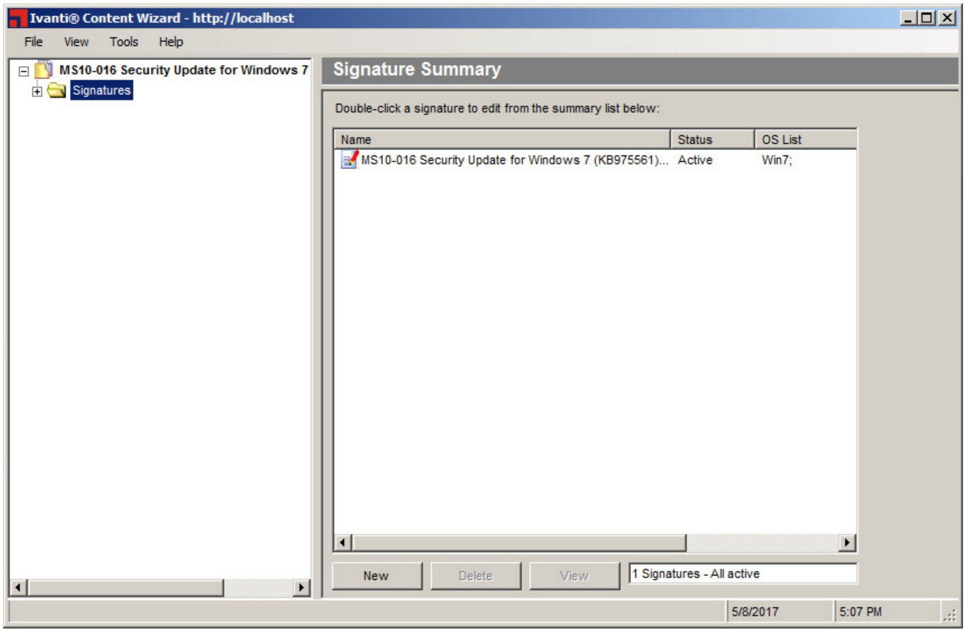
**In this chapter:**

Signatures are a component of a patch. A signature is used to recognize a specific operating system and installed software applications and services.

If there are multiple, unique configurations that must be recognized, the patch will contain multiple signatures. Likewise, if a patch requires unique installation files for each operating system, it will contain multiple signatures.

## The Signature Summary Page

The ***Signature Summary*** page allows you to perform various actions related to the signatures in a patch. You can add, edit, or delete signatures in the ***Signature Summary*** page.


Ivanti® Content Wizard - http://localhost
File
View
Tools
Help
MS10-016 Security Update for Windows 7
Signatures
Signature Summary
New
Delete
View

Double-click a signature to edit from the summary list below:

| Name | Status | OS List |
|---|---|---|
| MS10-016 Security Update for Windows 7 (KB975561)... | Active | Win7; |

1 Signatures - All active

5/8/2017 5:07 PM

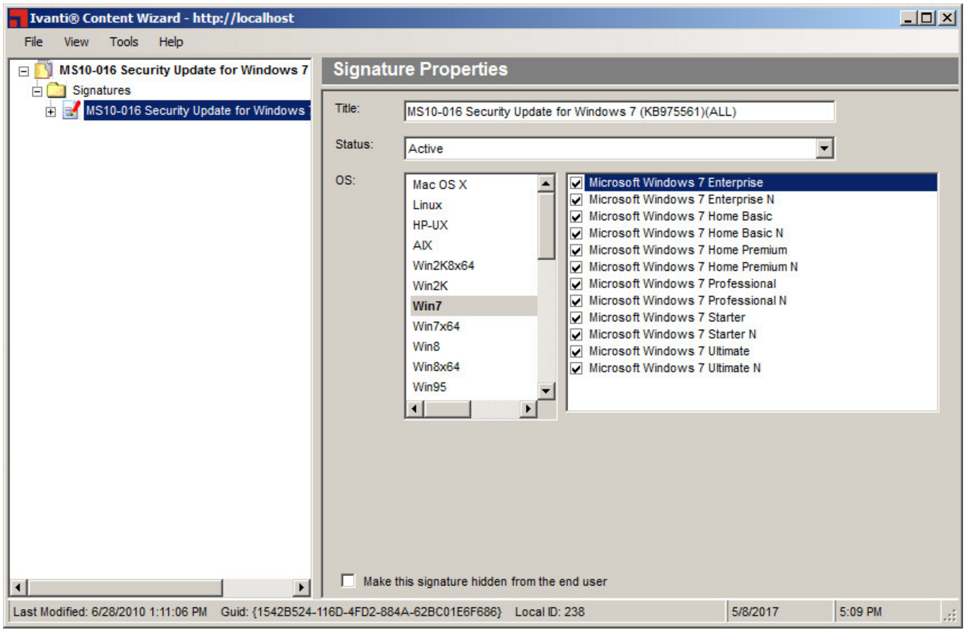
Figure 19: Signature Summary Page

The following list describes the buttons on the ***Signature Summary*** page.

| Button | Description |
|---|---|
| **New** | Creates and adds a new signature to the ***Signature Summary*** page. |
| **Delete** | Removes the selected signature. |
| **View** | Opens the ***Signature Properties*** window. For more information, see The Signature Properties Page on page 45. |

## The Signature Properties Page

Once a signature is created, you can add and edit the signatures properties in the ***Signature Properties*** page. The ***Signature Properties*** page contains the signature’s title, status, and applicable operating systems.



- MS10-016 Security Update for Windows 7
  - Signatures
    - MS10-016 Security Update for Windows

Signature Properties

Title: MS10-016 Security Update for Windows 7 (KB975561)(ALL)

Status: Active

OS:

- Mac OS X
- Linux
- HP-UX
- AIX
- Win2K8x64
- Win2K
- Win7
- Win7x64
- Win8
- Win8x64
- Win95

☑ Microsoft Windows 7 Enterprise
☑ Microsoft Windows 7 Enterprise N
☑ Microsoft Windows 7 Home Basic
☑ Microsoft Windows 7 Home Basic N
☑ Microsoft Windows 7 Home Premium
☑ Microsoft Windows 7 Home Premium N
☑ Microsoft Windows 7 Professional
☑ Microsoft Windows 7 Professional N
☑ Microsoft Windows 7 Starter
☑ Microsoft Windows 7 Starter N
☑ Microsoft Windows 7 Ultimate
☑ Microsoft Windows 7 Ultimate N

☐ Make this signature hidden from the end user

Last Modified: 6/28/2010 1:11:06 PM Guid: {1542B524-116D-4FD2-884A-62BC01E6F686} Local ID: 238 | 5/8/2017 | 5:09 PM

Figure 20: Signature Properties Page

The following list describes the ***Signature Properties*** page fields:

| Field or Control | Description |
|---|---|
| **Title** | Indicates the text identifier for the signature. This title is not visible in the Ivanti Endpoint Security (Endpoint Security) web interface. |
| **Status** | Indicates if the signature is for regular or beta use. If you set the status to **Active**, then Endpoint Security users will be able to see the package on the ***Packages*** page. For beta use, set the status to **Beta**, limiting use to only Endpoint Security beta sites. |
| **OS** | Indicates the operating systems to which the signature applies. When creating a signature, it is important that you select only those operating systems applicable for the signature. |

## Adding a Signature to a Patch

You can add a signature to a patch after creating the patch properties. For every signature, you can have one package and multiple fingerprints and pre-requisites.

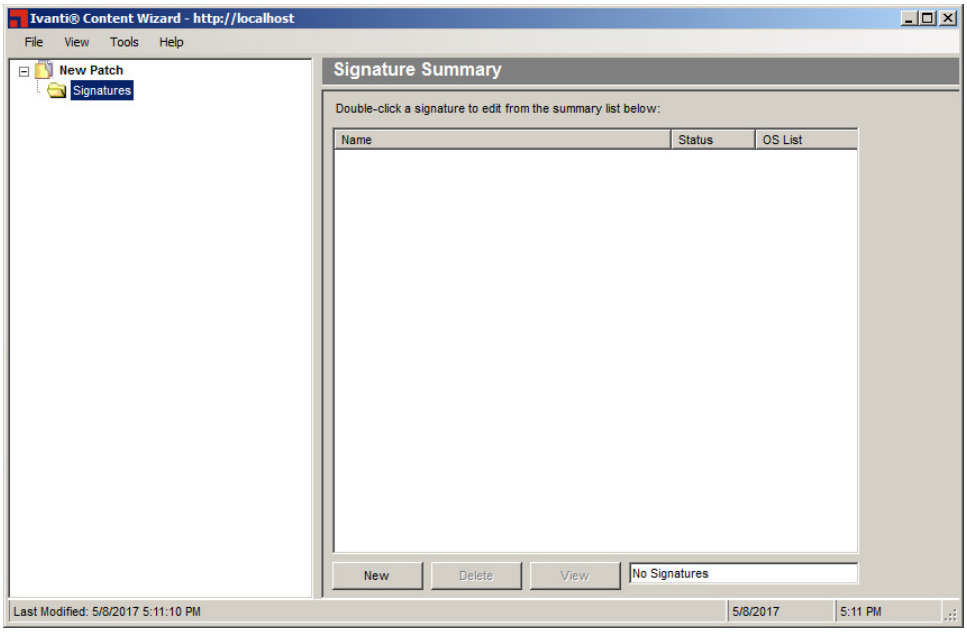
**Prerequisites:**

Specify the patch properties in the ***Patch Properties*** page. For more information about creating patch properties, refer to Creating and Editing Patch Properties on page 36.

1. Expand the patch properties to **Signatures** in the left pane.

   **Example:** ***New Patch*** > **Signatures**.

   **Step Result:** The ***Signature Summary*** page opens.



Double-click a signature to edit from the summary list below:

| Name | Status | OS List |
|---|---|---|

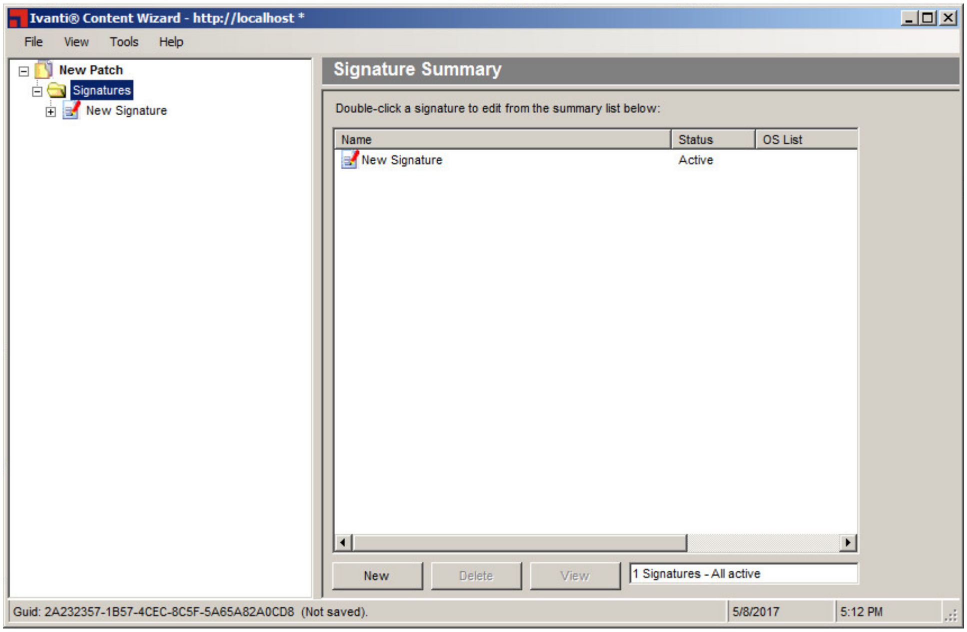
No Signatures

Last Modified: 5/8/2017 5:11:10 PM | 5/8/2017 | 5:11 PM

Figure 21: Signature Summary

2. Click **New**.

   **Step Result:** The ***Signature Summary*** page contains a new signature named **New Signature**.



Double-click a signature to edit from the summary list below:

New Signature Active

1 Signatures - All active

Guid: 2A232357-1B57-4CEC-8C5F-5A65A82A0CD8 (Not saved). 5/8/2017 5:12 PM

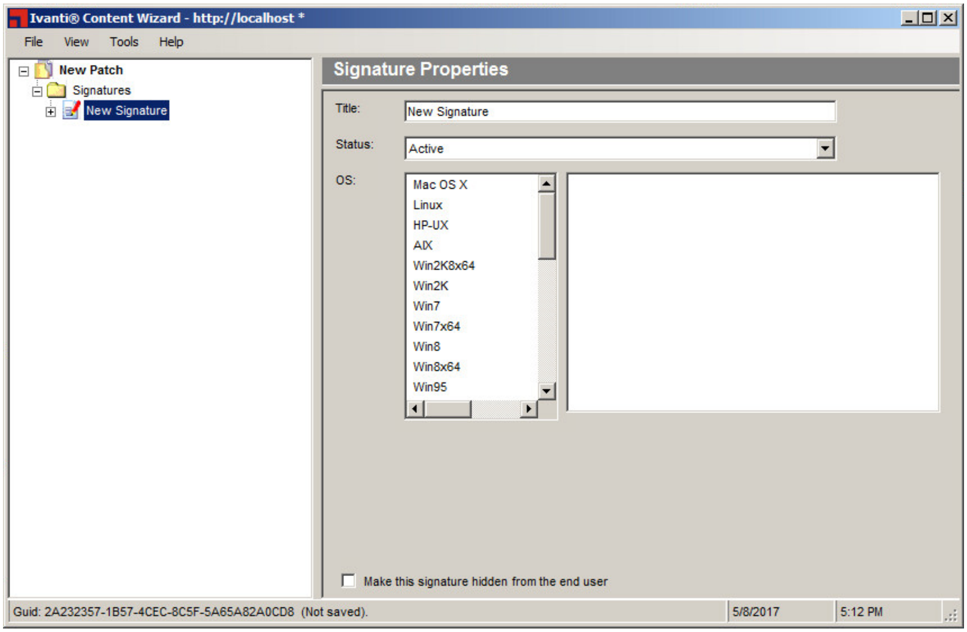
Figure 22: Signature Summary Page: New Signature

3. Select **New Signature** within the pane.

4. Click **View**.

**Tip:** Within the pane window you may double-click on a signature to open the ***Signature Properties*** page.

**Step Result:** The ***Signature Properties*** page opens.



Title: New Signature

Status: Active

OS:

☐ Make this signature hidden from the end user

Guid: 2A232357-1B57-4CEC-8C5F-5A65A82A0CD8 (Not saved). 5/8/2017 5:12 PM

Figure 23: Signature Properties Page

5. Type a name in the **Title** field.
6. Select the applicable patch status using the **Status** drop-down list.

   The following list items are available:

   - Active
   - Beta
   - Pending

7. Select the applicable operating systems in the **OS** field.

   **Step Result:** The versions of the selected operating system display in the list details field.

8. Select the version of the operating system for the signature in the list details field.

**Tip:** Double-clicking an operating system name in the **OS** field selects all the versions of that operating system within the details list.

9. [Optional] Check or clear the **Make this signature hidden from the end user** check box to hide the signature from the end user.

**Result:** The signature for the patch is created.

> **Note:** Ivanti Content Wizard supports the creation of multiple signatures for each patch.

**After Completing This Task:**
After creating a signature, you have to add at least one fingerprint to it. For more information on fingerprints, refer to Working with Fingerprints on page 53.

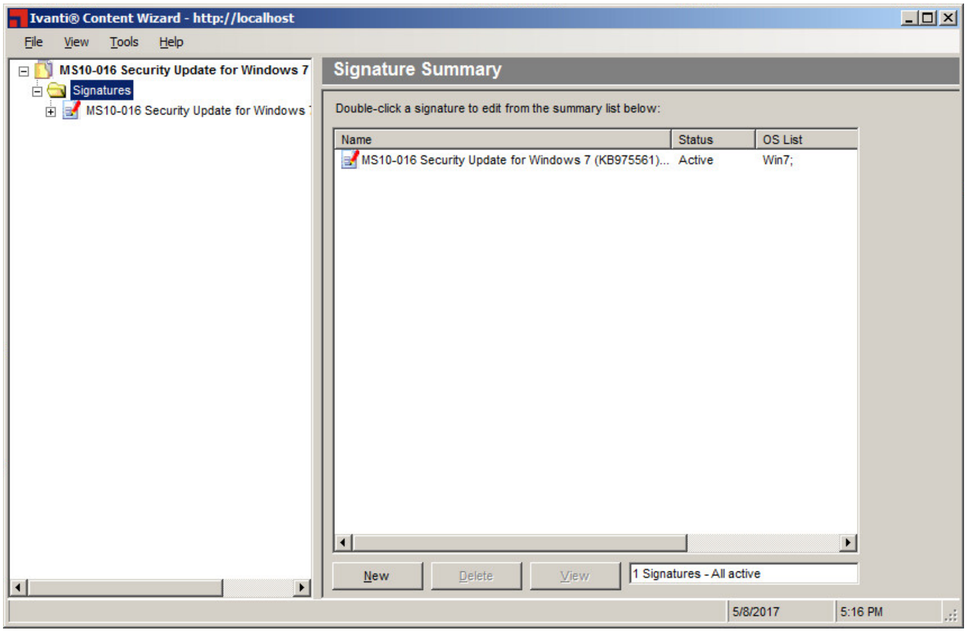
## Editing a Patch Signature

You can edit the details associated with a signature by selecting the signature and then making changes in the ***Signature Properties*** page.

1. Expand the patch properties to **Signatures** in the left pane.

   **Example:** ***New Patch*** > **Signatures**.

   **Step Result:** The ***Signature Summary*** page opens.



- MS10-016 Security Update for Windows 7
  - Signatures
    - MS10-016 Security Update for Windows 7

Signature Summary

Double-click a signature to edit from the summary list below:

| Name | Status | OS List |
|---|---|---|
| MS10-016 Security Update for Windows 7 (KB975561)... | Active | Win7; |

1 Signatures - All active

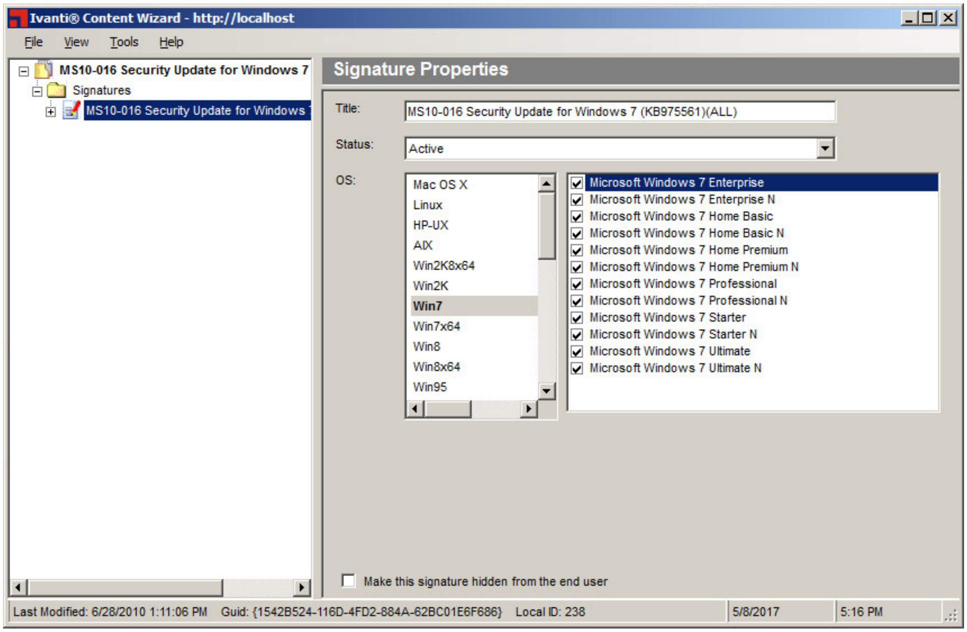
Figure 24: Signature Summary Page: Multiple Signatures

2. In the pane select the applicable signature you want to edit.

> **Note:** Each patch supports multiple signatures and each may be edited.

3. Click **View**.

   **Step Result:** The ***Signature Properties*** page opens.



- MS10-016 Security Update for Windows 7
  - Signatures
    - MS10-016 Security Update for Windows 7

Signature Properties

Title: MS10-016 Security Update for Windows 7 (KB975561)(ALL)

Status: Active

OS: Mac OS X, Linux, HP-UX, AIX, Win2K8x64, Win2K, **Win7**, Win7x64, Win8, Win8x64, Win95

☑ Microsoft Windows 7 Enterprise
☑ Microsoft Windows 7 Enterprise N
☑ Microsoft Windows 7 Home Basic
☑ Microsoft Windows 7 Home Basic N
☑ Microsoft Windows 7 Home Premium
☑ Microsoft Windows 7 Home Premium N
☑ Microsoft Windows 7 Professional
☑ Microsoft Windows 7 Professional N
☑ Microsoft Windows 7 Starter
☑ Microsoft Windows 7 Starter N
☑ Microsoft Windows 7 Ultimate
☑ Microsoft Windows 7 Ultimate N

☐ Make this signature hidden from the end user

Last Modified: 6/28/2010 1:11:06 PM Guid: {1542B524-116D-4FD2-884A-62BC01E6F686} Local ID: 238 5/8/2017 5:16 PM

Figure 25: Signature Properties Page

4. Edit the name in the **Title** field as applicable to you patch needs.
5. Select the applicable patch status using the **Status** drop-down list.

   The following list items are available:

   - Active
   - Beta
   - Pending

6. Select the applicable operating systems in the **OS** field.

   **Step Result:** The versions of the selected operating system display in the list details field.

7. Select the version of the operating system for the signature in the list details field.

   **Tip:** Double-clicking an operating system name in the **OS** field selects all the versions of that operating system within the details list.

8. [Optional] Check or clear the **Make this signature hidden from the end user** check box to hide the signature from the end user.
9. [Optional] Edit each applicable patch signature as needed.

**10.**Select **File** > **Save**.

**Result:** The signature is edited.

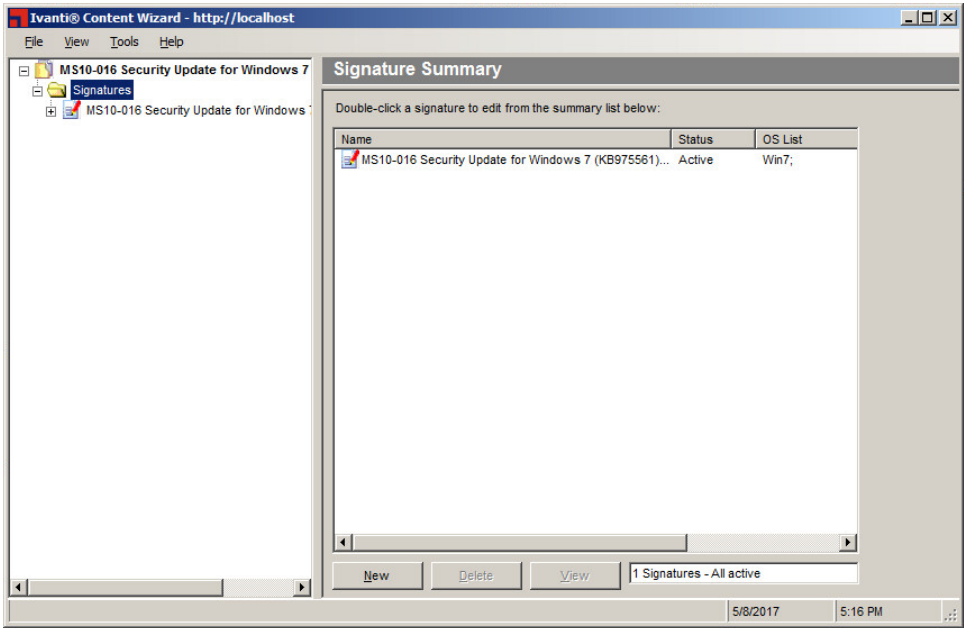
## Deleting a Patch Signature

If you no longer require a particular signature for a patch, you can delete it in the ***Signature Summary*** page.

1. Expand the patch properties to **Signatures** in the left pane.

   **Example:** ***New Patch*** > **Signatures**.

   **Step Result:** The ***Signature Summary*** page opens.



Ivanti® Content Wizard - http://localhost

File
View
Tools
Help
MS10-016 Security Update for Windows 7
Signatures
MS10-016 Security Update for Windows 7
Signature Summary
New
Delete
View

Double-click a signature to edit from the summary list below:

| Name | Status | OS List |
|---|---|---|
| MS10-016 Security Update for Windows 7 (KB975561)... | Active | Win7; |

1 Signatures - All active

5/8/2017 5:16 PM

Figure 26: Signature Summary Page: Multiple Signatures

2. In the pane select the applicable signature you want to delete.

**Note:** Each patch supports multiple signatures and each signature may be deleted.

3. Click **Delete**.

   **Step Result:** A confirmation message appears.

   Figure 27: Confirmation Message

4. Click **OK**.

   **Step Result:** The confirmation message dialog closes.

**Result:** The patch signature is deleted and is no longer visible in the ***Signature Summary*** page.

# Chapter 6

# Working with Fingerprints

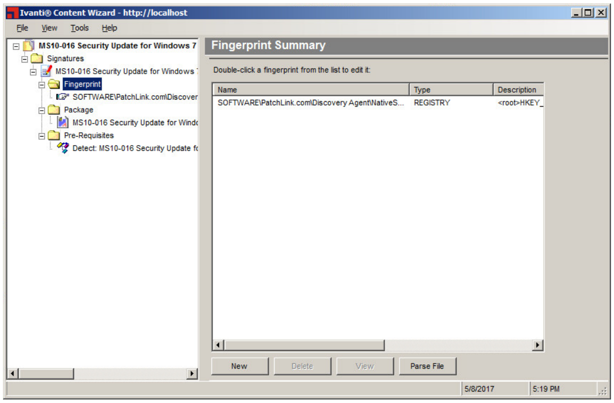
**In this chapter:**

- The Fingerprint Summary Page
- Types of Fingerprints
- Adding Fingerprints

A signature can have one or multiple fingerprints. A fingerprint detects if a patch is present within a device. A fingerprint can be a file, directory, registry key, or a value within a registry.

## The Fingerprint Summary Page

The ***Fingerprint Summary*** page allows you to view all fingerprints associated with a signature. To display the ***Fingerprint Summary*** page, click on the appropriate signature's **Fingerprints** folder in the left pane.



MS10-016 Security Update for Windows 7
Signatures
MS10-016 Security Update for Windows 7
Fingerprint
SOFTWARE\PatchLink.com\Discover
Package
MS10-016 Security Update for Windo
Pre-Requisites
Detect: MS10-016 Security Update fo

Double-click a fingerprint from the list to edit it:

| Name | Type | Description |
|---|---|---|
| SOFTWARE\PatchLink.com\Discovery Agent\NativeS... | REGISTRY | <root>HKEY_ |

Figure 28: Fingerprint Summary Page

The following buttons are available on the ***Fingerprint Summary*** page.

| Button | Description |
|---|---|
| **New** | Creates and adds a new fingerprint to the ***Fingerprint Summary*** page. |
| **Delete** | Removes the selected fingerprint. |

| Button | Description |
|---|---|
| **View** | Opens the ***Fingerprint Properties*** window. For more information, see Types of Fingerprints on page 54. |
| **Parse File** | Allows you to add multiple fingerprints using an XML text file. |

## Types of Fingerprints

The ***Fingerprint Properties*** page allows you to choose from among seven types of fingerprints. Depending on the fingerprint type you select, the ***Fingerprint Properties*** page fields change accordingly.

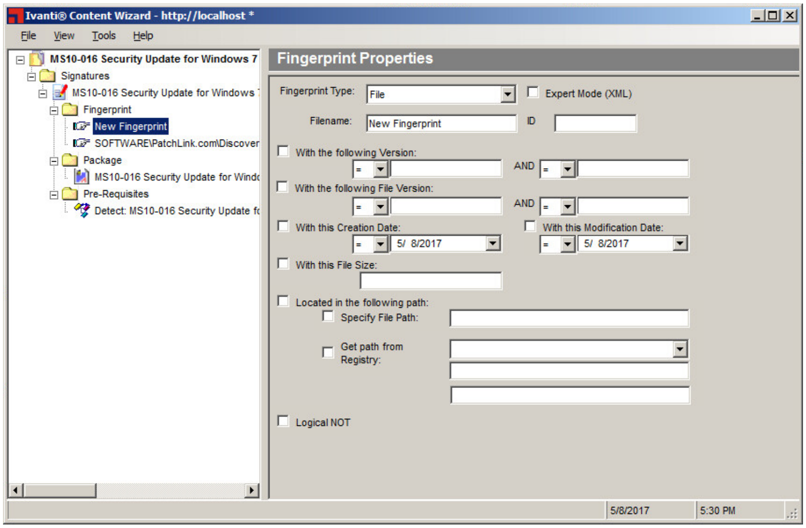
The following table describes the types of fingerprints you can select in the ***Fingerprint Properties*** page.

Table 2: Types of Fingerprints

| Type | Description | Target Operating System (OS) |
|---|---|---|
| **File** | Determine the presence and properties of files and directories. See Using the File Fingerprint on page 55. | Windows |
| **Registry** | Extract data from the Windows Registry. See Using the Registry Fingerprint on page 61. | Windows |
| **WMI** | Detect information about a system's operating system, name, distribution, or version. See Using the WMI Fingerprint on page 63. | UNIX/Linux/Mac |
| **SystemInfo** | Retrieve information about a device including the OS Name, version, and architecture. See Using the SystemInfo Fingerprint on page 68. | UNIX/Linux/Mac |
| **Expression** | Compute logical operations based on the presence or absence of other fingerprints. See Using the Expression Fingerprint on page 69. | UNIX/Linux/Mac |
| **Patch** | Determine the presence of special components such as patches. Using the Patch Fingerprint on page 70. | UNIX/Linux/Mac |
| **Script** | Allow custom XML script creation of fingerprints. See Using the Script Fingerprint on page 71. | Windows |

## Using the File Fingerprint

The **File** fingerprint determines the presence and properties of files and directories within Windows.


Ivanti® Content Wizard - http://localhost *
File
View
Tools
Help
MS10-016 Security Update for Windows 7
Signatures
MS10-016 Security Update for Windows 7
Fingerprint
New Fingerprint
SOFTWARE\PatchLink.com\Discover
Package
MS10-016 Security Update for Windc
Pre-Requisites
Detect: MS10-016 Security Update fc
Fingerprint Properties

Fingerprint Type: File □ Expert Mode (XML)

Filename: New Fingerprint ID

□ With the following Version: = AND =

□ With the following File Version: = AND =

□ With this Creation Date: = 5/ 8/2017 □ With this Modification Date: = 5/ 8/2017

□ With this File Size:

□ Located in the following path:
□ Specify File Path:
□ Get path from Registry:

□ Logical NOT

5/8/2017 5:30 PM

Figure 29: Fingerprint Type: File

The following table describes the properties, how to use them, and their equivalent XML tag used for expert mode. Not all properties are required.

Table 3: File Fingerprint Properties

| Properties | Description | Usage Suggestions | XML Tag |
|---|---|---|---|
| **Fingerprint Type**<br>(drop-down list) | Identifies the type of fingerprint. | Select the fingerprint needed for the signature. | N/A |
| **Expert Mode (XML)**<br>(check box) | Allows for entering fingerprint data in XML. | Toggle between the fingerprint property fields and a text field, allowing you to add and view the properties using XML. | N/A |
| **Filename**<br>(field) | Type a specific filename. | • Specify an environment variable that includes either the filename or the path and filename.<br>• Leave the field blank if you are looking for the existence of a directory. | `<name>` |

| Properties | Description | Usage Suggestions | XML Tag |
|---|---|---|---|
| **ID**<br>(field) | Patch identifier that can be customized by company. | The number can be specific to a company or department. Use this field for integrating with the Expression fingerprint. | N/A |
| **With the following Version**<br>(check box, drop-down list, and field) | Search for a minimum version or a range of versions. | • Type a specific version number (=).<br>• Search for a version less than or equal to (<=) or greater than or equal to (>=) a specific value.<br>• Search for a version within a range of values. | `<version>` |
| **AND**<br>( drop-down list and field) | Allows for additional qualifiers. | Add additional parameters. Both values must be true. | N/A |
| **With the following File Version**<br>(check box, drop-down list and field) | Search for a minimum file version, or a range of file versions. | • Type a specific file version number (=).<br>• Search for a file version less than or equal to (<=) or greater than or equal to (>=) a specific value.<br>• Search for a file version within a range of values. | `<fileversion>` |

| Properties | Description | Usage Suggestions | XML Tag |
|---|---|---|---|
| **AND**<br>(drop-down list and field) | Allows for additional qualifiers. | Add additional parameters. Both values must be true. | N/A |
| **With this Creation Date**<br>(check box and drop-down list) | Allows you to search based upon a creation date. | • Type a specific creation date.<br>• Search for a creation date less than or equal to (<=) or greater than or equal to (>=) a specific date. | `<created>` |
| **With this Modification Date**<br>(check box and drop-down list) | Allows for locating a patch with a specific modification date range. | • Type a specific modification date.<br>• Search for a modification date less than or equal to (<=) or greater than or equal to (>=) a specific date. | `<modified>` |
| **With this File Size**<br>(check box and field) | Searches for a file based upon an exact file size (in bytes.) | Can only be used to search for a specific size. | `<size>` |

| Properties | Description | Usage Suggestions | XML Tag |
|---|---|---|---|
| **Located in the following path:- Specify File Path**<br>(check box and field) | Allows you to specify a relative path to be used when looking for a file. | Specify an environment variable containing a path or a path/filename.<br>• If the environment variable has a filename included, and a filename was not specified in the **Filename** field, the filename returned from the variable is used.<br>• If the environment variable has a filename included, and a file was specified in the **Filename** field, the filename returned by the variable will be discarded.<br>Specify a relative path. Will search all local drives and look for a path that ends with the selected parameter.<br>Leave blank for a broad search for the file (not recommended since this will search every drive.)<br>Enter an absolute path such as `C:\winnt\system32` (not recommended because of the ability to customize the installation path of an application.) | `<path>` |

| Properties | Description | Usage Suggestions | XML Tag |
|---|---|---|---|
| **Located in the following path - Get path from Registry**<br>(check box, drop-down list, and field) | Retrieves the path from the registry. | The root for the entry is selected from the drop-down list. Type the **KEY** and **VALUE** into the respective fields. The available **ROOT** values are:<br>• HKEY_LOCAL_MACHINE<br>• HKEY_CLASSES_ROOT<br>• HKEY_CURRENT_USER<br>• HKEY_USERS<br>• HKEY_CURRENT_CONFIG<br>Manually type the **KEY**.<br>For the **VALUE** field, you can:<br>• Manually type the *VALUE*.<br>• Enter value of `(Default)` to use **KEY**'s default value. | `<root>`<br>`<key>`<br>`<value>` |

| Properties | Description | Usage Suggestions | XML Tag |
|---|---|---|---|
| **LogicalNOT**<br>(check box) | Changes search from checking if a file exists to checking if it does not exist. | Use for confirming if a file or directory was previously created. | `<not>` |

**Example:**

The following example represents an XML script that includes all the possible XML parameters.

```
<File>
    <name>outlook.exe</name>
    <version> > 4.01.2345b </version>
    <version> < 5.00.2789 </version>
    <fileversion> > 5.01.2345 </fileversion>
    <Created> > 5/30/2001 12:01:04 PM </Created>
    <modified> > 5/30/2001 12:01:04 PM </modified>
    <size>4252</size>
    <root>HKEY_LOCAL_MACHINE</root>
    <key>SOFTWARE\Classes\Software\Microsoft\Exe</key>
    <value>(Default)</value>
</File>
```

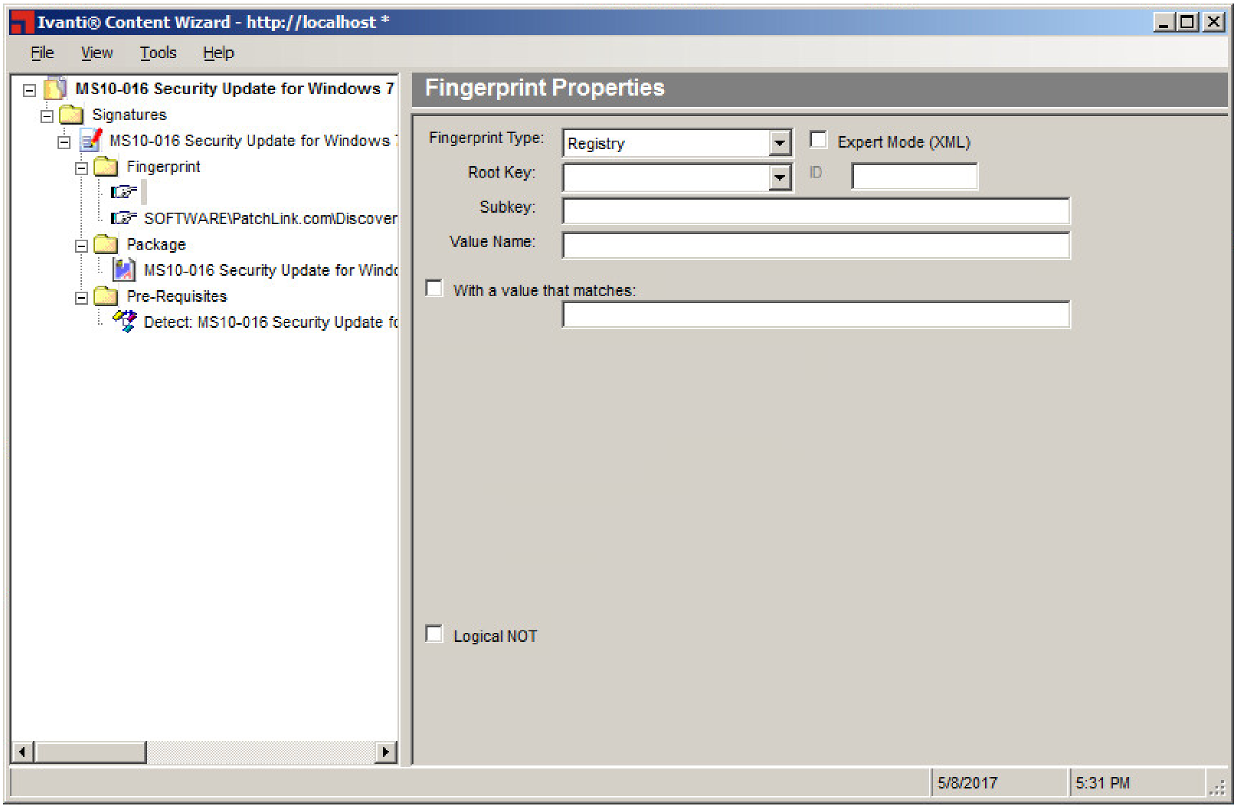
**Example:**

The following example represents a script using the **LogicalNOT** option.

```
<File>
    <name>temptest.txt</name>
    <path>%WINDIR%\temp\</path>
    <not>1</not>
</File>
```

## Using the Registry Fingerprint

The **Registry** fingerprint extracts data from the windows registry. It only works on Windows operating systems.



- MS10-016 Security Update for Windows 7
  - Signatures
    - MS10-016 Security Update for Windows 7
      - Fingerprint
        - SOFTWARE\PatchLink.com\Discover
      - Package
        - MS10-016 Security Update for Windo
      - Pre-Requisites
        - Detect: MS10-016 Security Update fo

Fingerprint Type: Registry

□ Expert Mode (XML)

Root Key:

ID

Subkey:

Value Name:

□ With a value that matches:

□ Logical NOT

5/8/2017 5:31 PM

Figure 30: Fingerprint Type: File

The following table describes the properties, how to use them, and their equivalent XML tag used for expert mode. Not all properties are required.

Table 4: Registry Fingerprint Properties

| Properties | Description | Usage Suggestions | XML Tag |
|---|---|---|---|
| **Fingerprint Type** | Identifies the type of fingerprint. | Select the fingerprint needed for the report. | N/A |
| **Expert Mode (XML)** | Allows for entering fingerprint data in XML. | Toggle between the fingerprint property fields and a text field, allowing you to add and view the properties using XML. | N/A |

| Properties | Description | Usage Suggestions | XML Tag |
|---|---|---|---|
| **Root Key** | Registry root key. | Searches for the root key. You must also specify the **Subkey** and **Value Name**. The following are possible values for **Root Key**:<br>• HKEY_LOCAL_MACHINE<br>• HKEY_CLASSES_ROOT<br>• HKEY_CURRENT_USER<br>• HKEY_USERS<br>• HKEY_CURRENT_CONFIG | `<root>` |
| **Subkey** | Registry subkey. | Searches for a registry subkey. When using the registry fingerprint type you must specify a subkey. | `<key>` |
| **Value Name** | Value of attribute. | Defines the registry value within the specified key that will be searched for. You can either type a specific value or use the default key by typing **(Default)**. | `<value>` |
| **With a value that matches** | Allows for a search of a matching value. | Type a specific value and add additional parameters. | N/A |

| Properties | Description | Usage Suggestions | XML Tag |
|---|---|---|---|
| **LogicalNOT** | Changes search from checking if a registry exists to checking if it does not exist. | Use for confirming if a registry was previously created. | `<not>` |

**Example:**

The following example represents an XML script that includes all the possible XML parameters.

```
<Registry>
    <root>HKEY_LOCAL_MACHINE</root>
    <key>SOFTWARE\Classes\Software\Adobe\Exe</key>
    <value>(Default)</value>
</Registry>
```

**Example:**

The following example represents a script using the **LogicalNOT** option.

```
<Registry>
    <name>temptest.txt</name>
    <path>%WINDIR%\temp\</path>
    <not>1</not>
</Registry>
```

## Using the WMI Fingerprint

The **WMI** fingerprint detects information about a system such as operating system name, distribution, or version. It works on UNIX/Linux operating systems.

The following table describes the properties, how to use them, and their equivalent XML tag used for expert mode. Not all properties are required.

Table 5: WMI Fingerprint Properties

| Properties | Description | Usage Suggestions | XML Tag |
|---|---|---|---|
| **Fingerprint Type**<br>(drop-down list) | Identifies the type of fingerprint. | Select the fingerprint needed for the report. | N/A |
| **Expert Mode (XML)**<br>(check box) | Allows for entering fingerprint data in XML. | Toggle between the fingerprint property fields and a text field, allowing you to add and view the properties using XML. | N/A |
| **Name**<br>(field) | The name of the script. | Contains the name of the script. | `<name>` |

| Properties | Description | Usage Suggestions | XML Tag |
|---|---|---|---|
| **ExpressionID** (field) | Expression ID. | Used to give this fingerprint an expression ID so that it can be used in a more complicated expression (UNIX/Linux patches only.) | `<eid>` |

| Properties | Description | Usage Suggestions | XML Tag |
|---|---|---|---|
| **Content**<br>(text box) | The content of the script. | Contains the content of the script to be run. | `<content>` |

**Example:**

The following example represents an XML script that includes all the possible XML parameters.

```
<WMI>
<name>LPRng requirements script</name>
<content>#!/bin/sh
if [ -f myfile.txt ]; then
echo "Detected"
else
echo "Not Detected"
exit 0
</content>
<eid>c7</eid>
</WMI>
```

**Example:**

Perl Example

```
<name>DetectNTPPerl</name>
<content>#!/usr/bin/perl
my $detected = 0;
if (`grep 6001 /etc/ntp.conf`){
$detected = 1;
}
if ($detected) {
print "detected";
} else {
print "Anything else";
}
</content>
```

**Example:**

Bash Example

```
<name>DetectNTP</name>
<content>#!/bin/sh
detected=`grep -c 6001 /etc/ntp.conf`
if [ "$detected" -ge 1 ]
then
echo DETECTED
else
echo NOT DETECTED
fi
</content>
```

## Using the Shell Script Fingerprint

The **Shell Script** fingerprint detects information about a system such as operating system name, distribution, or version. It works on UNIX/Linux operating systems.

The following table describes the properties, how to use them, and their equivalent XML tag used for expert mode. Not all properties are required.

Table 6: Shell Script Fingerprint Properties

| Properties | Description | Usage Suggestions | XML Tag |
|---|---|---|---|
| **Fingerprint Type**<br>(drop-down list) | Identifies the type of fingerprint. | Select the fingerprint needed for the report. | N/A |
| **Expert Mode (XML)**<br>(check box) | Allows for entering fingerprint data in XML. | Toggle between the fingerprint property fields and a text field, allowing you to add and view the properties using XML. | N/A |
| **Name**<br>(field) | The name of the script. | Contains the name of the script. | `<name>` |
| **ExpressionID**<br>(field) | Expression ID. | Used to give this fingerprint an expression ID so that it can be used in a more complicated expression (UNIX/Linux patches only.) | `<eid>` |

| Properties | Description | Usage Suggestions | XML Tag |
|---|---|---|---|
| **Content**<br>(text box) | The content of the script. | Contains the content of the script to be run. | `<content>` |

**Example:**

The following example represents an XML script that includes all the possible XML parameters.

```
<WMI>
<name>LPRng requirements script</name>
<content>#!/bin/sh
if [ -f myfile.txt ]; then
echo "Detected"
else
echo "Not Detected"
exit 0
</content>
<eid>c7</eid>
</WMI>
```

**Example:**

Perl Example

```
<name>DetectNTPPerl</name>
<content>#!/usr/bin/perl
my $detected = 0;
if (`grep 6001 /etc/ntp.conf`){
$detected = 1;
}
if ($detected) {
print "detected";
} else {
print "Anything else";
}
</content>
```

**Example:**

Bash Example

```
<name>DetectNTP</name>
<content>#!/bin/sh
detected=`grep -c 6001 /etc/ntp.conf`
if [ "$detected" -ge 1 ]
then
echo DETECTED
else
echo NOT DETECTED
fi
</content>
```

## Using the SystemInfo Fingerprint

The **SystemInfo** fingerprint retrieves information about an endpoint such as operating system name, architecture, and operating system version. It works on UNIX/Linux operating systems.

The following table describes the properties, how to use them, and their equivalent XML tag used for expert mode. Not all properties are required.

Table 7: SystemInfo Fingerprint Properties

| Properties | Description | Usage Suggestions | XML Tag |
|---|---|---|---|
| **Fingerprint Type**<br>(drop-down list) | Identifies the type of fingerprint. | Select the fingerprint needed for the report. | N/A |
| **Expert Mode (XML)**<br>(check box) | Allows for entering fingerprint data in XML. | Toggle between the fingerprint property fields and a text field, allowing you to add and view the properties using XML. | N/A |
| **Attribute**<br>(field) | The name of the script. | This field allows you to specify which system attribute is being determined. The attributes are:<br>• Architecture<br>• AgentVersion<br>• OSName<br>• OSDistribution<br>• OSVersion<br>• OSKernelVersion | `<systemattribute>` |
| **ID**<br>(field) | Expression ID. | Used to give this fingerprint an expression ID so that it can be used in a more complicated expression (UNIX/Linux patches only.) | `<eid>` |

| Properties | Description | Usage Suggestions | XML Tag |
|---|---|---|---|
| **Value**<br>(field) | The value of the attribute. | Allows you to specify which value the attribute will be compared against. | `<value>` |

**Example:**

The following example represents an XML script that includes all the possible XML parameters.

This example determines whether the architecture of the client machine is an `iX86` greater than or equal to `i386`. The result is put in the variable `c0`, which can then be used in a logical expression to determine if a signature is present.

```
<SystemInfo>
    <systemattribute>Architecture</systemattribute>
    <value>_GE_ i386</value>
    <eid>c0</eid>
</SystemInfo>
```

## Using the Expression Fingerprint

The **Expression** fingerprint computes logical operations based on the presence or absence of other fingerprints. It works on UNIX/Linux operating systems.

The following table describes the properties, how to use them, and their equivalent XML tag used for expert mode. Not all properties are required.

Table 8: Expression Fingerprint Properties

| Properties | Description | Usage Suggestions | XML Tag |
|---|---|---|---|
| **Fingerprint Type**<br>(drop-down list) | Identifies the type of fingerprint. | Select the fingerprint needed for the report. | N/A |
| **Expert Mode (XML)**<br>(check box) | Allows for entering fingerprint data in XML. | Toggle between the fingerprint property fields and a text field, allowing you to add and view the properties using XML. | N/A |
| **Name**<br>(field) | The name of the script. | Contains the name of the script. | `<name>` |

| Properties | Description | Usage Suggestions | XML Tag |
|---|---|---|---|
| **Content**<br>(field) | The content of the script. | Contains the content of the script to be evaluated. | `<content>` |

**Note:** Prior to using a term in an expression it must be already defined by setting the ID (or Entity ID) of the other components.

**Example:**

The following example represents an XML script that includes all the possible XML parameters. This example determines whether the client machine has:

1. Any version of the application called KDE.
2. A new agent.
3. An ix86 architecture of at least i386.

This was accomplished by associating other fingerprint types to the cX variables that are in the logical expression. In this example:

- `c0` is the result of attempting to detect a new agent.
- `c1` is the result of attempting to detect an ix86 architecture >= to i386.
- `c2` through `c5` are used to detect the presence of the KDE application (`c0` and `c1` must be present.)
- `c2` through `c4` are the result of attempting to detect components, any one of which must be present in the KDE application. (i.e. either `c2` or `c3` or `c4` must be present.)
- `c5` is the result of attempting to detect components, each of which must be present in the KDE application.

```
<Expression>
<name>Any kde with new agent and -GE- i386 </name>
<content>c0 AND c1 AND (c2 | c3 | c4 ) AND c5 </content>
</Expression>
```

## Using the Patch Fingerprint

The **Patch** fingerprint determines the presence of special packages such as patches. It works on UNIX/ Linux operating systems.

The following table describes the properties, how to use them, and their equivalent XML tag used for expert mode. Not all properties are required.

Table 9: Patch Fingerprint Properties

| Properties | Description | Usage Suggestions | XML Tag |
|---|---|---|---|
| **Fingerprint Type**<br>(drop-down list) | Identifies the type of fingerprint. | Select the fingerprint needed for the report. | N/A |

| Properties | Description | Usage Suggestions | XML Tag |
|---|---|---|---|
| **Expert Mode (XML)**<br>(check box) | Allows for entering fingerprint data in XML. | Toggle between the fingerprint property fields and a text field, allowing you to add and view the properties using XML. | N/A |
| **Name**<br>(field) | Indicates the name of the package. | Contains the name of the package. | `<name>` |
| **ID**<br>(field) | Indicates the Expression ID. | Used to give this fingerprint an expression ID so that it can be used in a more complicated expression (UNIX/Linux patches only.) | `<eid>` |
| **Version**<br>(field) | Indicates the package version. | The version against which the package will be compared. | `<version>` |
| **Release**<br>(field) | Indicates the release version. | The release against which the package will be compared. | `<release>` |

**Example:**

The following example represents an XML script that includes all the possible XML parameters. This example determines whether a patch with the Solaris Patch ID of 106468-05 exists on an endpoint hosting a Solaris operating system.

```
<name>106468-05</name>
<version>106468</version>
<release>_GE_ 05</release>
<eid>c0</eid>
```

## Using the Script Fingerprint

The **Script** fingerprint retrieves information about an endpoint such as operating system name, version, services, and other values using queries similar to those used in SQL. It works on Windows operating systems.

The following table describes the properties, how to use them, and their equivalent XML tag used for expert mode. Not all properties are required.

Table 10: Script Fingerprint Properties

| Properties | Description | Usage Suggestions | XML Tag |
|---|---|---|---|
| **Fingerprint Type**<br>(drop-down list) | Identifies the type of fingerprint. | Select the fingerprint needed for the report. | N/A |

| Properties | Description | Usage Suggestions | XML Tag |
|---|---|---|---|
| **Expert Mode (XML)**<br>(check box) | Allows for entering fingerprint data in XML. | Toggle between the fingerprint property fields and a text field, allowing you to add and view the properties using XML. | N/A |
| **Name**<br>(field) | Indicates the name of the script. | Contains the name of the script. | `<name>` |
| **Script Type**<br>(field) | Indicates the type of script. | Contains the type of script to be executed. VBScript scripts are supported for Windows and Schell scripts are supported for Linux and Unix. | `<type>` |
| **Validate**<br>(button) | Validates the fingerprint script. script. | Use to validate the script within the text box. VBScript scripts are supported for Windows and Schell scripts are supported for Linux and Unix. | `N/A` |
| **Content**<br>(text box) | Indicates the content of the script. | Type the actual script to be used. The VBScript must reference the SetReturnCode subroutine and return a value either 1 (True) or 0 (False). | `<content>` |

When developing a script fingerprint, it is highly recommended that you use a Visual Basic compatible editor so that capitalization and language syntax are validated properly before you try running your script. Visual Basic can be used to quickly prototype and test functionality, if desired. All fingerprint scripts should be tested thoroughly in isolation, using the Windows Scripting Host `CSCRIPT.EXE` to run the script stand alone on a test machine.

**Note:** Any errors in your script will cause the script fingerprint to fail and return a **Not-Patched** value. For this reason it is recommended that the `On Error Resume Next` directive is used to ensure that your script will run to completion.

**Example:**

The following example represents an XML script that includes all the possible XML parameters.

```
<name>Check Myfile</name>
<type>VBScript</type>
<contents>
    On Error Resume Next
    Dim RetCode
    Dim szTempFileName
    Dim FileObject
    RetCode = 0
    ' Create the File System Object
    Set FileObject = CreateObject("Scripting.FileSystemObject")
    ' Detect if the specified file exists
    szTempFileName="C:\testfile.txt"
    If FileObject.FileExists(szTempFileName) Then
        RetCode = 1
    Else
        RetCode = 0
    End If
    ' MsgBox RetCode
    WScript.Quit RetCode
</contents>
```

**Note:** No error messages will be seen in the Detection Log if your script fails.

# Adding Fingerprints

You can add a single fingerprint or multiple fingerprints to a signature, depending on your signature requirements. The Ivanti Content Wizard is pre-filled with a suitable registry fingerprint that was generated based on the information in the selected installable file.

## Adding a Single Fingerprint

You can add a single fingerprint to a signature from the ***Fingerprint Summary*** page.

**Prerequisites:**

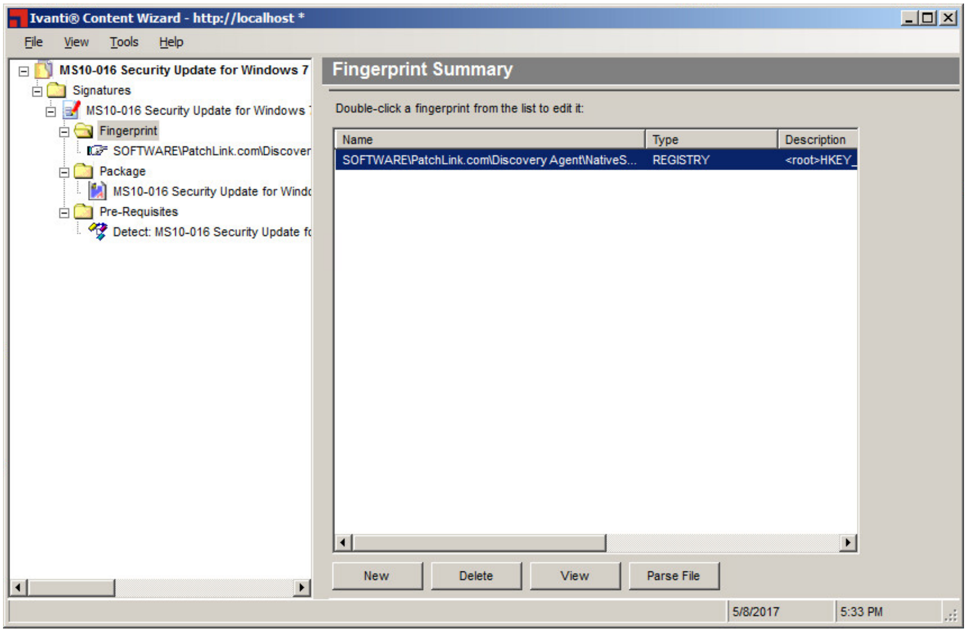
Create a signature for a patch. For more information about creating signatures, refer to Adding a Signature to a Patch on page 46.

Add a new fingerprint and define its properties in the ***Fingerprint Properties*** page.

1. Expand the patch properties to **Fingerprint** in the left pane.

   **Example:** ***Patch Name*** > **Signatures** > ***Signature Title*** > **Fingerprint**.

   **Step Result:** The ***Fingerprint Summary*** page opens.



Ivanti® Content Wizard - http://localhost *
File
View
Tools
Help
MS10-016 Security Update for Windows 7
Signatures
MS10-016 Security Update for Windows 7
Fingerprint
SOFTWARE\PatchLink.com\Discover
Package
MS10-016 Security Update for Windo
Pre-Requisites
Detect: MS10-016 Security Update fo
New
Delete
View
Parse File
5/8/2017
5:33 PM

Fingerprint Summary

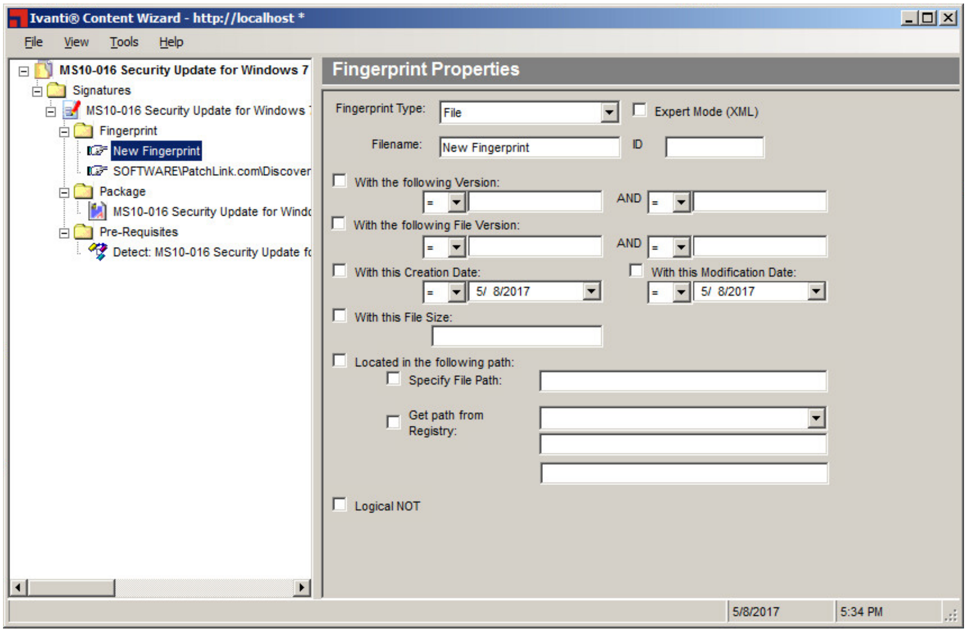
Double-click a fingerprint from the list to edit it:

| Name | Type | Description |
|---|---|---|
| SOFTWARE\PatchLink.com\Discovery Agent\NativeS... | REGISTRY | <root>HKEY_ |

Figure 31: Fingerprint Summary Page

2. Select **New**.

   **Step Result:** The panel contains a new fingerprint named **New Fingerprint**.



Ivanti® Content Wizard - http://localhost *
File
View
Tools
Help
MS10-016 Security Update for Windows 7
Signatures
MS10-016 Security Update for Windows 7
Fingerprint
New Fingerprint
SOFTWARE\PatchLink.com\Discover
Package
MS10-016 Security Update for Windo
Pre-Requisites
Detect: MS10-016 Security Update fo
Fingerprint Properties

Fingerprint Type: File

☐ Expert Mode (XML)

Filename: New Fingerprint

ID

☐ With the following Version: = AND =

☐ With the following File Version: = AND =

☐ With this Creation Date: = 5/ 8/2017

☐ With this Modification Date: = 5/ 8/2017

☐ With this File Size:

☐ Located in the following path:

☐ Specify File Path:

☐ Get path from Registry:

☐ Logical NOT

5/8/2017 5:34 PM

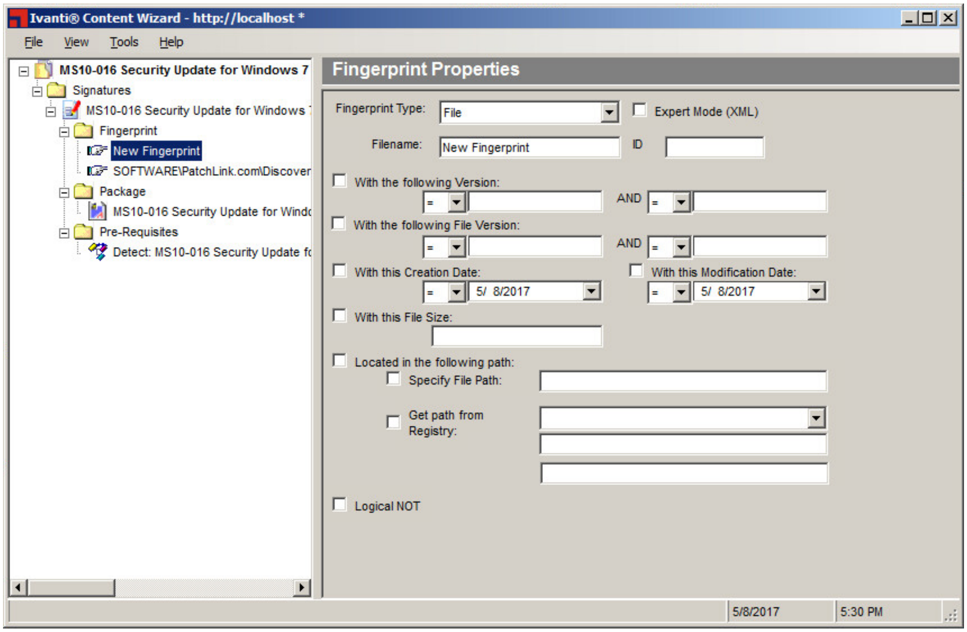
Figure 32: Fingerprint Summary Page: New Fingerprint

3. Select **New Fingerprint** within the pane.

4. Click **View**.

**Tip:** Within the pane window you may double-click on a signature to open the ***Fingerprint*** page.

**Step Result:** The ***Fingerprint Properties*** page opens.


Ivanti® Content Wizard - http://localhost *
File
View
Tools
Help
MS10-016 Security Update for Windows 7
Signatures
MS10-016 Security Update for Windows
Fingerprint
New Fingerprint
SOFTWARE\PatchLink.com\Discover
Package
MS10-016 Security Update for Windo
Pre-Requisites
Detect: MS10-016 Security Update fo

Fingerprint Properties

Fingerprint Type: File

□ Expert Mode (XML)

Filename: New Fingerprint

ID

□ With the following Version: = AND =

□ With the following File Version: = AND =

□ With this Creation Date: = 5/ 8/2017

□ With this Modification Date: = 5/ 8/2017

□ With this File Size:

□ Located in the following path:

□ Specify File Path:

□ Get path from Registry:

□ Logical NOT

5/8/2017 5:30 PM

Figure 33: Fingerprint Properties Page

5. Select the **Fingerprint Type**.

   By default, the **File** fingerprint type is selected. For more information on the fingerprint types available, refer to Types of Fingerprints on page 54.

6. Define the appropriate fingerprint properties.

   Fingerprint properties are different for different fingerprint types. For detailed information on each fingerprint type, field definitions, and usage suggestions, see Types of Fingerprints on page 54.

7. Select **File** > **Save**.

**Result:** The fingerprint is created for the selected signature.

## Adding Multiple Fingerprints

You can create multiple fingerprints for a patch signature. This allows you to use multiple methods of detecting the presence of a patch.

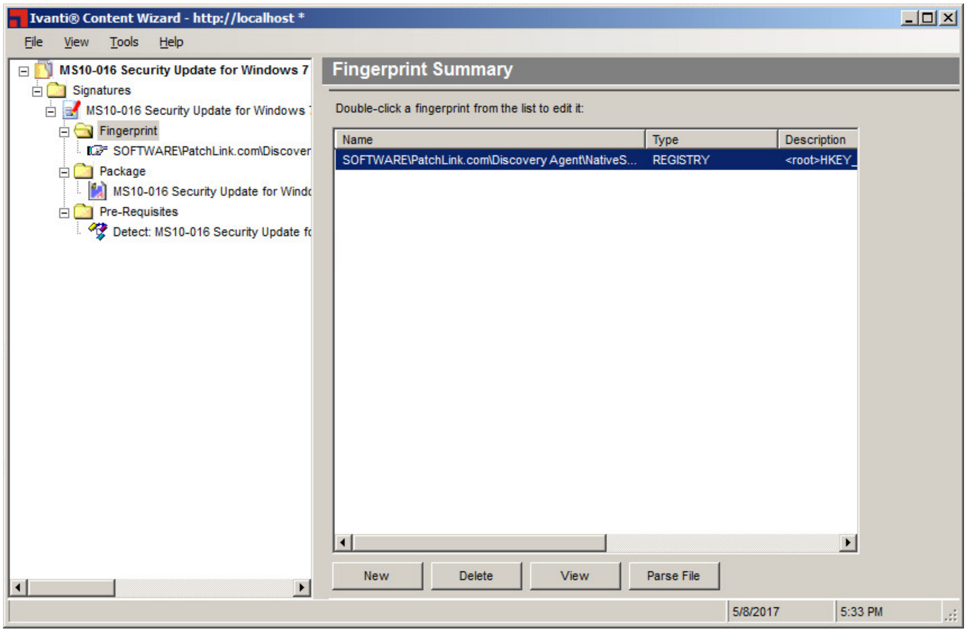
**Prerequisites:**

- Create a signature for a patch. For more information about creating signatures, refer to Adding a Signature to a Patch on page 46.
- Create an `XML` document with the fingerprint details. Write the `XML` document in Expert XML mode. For more information, see Creating Fingerprints in Expert Mode (XML) on page 78.

1. Expand the patch properties to **Fingerprint** in the left pane.

   **Example:** ***Patch Name*** > **Signatures** > ***Signature Title*** > **Fingerprint**.

   **Step Result:** The ***Fingerprint Summary*** page opens.


Ivanti® Content Wizard - http://localhost *
File
View
Tools
Help
MS10-016 Security Update for Windows 7
Signatures
MS10-016 Security Update for Windows 7
Fingerprint
SOFTWARE\PatchLink.com\Discover
Package
MS10-016 Security Update for Windo
Pre-Requisites
Detect: MS10-016 Security Update fo
Fingerprint Summary
New
Delete
View
Parse File
5/8/2017
5:33 PM

Double-click a fingerprint from the list to edit it:

| Name | Type | Description |
|---|---|---|
| SOFTWARE\PatchLink.com\Discovery Agent\NativeS... | REGISTRY | <root>HKEY_ |

Figure 34: Fingerprint Summary Page

2. Click **Parse File**.

   **Step Result:** The ***Open*** window opens.

3. Select the `XML` file you have created using Expert XML mode.

   For more information on creating `XML` files in Expert XML mode, see Creating Fingerprints in Expert Mode (XML) on page 78.

4. Click **Open**.

   **Step Result:** The ***Open*** window closes.

5. Select **File** > **Save**.

**Result:** The fingerprints in the `XML` file are added to the ***Fingerprint Summary*** page.

## Creating Fingerprints in Expert Mode (XML)

The **Expert Mode (XML)** check box in the ***Fingerprint Properties*** page lets you create an `XML` document with the fingerprint details. You can then use this document to add multiple fingerprints to a signature.

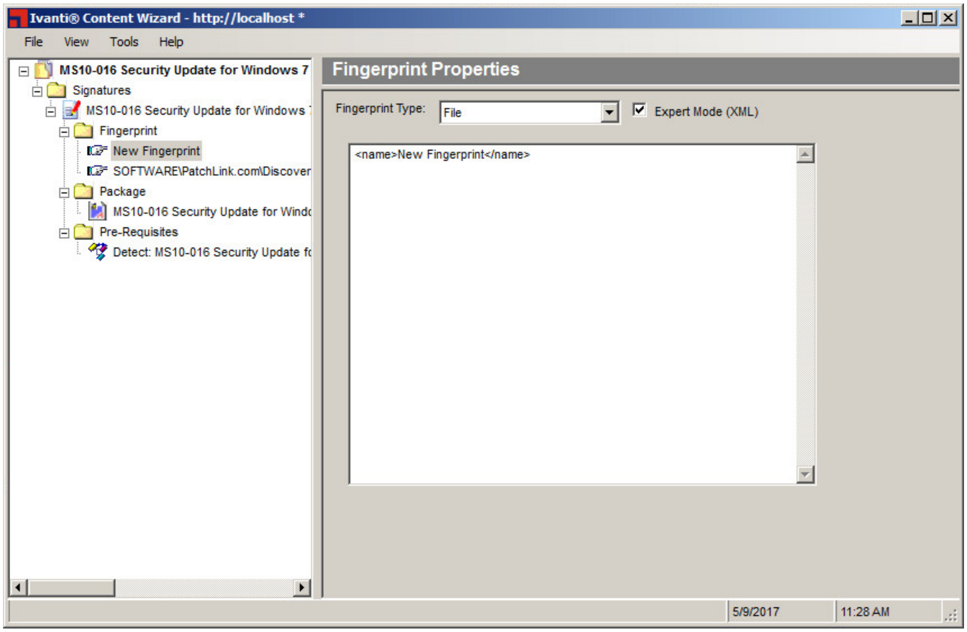
1. Expand the patch properties to **Fingerprint Type** in the left pane.

   **Example:** ***Patch Name*** > **Signatures** > ***Signature Title*** > **Fingerprint** > ***Fingerprint Type***.

   **Step Result:** The ***Fingerprint Properties*** page displays.

2. Select the **Expert Mode (XML)** check box in the ***Fingerprint Properties*** page.

   **Step Result:** A blank field is displayed within the pane.


Ivanti® Content Wizard - http://localhost *
File
View
Tools
Help
MS10-016 Security Update for Windows 7
Signatures
MS10-016 Security Update for Windows
Fingerprint
New Fingerprint
SOFTWARE\PatchLink.com\Discover
Package
MS10-016 Security Update for Windo
Pre-Requisites
Detect: MS10-016 Security Update fo
Fingerprint Properties
5/9/2017
11:28 AM

Fingerprint Type: File

☑ Expert Mode (XML)

```
<name>New Fingerprint</name>
```

Figure 35: Fingerprint Properties Page: Expert Mode (XML)

3. Within the pane window type the XML fingerprint code.

4. SelectFile > **Save**.

   **Step Result:** Your changes are saved.

**Result:** The fingerprint properties are created in `.xml` format.

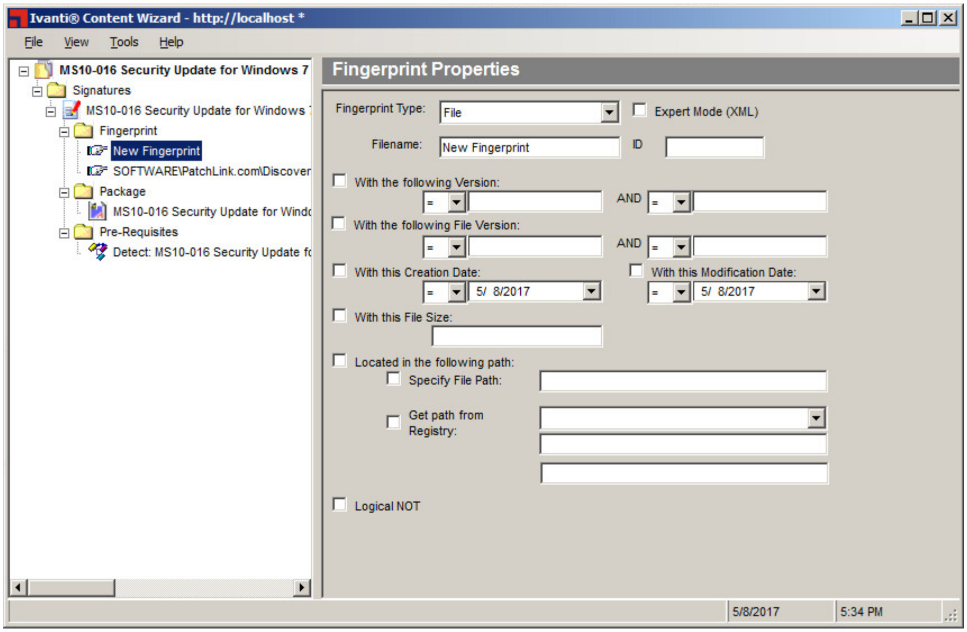
## Deleting a Fingerprint

If you no longer require a particular fingerprint for a signature, you can delete it in the ***Fingerprint Summary*** page.

1. Expand the patch properties to **Fingerprint** in the left pane.

   **Example:** ***Patch Name*** > **Signatures** > ***Signature Title*** > **Fingerprint**.

   **Step Result:** The ***Fingerprint Summary*** page opens.


Ivanti® Content Wizard - http://localhost *
File
View
Tools
Help
MS10-016 Security Update for Windows 7
Signatures
MS10-016 Security Update for Windows 7
Fingerprint
New Fingerprint
SOFTWARE\PatchLink.com\Discover
Package
MS10-016 Security Update for Windo
Pre-Requisites
Detect: MS10-016 Security Update fo
Fingerprint Properties

Fingerprint Type: File

□ Expert Mode (XML)

Filename: New Fingerprint

ID

□ With the following Version: = AND =

□ With the following File Version: = AND =

□ With this Creation Date: = 5/ 8/2017

□ With this Modification Date: = 5/ 8/2017

□ With this File Size:

□ Located in the following path:

□ Specify File Path:

□ Get path from Registry:

□ Logical NOT

5/8/2017 5:34 PM

Figure 36: Fingerprint Summary Page

2. In the pane select the applicable fingerprint you want to delete.

**Note:** Each signature supports multiple fingerprints and each fingerprint may be deleted.

3. Click **Delete**.

   **Step Result:** A confirmation message appears.

4. Click **OK**.

   **Step Result:** The confirmation message dialog closes.

5. Select **File** > **Save**.

**Result:** The fingerprint is deleted and is no longer visible in the ***Fingerprint Summary*** page.

# Chapter 7

# Working with Packages

**In this chapter:**

A package includes the executable files, compressed data files, and the scripts required to install the application or patch.

## The Package Summary Page

The ***Package Summary*** page allows you to view and define the package options for a patch.

To display the ***Package Summary*** page, click the **Package** folder from the menu tree in the left pane.

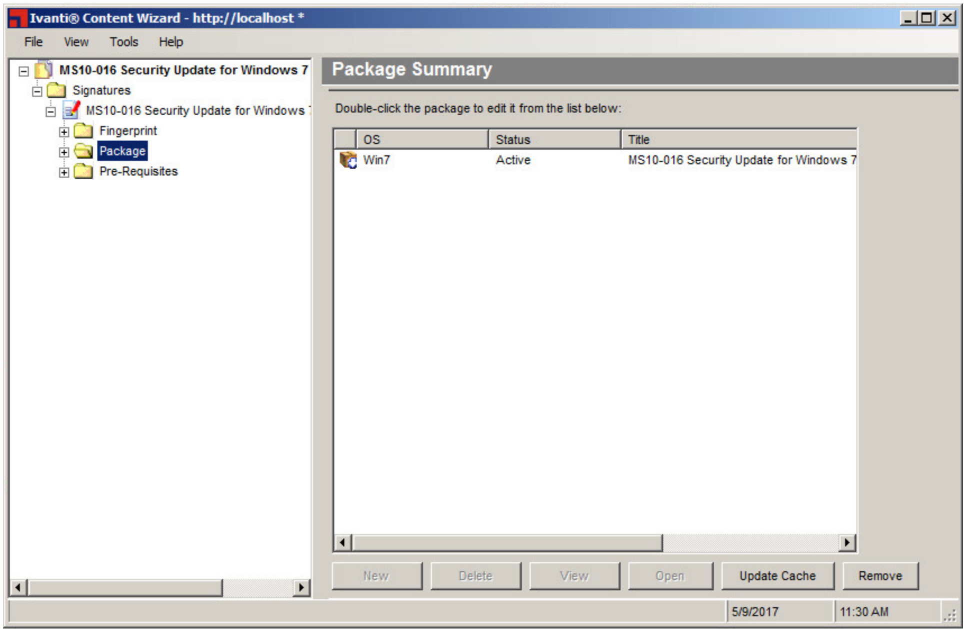

Ivanti® Content Wizard - http://localhost *
File
View
Tools
Help
MS10-016 Security Update for Windows 7
Signatures
MS10-016 Security Update for Windows
Fingerprint
Package
Pre-Requisites
Package Summary
Double-click the package to edit it from the list below:
OS
Status
Title
Win7
Active
MS10-016 Security Update for Windows 7
New
Delete
View
Open
Update Cache
Remove
5/9/2017
11:30 AM

Figure 37: Package Summary Page

The following list describes the buttons on the ***Package Summary*** page.

| Button | Description |
|---|---|
| **New** | Creates and adds a new package to the ***Package Summary*** page. |
| **Delete** | Deletes the currently selected package from this patch, all other patches, and the Ivanti Endpoint Security (Endpoint Security). |
| **View** | Opens the ***Package Properties*** page. For more information, see The Package Properties Page on page 83. |
| **Open** | Adds an existing package to the signature. You can only add one existing package to a signature. For more information, see Adding an Existing Package on page 94. |
| **Update Cache** | Downloads a new copy of the package to the Endpoint Security. |

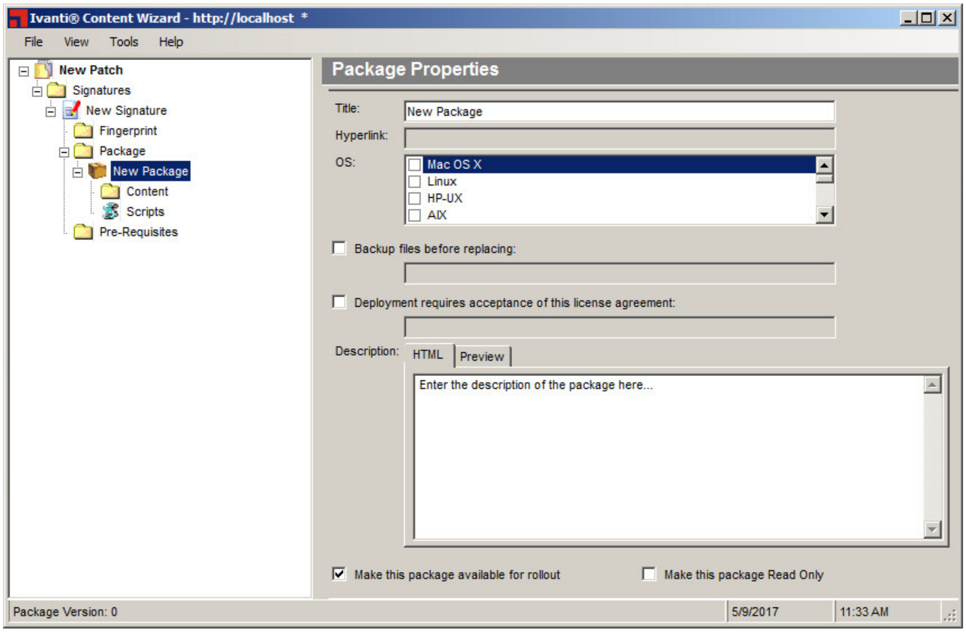
| Button | Description |
|---|---|
| **Remove** | Removes the currently selected package from this patch. For more information, see Removing a Package on page 98. |

**Warning:** The **Delete** button permanently deletes the package from this patch and all other patches. The package can only be recovered if you have previously made a backup (outside of the Endpoint Security) of the package.

## The Package Properties Page

The ***Package Properties*** page defines the applicable operating systems, behavior, and description of a package.

To display the ***Package Properties*** page, select a package and click **View**.



Title: New Package

Hyperlink:

OS: □ Mac OS X □ Linux □ HP-UX □ AIX

□ Backup files before replacing:

□ Deployment requires acceptance of this license agreement:

Description: Enter the description of the package here...

☑ Make this package available for rollout

□ Make this package Read Only

Package Version: 0 5/9/2017 11:33 AM

Figure 38: Package Properties Page

The following list describes the ***Package Properties*** page fields and their functions.

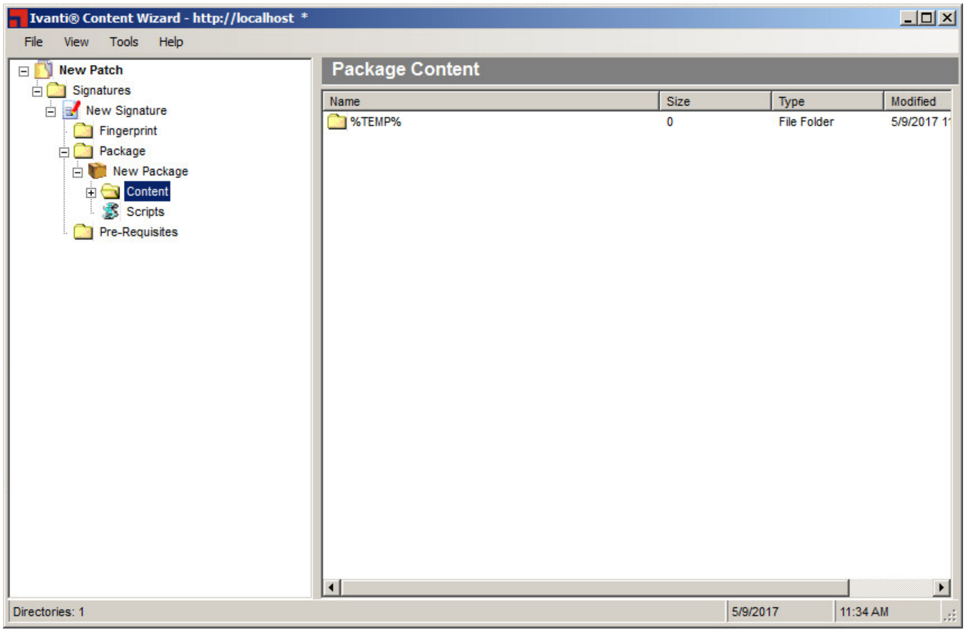
| Properties | Description |
|---|---|
| **Title** | Displays the package name.<br>**Tip:** `New Package` is the given default name and is usually changed to the same name given to its associated signature. |
| **Hyperlink** | References a web page that further defines the package. |

| Properties | Description |
|---|---|
| **OS** | Defines which operating systems to which the package applies. |
| **Backup files before replacing** | Defines the backup directory and enables the Ivanti Content Wizard to archive the files. |
| **Deployment requires acceptance of this license agreement** | Requires that the license and license agreement must be displayed and accepted before deployment of this package. |
| **Description** | Contains a brief description of the package contents. This field also contains Ivanti deployment flags that are interpreted as options within the deployment wizard. |
| **Make this package available for rollout** | Indicates the package is available for deployment. If this check box is not selected, the package will not be deployed. |
| **Make this package Read Only** | Indicates the package will be read-only. |

# The Package Content Page

The ***Package Content*** page displays the files and directories included in the package.

To display the ***Package Content*** page, click on the **Content** folder within the selected package in the left pane.



| Name | Size | Type | Modified |
|---|---|---|---|
| %TEMP% | 0 | File Folder | 5/9/2017 1' |

Directories: 1 | 5/9/2017 | 11:34 AM

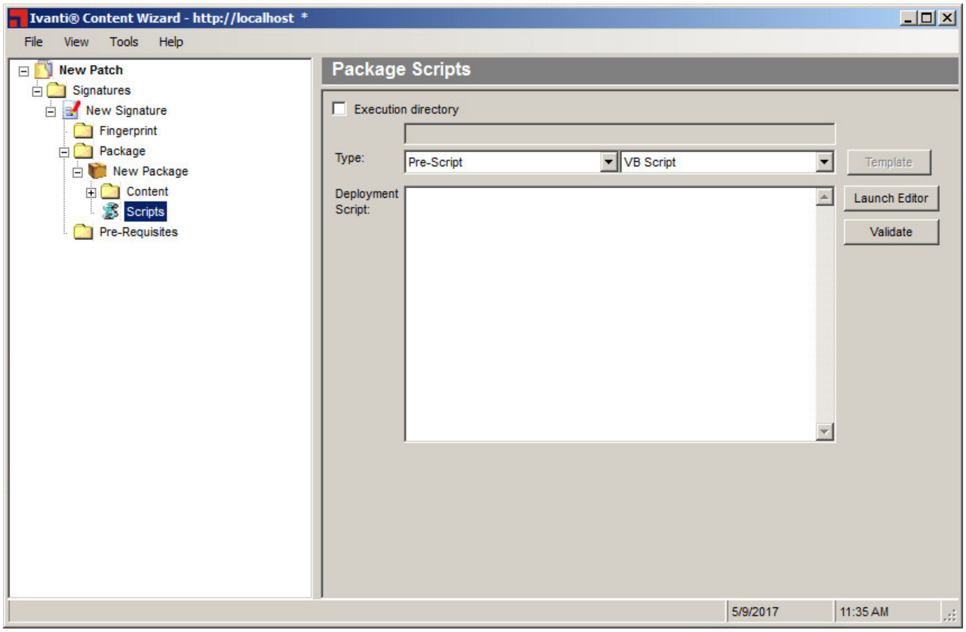
Figure 39: Package Content Page

For more information on adding files to the **Content** folder of a package, refer to Adding Content to a Package on page 99.

# The Package Scripts Page

The ***Package Scripts*** page displays the Pre-Script, Command Line Script, and Post-Script when applicable.

To display the ***Package Scripts*** page, click on the **Scripts** folder within the selected package in the left pane.



□ Execution directory

Type: Pre-Script | VB Script

Deployment Script:

Figure 40: Package Scripts Page

The following list describes the ***Package Scripts*** page fields and their functions.

| Properties | Description |
|---|---|
| **Execution directory** | Displays the directory under which the selected script will execute, preventing the need for full paths in the script. |

| Properties | Description |
|---|---|
| **Type** | Defines the script. The options available are:<br>• **Pre-Script**: Tests the condition of the machine.<br>• **Post-Script**: Performs operations, deletes files, starts services, or opens installers. This can take the form of a VB Script or JScript.<br>• **Command Line Script**: Starts executable files. The format is the same as a standard `.cmd` or `.bat` file.<br>• **VB Script**: Indicates the language option for the script.<br>• **JScript**: Indicates the language option for the script.<br>• **.BAT file**: Runs commands from the command prompt. |
| **Template** | Available for Post-Script type only. Provides an easy way to create scripts on Windows-based patches using simple `.msi`- or `.exe`-based software installation programs. For more information, see Using a Template to Add a Package Script on page 116. |
| **Deployment Script** | Contains the actual script to be executed. |

## Types of Package Scripts

There are three types of package scripts. These scripts can be written in Microsoft Visual Basic Script or Microsoft Jscript.

For more documentation on scripting languages, refer to Introduction to Windows Script Technologies (http://technet.microsoft.com/en-us/library/ee176792.aspx).

A software package can have a maximum of one of each type of script. When all three scripts are present, they will be executed in the following order:

1. Pre-Script: Tests for a condition or shuts down a service on a computer or device. If you're going to use command line scripts, you *must* enter a Pre-script, which should set return code values for

PLCCAgent.SetReturnCode. These values are used later to return deployment results back to the Agent. See the code example below.

```
' Create The Objects
Set Shell = CreateObject("WScript.Shell"): Set FSO =CreateObject("Scripting.FileSystemObject")

Set windir = FSO.GetSpecialFolder(0)

If Err.number Then
  EMsg =  "An error while attempting to create the required objects." & vbNewLine & _

    "Error Number: " & Cstr(Err.number) & vbNewLine & "Error Description: " &
        Err.Description & vbNewLine & vbNewLine
& _
        "NOTE: Please verify that you have Windows Scripting Host 2.0 or higher installed."

  Err.Clear
Else
        'Do other functions
End If

'Stop deployment for error
If LenB(EMsg) Then
  PLCCAgent.SetReturnCode 1, EMsg
Else
'Success
  PLCCAgent.SetReturnCode 0, vbNullString
End If
```

**Note:** You can substitute any error code listed on MSDN in place of '1' to produce a more specific error message.

2. Command Line Script: Starts executable files. The format is the same as a standard `.cmd` or `.bat` file.
3. Post-Script: Performs operations such as the deletion of files, starting services, or running an installer.

**Note:** Unless the **Execution directory** option is selected and a valid directory is defined, all scripts run in the `ROOT` directory.

## Editing a Package Script

You can create or edit a package script from the ***Package Scripts*** page.

**Prerequisites:**

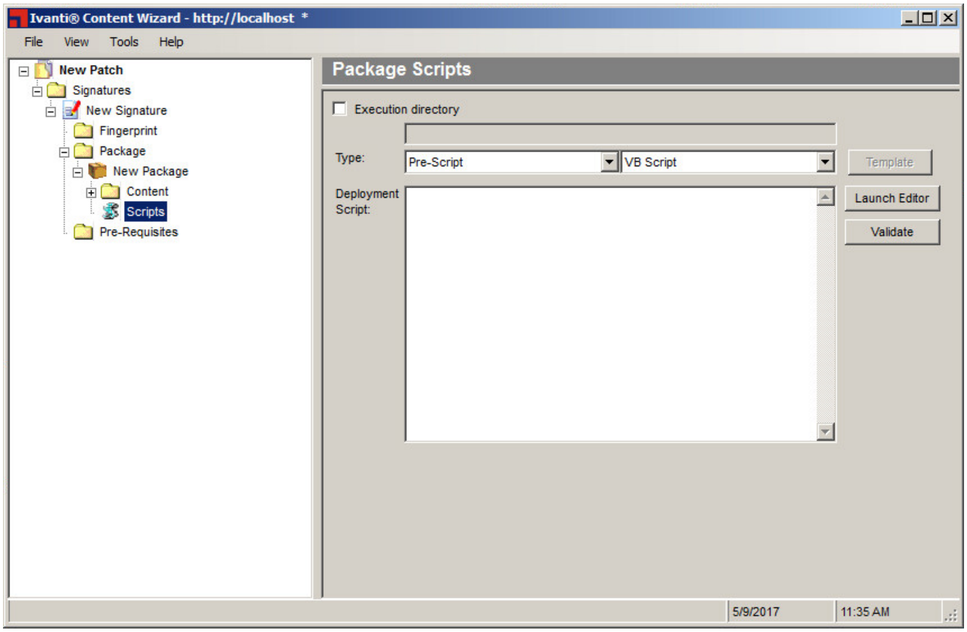
A package for the patch has been created. Refer to Adding a New Package on page 91 for additional information.

Edit existing package script properties from the ***Package Scripts*** page.

1. Expand the patch properties to **Scripts** in the left pane.

   **Example:** ***New Patch*** > **Signatures** > ***New Signature*** > **Package** > ***New Package*** > **Scripts**.

   **Step Result:** The ***Package Scripts*** page opens.



□ Execution directory

Type: Pre-Script | VB Script

Figure 41: Package Scripts Page

2. In the left pane select **Scripts**.
3. Define the directory location.
   a) Select the **Execution directory** check box.

      **Step Result:** The associated directory field becomes active.

   b) Type the directory location from which the selected script will execute in the associated directory field.
4. Select the script type drop-down list items based on your needs.

   The following table describes each script type.

Table 11: Script Types

| Type | Script Language | Description |
|---|---|---|
| **Pre-Script** | | Test the condition on the machine. |
| | **VB Script** | VB Script Language option. |
| | **JScript** | JScript Language option. |

| Type | Script Language | Description |
|---|---|---|
| **Post-Script** | | Performs operations, deletes files, starts services, or open installers. |
| | **VB Script** | VB Script Language option. |
| | **JScript** | JScript Language option. |
| **Command Line Script** | | Starts executable files. The format is the same as a standard `.cmd` or `.bat` file. |

**Tip:** The **Template** button is available for the Post-Script type only and provides an easy way to create scripts on Windows-based patches using simple `.msi`- or `.exe`-based software installation programs. For more information, see Using a Template to Add a Package Script on page 116.

5. [Optional] Use the **Launch Editor** to create a script.
   a) Click **Launch Editor**.

      **Step Result:** A text editor opens.

   b) Edit the script as desired.
   c) Select **File** > **Save**.

      **Step Result:** The text is saved.

   d) Select **File** > **Exit**.

      **Step Result:** The text editor closes and the text displays within the **Deployment Script** panel.

6. Click **Validate**.

   **Step Result:** The package script is validated and a validation message appears.

   **Note:** If a script error occurs, use the text editor to fix the script content prior to continuing.

7. Click **OK**.

   **Step Result:** The validation message closes.

**Result:** The package script is edited.

# Adding Packages

You can create a new package or add an existing package to a patch, depending on your requirements. After adding a package, define its properties.

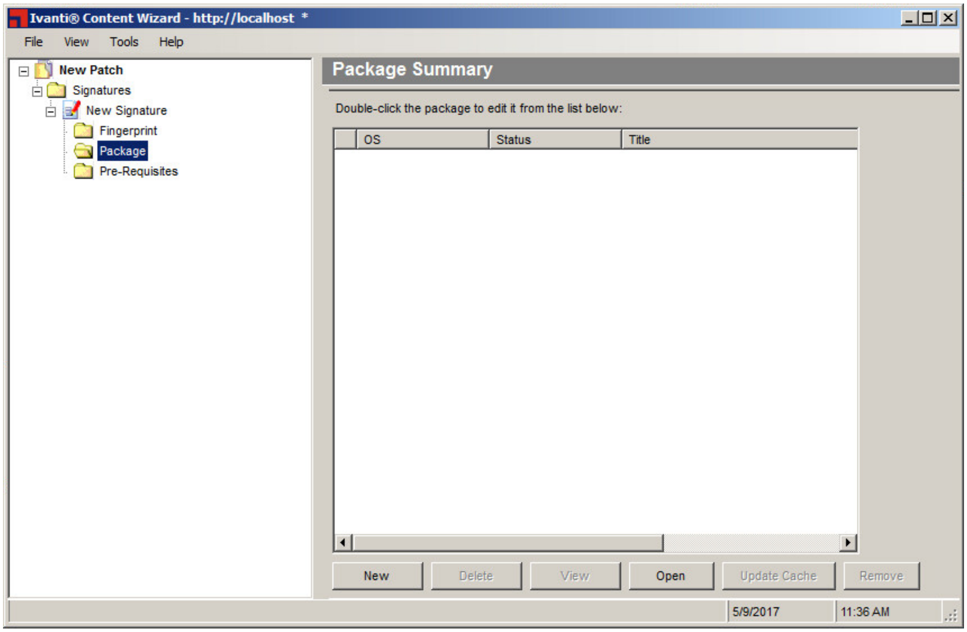
## Adding a New Package

You can add a new package to the patch from the ***Package Summary*** page. After you add the new fingerprint, define its properties in the ***Package Properties*** page.

1. Expand the patch properties to **Package** in the left pane.

   **Example:** ***New Patch*** > **Signatures** > ***New Signature*** > **Package**.

   **Step Result:** The ***Package Summary*** page opens.

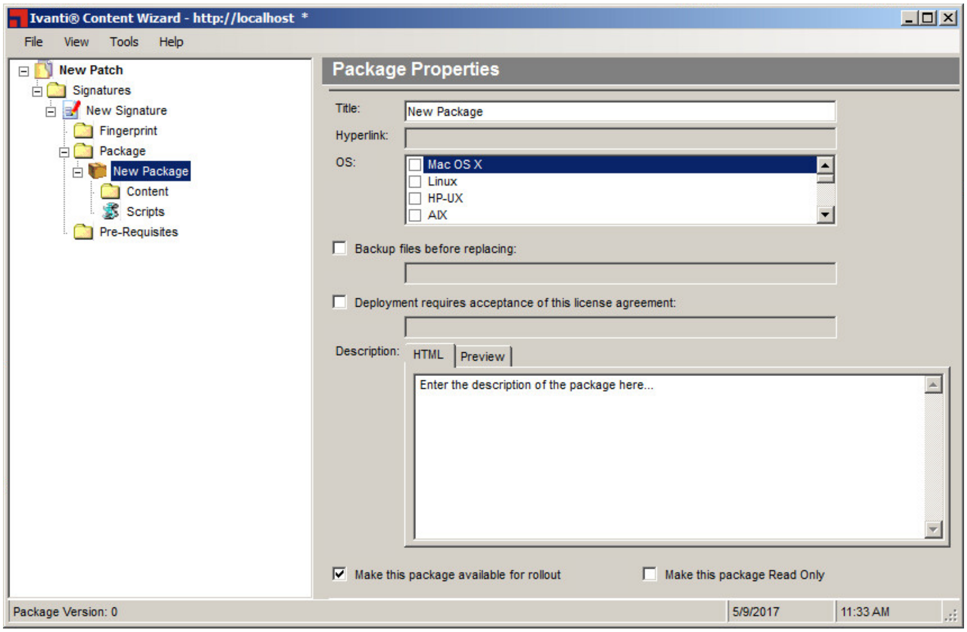


Double-click the package to edit it from the list below:

Figure 42: Package Summary Page

2. Click **New**.

   **Step Result:** The ***Package Properties*** page opens.



Package Properties

Title: New Package

Hyperlink:

OS:
□ Mac OS X
□ Linux
□ HP-UX
□ AIX

□ Backup files before replacing:

□ Deployment requires acceptance of this license agreement:

Description: Enter the description of the package here...

☑ Make this package available for rollout □ Make this package Read Only

Package Version: 0 5/9/2017 11:33 AM

Figure 43: Package Properties Page

3. Modify the package name in the **Title** field.

**Note:** For more information on properties and controls on the ***Package Properties*** page, refer to The Package Properties Page on page 83.

4. Enter a hyperlink to a web page containing further information about the package in the **Hyperlink** field.

5. Select the operating system(s) to which the package applies in the **OS** list.

**Tip:** You must select at least one operating system in order save any changes.

6. [Optional] Enable a file backup.

   a) Select the **Backup files before replacing** check box.

      **Step Result:** The accompanying field becomes available.

   b) Specify the backup directory location in the accompanying field.

7. [Optional] To require the display and acceptance of a license agreement before installing the package.

   a) Select the **Deployment requires acceptance of this license agreement** check box.

      **Step Result:** The accompanying field becomes available.

   b) Type a description in the accompanying field.

8. Type a description of the package in the **Description** field.

9. To enable the package to be deployed, ensure the **Make this package available for rollout** check box is selected.

   The check box is checked by default when a new package is created.

10. [Optional] To make the package read only, select the **Make this package Read Only** check box.

11. Select **File** > **Save**.

**Result:** A new package is created.

**After Completing This Task:**
After creating a package, you need to add content to it. For more information, see Adding Content to a Package on page 99.

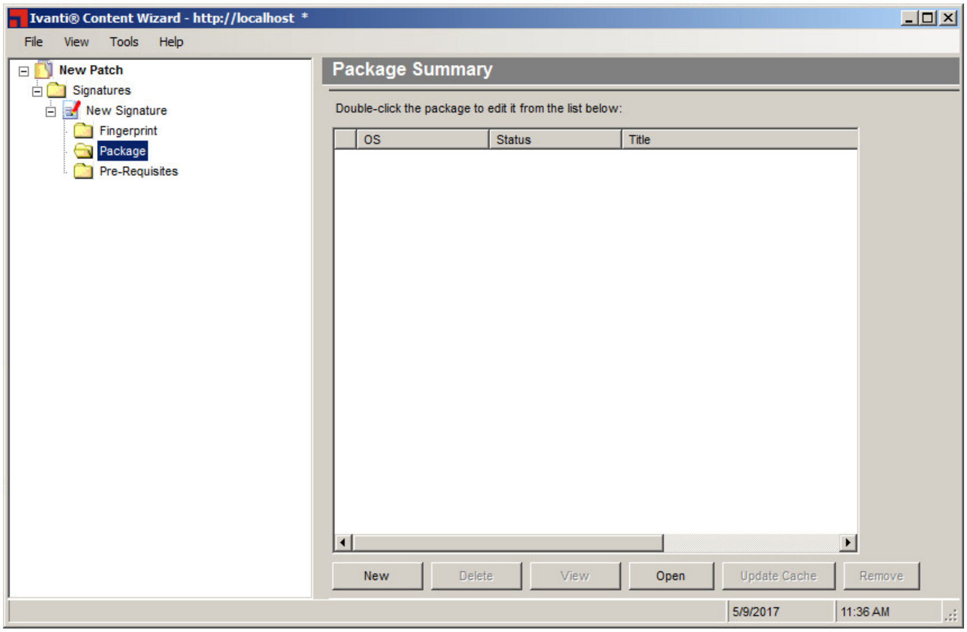
## Adding an Existing Package

If you want to add an existing package to a patch, you can do so from the ***Package Summary*** page. You can add only user-created patches.

1. Expand the patch properties to **Package** in the left pane.

   **Example:** ***New Patch*** > **Signatures** > ***Signature Title*** > **Package**.

   **Step Result:** The ***Package Summary*** page opens.



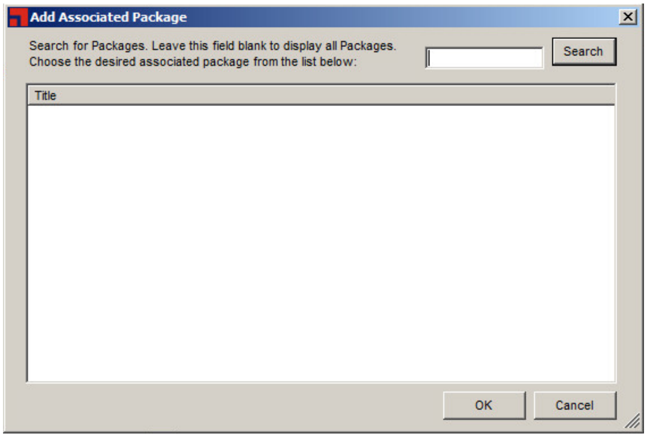
Double-click the package to edit it from the list below:

Figure 44: Package Summary Page

2. Click **Open**.

   **Open** is only available if there is no existing package. You can only add one existing package to a signature.

   **Step Result:** The ***Add Associated Package*** page opens.



Add Associated Package

Search for Packages. Leave this field blank to display all Packages.
Choose the desired associated package from the list below:

Figure 45: Add Associated Package Page

3. Type a package name in the **Search** field.
4. Click **Search**.

   **Step Result:** The packages corresponding to the search term appear in the ***Add Associated Package*** window.

5. Select a package.
6. Click **OK**.

   **Step Result:** The ***Add Associated Package*** window closes and the package displays in the ***Package Summary*** page.

**Result:** The selected existing package is added.

**Note:** You cannot add a package to a patch if it is already included in an existing patch.

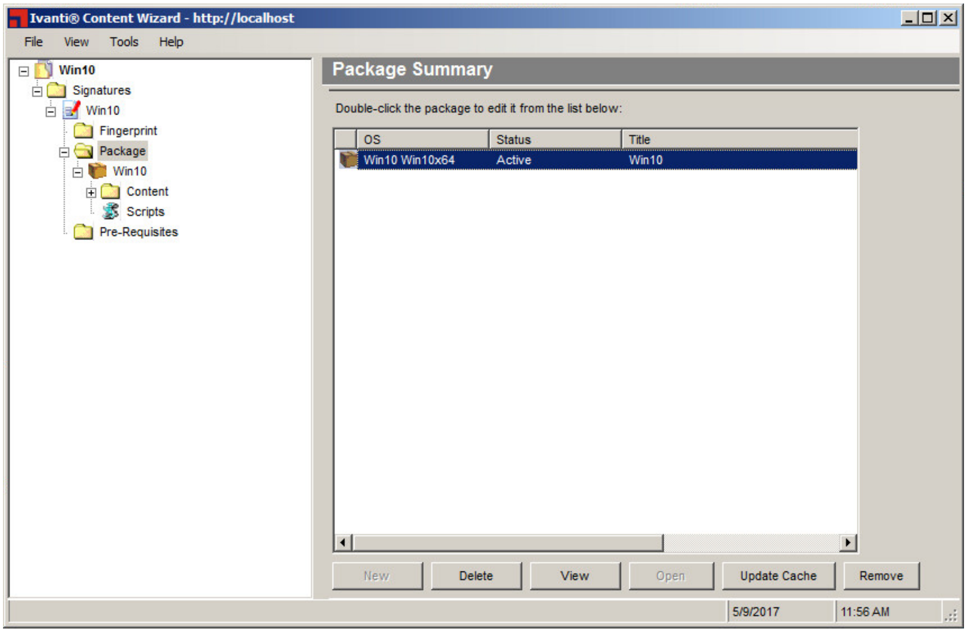
## Editing a Package

You can edit the details associated with a package by selecting the package and then making changes in the ***Package Properties*** page.

1. Expand the patch properties to **Package** in the left pane.

   **Example:** ***New Patch*** > **Signatures** > ***Signature Title*** > **Package**.

   **Step Result:** The ***Package Summary*** page opens.



Double-click the package to edit it from the list below:

| OS | Status | Title |
|---|---|---|
| Win10 Win10x64 | Active | Win10 |

Figure 46: Package Summary Page

2. Select the package you want to edit in the ***Package Summary*** page.
3. Click **View**.

**Tip:** Within the pane, you may double-click on a package to open the ***Package Properties*** page.

4. Modify the package name in the **Title** field.

**Note:** For more information on properties and controls on the ***Package Properties*** page, refer to The Package Properties Page on page 83.

5. Enter a hyperlink to a web page containing further information about the package in the **Hyperlink** field.

6. Select the operating system(s) to which the package applies in the **OS** list.

   **Tip:** You must select at least one operating system in order save any changes.

7. [Optional] Enable a file backup.
   a) Select the **Backup files before replacing** check box.

      **Step Result:** The accompanying field becomes available.

   b) Specify the backup directory location in the accompanying field.
8. [Optional] To require the display and acceptance of a license agreement before installing the package.
   a) Select the **Deployment requires acceptance of this license agreement** check box.

      **Step Result:** The accompanying field becomes available.

   b) Type a description in the accompanying field.
9. Type a description of the package in the **Description** field.
10. To enable the package to be deployed, ensure the **Make this package available for rollout** check box is selected.

    The check box is checked by default when a new package is created.
11. [Optional] To make the package read only, select the **Make this package Read Only** check box.
12. Select **File** > **Save**.

**Result:** The package properties are changed.

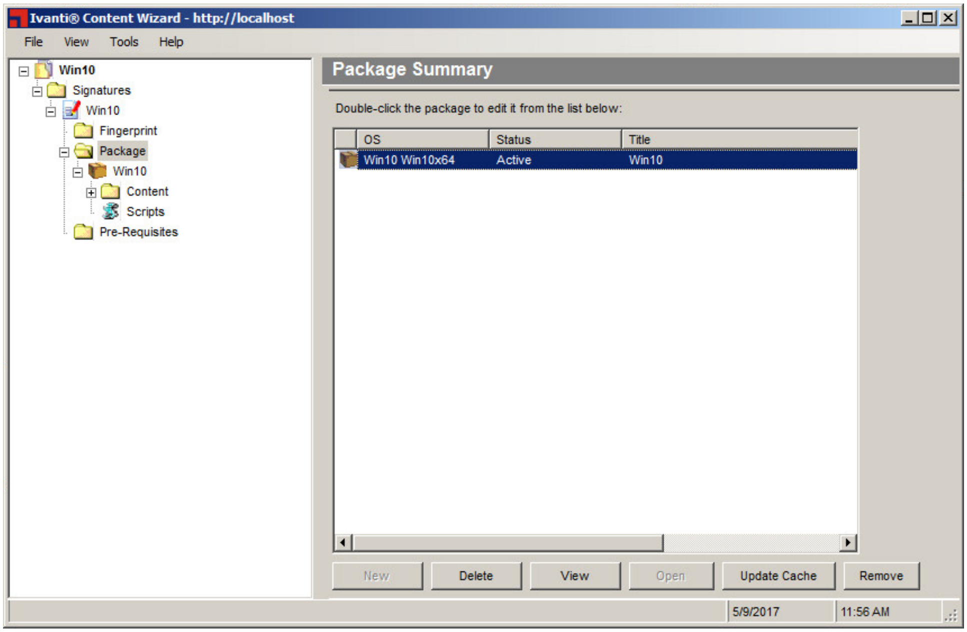
## Removing a Package

If you no longer need a package, you can remove it from the patch in the ***Package Summary*** page.

1. Expand the patch properties to **Package** in the left pane.

   **Example:** ***New Patch*** > **Signatures** > ***Signature Title*** > **Package**.

   **Step Result:** The ***Package Summary*** page opens.



Double-click the package to edit it from the list below:

| OS | Status | Title |
|---|---|---|
| Win10 Win10x64 | Active | Win10 |

Figure 47: Package Summary Page

2. In the pane select the package you want to remove.
3. Click **Delete**.

   **Step Result:** A confirmation message appears.

4. Click **OK**.

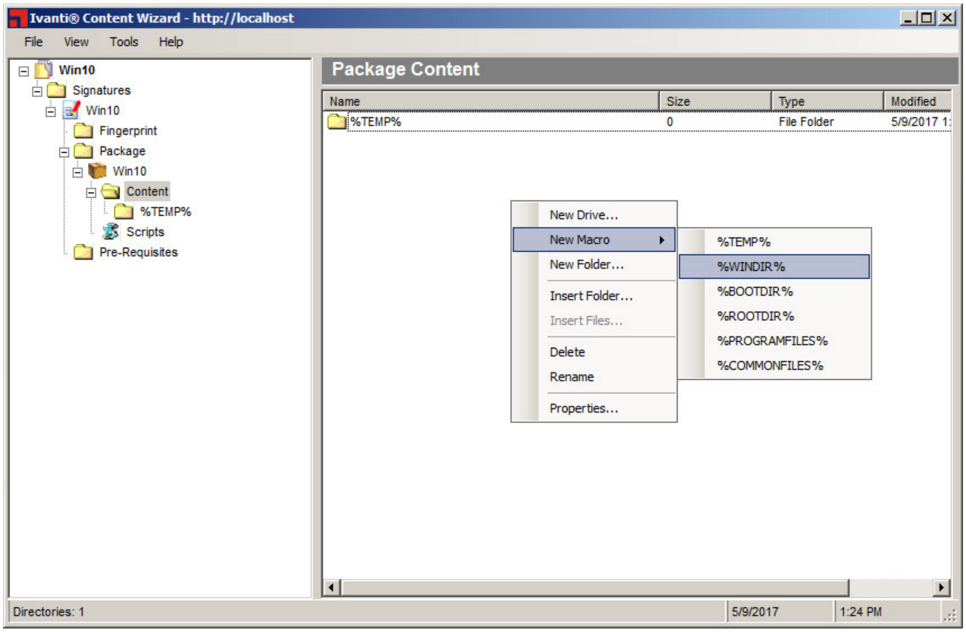
   **Step Result:** The confirmation message dialog closes.

**Result:** The selected package is removed from the patch.

> **Note:** Removing a package from a patch does not delete the package from the Ivanti Content Wizard database.

## Adding Content to a Package

The ***Package Content*** page allows you to add files and directories to the package. Right-click inside the ***Package Content*** page and select one of the available content types.



| Name | Size | Type | Modified |
|---|---|---|---|
| %TEMP% | 0 | File Folder | 5/9/2017 1: |

Figure 48: Package Content Page: Content Types

When you right-click inside the ***Package Content*** page, the following options are available:

| Option | Description |
|---|---|
| **New Drive** | Allows you to add a new drive to a package. For more information, see Adding a New Drive to a Package on page 100. |
| **New Macro** | Allows you to add a new macro to a package. For more information, see Adding a New Macro to a Package on page 101. |
| **New Folder** | Allows you to add a new folder to a package. For more information, see Adding a New Folder to a Package on page 106. |
| **Insert Folder** | Allows you to add an existing folder to a package. For more information, see Inserting a Folder into a Package on page 107. |
| **Insert Files** | Allows you to add an existing file to a package. For more information, see Inserting a File into a Package on page 110. |
| **Delete** | Allows you to delete a file from a package. For more information, see Deleting a File from a Package on page 111. |

| Option | Description |
|---|---|
| **Rename** | Allows you to rename a file within a package. For more information, see Renaming a File in a Package on page 113. |
| **Properties** | Allows you to modify the file properties within a package. For more information, see Overwriting the Properties of a File in a Package on page 114. |

## Adding a New Drive to a Package

Use the **New Drive** option to deploy a package to a drive other than the `C:\` or `%TEMP%` drives.

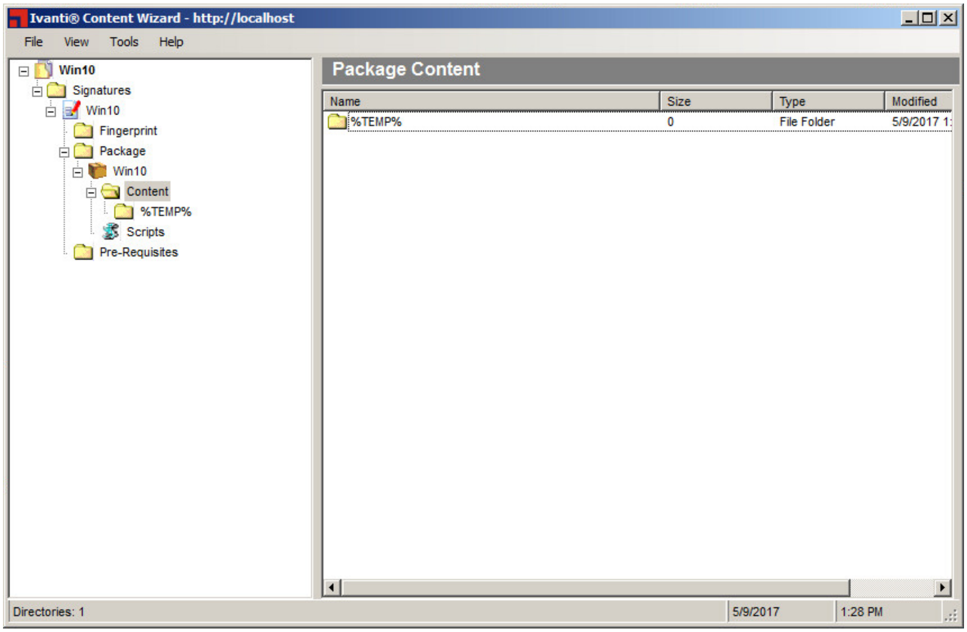
**Prerequisites:**

Create a package for the patch. For more information about creating packages, see Adding a New Package on page 91.

1. Expand the patch properties in the left pane to **Content**.

   **Example:** ***New Patch*** > **Signatures** > ***New Signature*** > **Package** > ***New Package*** > **Content**.

   **Step Result:** The ***Package Content*** page opens.



| Name | Size | Type | Modified |
|---|---|---|---|
| %TEMP% | 0 | File Folder | 5/9/2017 1: |

Figure 49: Package Content Page

2. Right-click in the pane inside the ***Package Content*** page.

   **Step Result:** The **Content Types** menu appears.

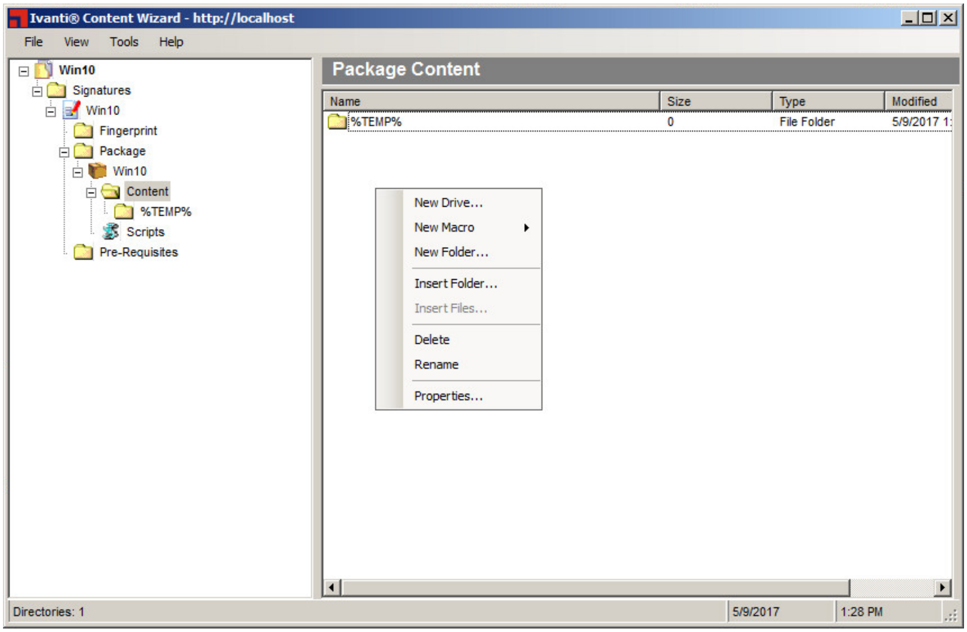


Figure 50: Content Types Menu

3. Select **New Drive**.

   **Step Result:** The ***Create Drive*** dialog opens.

4. In the **Drive or Volume Name** field, type the letter you require for the drive name, followed by a colon.

   **Example:** `X:`

5. Click **OK**.

   **Step Result:** The ***Create Drive*** dialog closes.

**Result:** The drive is added to the ***Package Content*** page.

## Adding a New Macro to a Package

Use the **New Macro** option to deploy a package across existing system directories.

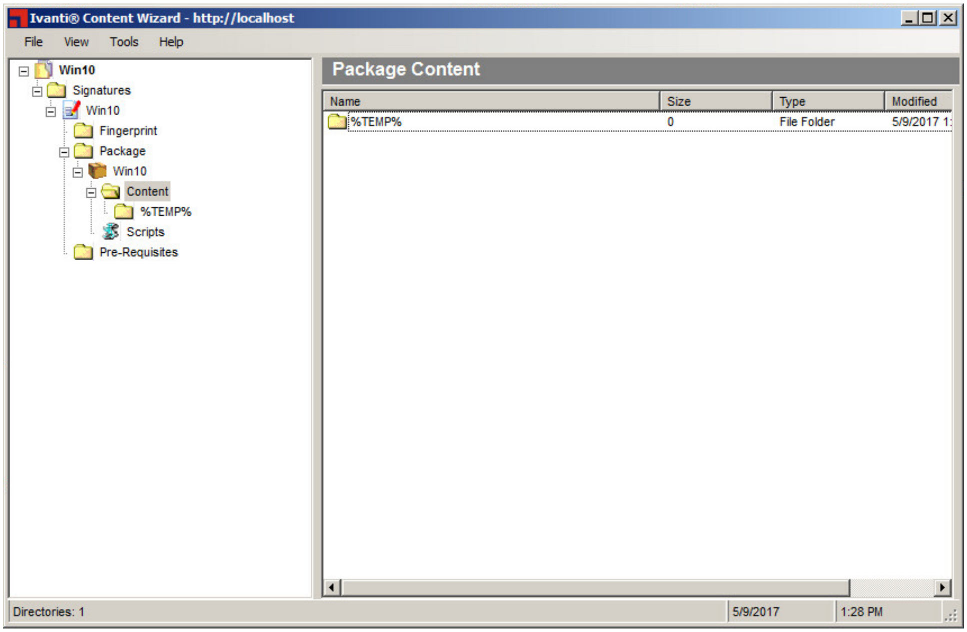
**Prerequisites:**

Create a package for the patch. For more information about creating packages, see Adding a New Package on page 91.

1. Expand the patch properties in the left pane to **Content**.

   **Example:** ***New Patch*** > **Signatures** > ***New Signature*** > **Package** > ***New Package*** > **Content**.

   **Step Result:** The ***Package Content*** page opens.



| Name | Size | Type | Modified |
|---|---|---|---|
| %TEMP% | 0 | File Folder | 5/9/2017 1: |

Figure 51: Package Content Page

2. Right-click in the pane inside the ***Package Content*** page.

   **Step Result:** The **Content Types** menu appears.

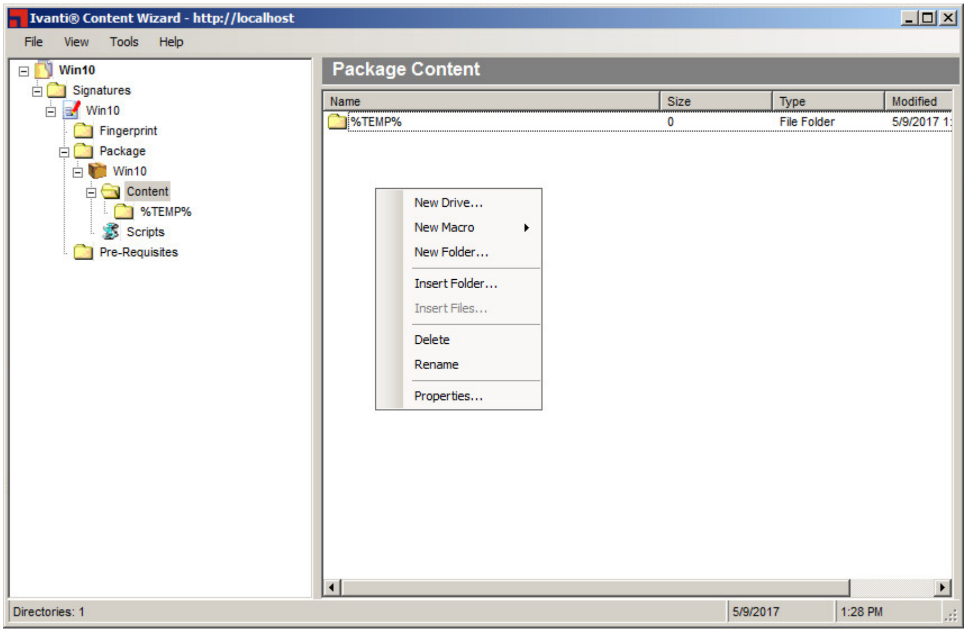


Figure 52: Content Types Menu

3. Select **New Macro**.

   **Step Result:** The ***Macros Types*** menu opens.

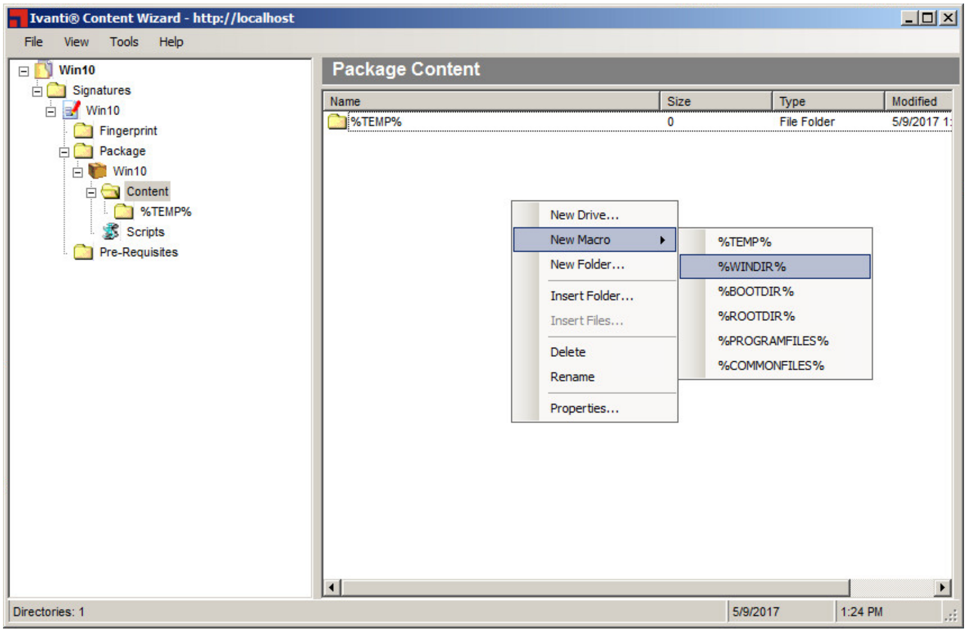
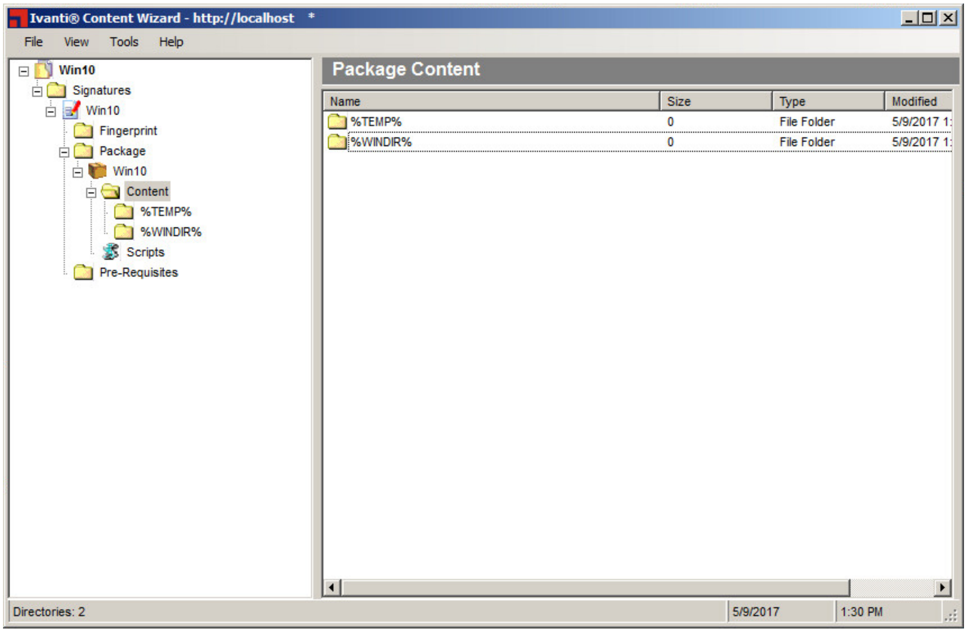


Figure 53: Macros Types Menu

4. Select the type of macro to add to the package.

   For more information on the types of macros available, see Types of Macros on page 105.

**Result:** The selected macro is added to the ***Package Content*** page.



| Name | Size | Type | Modified |
|---|---|---|---|
| %TEMP% | 0 | File Folder | 5/9/2017 1: |
| %WINDIR% | 0 | File Folder | 5/9/2017 1: |

Directories: 2 5/9/2017 1:30 PM

Figure 54: Package Content Page

### Types of Macros

The ***New Macro*** menu allows you to add macros to a package. A macro can be either an environment variable as defined by the operating system, or a macro that only the Agent can expand.

The following predefined macros are available in the ***New Macro*** menu:

| Macro Type | Description |
|---|---|
| **%TEMP%** | The operating system's temp directory location. This macro expands to `C:\Windows\Temp`, `C:\Temp`, `C:\WinNT\Temp`, or `/tmp` depending upon the operating system and configuration. |
| **%WINDIR%** | The operating system's windows directory location. This macro typically expands to `C:\Windows`. |
| **%BOOTDIR%** | The operating system's boot directory location. This macro typically expands to `C:\`. |
| **%ROOTDIR%** | The operating system's root directory location. This macro typically expands to `C:\`. |

| Macro Type | Description |
|---|---|
| **%PROGRAM FILES%** | The operating system's program files location. This macro typically expands to `C:\Program Files`. |
| **%COMMONFILES%** | The operating system's common files location. This macro typically expands to `C:\`. |

## Adding a New Folder to a Package

Use the **New Folder** option to create a folder inside the package.

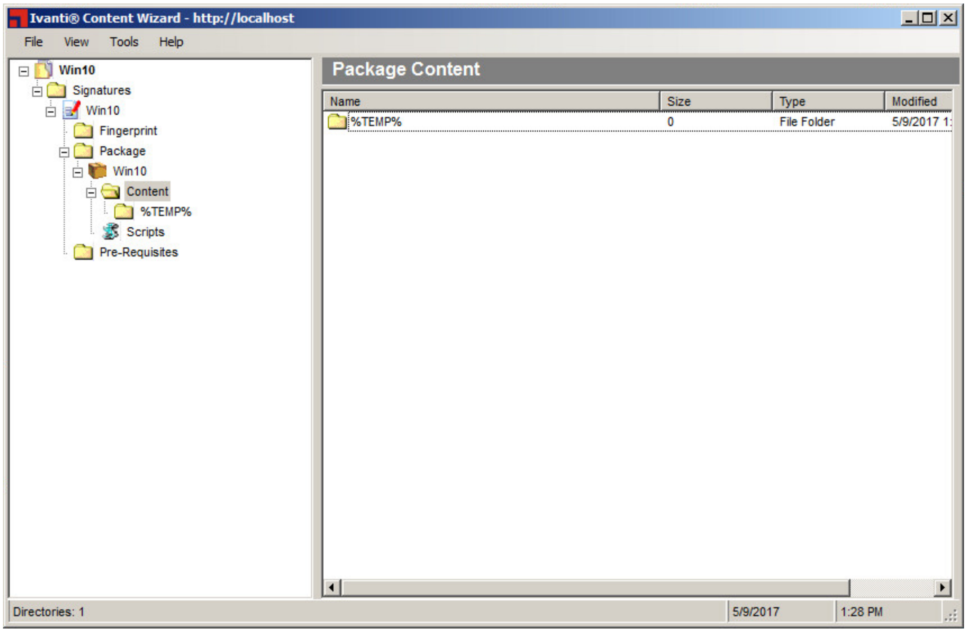
**Prerequisites:**

Create a package for the patch. For more information about creating packages, see Adding a New Package on page 91.

1. Expand the patch properties in the left pane to **Content**.

   **Example:** ***New Patch*** > **Signatures** > ***New Signature*** > **Package** > ***New Package*** > **Content**.

   **Step Result:** The ***Package Content*** page opens.

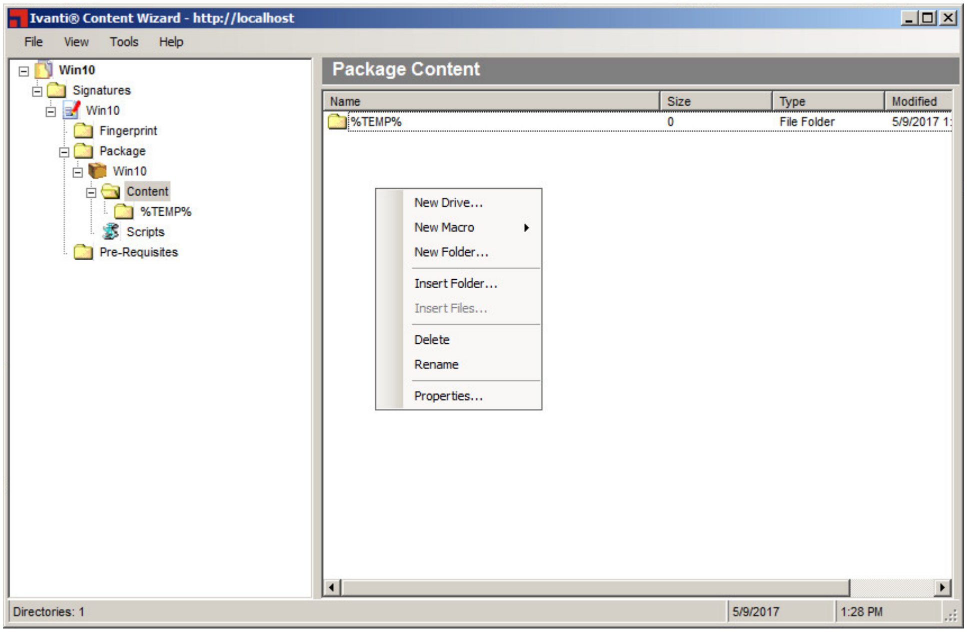


| Name | Size | Type | Modified |
|---|---|---|---|
| %TEMP% | 0 | File Folder | 5/9/2017 1: |

Figure 55: Package Content Page

2. Right-click in the pane inside the ***Package Content*** page.

   **Step Result:** The **Content Types** menu appears.



| Name | Size | Type | Modified |
|---|---|---|---|
| %TEMP% | 0 | File Folder | 5/9/2017 1: |

Directories: 1 | 5/9/2017 | 1:28 PM

Figure 56: Content Types Menu

3. Select **New Folder**.

   **Step Result:** The ***Create Folder*** dialog opens.

4. In the **Folder Name** field, type the name of the new folder.
5. Click **OK**.

   **Step Result:** The ***Create Folder*** dialog closes.

**Result:** The folder is added to the ***Package Content*** page.

## Inserting a Folder into a Package

Use the **Insert Folder** option to locate and select an existing directory to add to the package.

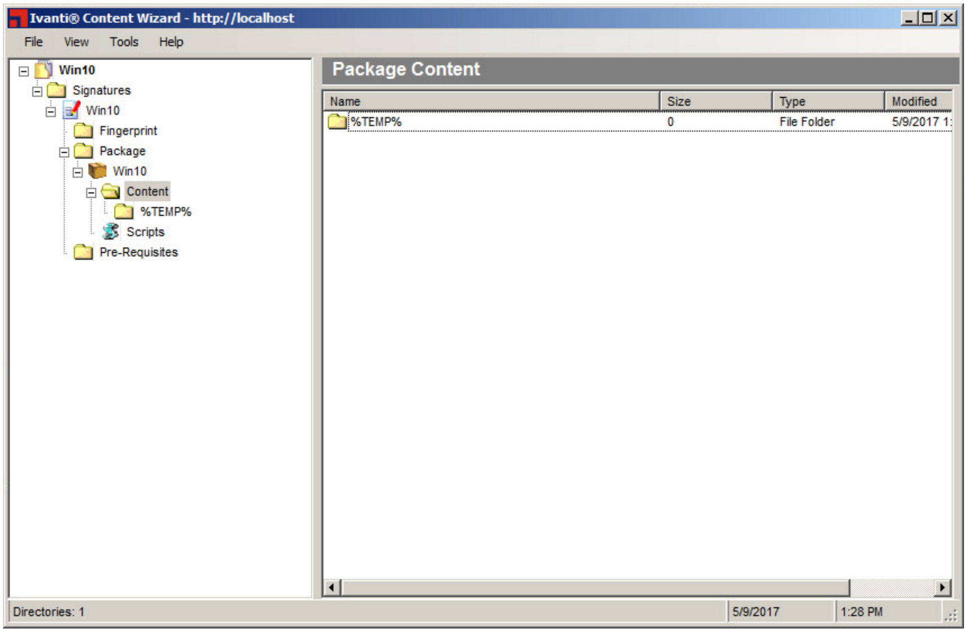
**Prerequisites:**

Create a package for the patch. For more information about creating packages, see Adding a New Package on page 91.

1. Expand the patch properties in the left pane to **Content**.

   **Example:** ***New Patch*** > **Signatures** > ***New Signature*** > **Package** > ***New Package*** > **Content**.

   **Step Result:** The ***Package Content*** page opens.



| Name | Size | Type | Modified |
|---|---|---|---|
| %TEMP% | 0 | File Folder | 5/9/2017 1: |

Directories: 1 | 5/9/2017 | 1:28 PM

Figure 57: Package Content Page

**2.** Right-click in the pane inside the ***Package Content*** page.

**Step Result:** The **Content Types** menu appears.

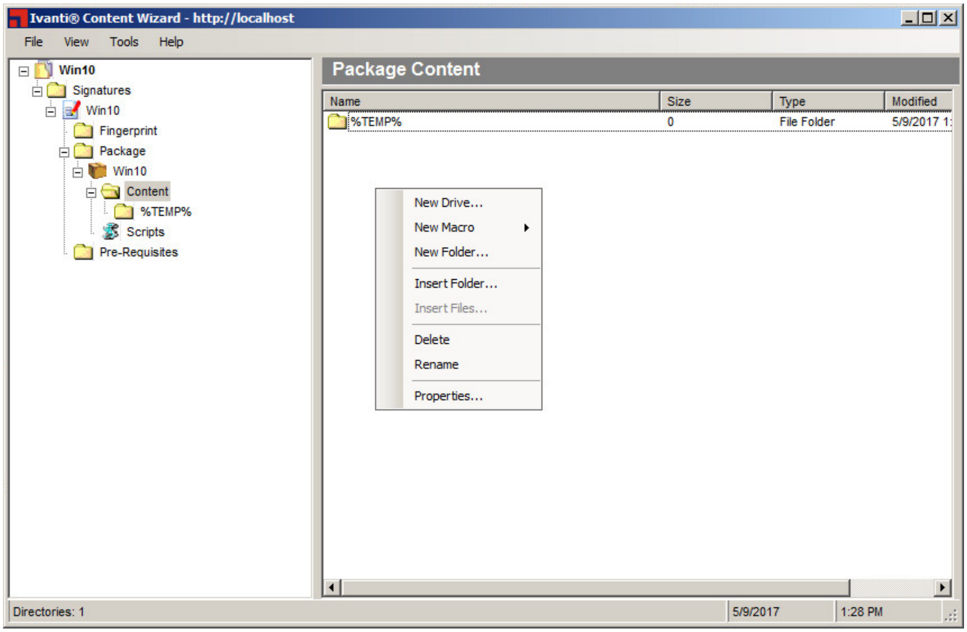


Figure 58: Content Types Menu

**3.** Select **Insert Folder**.

**Step Result:** The ***Insert Folder*** dialog opens.

**4.** Select the folder you need for the package.

**Note:** Select **Insert Folder** option inserts the folder and all folder content to the package. To insert individual file content, refer to Inserting a File into a Package on page 110 for instruction.

**5.** Click **OK**.

**Step Result:** The ***Insert Folder*** dialog closes and the folder is added to the ***Package Content*** window.

**Tip:** In addition to the procedure described above, you can add folders to a package using drag and drop. Select the folder that you want to add, then drag and drop it into the ***Package Content*** window.

**Result:** The folder is added to the ***Package Content*** page.

## Inserting a File into a Package

Use the **Insert File** option to locate and select an existing file to add to a folder in the package.

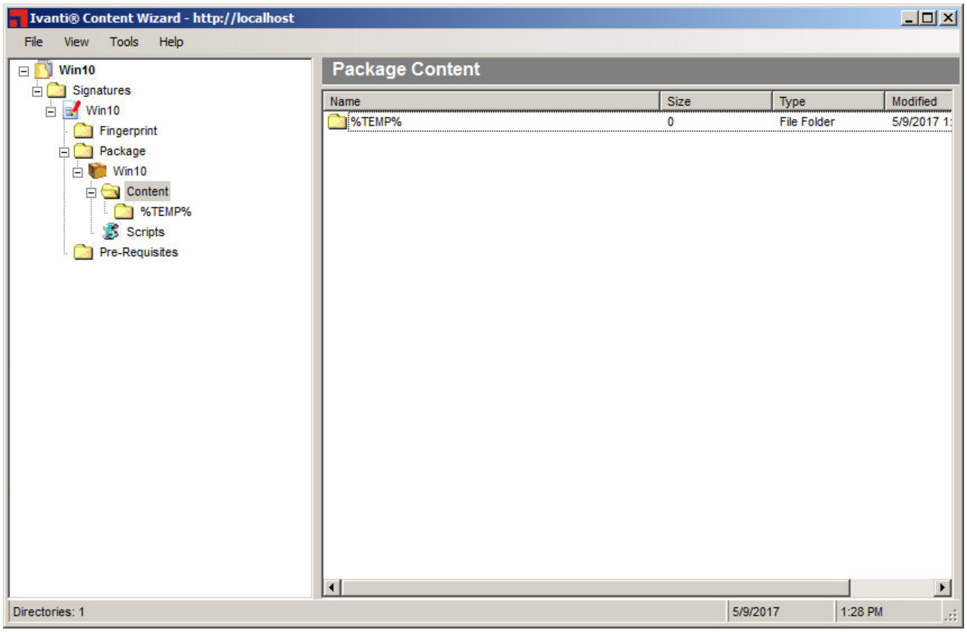
**Prerequisites:**

- Create a package for the patch. For more information, see Adding a New Package on page 91.
- Create a folder for the package. For more information, see Adding a New Folder to a Package on page 106.

1. Expand the patch properties in the left pane to **Content**.

   **Example:** ***New Patch*** > **Signatures** > ***New Signature*** > **Package** > ***New Package*** > **Content**.

   **Step Result:** The ***Package Content*** page opens.



| Name | Size | Type | Modified |
|---|---|---|---|
| %TEMP% | 0 | File Folder | 5/9/2017 1: |

Directories: 1 | 5/9/2017 | 1:28 PM

Figure 59: Package Content Page

2. In the left pane, select a folder directory beneath **Content**.

   **Tip:** The `%Temp%` folder is the default folder when a new package is created.

   **Step Result:** A blank ***Package Content*** page opens.

3. Right-click in the pane inside the ***Package Content*** page.

   **Step Result:** The **Content Types** menu appears.

4. Select **Insert Files**.

   **Step Result:** The ***Open*** window opens.

5. Select the file you need for the package.
6. Click **Open**.

   **Step Result:** The ***Open*** window closes and the package is added to the ***Package Content*** page.

**Result:** The file is added to the ***Package Content*** page.

## Deleting a File from a Package

Use the **Delete** option to remove a selected file from a folder in the package.

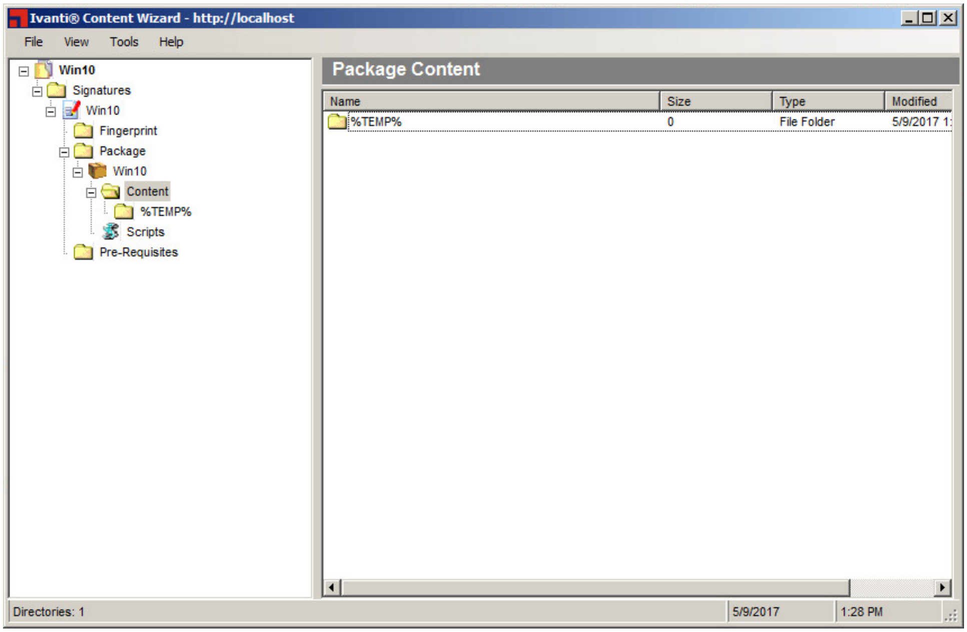
**Prerequisites:**

- Create a package for the patch. For more information, see Adding a New Package on page 91.
- Create a folder for the package. For more information, see Adding a New Folder to a Package on page 106.
- Insert files into the package folder. For more information, see Inserting a File into a Package on page 110.

1. Expand the patch properties in the left pane to **Content**.

   **Example:** ***New Patch*** > **Signatures** > ***New Signature*** > **Package** > ***New Package*** > **Content**.

   **Step Result:** The ***Package Content*** page opens.



| Name | Size | Type | Modified |
|---|---|---|---|
| %TEMP% | 0 | File Folder | 5/9/2017 1: |

Directories: 1 | 5/9/2017 | 1:28 PM

Figure 60: Package Content Page

2. In the left pane under **Content** select the folder containing the file to be deleted.

   **Step Result:** The ***Package Content*** page for the selected folder opens.

3. In the pane, select the file you want to delete and right-click.

   **Step Result:** The **Content Types** menu appears.

   > **Tip:** You may select multiple, non-concurrent items by using `CTRL+Click` within the ***Package Content*** page.

4. Select **Delete**.

   **Step Result:** The file is removed.

5. Verify that the deleted file does not appear in the ***Package Content*** page.

**Result:** The file is deleted from the selected folder.

## Renaming a File in a Package

Use the **Rename** option to edit the filenames of files in a package.

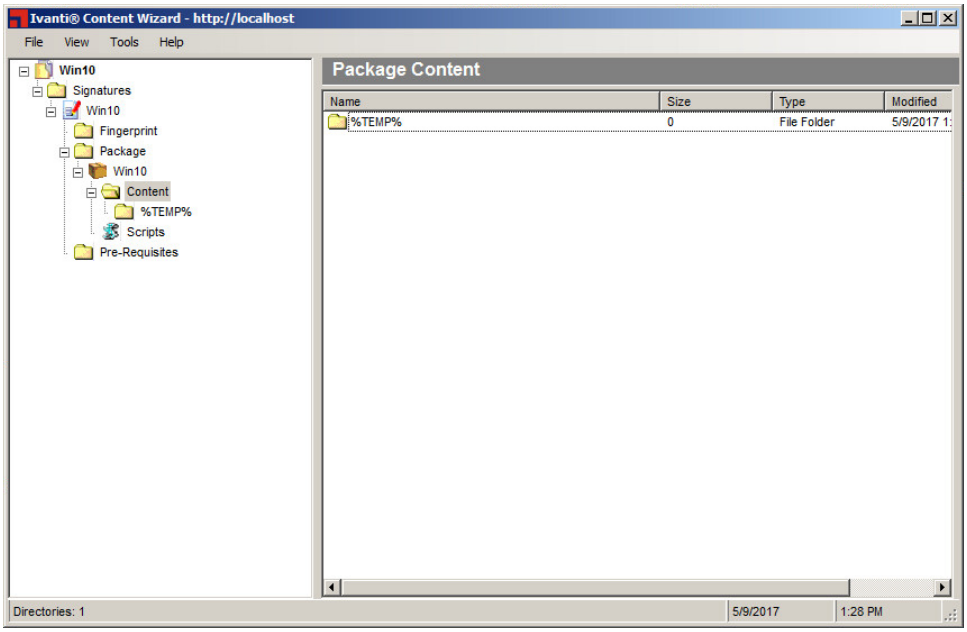
**Prerequisites:**

- Create a package for the patch. For more information, see Adding a New Package on page 91.
- Create a folder for the package. For more information, see Adding a New Folder to a Package on page 106.
- Insert files into the package folder. For more information, see Inserting a File into a Package on page 110.

**1.** Expand the patch properties in the left pane to **Content**.

**Example:** ***New Patch*** > **Signatures** > ***New Signature*** > **Package** > ***New Package*** > **Content**.

**Step Result:** The ***Package Content*** page opens.



| Name | Size | Type | Modified |
|---|---|---|---|
| %TEMP% | 0 | File Folder | 5/9/2017 1: |

Directories: 1 | 5/9/2017 | 1:28 PM

Figure 61: Package Content Page

**2.** In the left pane under **Content** select the folder containing the file you want to rename.

**Step Result:** The ***Package Content*** page for the selected folder opens.

**3.** In the pane, select the file you want to rename and right-click.

**Step Result:** The **Content Types** menu appears.

4. Select **Rename**.

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

5. Type the new filename in the **Enter new filename:** field.
6. Click **OK**.

   **Step Result:** The ***Rename*** dialog closes.

7. Verify that the new filename appears in the ***Package Content*** page.

**Result:** The filename is changed.

## Overwriting the Properties of a File in a Package

Use the **Properties** option to view and edit file properties in a package.

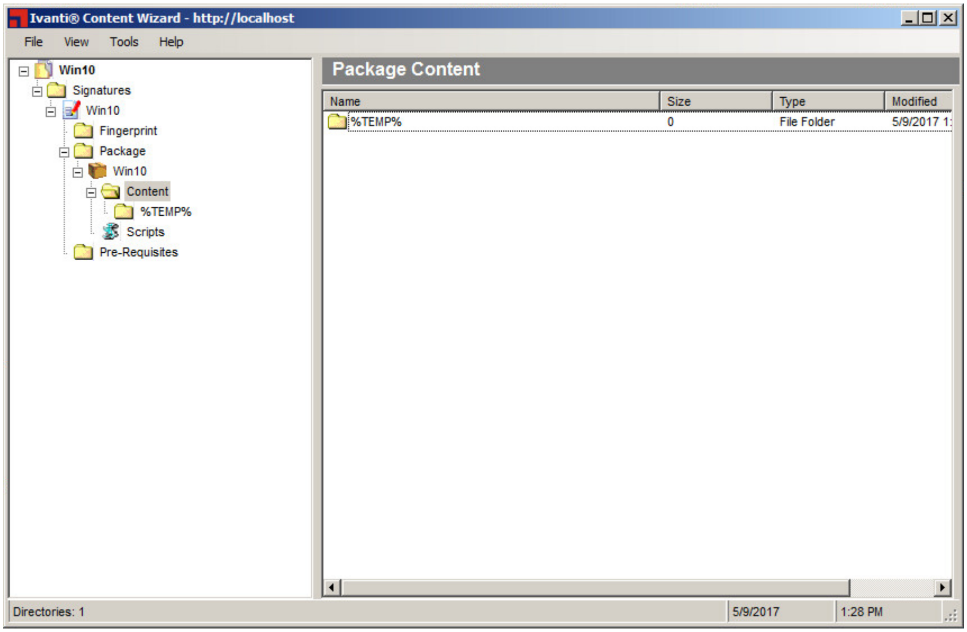
**Prerequisites:**

- Create a package for the patch. For more information, see Adding a New Package on page 91.
- Create a folder for the package. For more information, see Adding a New Folder to a Package on page 106.
- Insert files into the package folder. For more information, see Inserting a File into a Package on page 110.

1. Expand the patch properties in the left pane to **Content**.

   **Example:** ***New Patch*** > **Signatures** > ***New Signature*** > **Package** > ***New Package*** > **Content**.

   **Step Result:** The ***Package Content*** page opens.



| Name | Size | Type | Modified |
|---|---|---|---|
| %TEMP% | 0 | File Folder | 5/9/2017 1: |

Figure 62: Package Content Page

2. In the left pane under **Content** select the folder containing the file you want to edit.

   **Step Result:** The ***Package Content*** page for the selected folder opens.

3. In the pane, select the file you want to edit and right-click.

   **Step Result:** The **Content Types** menu appears.

4. Select **Properties**.

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

5. [Optional] Rename the file, if applicable.
6. [Optional] Edit the **Overwritable** check box, if applicable.

> **Warning:** Removing the check mark from the **Overwritable** check box prevents subsequent patches that contain the same file from overwriting that file.

7. Edit the **Compressed** check box, if applicable.
8. Click **Apply**.

   **Step Result:** The file properties are changed.

9. Click **OK**.

   **Step Result:** The ***Properties*** dialog closes.

**Result:** The file properties are changed.

## Using a Template to Add a Package Script

The Ivanti Content Wizard contains templates to assist users in creating package scripts. The templates use `.msi`- or `.exe`-based software installation programs.

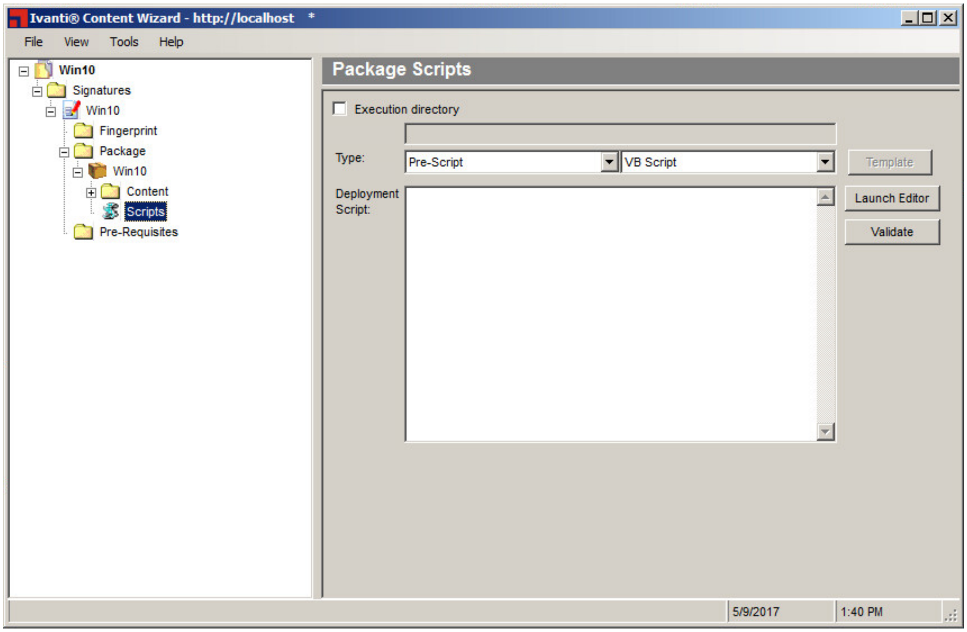
**Prerequisites:**

- Create a package for the patch. For more information, see Adding a New Package on page 91.
- Add content to the package. For more information, see Adding Content to a Package on page 99.

1. Expand the patch properties to **Scripts** in the left pane.

   **Example:** ***New Patch*** > **Signatures** > ***New Signature*** > **Package** > ***New Package*** > **Scripts**.

   **Step Result:** The ***Package Scripts*** page opens.



□ Execution directory

Type: Pre-Script VB Script

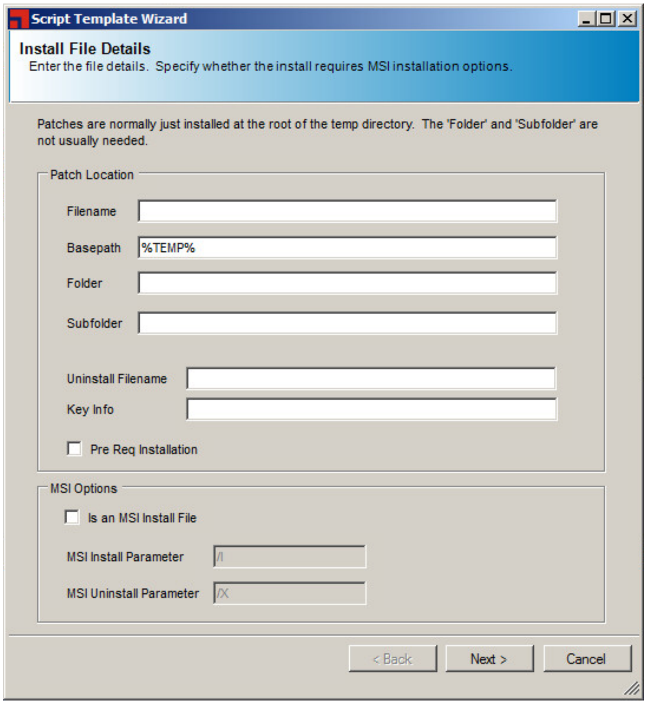
Deployment Script:

5/9/2017 1:40 PM

Figure 63: Package Scripts Page

2. Click **Template**.

   **Step Result:** The ***Script Template Wizard*** opens.



Script Template Wizard

Install File Details

Enter the file details. Specify whether the install requires MSI installation options.

Patches are normally just installed at the root of the temp directory. The 'Folder' and 'Subfolder' are not usually needed.

Patch Location

Filename:

Basepath: %TEMP%

Folder:

Subfolder:

Uninstall Filename:

Key Info:

□ Pre Req Installation

MSI Options

□ Is an MSI Install File

MSI Install Parameter: /I

MSI Uninstall Parameter: /X

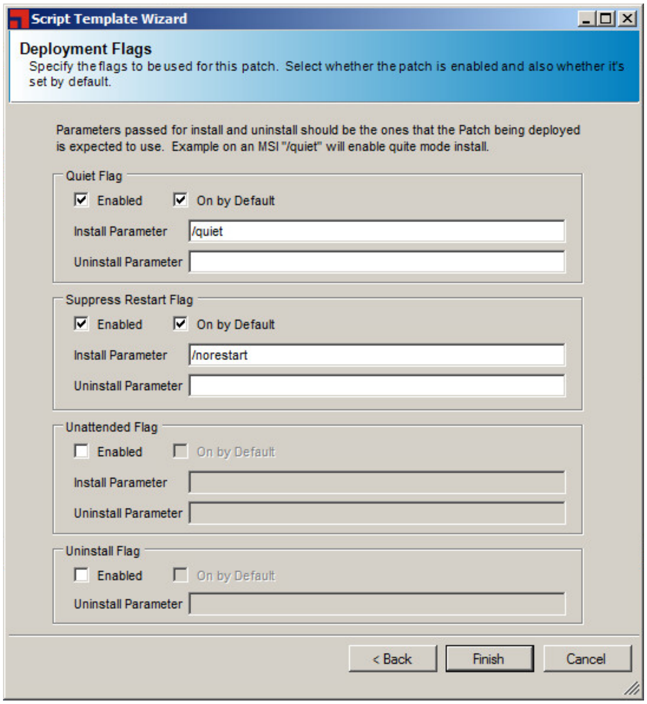
Figure 64: Script Template Wizard

3. Specify the patch details.
   a) Type a name for the script in the **Filename** field.
   b) Type the location of the installable file in the **Basepath** field.

      By default, files are placed in the root directory.
   c) Type the name of the of the folder in which the script will reside in the **Folder** field, if necessary.
   d) Type the name of the of the subfolder in which the script will reside in the **Subfolder** field, if necessary.
   e) Type the name of the uninstall file in the **Uninstall Filename** field.
   f) To include keystrokes in the package, type the keystroke parameters in the **Key Info** field. For more information, see Key Info Parameters on page 118.
   g) To indicate the patch requires a pre-requisite signature, select the **Pre Req Installation** check box.
4. If the installable file is in `.msi` format, select the **Is an MSI Install File** check box and complete the following substeps.
   a) Set the **MSI Install Parameter**.
   b) Set the **MSI Uninstall Parameter**.

5. Click **Next**.

   **Step Result:** The ***Deployment Flags*** page opens.



Deployment Flags

Specify the flags to be used for this patch. Select whether the patch is enabled and also whether it's set by default.

Parameters passed for install and uninstall should be the ones that the Patch being deployed is expected to use. Example on an MSI "/quiet" will enable quite mode install.

Quiet Flag

☑ Enabled ☑ On by Default

Install Parameter: /quiet

Uninstall Parameter:

Suppress Restart Flag

☑ Enabled ☑ On by Default

Install Parameter: /norestart

Uninstall Parameter:

Unattended Flag

□ Enabled □ On by Default

Install Parameter:

Uninstall Parameter:

Uninstall Flag

□ Enabled □ On by Default

Uninstall Parameter:

Figure 65: Deployment Flags Page

6. Select the flags you want to use with your patch.

   For more information on flag descriptions, refer to Patch Deployment Flags on page 119.

7. Click **Finish**.

   **Step Result:** The ***Script Template Wizard*** closes.

**Result:** A script for the package is created with the options specified in the ***Script Template Wizard***.

## Key Info Parameters

The **Key Info** field in the ***Script Template Wizard*** allows you to specify keystrokes required for use with executables that do not support an unattended installation.

There are five different parameters for the **Key Info** string. For each key stroke you wish to include you must enter all five parameter values inside of the string divided by the pipe character ( | ). The pipe character is not required at the end of the **Key Info** string if you are only including one keystroke. You also do not need a pipe on the last set of **Key Info** parameters in cases where you are including multiple key strokes.

The **Key Info** string format is as follows: `Application Name,Application Time-Out,Key Name,Key Time-Out,Mandatory,Wait For`

The following list describes each **Key Info** parameter.

| Parameter | Description |
|---|---|
| **`Application Name`** | Indicates the name of the application to send keystrokes to. The application name is case-sensitive. |
| **`Application Time-Out`** | Indicates the application's time-out period (in seconds). If the script is unable to activate the application within the specified time-out period then the script will throw an error. |
| **`Key Name`** | Indicates the key that will be sent to the application. The Enter key can be represented by either `Enter` or the tilde character (~). |
| **`Key Time-Out`** | Indicates the key's time-out period (in seconds). If the script was able to activate the application within the specified time-out period then it will attempt to send the keystroke to the application. The script attempts to send the keystrokes to the specified application until the key time-out time period has been met. |
| **`Mandatory`** | Indicates if the keystroke is a mandatory key or not. If the key is mandatory and either the key or application time-out is met then the script will throw an error. Otherwise, if the key is not mandatory and either of the time-outs are met then the script will not throw an error. |
| **`Wait For`** | Indicates the amount of time to wait after the keystroke as been sent. Typically this is used only when you have to wait for a process, such as the next form, to load. |

## Patch Deployment Flags

You can add flags to a package script in the ***Deployment Flags*** page of the ***Script Template Wizard***. Specify which flags are available and their default settings when performing a deployment.

The following table defines the flag behavior:

Table 12: Package Flag Descriptions

| Description (flag behavior) | Display Flag | Select Flag |
|---|---|---|
| Perform an uninstall; can be used with -mu or -q. | -yd | -y |
| Force other applications to close at shutdown. | -fd | -f |
| Do not back up files for uninstall. | -nd | -n |
| Do not restart the computer when the installation is done. | -zd | -z |
| Use quiet mode, no user interaction is required. | -qd | -q |

| Description (flag behavior) | Display Flag | Select Flag |
|---|---|---|
| Use unattended setup mode. | -dmu | -mu |
| Install in multi-user mode (UNIX, Linux only). | -dsu | -su |
| Restart service after installation (UNIX, Linx only). | -drestart | -restart |
| Do not restart service after installation (UNIX, Linux only). | -dnorestart | -norestart |
| Reconfigure after installation (UNIX, Linux only). | -dreconfig | -reconfig |
| Do not reconfigure after installation (UNIX, Linux only). | -dnoreconfig | -noreconfig |
| This package is chainable and will run Qchain.exe (Windows) or (UNIX/Linux). | -dc | -c |
| Suppress the final chained reboot. | -dc | -sc |
| Repair permissions. | -dr | -r |
| Deploy only. | -PLD1 | -PLD0 |
| No Pop-up | -PLN1 | -PLNP |
| Debug | -PLDG | -PLDEBUG |
| Suppress Repair | -dsr | -sr |
| Force the script to reboot when the installation is done. | -1d | -1 |
| Reboot is required. | Not applicable | -2 |
| Reboot may occur. | Not applicable | -3 |
| Reboot is required, and may occur. | Not applicable | -4 |

# Chapter 8

## Working with Pre-Requisites

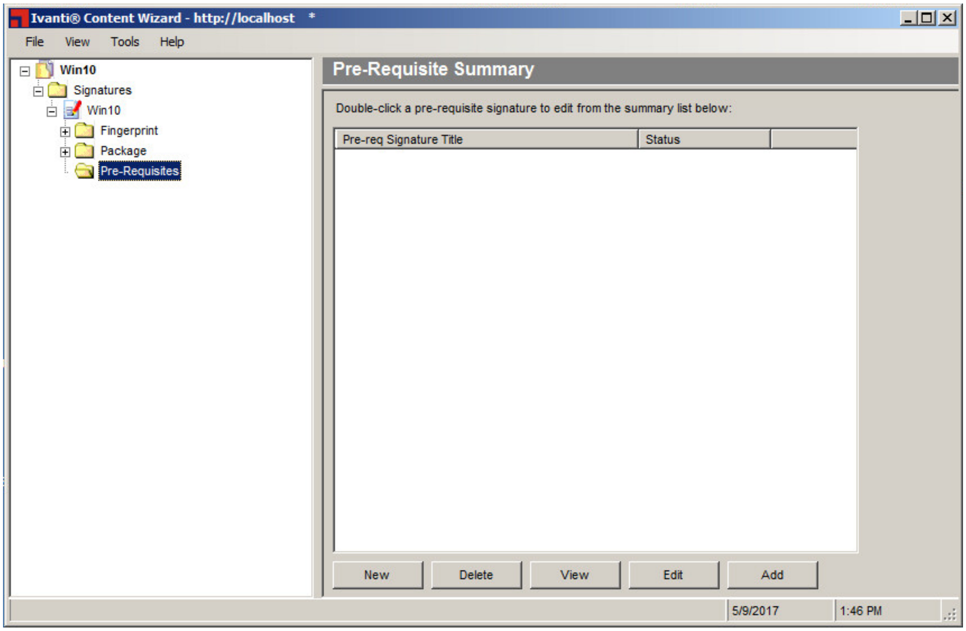
**In this chapter:**

A pre-requisite is a signature that determines if another signature is applicable to a patch. The Ivanti Content Wizard allows you to add new pre-requisites for a signature as well as add existing pre-requisites to a signature.

## The Pre-Requisite Summary Page

The ***Pre-Requisite Summary*** page allows you to view and define pre-requisite signature options for a patch.

To display the ***Pre-Requisite Summary*** page, click the **Pre-Requisites** folder from the menu tree in the left pane.



Double-click a pre-requisite signature to edit from the summary list below:

Figure 66: Pre-Requisite Summary Page

The following list describes the buttons on the ***Pre-Requisite Summary*** page.

| Button | Description |
|---|---|
| **New** | Takes you to the ***Patch Properties*** page to create a new patch. For more information, see Creating a New Patch on page 132.<br>**Note:** To add the new pre-requisite that you create, refer to, Adding a Pre-Requisite on page 123. |
| **Delete** | Deletes the currently selected pre-requisite signature from this patch, all other patches, and the Ivanti Endpoint Security (Endpoint Security). For more information, see Removing a Pre-Requisite on page 130. |
| **View** | Opens the ***Pre-Requisite Properties*** page. The page is read-only. For more information, see Viewing a Pre-Requisite on page 128. |

| Button | Description |
|---|---|
| **Edit** | Allows you to edit patch properties for the pre-requisite. For more information, see Editing a Pre-Requisite on page 126. |
| **Add** | Allows you to search for and add the pre-requisite signature to the patch package. For more information, see Adding a Pre-Requisite on page 123. |

**Tip:** Right-click inside the ***Pre-Requisite Summary*** page window to bring up a selectable menu that mimics the available buttons.

## Adding a Pre-Requisite

You can add a pre-requisite that you created for a signature from the ***Pre-Requisite Properties*** page. You can also import a pre-requisite from an existing vendor list.

**Prerequisites:**

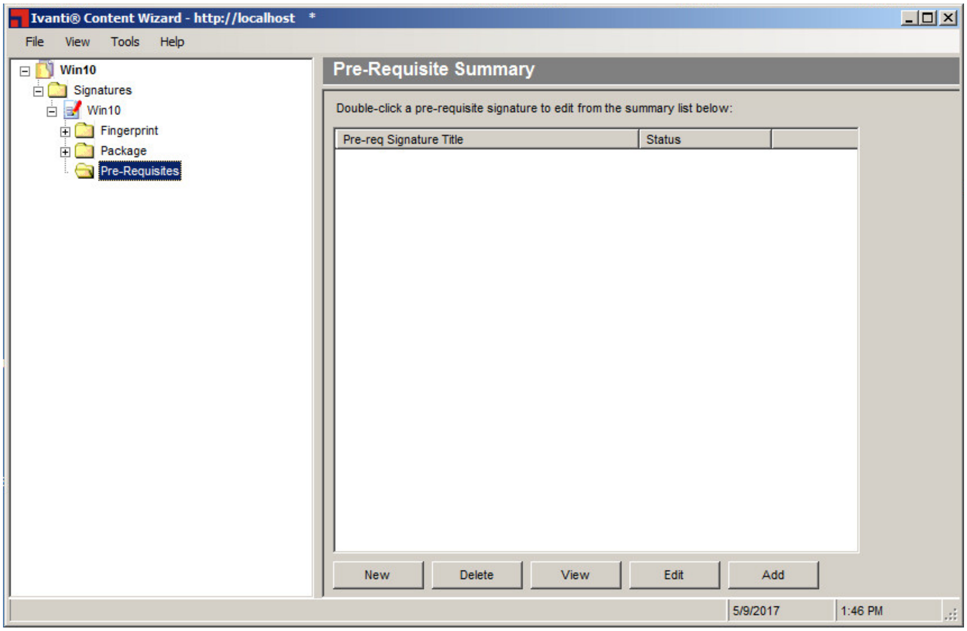
Specify the patch properties in the ***Patch Properties*** page. For more information about creating patch properties, refer to Creating and Editing Patch Properties on page 36.

Add a pre-requisite to an applicable signature.

1. Expand the patch properties in the left pane to **Pre-Requisites**.

   **Example:** ***New Patch*** > **Signatures** > ***New Signature*** > **Pre-Requisites**.

   **Step Result:** The ***Pre-Requisite Summary*** page opens.



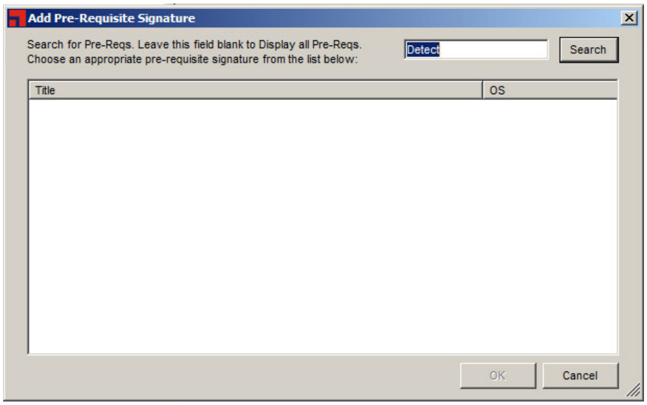
Double-click a pre-requisite signature to edit from the summary list below:

Figure 67: Pre-Requisite Summary Page

2. Click **Add**.

**Tip:** Right-click inside the ***Pre-Requisite Summary*** page window to bring up a selectable menu that mimics the available buttons.

**Step Result:** The ***Add Pre-Requisite Signature*** dialog opens with `Detect` defaulted in the **Search** field.



Search for Pre-Reqs. Leave this field blank to Display all Pre-Reqs.
Choose an appropriate pre-requisite signature from the list below:

Figure 68: Add Pre-Requisite Signature Dialog

3. Remove `Detect` from **Search** field.

   A blank field allows all pre-requisite signatures to display.

**Tip:** When searching for a particular pre-requisite, type the name of the signature in the search field and click **Search**.

4. Click **Search**.

   **Step Result:** Any signatures already created are displayed in the ***Add Pre-Requisite Signature*** window.

5. Select a pre-requisite from the available list.
6. Click **OK**.

   **Step Result:** The ***Add Pre-Requisite Signature*** window closes and the pre-requisite is added to the pane.

7. [Optional] Repeat steps 2 through 6, to add additional pre-requisites to the signature as needed.

8. Select **File** > **Save**.

**Result:** The pre-requisite is added to the signature.

> **Tip:** In the event that communication is lost between the agent and server due to a server reboot, you may receive an communication error message after clicking **Search**. When this occurs, close the Ivanti Content Wizard, and then log in again to reestablish a server connection.

## Editing a Pre-Requisite

You can edit a pre-requisite signature by selecting it and editing its details in the ***Patch Properties*** window.

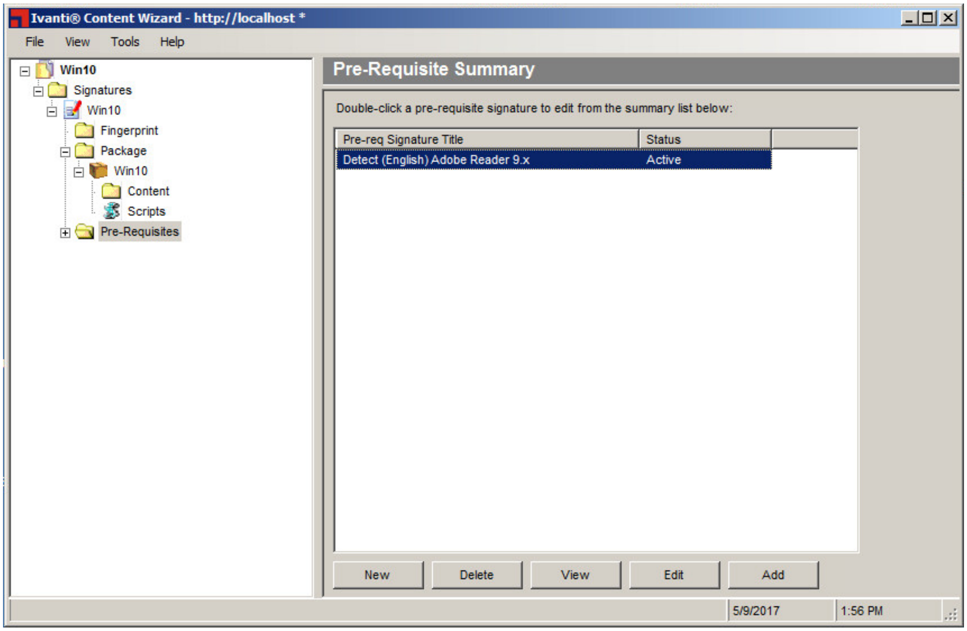
**Prerequisites:**

A pre-requisite to a signature for the selected patch has been added. For more information on adding a pre-requisite, refer to Adding a Pre-Requisite on page 123.

1. Expand the patch properties in the left pane to **Pre-Requisites**.

   **Example:** ***New Patch*** > **Signatures** > ***New Signature*** > **Pre-Requisites**.

   **Step Result:** The ***Pre-Requisite Summary*** page opens.



Pre-Requisite Summary

Double-click a pre-requisite signature to edit from the summary list below:

| Pre-req Signature Title | Status |
|---|---|
| Detect (English) Adobe Reader 9.x | Active |

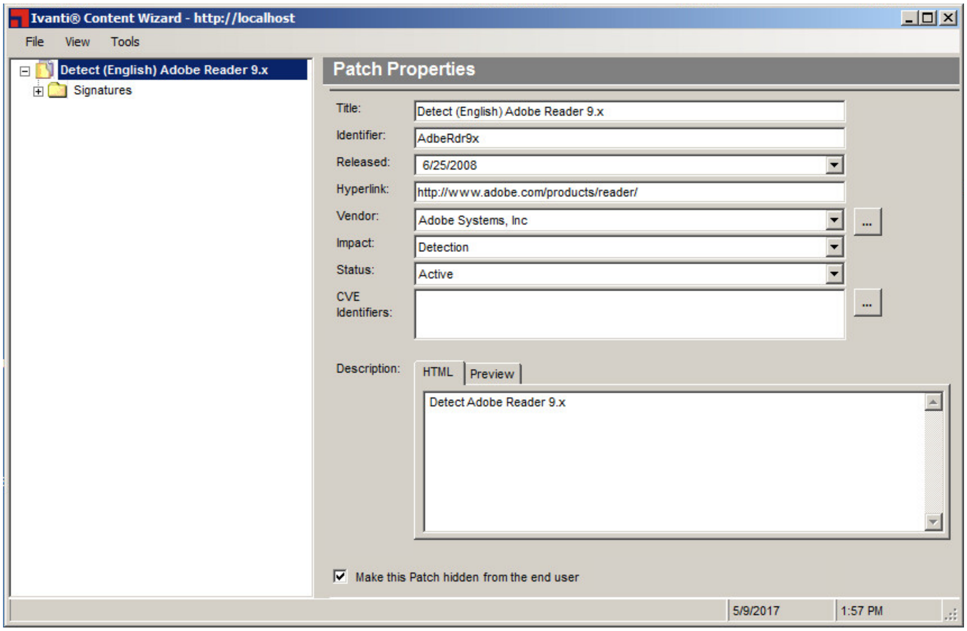
Figure 69: Pre-Requisite Summary Page: Sample Pre-Requisites

2. In the pane select the applicable prerequisite you want to edit.

**3.** Click **Edit**.

> **Tip:** Right-click inside the ***Pre-Requisite Summary*** page window to bring up a selectable menu that mimics the available buttons.

**Step Result:** The ***Patch Properties*** page opens.



Ivanti® Content Wizard - http://localhost
File
View
Tools
Detect (English) Adobe Reader 9.x
Signatures
Patch Properties

Title: Detect (English) Adobe Reader 9.x
Identifier: AdbeRdr9x
Released: 6/25/2008
Hyperlink: http://www.adobe.com/products/reader/
Vendor: Adobe Systems, Inc
Impact: Detection
Status: Active
CVE Identifiers:
Description: HTML Preview
Detect Adobe Reader 9.x
☑ Make this Patch hidden from the end user
5/9/2017 1:57 PM

Figure 70: Patch Properties Page

**4.** [Optional] Edit the patch properties for the pre-requisite as needed.

> **Note:** For more information on the various properties and fields in the ***Patch Properties*** page, refer to The Patch Properties Page on page 35.

a) Type a unique name for the patch in the **Title** field.

   The default title is **New Patch**.

b) Type a unique identifier for the patch in the **Identifier** field.

   You may determine the identifier or you may choose to use one supplied by the vendor.

c) Type the release date for the patch in the **Released** field.

   By default, the current date is specified. You can use the vendor's date if necessary.

d) Type the vendor's URL in the **Hyperlink** field.

e) Select a vendor from the **Vendor** drop-down list.

   Vendors must be added before they can show up as an item in the **Vendor** drop-down list. For more information, see Adding a New Vendor on page 39.

f) Select an impact from the drop-down list in the **Impact** field.

   To understand the various impact options available, refer to Understanding Patch Severity Levels on page 33.

g) Select an applicable patch status from the drop-down list in the **Status** field:

   - **Active**
   - **Beta**
   - **Pending**

   To understand the various status options available, refer to The Patch Properties Page on page 35.

h) Select CVE Identifiers.

   1. Click the **CVE Identifiers** button.
   2. Select **File** > **Add** to display the list of CVE Identifiers..
   3. Double-click on the CVE Identifier that is applicable to your needs.
   4. Click **Save**.

i) Type a description in the **Description** field.

   This description will be visible in the ***Patches*** page of the Ivanti Endpoint Security.

j) [Optional] Select the **Make this Patch hidden from the end user** check box.

5. Select **File** > **Save**.
6. [Optional] Repeat steps 2 through 5, to edit additional pre-requisites as needed.
7. Select **File** > **Save**.

**Result:** The pre-requisite details are modified.

## Viewing a Pre-Requisite

You can view the pre-requisite properties that you created for a signature from the ***Pre-Requisite Properties*** page.

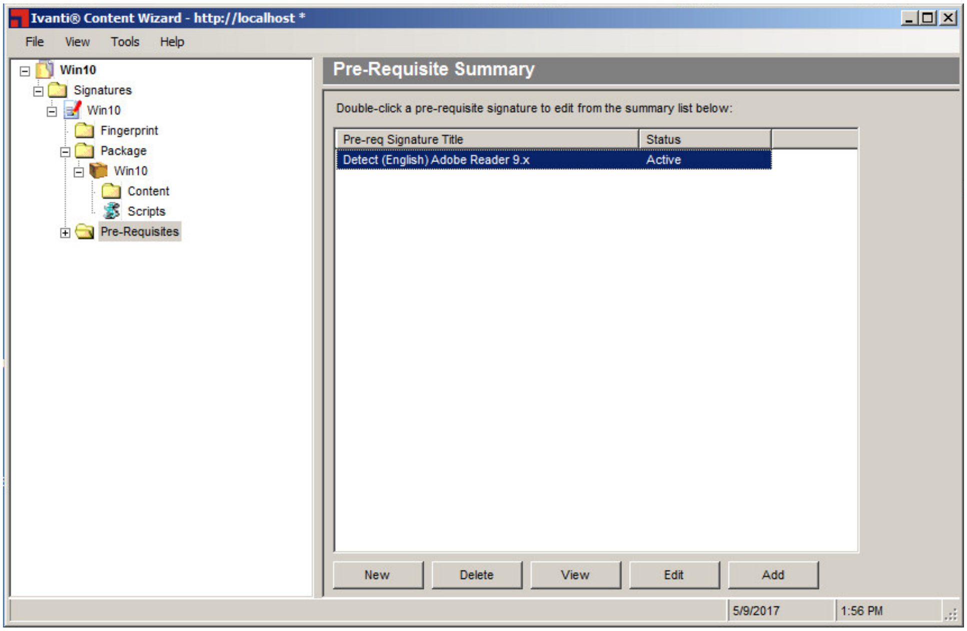
**Prerequisites:**

A pre-requisite to a signature for the selected patch has been added. For more information on adding a pre-requisite, refer to Adding a Pre-Requisite on page 123.

1. Expand the patch properties in the left pane to **Pre-Requisites**.

   **Example:** ***New Patch*** > **Signatures** > ***Signature Title*** > **Pre-Requisites**.

   **Step Result:** The ***Pre-Requisite Properties*** page opens.



Double-click a pre-requisite signature to edit from the summary list below:

| Pre-req Signature Title | Status |
|---|---|
| Detect (English) Adobe Reader 9.x | Active |

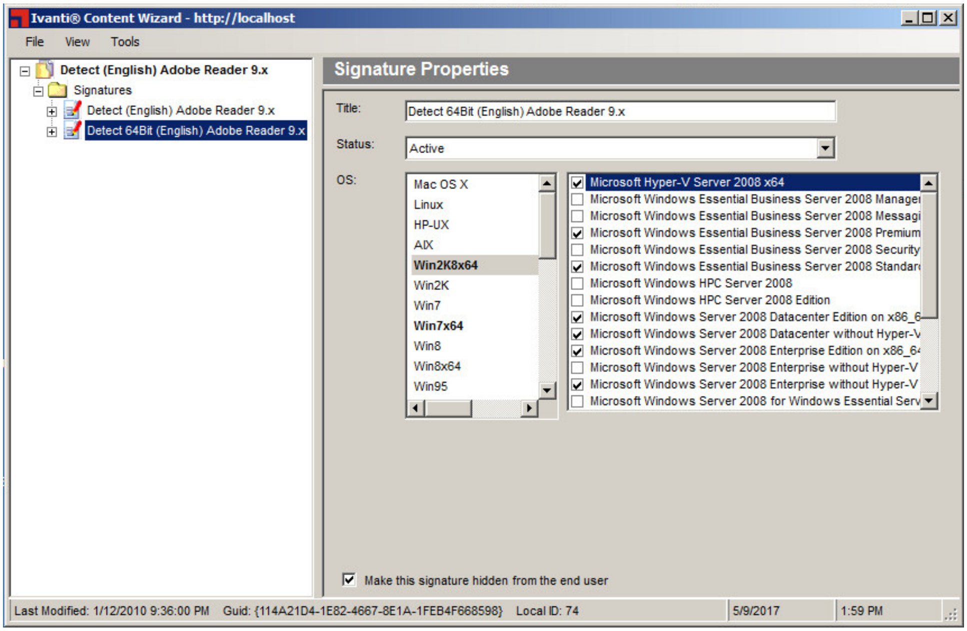
Figure 71: Pre-Requisite Summary Page: Sample Pre-Requisites

2. In the pane select the applicable prerequisite you want to view.

3. Click **View**.

**Tip:** Right-click inside the ***Pre-Requisite Summary*** page window to bring up a selectable menu that mimics the available buttons.

**Step Result:** The ***Pre-Requisite Properties*** page opens. The view is read-only.


Ivanti® Content Wizard - http://localhost
File
View
Tools
Detect (English) Adobe Reader 9.x
Signatures
Detect (English) Adobe Reader 9.x
Detect 64Bit (English) Adobe Reader 9.x
Signature Properties

Title: Detect 64Bit (English) Adobe Reader 9.x

Status: Active

OS:

Mac OS X
Linux
HP-UX
AIX
Win2K8x64
Win2K
Win7
Win7x64
Win8
Win8x64
Win95

☑ Microsoft Hyper-V Server 2008 x64
☐ Microsoft Windows Essential Business Server 2008 Managei
☐ Microsoft Windows Essential Business Server 2008 Messagi
☑ Microsoft Windows Essential Business Server 2008 Premium
☐ Microsoft Windows Essential Business Server 2008 Security
☑ Microsoft Windows Essential Business Server 2008 Standard
☐ Microsoft Windows HPC Server 2008
☐ Microsoft Windows HPC Server 2008 Edition
☑ Microsoft Windows Server 2008 Datacenter Edition on x86_6
☑ Microsoft Windows Server 2008 Datacenter without Hyper-V
☑ Microsoft Windows Server 2008 Enterprise Edition on x86_64
☐ Microsoft Windows Server 2008 Enterprise without Hyper-V
☑ Microsoft Windows Server 2008 Enterprise without Hyper-V
☐ Microsoft Windows Server 2008 for Windows Essential Serv

☑ Make this signature hidden from the end user

Last Modified: 1/12/2010 9:36:00 PM Guid: {114A21D4-1E82-4667-8E1A-1FEB4F668598} Local ID: 74 5/9/2017 1:59 PM

Figure 72: Patch Properties Page

**Tip:** To return to the list of pre-requites, select **Pre-Requisite** in the left pane.

**Result:** The pre-requisite is displayed.

## Removing a Pre-Requisite

If you do not need a pre-requisite, you can remove it from a signature by using the ***Pre-Requisite Summary*** page.

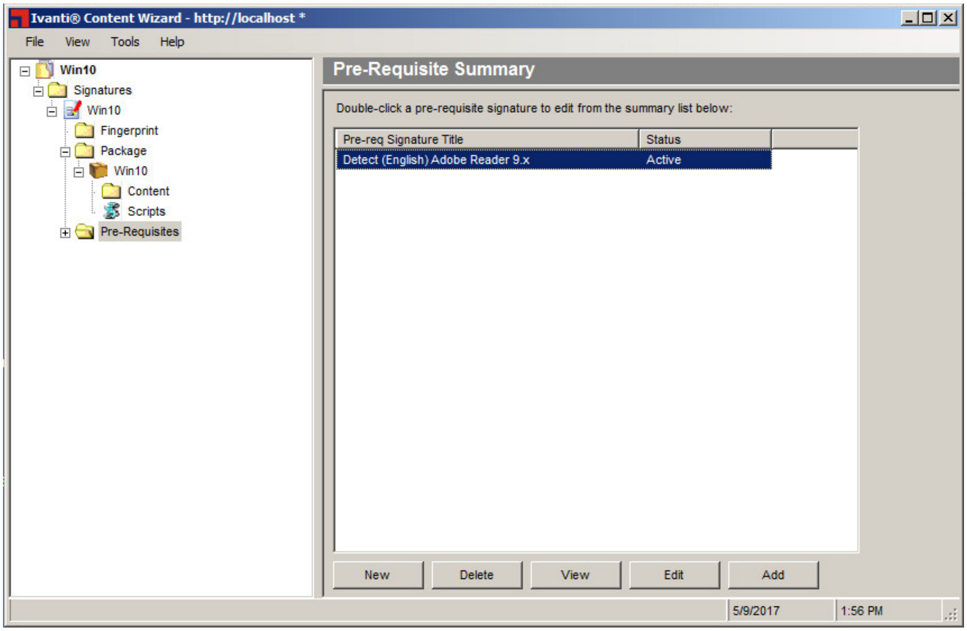
**Prerequisites:**

A pre-requisite to a signature for the selected patch has been added. For more information on adding a pre-requisite, refer to Adding a Pre-Requisite on page 123.

1. Expand the patch properties in the left pane to **Pre-Requisites**.

   **Example:** ***New Patch*** > **Signatures** > ***New Signature*** > **Pre-Requisites**.

   **Step Result:** The ***Pre-Requisite Properties*** page opens.



Double-click a pre-requisite signature to edit from the summary list below:

| Pre-req Signature Title | Status |
|---|---|
| Detect (English) Adobe Reader 9.x | Active |

Figure 73: Pre-Requisite Summary Page: Sample Pre-Requisites

2. In the left pane, click **Pre-Requisites**.

   **Step Result:** The ***Pre-Requisite Summary*** page opens.

3. In the pane select the applicable prerequisite you want to delete.
4. Click **Delete**.

   **Tip:** Right-click inside the ***Pre-Requisite Summary*** page window will bring up a selectable menu that mimics the available buttons.

   **Step Result:** A confirmation message appears.

5. Click **OK**.

   **Step Result:** The confirmation message dialog closes.

6. [Optional] Repeat steps 2 through 5, to remove additional pre-requisites as needed.
7. Select **File** > **Save**.

**Result:** The selected pre-requisite is deleted from the signature.

# Creating a New Patch

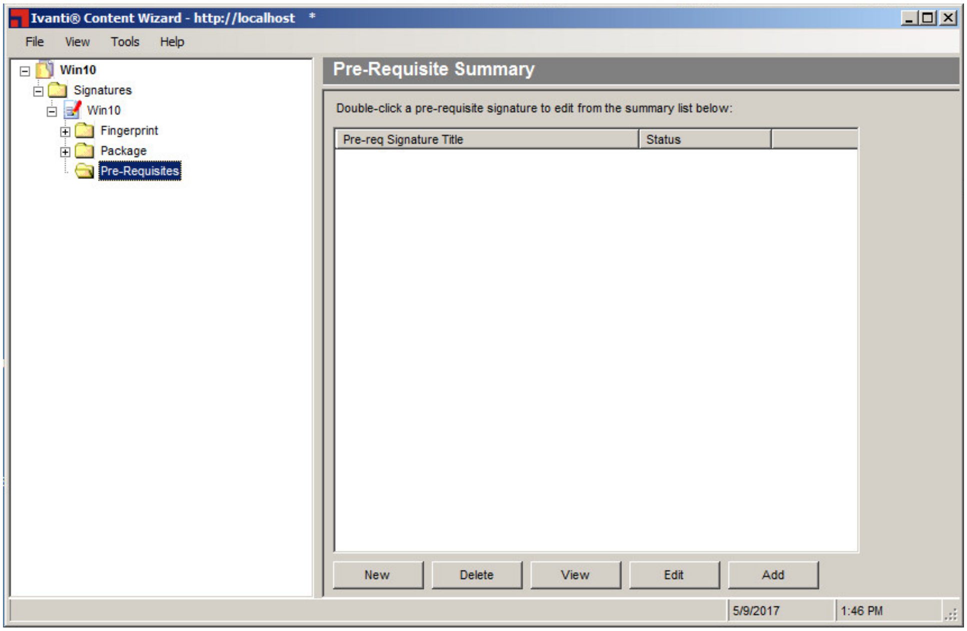
If you require a new pre-requisite patch to be created, you can create it using the ***Pre-Requisite Summary*** page.

Use the ***Pre-Requisite Summary*** page to launch the ***Patch Properties*** page to create a pre-requisite signature patch.

1. Expand the patch properties in the left pane to **Pre-Requisites**.

   **Example:** ***New Patch*** > **Signatures** > ***New Signature*** > **Pre-Requisites**.

   **Step Result:** The ***Pre-Requisite Summary*** page opens.



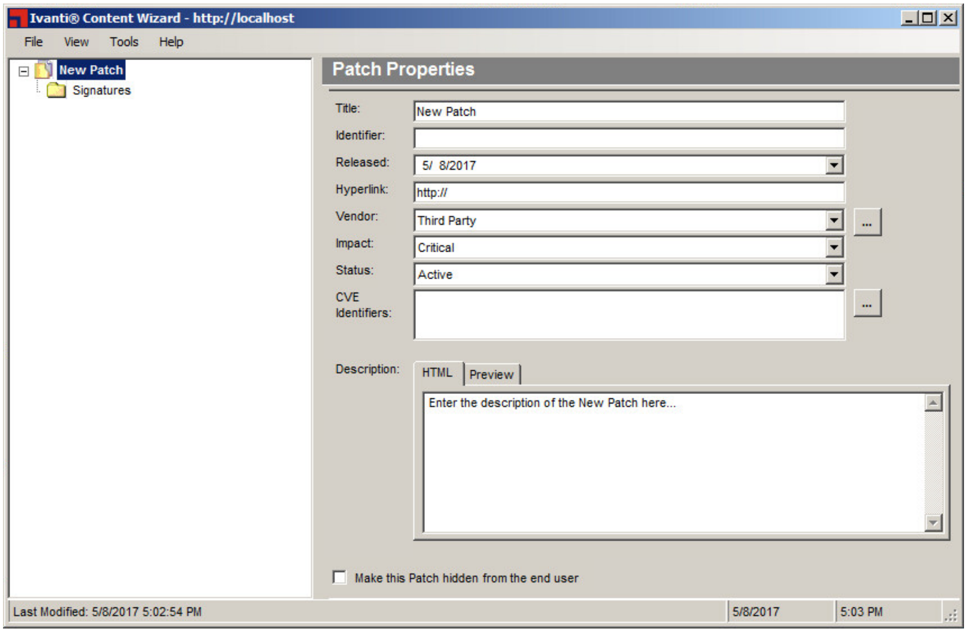
Double-click a pre-requisite signature to edit from the summary list below:

Figure 74: Pre-Requisite Summary Page

2. Click **New**.

**Tip:** Right-click inside the ***Pre-Requisite Summary*** page window will bring up a selectable menu that mimics the available buttons.

**Step Result:** The ***Patch Properties*** page opens.



Patch Properties

Title: New Patch

Identifier:

Released: 5/ 8/2017

Hyperlink: http://

Vendor: Third Party

Impact: Critical

Status: Active

CVE Identifiers:

Description: Enter the description of the New Patch here...

□ Make this Patch hidden from the end user

Last Modified: 5/8/2017 5:02:54 PM | 5/8/2017 | 5:03 PM

Figure 75: Patch Properties Page

**Note:** For more information on the various properties and fields in the ***Patch Properties*** page, refer to The Patch Properties Page on page 35.

3. Type a unique name for the patch in the **Title** field.

   The default title is **New Patch**.

4. Type a unique identifier for the patch in the **Identifier** field.

   You may determine the identifier or you may choose to use one supplied by the vendor.

5. Type the release date for the patch in the **Released** field.

   By default, the current date is specified. You can use the vendor's date if necessary.

6. Type the vendor's URL in the **Hyperlink** field.

7. Select a vendor from the **Vendor** drop-down list.

   Vendors must be added before they can show up as an item in the **Vendor** drop-down list. For more information, see Adding a New Vendor on page 39.

8. Select an impact from the drop-down list in the **Impact** field.

   To understand the various impact options available, refer to Understanding Patch Severity Levels on page 33.

9. Select an applicable patch status from the drop-down list in the **Status** field:

   - **Active**
   - **Beta**
   - **Pending**

   To understand the various status options and their meaning, refer to The Patch Properties Page on page 35.

10. [Optional] Select CVE Identifiers.

    a) Click the **CVE Identifiers** button.

    **Step Result:** The ***CVE Identifiers*** dialog opens.

    b) Select **File** > **Add**.

    **Step Result:** The ***Add CVE Code*** dialog opens and lists the available CVE Identifiers.

    c) Double-click on the CVE Identifier that is applicable to your needs.

    **Step Result:** The ***Add CVE Code*** dialog closes and the item is added to the ***CVE Identifiers*** dialog.

    d) Click **Save**.

    **Step Result:** The ***CVE Identifiers*** dialog closes and the item is added to **CVE Identifiers** field.

    e) [Optional] Repeat steps a, b, c and d to add additional CVE Identifiers.

11. Type a description in the **Description** field.

    This description will be visible in the ***Patches*** page of the Ivanti Endpoint Security.

12. [Optional] Select the **Make this Patch hidden from the end user** check box.

13. Select **File** > **Save**.

    > **Note:** If you save the patch without adding a package, you are asked if you want to save without adding a package. Click **Yes** to proceed.

14. Exit the ***Patch Properties*** page.

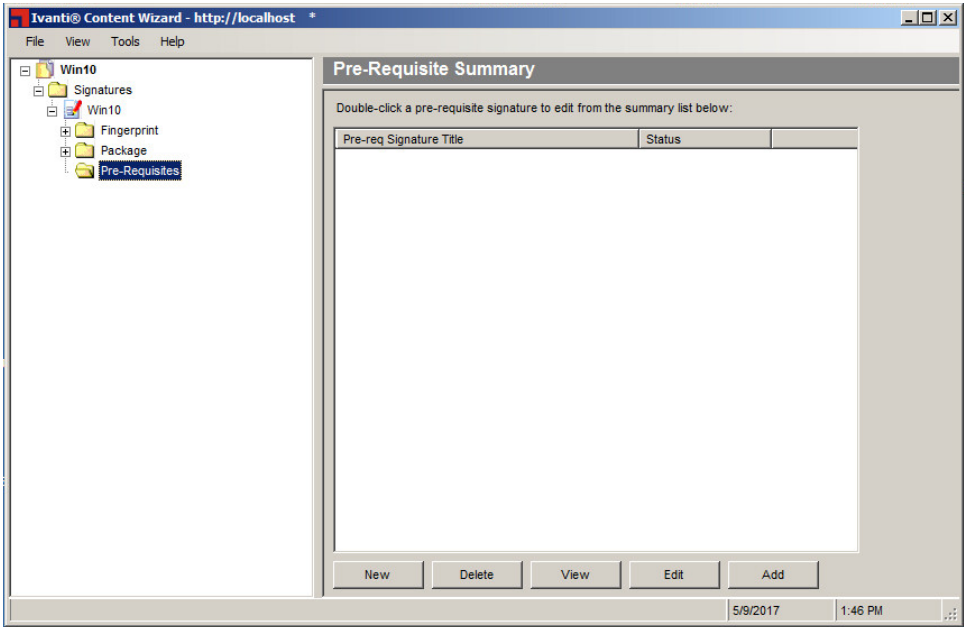
    a) Select **File** > **Exit**.

    **Step Result:** A dialog displays.

    > **Note:** The dialog indicates that to apply the newly created pre-requisite signature patch you must use the **Add** button on the ***Pre-Requisite Summary*** page. Refer to Adding a Pre-Requisite on page 123.

b) Click **OK**.

**Step Result:** The ***Patch Properties*** page exits and is replaced by the ***Pre-Requisite Summary*** page.



Double-click a pre-requisite signature to edit from the summary list below:

Figure 76: Pre-Requisite Summary Page

**After Completing This Task:**

Apply the newly created pre-requisite signature patch to the applicable signature, refer to Adding a Pre-Requisite on page 123.

# Chapter 9

# Performing Patch Tasks

**In this chapter:**

The Ivanti Content Wizard menu items allow you to perform tasks for patching and maintaining a company network. The **File** menu function is to organize product features that assist you in performing basic tasks for patching.

You can perform the following tasks from the **File** menu:

- Creating a Linux Patch on page 137
- Finding a Patch on page 143
- Deleting Obsolete Patches on page 146
- Saving a Copy of a Patch on page 147
- Importing Patches Using the Import Wizard on page 150
- Exporting Patches Using the Export Wizard on page 153
- Exiting the Ivanti Content Wizard on page 29

**Tip:** Menu items list their keyboard shortcuts.

## Creating a Linux Patch

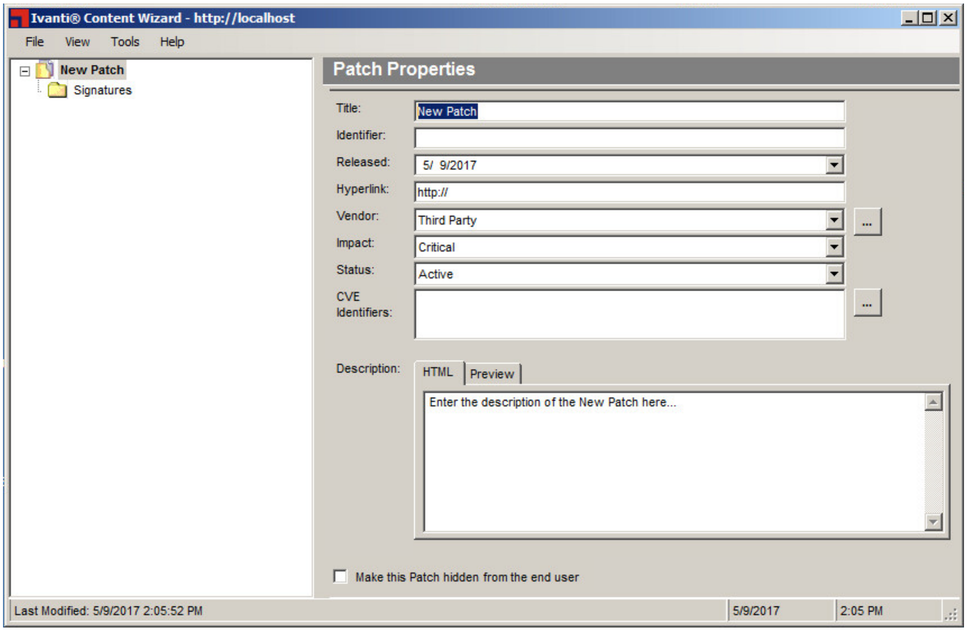
The ***Patch Properties*** page allows you to create patches for non-Windows operating systems, including Linux and other Unix-based operating system.

Create a Linux patch using the ***Patch Properties*** page.

**Note:** The ***Patch Creation Wizard*** is used create patches for Windows operating systems. Refer to Using the New Patch Wizard on page 162 for additional information.

1. Select **File** > **New**.

   **Step Result:** The ***Patch Properties*** page opens.



Title: New Patch

Identifier:

Released: 5/ 9/2017

Hyperlink: http://

Vendor: Third Party

Impact: Critical

Status: Active

CVE Identifiers:

Description: HTML | Preview

Enter the description of the New Patch here...

☐ Make this Patch hidden from the end user

Last Modified: 5/9/2017 2:05:52 PM | 5/9/2017 | 2:05 PM

Figure 77: Patch Properties Page

> **Note:** For additional information about the properties on the ***Patch Properties*** page, refer to The Patch Properties Page on page 35.

2. Type a unique name for the patch in the **Title** field.

   The default title is **New Patch**.
3. Type a unique identifier for the patch in the **Identifier** field.

   You may determine the identifier or you may choose to use one supplied by the vendor.
4. Type the release date for the patch in the **Released** field.

   By default, the current date is specified. You can use the vendor's date if necessary.
5. Type the vendor's URL in the **Hyperlink** field.
6. Select a vendor from the **Vendor** drop-down list.

   Vendors must be added before they can show up as an item in the **Vendor** drop-down list. For more information, see Adding a New Vendor on page 39.
7. Select an impact from the drop-down list in the **Impact** field.

   To understand the various impact options available, refer to Understanding Patch Severity Levels on page 33.

8. Select an applicable patch status from the drop-down list in the **Status** field:
   - **Active**
   - **Beta**
   - **Pending**

   To understand the various status options and their meaning, refer to The Patch Properties Page on page 35.
9. [Optional] Select CVE Identifiers.
   a) Click the **CVE Identifiers** button.

   **Step Result:** The ***CVE Identifiers*** dialog opens.

   b) Select **File** > **Add**.

   **Step Result:** The ***Add CVE Code*** dialog opens and lists the available CVE Identifiers.

   c) Double-click on the CVE Identifier that is applicable to your needs.

   **Step Result:** The ***Add CVE Code*** dialog closes and the item is added to the ***CVE Identifiers*** dialog.

   d) Click **Save**.

   **Step Result:** The ***CVE Identifiers*** dialog closes and the item is added to **CVE Identifiers** field.

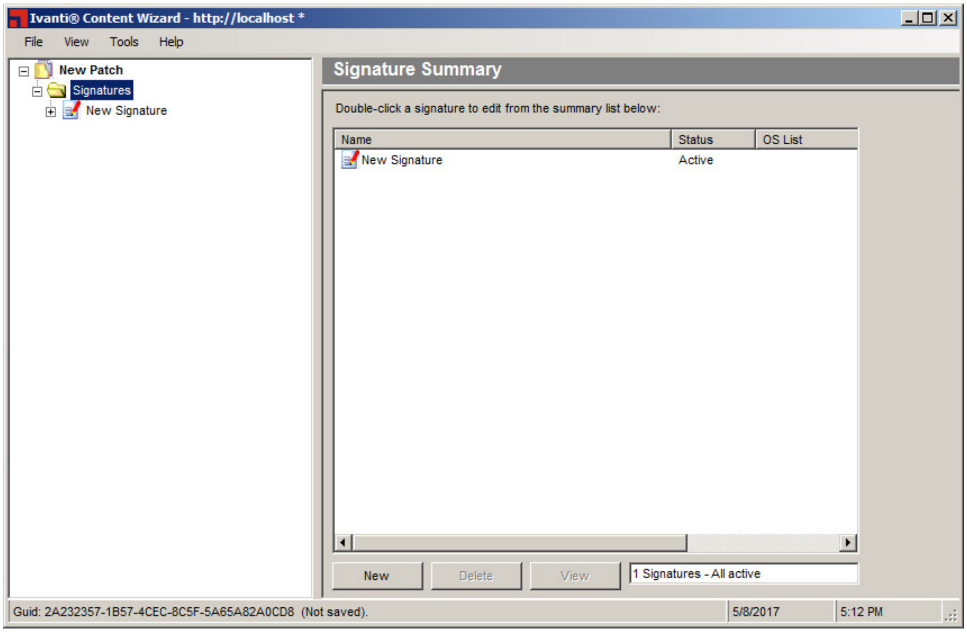
   e) [Optional] Repeat steps a, b, c and d to add additional CVE Identifiers.
10. Type a description in the **Description** field.

    This description will be visible in the ***Patches*** page of the Ivanti Endpoint Security.
11. In menu tree located in the left pane, select **Signatures**.

    **Step Result:** The ***Signature Summary*** dialog appears in the right pane.

**12.**Click **New**.

**Step Result:** The ***Signature Summary*** page opens.



Double-click a signature to edit from the summary list below:

| Name | Status | OS List |
|---|---|---|
| New Signature | Active | |

1 Signatures - All active

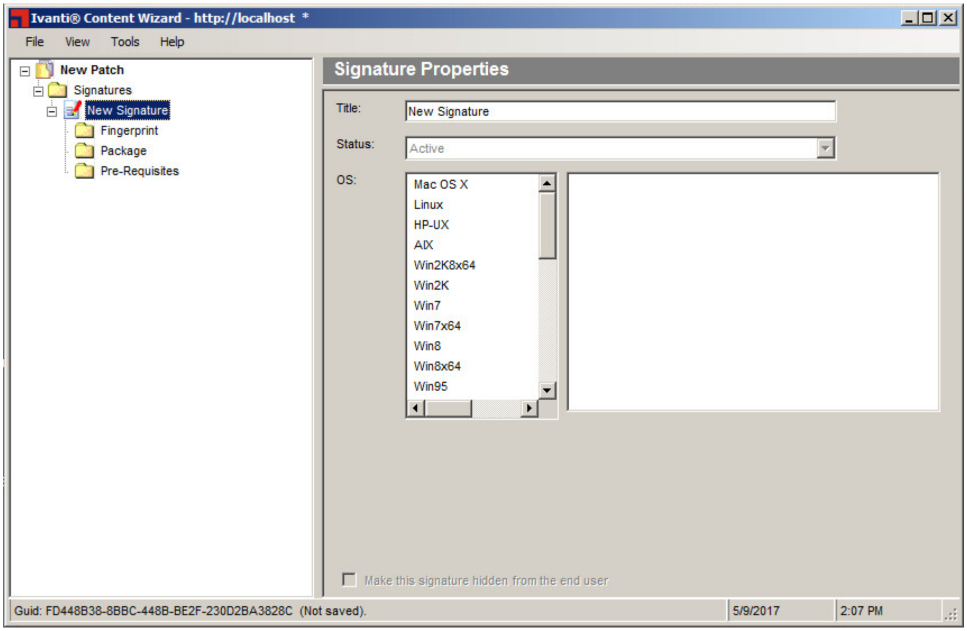
Guid: 2A232357-1B57-4CEC-8C5F-5A65A82A0CD8 (Not saved). 5/8/2017 5:12 PM

Figure 78: Signature Summary Page

**13.**Select **New Signature** in the right pane.

**14.**Click **View**.

**Step Result:** The ***Signature Properties*** page opens.



Title: New Signature

Status: Active

OS: Mac OS X, Linux, HP-UX, AIX, Win2K8x64, Win2K, Win7, Win7x64, Win8, Win8x64, Win95

□ Make this signature hidden from the end user

Guid: FD448B38-8BBC-448B-BE2F-230D2BA3828C (Not saved). 5/9/2017 2:07 PM

Figure 79: Signature Properties Page

> **Note:** For additional information about the properties on the ***Signature Properties*** page, refer to The Signature Properties Page on page 45.

**15.**[Optional] Type a new title in the **Title** field.

**Step Result:** The signature title is added to the left pane.

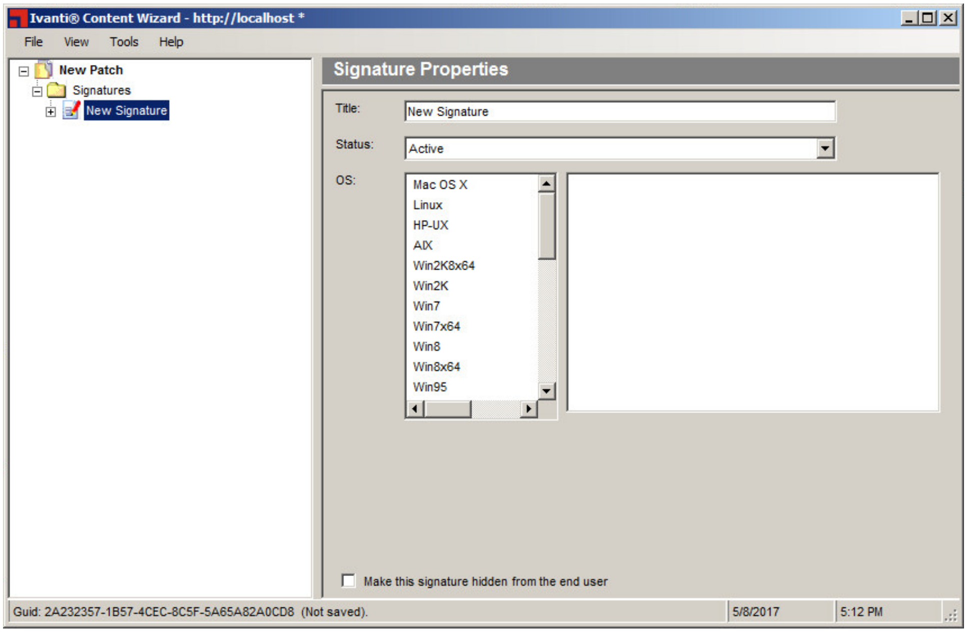
**16.**Select the applicable patch status using the **Status** drop-down list.

The following list items are available:

- Active
- Beta
- Pending

17. Select **Linux**.

    **Step Result:** A list of available Linux distributions appears.



Title: New Signature

Status: Active

OS:
Mac OS X
Linux
HP-UX
AIX
Win2K8x64
Win2K
Win7
Win7x64
Win8
Win8x64
Win95

□ Make this signature hidden from the end user

Guid: 2A232357-1B57-4CEC-8C5F-5A65A82A0CD8 (Not saved). 5/8/2017 5:12 PM

Figure 80: Signature Properties Page

18. Select the version of the operating system for the signature in the list details field.

**Tip:** Double-clicking an operating system name in the **OS** field selects all the versions of that operating system within the details list.

19. [Optional] Check or clear the **Make this signature hidden from the end user** check box to hide the signature from the end user.

20. [Optional] Edit the **Fingerprint**.

    a) In the left pane, expand the **Signatures** directory and select **Fingerprint**.

    b) Click **New**.

       **Step Result:** The fingerprint is added to the pane.

    c) Click **View**.

       **Step Result:** The ***Fingerprint Properties*** page opens.

    d) Make your edits.

**Note:** This action is necessary only if you intend to add the fingerprint for the patch. For additional information refer, to The Fingerprint Summary Page on page 53.

**21.**[Optional] Add **Package** content.

a) In the left pane, expand the **Signatures** directory and select **Package**.

**Step Result:** The ***Package Summary*** page opens.

b) In the right pane select **New**.

**Step Result:** A **New Package** is created, and the subsequent **Content** folder appears under the **New Package** folder in the left pane.

c) In the left pane, select **Content**.

d) Right-click in the right pane and add applicable content. For details on adding package content, refer to Adding Content to a Package on page 99.

**22.**[Optional] Add a **Pre-Requisite**.

You may add a pre-requisite signature to the patch.

a) In the left pane, expand the **Signatures** directory and select **Pre-Requisites**.

b) In the right pane select **Add**.

**Step Result:** The **Add Pre-Requisite Signature** dialog opens.

c) Search for pre-requisites to add.

1. Remove `Detect` from **Search** field.
2. Click **Search**.
3. Select a pre-requisite from the available list.
4. Click **OK** and the pre-requisite is displayed in the ***Pre-Requisite Summary*** page.

d) Repeat steps b and c to add additional pre-requisite signatures to the patch.

For details on creating a new pre-requisite signature patch, refer Creating a New Patch on page 132.

**23.**Select **File** > **Save**.

**Step Result:** The ***Patch Properties*** are saved.

**Result:** The Linux patch with the attributes you have specified is created.

## Finding a Patch

Once a patch is created, you can find it in the Ivanti Content Wizard database.

1. Select **File** > **Open**.

   **Step Result:** The ***Open Patch*** page opens.

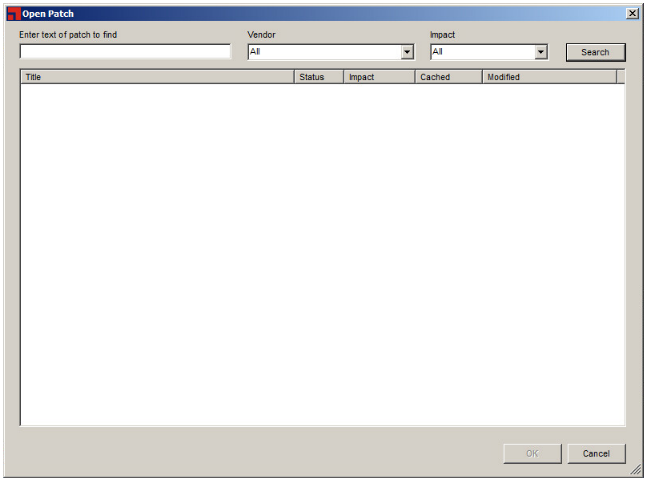
   

   Figure 81: Open Patch Page

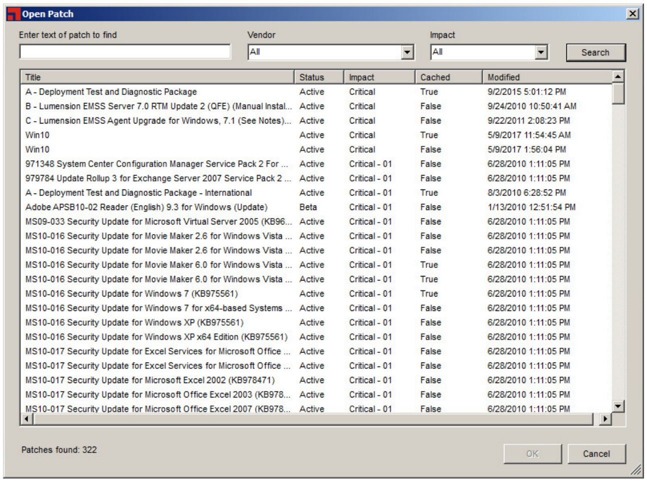
2. In the **Enter text of patch to find** field type the name of the patch you wish to locate.
3. [Optional] Select a vendor from the **Vendor** drop-down list.

   Vendors must be added before they can show up as an item in the **Vendor** drop-down list. For more information, see Adding a New Vendor on page 39.
4. [Optional] Select an impact from the drop-down list in the **Impact** field.

   To understand the various impact options available, refer to Understanding Patch Severity Levels on page 33.

5. Click **Search**.

   **Step Result:** The patches corresponding to the name filter appear in the ***Open Patch*** page.



Enter text of patch to find:

Vendor: All

Impact: All

| Title | Status | Impact | Cached | Modified |
|---|---|---|---|---|
| A - Deployment Test and Diagnostic Package | Active | Critical | True | 9/2/2015 5:01:12 PM |
| B - Lumension EMSS Server 7.0 RTM Update 2 (QFE) (Manual Instal... | Active | Critical | False | 9/24/2010 10:50:41 AM |
| C - Lumension EMSS Agent Upgrade for Windows, 7.1 (See Notes)... | Active | Critical | False | 9/22/2011 2:08:23 PM |
| Win10 | Active | Critical | True | 5/9/2017 11:54:45 AM |
| Win10 | Active | Critical | False | 5/9/2017 1:56:04 PM |
| 971348 System Center Configuration Manager Service Pack 2 For ... | Active | Critical - 01 | False | 6/28/2010 1:11:05 PM |
| 979784 Update Rollup 3 for Exchange Server 2007 Service Pack 2 ... | Active | Critical - 01 | False | 6/28/2010 1:11:05 PM |
| A - Deployment Test and Diagnostic Package - International | Active | Critical - 01 | True | 8/3/2010 6:28:52 PM |
| Adobe APSB10-02 Reader (English) 9.3 for Windows (Update) | Beta | Critical - 01 | False | 1/13/2010 12:51:54 PM |
| MS09-033 Security Update for Microsoft Virtual Server 2005 (KB96... | Active | Critical - 01 | False | 6/28/2010 1:11:05 PM |
| MS10-016 Security Update for Movie Maker 2.6 for Windows Vista ... | Active | Critical - 01 | False | 6/28/2010 1:11:05 PM |
| MS10-016 Security Update for Movie Maker 2.6 for Windows Vista ... | Active | Critical - 01 | False | 6/28/2010 1:11:05 PM |
| MS10-016 Security Update for Movie Maker 6.0 for Windows Vista ... | Active | Critical - 01 | True | 6/28/2010 1:11:05 PM |
| MS10-016 Security Update for Movie Maker 6.0 for Windows Vista ... | Active | Critical - 01 | True | 6/28/2010 1:11:05 PM |
| MS10-016 Security Update for Windows 7 (KB975561) | Active | Critical - 01 | True | 6/28/2010 1:11:05 PM |
| MS10-016 Security Update for Windows 7 for x64-based Systems ... | Active | Critical - 01 | False | 6/28/2010 1:11:05 PM |
| MS10-016 Security Update for Windows XP (KB975561) | Active | Critical - 01 | False | 6/28/2010 1:11:05 PM |
| MS10-016 Security Update for Windows XP x64 Edition (KB975561) | Active | Critical - 01 | False | 6/28/2010 1:11:05 PM |
| MS10-017 Security Update for Excel Services for Microsoft Office ... | Active | Critical - 01 | False | 6/28/2010 1:11:05 PM |
| MS10-017 Security Update for Excel Services for Microsoft Office ... | Active | Critical - 01 | False | 6/28/2010 1:11:05 PM |
| MS10-017 Security Update for Microsoft Excel 2002 (KB978471) | Active | Critical - 01 | False | 6/28/2010 1:11:05 PM |
| MS10-017 Security Update for Microsoft Office Excel 2003 (KB978... | Active | Critical - 01 | False | 6/28/2010 1:11:05 PM |
| MS10-017 Security Update for Microsoft Office Excel 2007 (KB978... | Active | Critical - 01 | False | 6/28/2010 1:11:05 PM |

Patches found: 322

Figure 82: Open Patch Page

> **Note:** There can be multiple versions of a patch.

6. Select the specific patch you want to open and click **OK**.

   **Step Result:** The ***Patch Properties*** page opens for the patch.

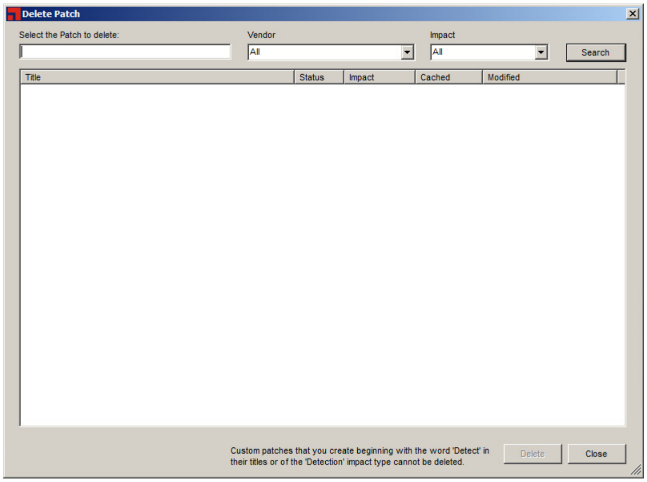
> **Note:** For additional information on ***Patch Properties***, refer to Defining Patch Properties on page 33.

## Deleting Obsolete Patches

Once a patch is no longer required, you can remove it from the Ivanti Content Wizard database. If you delete a patch created by the Ivanti Content Wizard, the patch will be deleted permanently.

1. Select **File** > **Delete**.

   **Step Result:** The ***Delete Patch*** page opens.

   Custom patches that you create beginning with the word 'Detect' in their titles or of the 'Detection' impact type cannot be deleted.

   Figure 83: Delete Patch Page

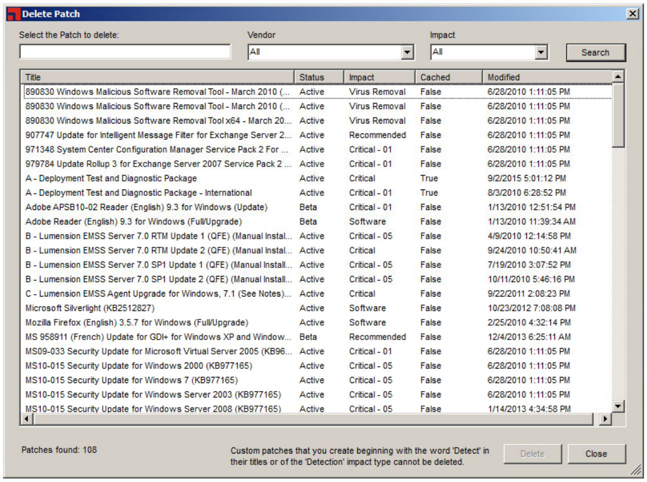
2. Specify search criteria.

   a) [Optional] Specify a patch name in the **Select the Patch to delete** field.
   b) [Optional] Choose a vendor from the **Vendor** drop-down list.
   c) Select an impact status from the **Impact** drop-down list.

   **Tip:** Narrow your search by specifying multiple search criteria.

3. Click **Search**.

   **Step Result:** The patches corresponding to the name filter appear in the ***Delete Patch*** page.



| Title | Status | Impact | Cached | Modified |
|---|---|---|---|---|
| 890830 Windows Malicious Software Removal Tool - March 2010 (... | Active | Virus Removal | False | 6/28/2010 1:11:05 PM |
| 890830 Windows Malicious Software Removal Tool - March 2010 (... | Active | Virus Removal | False | 6/28/2010 1:11:05 PM |
| 890830 Windows Malicious Software Removal Tool x64 - March 20... | Active | Virus Removal | False | 6/28/2010 1:11:05 PM |
| 907747 Update for Intelligent Message Filter for Exchange Server 2... | Active | Recommended | False | 6/28/2010 1:11:05 PM |
| 971348 System Center Configuration Manager Service Pack 2 For ... | Active | Critical - 01 | False | 6/28/2010 1:11:05 PM |
| 979784 Update Rollup 3 for Exchange Server 2007 Service Pack 2 ... | Active | Critical - 01 | False | 6/28/2010 1:11:05 PM |
| A - Deployment Test and Diagnostic Package | Active | Critical | True | 9/2/2015 5:01:12 PM |
| A - Deployment Test and Diagnostic Package - International | Active | Critical - 01 | True | 8/3/2010 6:28:52 PM |
| Adobe APSB10-02 Reader (English) 9.3 for Windows (Update) | Beta | Critical - 01 | False | 1/13/2010 12:51:54 PM |
| Adobe Reader (English) 9.3 for Windows (Full/Upgrade) | Beta | Software | False | 1/13/2010 11:39:34 AM |
| B - Lumension EMSS Server 7.0 RTM Update 1 (QFE) (Manual Instal... | Active | Critical - 05 | False | 4/9/2010 12:14:58 PM |
| B - Lumension EMSS Server 7.0 RTM Update 2 (QFE) (Manual Instal... | Active | Critical | False | 9/24/2010 10:50:41 AM |
| B - Lumension EMSS Server 7.0 SP1 Update 1 (QFE) (Manual Install... | Active | Critical - 05 | False | 7/19/2010 3:07:52 PM |
| B - Lumension EMSS Server 7.0 SP1 Update 2 (QFE) (Manual Install... | Active | Critical - 05 | False | 10/11/2010 5:46:16 PM |
| C - Lumension EMSS Agent Upgrade for Windows, 7.1 (See Notes)... | Active | Critical | False | 9/22/2011 2:08:23 PM |
| Microsoft Silverlight (KB2512827) | Active | Software | False | 10/23/2012 7:08:08 PM |
| Mozilla Firefox (English) 3.5.7 for Windows (Full/Upgrade) | Active | Software | False | 2/25/2010 4:32:14 PM |
| MS 958911 (French) Update for GDI+ for Windows XP and Window... | Beta | Recommended | False | 12/4/2013 6:25:11 AM |
| MS09-033 Security Update for Microsoft Virtual Server 2005 (KB96... | Active | Critical - 01 | False | 6/28/2010 1:11:05 PM |
| MS10-015 Security Update for Windows 2000 (KB977165) | Active | Critical - 05 | False | 6/28/2010 1:11:05 PM |
| MS10-015 Security Update for Windows 7 (KB977165) | Active | Critical - 05 | False | 6/28/2010 1:11:05 PM |
| MS10-015 Security Update for Windows Server 2003 (KB977165) | Active | Critical - 05 | False | 6/28/2010 1:11:05 PM |
| MS10-015 Security Update for Windows Server 2008 (KB977165) | Active | Critical - 05 | False | 1/14/2013 4:34:58 PM |

Patches found: 108

Custom patches that you create beginning with the word 'Detect' in their titles or of the 'Detection' impact type cannot be deleted.

Figure 84: Delete Patch Page: Search Results

4. Select the patch item to delete.
5. Click **Delete**.

   **Step Result:** A confirmation dialog appears.

6. Click **Yes** to confirm the deletion.

   **Step Result:** The patch item is removed from the ***Delete Patch*** page.

   > **Note:**

**Result:** The selected patch gets deleted from the Ivanti Content Wizard database.

> **Note:** Any patches deleted from the patch subscription will be automatically downloaded again during the next full patch replication cycle.

## Saving a Copy of a Patch

The Ivanti Content Wizard lets you create patches and save a copy of the patch.

TheIvanti Content Wizard lets you save a copy of a patch. This may save time and effort if you require a patch that has desirable content and do not want recreate the patch from scratch.

1. Select **File** > **Save Copy**.

   **Step Result:** The ***Copy Patch*** dialog opens.

2. [Optional] Type a new patch name in the **Patch Name** field.

   The **Patch Name** field defaults to the original name of the patch followed by `- Copy`.

3. Click **OK**.

   **Step Result:** The patch is saved and the new patch is now opened in the ***Patch Properties*** page.

   **Tip:** The **Title** field in ***Patch Properties*** page contains the name given to the patch.

# Chapter 10

# Importing and Exporting Patches

**In this chapter:**

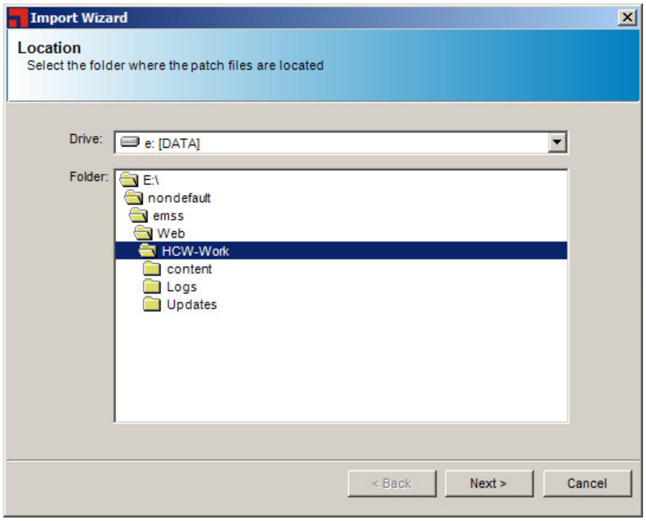
The Ivanti Content Wizard allows for transferring custom patches from one Ivanti Endpoint Security (Endpoint Security) server to another. The import and export features allow for exporting a patch to a physical `.plfz` file. After export, the patch can be stored, emailed, or uploaded to another Endpoint Security server.

## Importing Patches Using the Import Wizard

The Ivanti Content Wizard ***Import Wizard*** lets you import patches from an external folder into the wizard. The wizard is especially useful for importing multiple variations of a patch.

1. Select **File** > **Import Wizard**.

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



Import Wizard

Location

Select the folder where the patch files are located

Drive: e: [DATA]

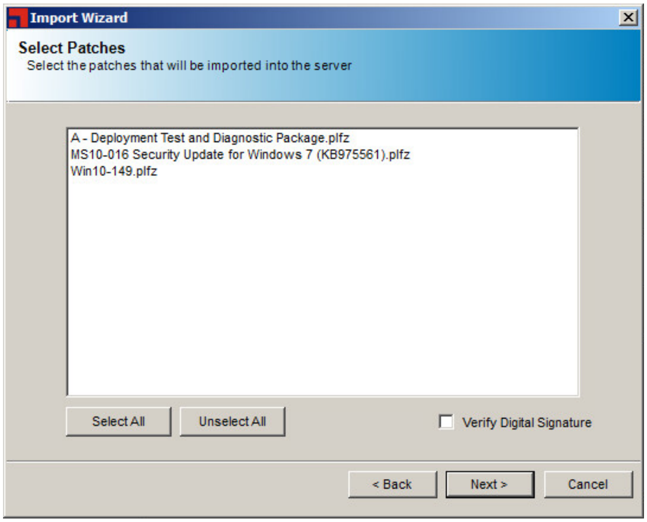
Folder: E:\ nondefault emss Web HCW-Work content Logs Updates

Figure 85: Location Page

2. Navigate to the folder where the patches that you want to import are located.

3. Click **Next**.

   **Step Result:** The ***Select Patches*** page opens.



Select Patches

Select the patches that will be imported into the server

A - Deployment Test and Diagnostic Package.plfz
MS10-016 Security Update for Windows 7 (KB975561).plfz
Win10-149.plfz

□ Verify Digital Signature

Figure 86: Select Patches Page

4. Select the patches you want to import.

   **Note:** If there are multiple variations of the same patch, it may be due to different signatures for different operating systems, languages, and regions.

5. To verify the patch's digital signature, select the **Verify Digital Signature** check box.
6. Click **Next**.

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

7. [Optional] View the ***Import Summary*** page.

   a) Click **Preview** to view the ***Import Summary*** page prior to selecting **Import**.

      **Step Result:** The ***Import Summary*** page displays information concerning the patch.

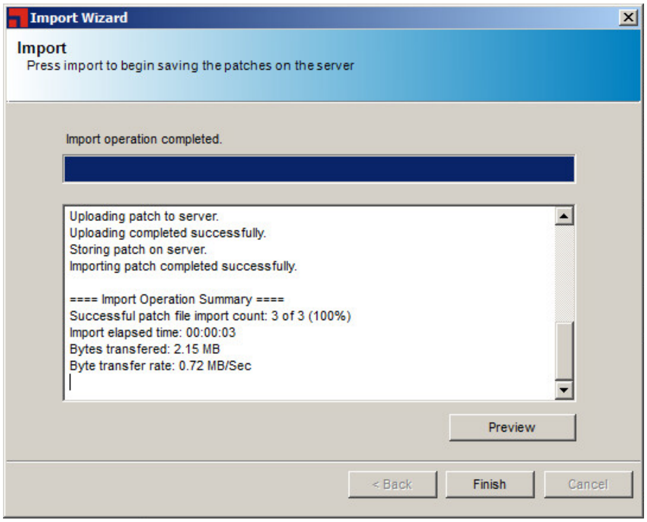
      **Note:** For information on patch properties, refer to The Patch Properties Page on page 35.

   b) Click **File** > **Exit**.

      **Step Result:** The ***Import Summary*** page closes.

8. Click **Import**.

   **Step Result:** The import begins and finishes.



Import operation completed.

```
Uploading patch to server.
Uploading completed successfully.
Storing patch on server.
Importing patch completed successfully.

==== Import Operation Summary ====
Successful patch file import count: 3 of 3 (100%)
Import elapsed time: 00:00:03
Bytes transfered: 2.15 MB
Byte transfer rate: 0.72 MB/Sec
```

Figure 87: Import Page: Completion

> **Note:** The ***Import Wizard*** may take several minutes depending on the number of patches, size of each patch, and the total number of files and directories it contains.

9. Click **Finish**.

   **Step Result:** The ***Import*** page closes.

**Result:** The patches are imported into the Ivanti Endpoint Security server.

## Importing Patches from the Command Line

You can use specific commands to import patches into the Ivanti Endpoint Security server. Command line patch importing makes the use of specific switch commands to carry out the task.

Use a command line to import patches into the Ivanti Endpoint Security server.

1. Open a command prompt window on the computer that contains Ivanti Content Wizard client component.
2. Navigate to the Ivanti Content Wizard directory.

   a) Type `cd\`.
   b) Type the location of the Ivanti Content Wizard directory.

   **Example:** Type `cd Program Files\HEAT Software\Content Wizard` and press `ENTER`.

3. Type the command to import the patch file.

   Following the prompt type the following command syntax: **`ICW.exe -i -u -s "SERVERNAME" -p "SERIAL NUMBER or SA PASSWORD" -plf "FULL PATH TO PLFZ FILE" -l ["FULL PATH TO LOG FILE"]`**.

   The following table explains the switch commands used in the syntax:

   Table 13: Command Line Switch Descriptions

| Switch | Description |
|---|---|
| `-i` | Use Import Mode (Required). |
| `-u` | Use Unattended Mode (Required). |
| `-s` | Set the server name (Required). |
| `-p` | Set the serial number or SA password if the default SA password has been changed (Required). |
| `-plf` | Set the full path to the .plfz file. Each patch may be separated by a vertical bar "\|" in order to include multiple patches (Required). |
| `-l` | Create a log file. If a path is not specified the log will be created in the Ivanti Content Wizard Program Files Directory (Optional). |

**Result:** The patches are imported into the Ivanti Endpoint Security server.

**Example:**

Import the patch `MS02-04.PLFZ` without a log file. **`ICW.exe -i -u -s "myserver" -p "xxxxxxxx-xxxxxxxx" -plf "C:\Patches\MS02-04.PLFZ"`**

Import the patch `MS02-04.PLFZ` with a log file. **`ICW.exe -i -u -s "myserver" -p "xxxxxxxx-xxxxxxxx" -plf "C:\Patches\MS02-04.PLFZ" -l "log.txt"`**

## Exporting Patches Using the Export Wizard

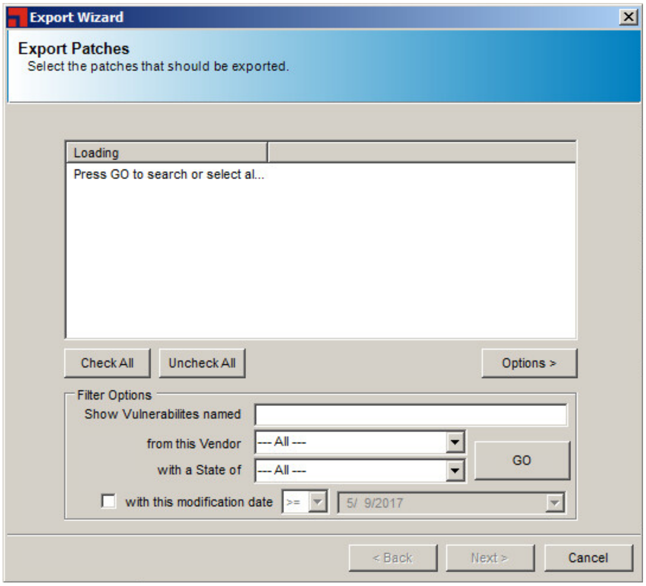
The ***Export Wizard*** exports custom patches from the Ivanti Endpoint Security server to a specified folder. By exporting patches, you can import them into other Endpoint Security servers without having to recreate the patch.

**Prerequisites:**

Ensure that the selected archive folder has sufficient free space for the exported patches. Your `%TEMP%` folder must also have several hundred megabytes free to successfully export large patches.

1. Select **File** > **Export Wizard**.

   **Step Result:** The ***Export Patches*** page opens.



Export Patches

Select the patches that should be exported.

Loading

Press GO to search or select al...

Show Vulnerabilites named

from this Vendor: --- All ---

with a State of: --- All ---

☐ with this modification date >= 5/ 9/2017

Figure 88: Export Patches Page

2. [Optional] Set filter options to find the patches you want to export.

   Configure one or more of the filters.

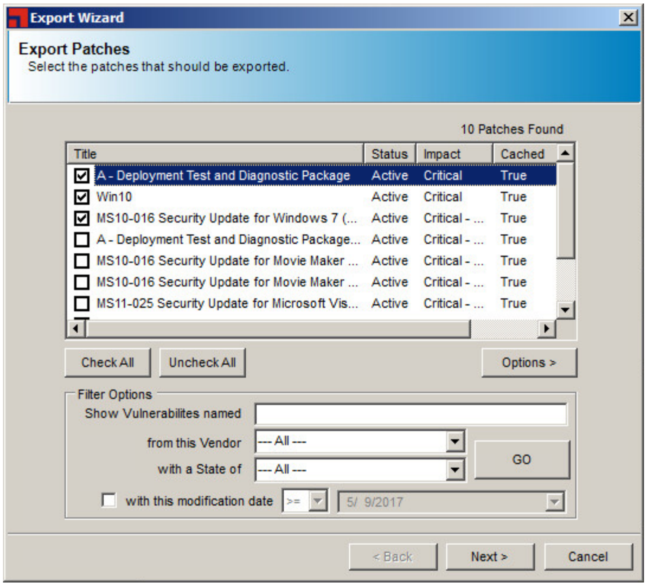
   - To filter by name, type a patch name in the **Show Vulnerabilities named** field.

   **Tip:** You can use the underscore character ( _ ) as a wildcard.

   - To filter by vendor, make a selection from the **from this Vendor** drop-down.
   - To filter by patch state, make a selection from the **with a State of** drop-down.
   - To filter by date, select **with this modification date** checkbox, and then choose date options.

3. Click **GO**.

   **Step Result:** The list is displayed in the ***Export Patches*** window.



Export Wizard

Export Patches

Select the patches that should be exported.

10 Patches Found

| Title | Status | Impact | Cached |
|---|---|---|---|
| ☑ A - Deployment Test and Diagnostic Package | Active | Critical | True |
| ☑ Win10 | Active | Critical | True |
| ☑ MS10-016 Security Update for Windows 7 (... | Active | Critical - ... | True |
| □ A - Deployment Test and Diagnostic Package... | Active | Critical - ... | True |
| □ MS10-016 Security Update for Movie Maker ... | Active | Critical - ... | True |
| □ MS10-016 Security Update for Movie Maker ... | Active | Critical - ... | True |
| □ MS11-025 Security Update for Microsoft Vis... | Active | Critical - ... | True |

Filter Options

Show Vulnerabilites named

from this Vendor --- All ---

with a State of --- All ---

□ with this modification date >= 5/ 9/2017

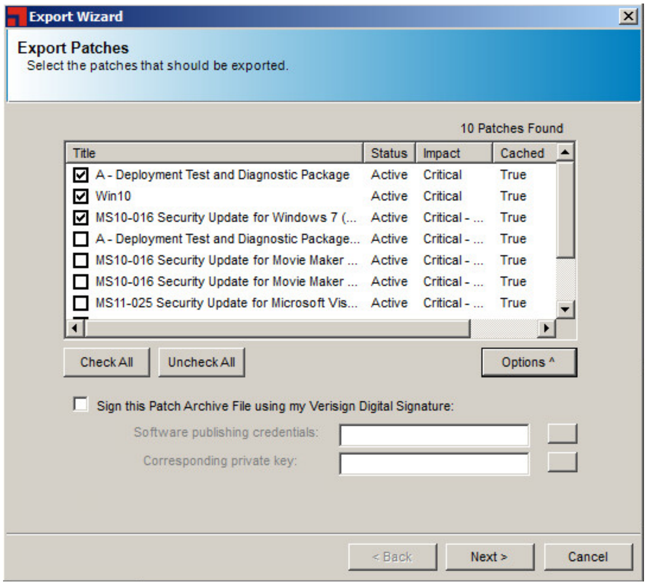
Figure 89: Export Patches Page: List

4. Select the patches you want to export.

5. If you want to sign the patches you're exporting with a digital signature, toggle **Options**.

   If you don't want to sign them, skip to step 14.

   **Step Result:** The ***Filter Options*** area closes and is replaced by a ***Digital Signature*** area.



Export Patches

Select the patches that should be exported.

10 Patches Found

| Title | Status | Impact | Cached |
|---|---|---|---|
| ☑ A - Deployment Test and Diagnostic Package | Active | Critical | True |
| ☑ Win10 | Active | Critical | True |
| ☑ MS10-016 Security Update for Windows 7 (... | Active | Critical - ... | True |
| □ A - Deployment Test and Diagnostic Package... | Active | Critical - ... | True |
| □ MS10-016 Security Update for Movie Maker ... | Active | Critical - ... | True |
| □ MS10-016 Security Update for Movie Maker ... | Active | Critical - ... | True |
| □ MS11-025 Security Update for Microsoft Vis... | Active | Critical - ... | True |

□ Sign this Patch Archive File using my Verisign Digital Signature:

Software publishing credentials:

Corresponding private key:

Figure 90: Export Patches Page: Digital Signature

6. [Optional] To include a digital signature, select the **Sign this Patch Archive File using My Verisign Digital Signature** check box.

   **Step Result:** The **Software publishing credentials** and the **Corresponding private key** fields become active.

7. In the **Software publishing credentials** field, click **Search**.

   **Step Result:** A ***Locate Software Publishing Credential*** page opens.

8. Locate the Verisign certificate you want to use.

   The certificate will be in the form of a `.spc` file.

9. Click **Open**.

   **Step Result:** The **Software publishing credentials** field displays the `.spc` file.

10. In the **Corresponding private key** field, click **Search**.

    **Step Result:** The ***Locate Private Key*** page opens.

11. Locate the Verisign private key you want to use.

    The key will be in the form of a `.pvk` file.

**12.**Click **Open**.

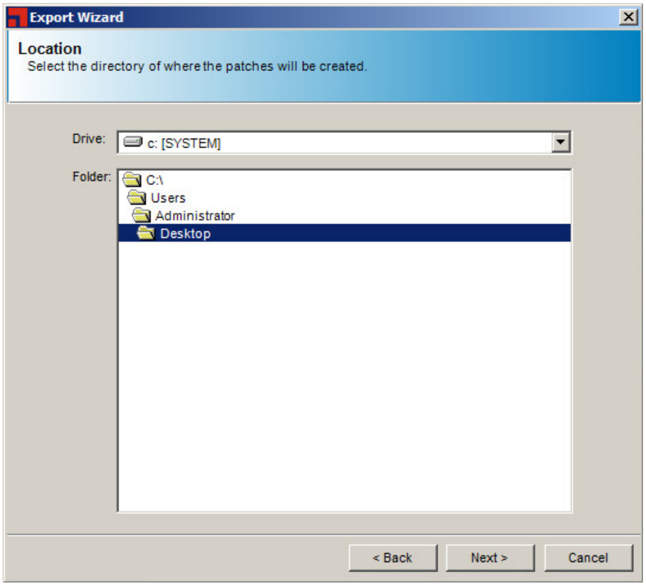
**Step Result:** The **Corresponding private key** field displays the `.pvk` file.

**13.**Verify the patch information is correct.

**Note:** If you want to sign a patch with your Verisign digital signature, you must make sure the internet connection is working. This functionality will not work in an AirGap environment because the timestamp part of the signature requires an internet connection.

**14.**Click **Next**.

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



Export Wizard

Location

Select the directory of where the patches will be created.

Drive: c: [SYSTEM]

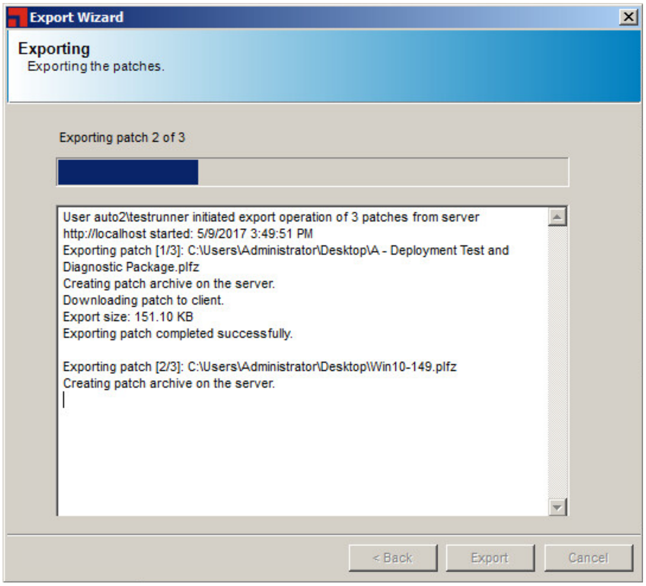
Folder: C:\ Users Administrator Desktop

Figure 91: Location Page

**15.**Select the folder where the patches will be exported.

16. Click **Next**.

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



Exporting patch 2 of 3

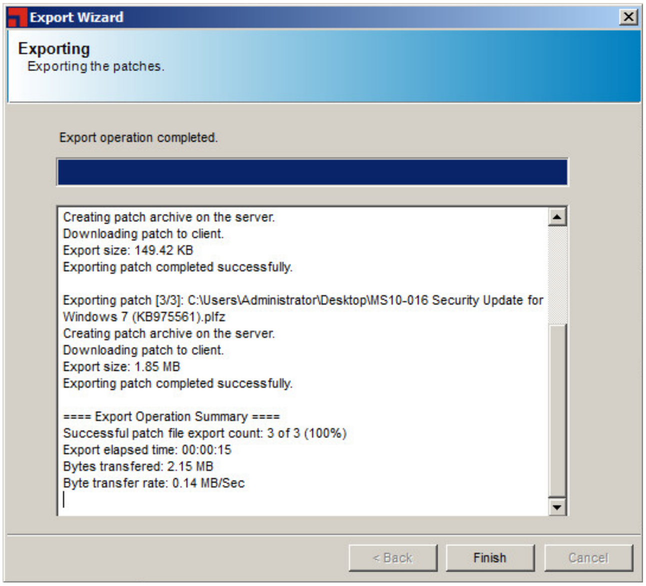
```
User auto2\testrunner initiated export operation of 3 patches from server
http://localhost started: 5/9/2017 3:49:51 PM
Exporting patch [1/3]: C:\Users\Administrator\Desktop\A - Deployment Test and
Diagnostic Package.plfz
Creating patch archive on the server.
Downloading patch to client.
Export size: 151.10 KB
Exporting patch completed successfully.

Exporting patch [2/3]: C:\Users\Administrator\Desktop\Win10-149.plfz
Creating patch archive on the server.
```

Figure 92: Exporting Page

17.Click **Export**.

The **Export operation completed** bar displays the progress of the export process.

**Step Result:**



```
Creating patch archive on the server.
Downloading patch to client.
Export size: 149.42 KB
Exporting patch completed successfully.

Exporting patch [3/3]: C:\Users\Administrator\Desktop\MS10-016 Security Update for
Windows 7 (KB975561).plfz
Creating patch archive on the server.
Downloading patch to client.
Export size: 1.85 MB
Exporting patch completed successfully.

==== Export Operation Summary ====
Successful patch file export count: 3 of 3 (100%)
Export elapsed time: 00:00:15
Bytes transfered: 2.15 MB
Byte transfer rate: 0.14 MB/Sec
```

Figure 93: Exporting Page: Completion

18.Click **Finish**.

**Step Result:** The ***Exporting*** page closes.

**Result:** The patches are exported to the selected folder. The `.plfz` file generated will have a maximum filename length of 120 characters.

# Chapter 11

# Using Content Wizard Tools

**In this chapter:**

The **Tools** menu in the Ivanti Content Wizard uses simple wizards to help you perform tasks for creating patches and maintaining a company network.

## The New Patch Wizard

The ***New Patch Wizard*** allows you to use the ***Patch Creation Wizard*** to create patches for endpoints hosting Windows operating systems.

For details on creating patches for endpoints hosting Windows operating systems, refer to Using the New Patch Wizard on page 162.

**Important:** You cannot create non-Windows patches using the ***Patch Creation Wizard***. If you want to create a non-Windows patch, refer to Creating a Linux Patch on page 137.

## Available Patch Types in the Patch Creation Wizard

The **New Patch Wizard** allows you to use the ***Patch Creation Wizard*** to create patches for endpoints hosting Windows operating systems. Using the wizard, you can create patches for installers, setup programs, Windows script files, and so on.

The following defines each patch type.

| Patch Type | Description |
|---|---|
| **Microsoft System Install (MSI)** | A patch that utilizes a `Microsoft Installer` (`*.msi`) file type. Provides the most common type of installable file on the Windows platform. |
| **Microsoft System Install Patch (MSP)** | A patch that utilizes a `Microsoft Installer Patch` (`*.msp`) file type. Provides the ability to install a patch update to an existing `.msi`-based software installation. |
| **Windows Update Stand-alone Installer (MSU)** | A patch that utilizes the `Windows Update` (`*.msu`) file type. This allows for the updates of applications and files that are installed by the `Windows Update Stand-alone Installer(Wusa.exe).`<br>**Note:** The `Windows Update` (`*.msu`) file type was first introduced by Microsoft in Windows Vista and higher. |
| **Legacy InstallShield Setup** | Allows a setup program (`SETUP.EXE`) and a silent response file (`SETUP.ISS`) to be specified. To create a silent response file for one of these legacy installation programs, run **`SETUP.EXE -r`**; then fill out the install parameters as usual and the InstallShield setup program will create an output response file `SETUP.ISS`. |
| **Command Line Executable** | Turns any command-line DOS or Windows program into a deployable patch that can be used with the Ivanti Endpoint Security (Endpoint Security). |
| **VBScript or JavaScript** | Converts any working Windows script file written in VBScript or JavaScript into a deployable patch. Typical uses would include the automation of certain daily tasks or software cleanup for workstations managed by the Endpoint Security. |

## Using the New Patch Wizard

The ***New Patch Wizard*** allows the creation of patches for Windows only operating systems using a variety of common installable file types.

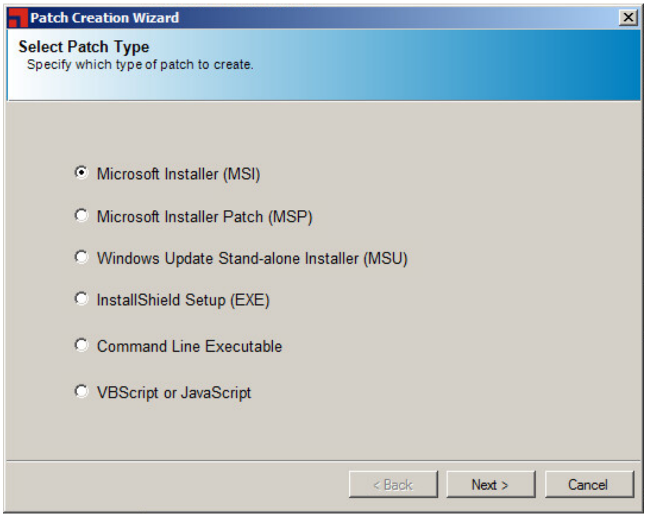
Use the ***New Patch Wizard*** to create patch content based on the **Microsoft Installer (MSI)** file type.

1. Select **Tools** > **New Patch Wizard**.

   **Step Result:** The ***Select Patch Type*** page opens.

2. Select one of the following patch types:
   - **Microsoft Installer (MSI)**
   - **Microsoft Installer Patch (MSP)**
   - **Windows Update Stand-alone Installer (MSU)**
   - **Legacy InstallShield Setup**
   - **Command Line Executable**
   - **VBScript or JavaScript**

   For a description of available patch types, see Available Patch Types in the Patch Creation Wizard on page 162.



Patch Creation Wizard

**Select Patch Type**

Specify which type of patch to create.

● Microsoft Installer (MSI)

○ Microsoft Installer Patch (MSP)

○ Windows Update Stand-alone Installer (MSU)

○ InstallShield Setup (EXE)

○ Command Line Executable

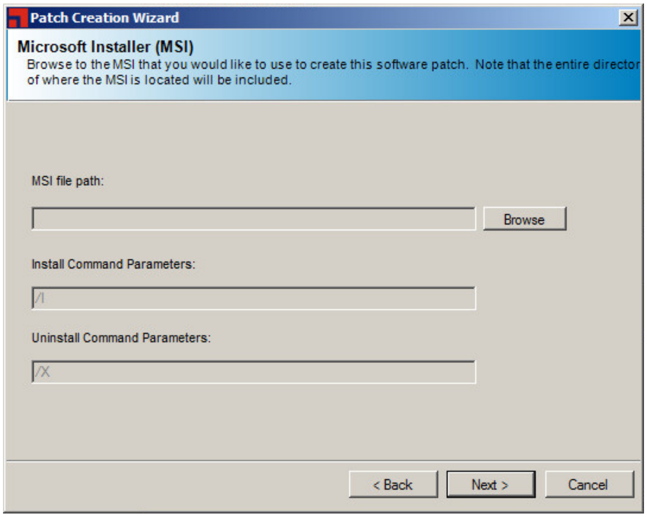
○ VBScript or JavaScript

Figure 94: Select Patch Type Page

3. Click **Next**.

   **Step Result:** The applicable patch type page opens.

   > **Note:** The following steps were created using the **Microsoft Installer (MSI)** option, which is the most common type of installable file on the Windows platform. Other patch types use similar steps.



Patch Creation Wizard

Microsoft Installer (MSI)

Browse to the MSI that you would like to use to create this software patch. Note that the entire director of where the MSI is located will be included.

MSI file path:

Install Command Parameters: /I

Uninstall Command Parameters: /X

Figure 95: Microsoft Installer (MSI) Page

4. Specify the installer details.

   a) Click **Browse** to add the installer you want to include in the patch.

   b) [Optional] If needed, change the **Install Command Parameters**

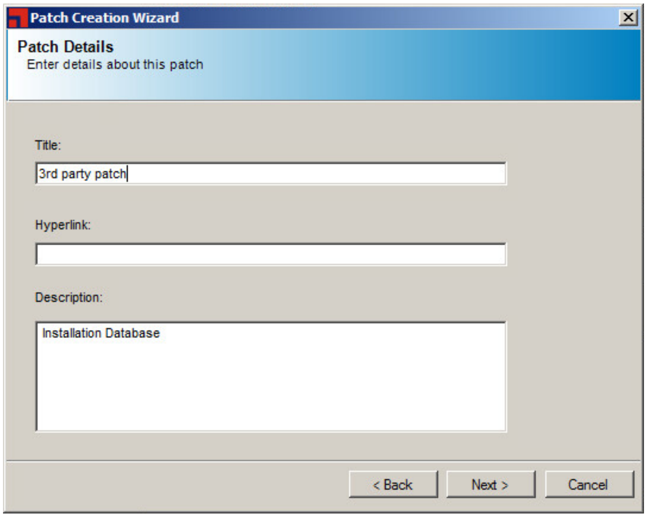
      By default, the field displays **/I**.

   c) [Optional] If needed, change the **Uninstall Command Parameters**.

      By default, the field displays **/X**.

5. Click **Next**.

   **Step Result:** The ***Patch Details*** page opens.



Title:

3rd party patch

Description:

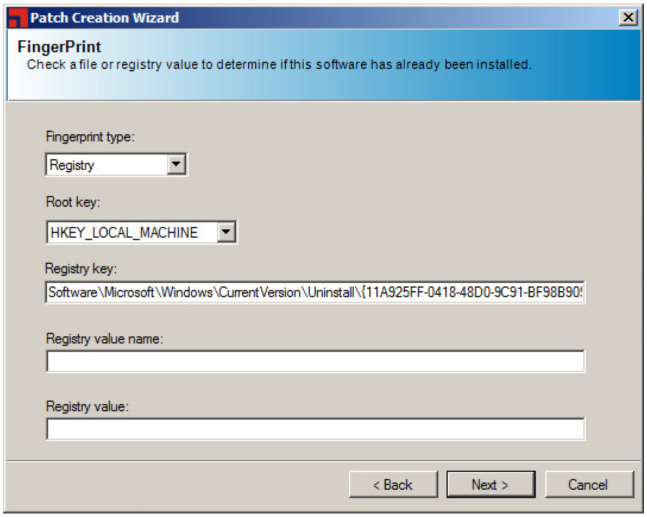
Installation Database

Figure 96: Patch Details Page

6. Add or modify the title of the patch in the **Title** field.
7. Add or modify the hyperlink to the location where users can find more information about the patch in the **Hyperlink** field.
8. Add or modify the patch's description in the **Description** field.

9. Click **Next**.

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



**FingerPrint**

Check a file or registry value to determine if this software has already been installed.

Fingerprint type: Registry

Root key: HKEY_LOCAL_MACHINE

Registry key: Software\Microsoft\Windows\CurrentVersion\Uninstall\{11A925FF-0418-48D0-9C91-BF98B90

Registry value name:

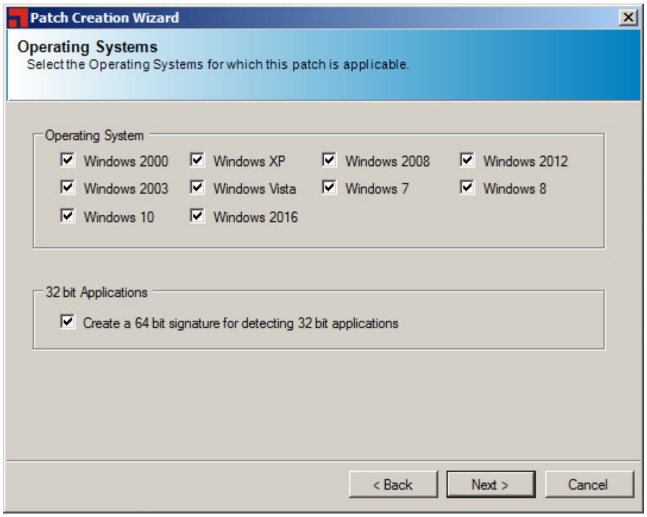
Registry value:

Figure 97: FingerPrint Page

10. Select the type of fingerprint from the **Fingerprint type** drop-down list.
11. Select a root key from the **Root Key** drop-down list.
12. [Optional] If required, type the registry key (including the key path) in the **Registry Key** field.
13. [Optional] If required, include a registry value data:
    a) Type the name of the registry value in the **Registry value name** field.
    b) Type the value of the registry key in the **Registry Value** field.

c) Click **Next**.

**Step Result:** The ***Operating Systems*** page opens.



Operating Systems

Select the Operating Systems for which this patch is applicable.

Operating System

☑ Windows 2000 ☑ Windows XP ☑ Windows 2008 ☑ Windows 2012
☑ Windows 2003 ☑ Windows Vista ☑ Windows 7 ☑ Windows 8
☑ Windows 10 ☑ Windows 2016

32 bit Applications

☑ Create a 64 bit signature for detecting 32 bit applications

Figure 98: Operating Systems Page

**14.**Select the Windows operating systems to which the patch applies.

**15.**To create a signature for detecting 32-bit applications, select the **Create a 64 bit signature for detecting 32 bit applications** check box.

**16.**Click **Next**.

**Step Result:** The ***Summary*** page opens allowing you to verify details.

**17.**Click **Finish**.

**Step Result:** The ***Summary*** page closes and the ***Patch Properties*** page displays.

**18.**[Optional] The ***Patch Properties*** page displays properties associated with the selected patch. Review and edit the patch properties as needed.

**Note:** For information on ***Patch Properties***, refer to The Patch Properties Page on page 35.

19. Select **File** > **Save**.

    **Step Result:** The patch is stored within the Ivanti Endpoint Security server.

**Result:** The ***Patch Creation Wizard*** creates a Windows patch with all of the attributes you have specified. The patch editing window opens after patch creation completes, allowing you to modify the attributes of the new patch.

> **Note:** You cannot create non-Windows patches using the ***Patch Creation Wizard***. If you want to create a non-Windows patch, refer to Creating a Linux Patch on page 137.

# The Uninstall Wizard

The ***Uninstall Wizard*** allows administrators to create policy patches that can uninstall unwanted software from workstations in a network.

Most organizations today allow employees to install software on their workstations. This can lead to a wide variety of unwanted applications that may pose potential risks from security vulnerabilities within the software itself or data breach through file-sharing and chat software.

The ***Uninstall Wizard*** helps administrators guard their network against the risks posed by unauthorized software installation. While this wizard cannot remove viruses or malicious software from a system, it can be used to uninstall all types of unwanted software.

## Using the Uninstall Wizard

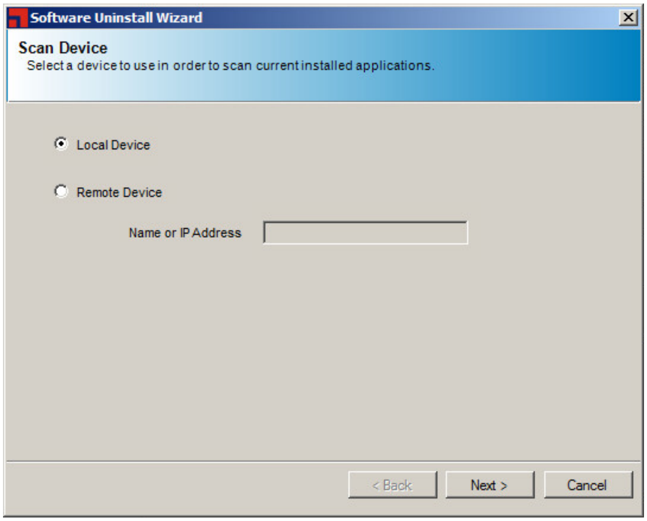
Use the ***Uninstall Wizard*** to scan workstations for unauthorized software. If unauthorized software is found, the wizard lets you remove it from the workstation.

**Prerequisites:**

Log in to the Ivanti Endpoint Security server from the Ivanti Content Wizard.

1. Select **Tools** > **Uninstall Wizard**.

   **Step Result:** The ***Scan Device*** page of the ***Software Uninstall Wizard*** window opens.



Software Uninstall Wizard

Scan Device

Select a device to use in order to scan current installed applications.

● Local Device

○ Remote Device

Name or IP Address

Figure 99: Scan Device Page

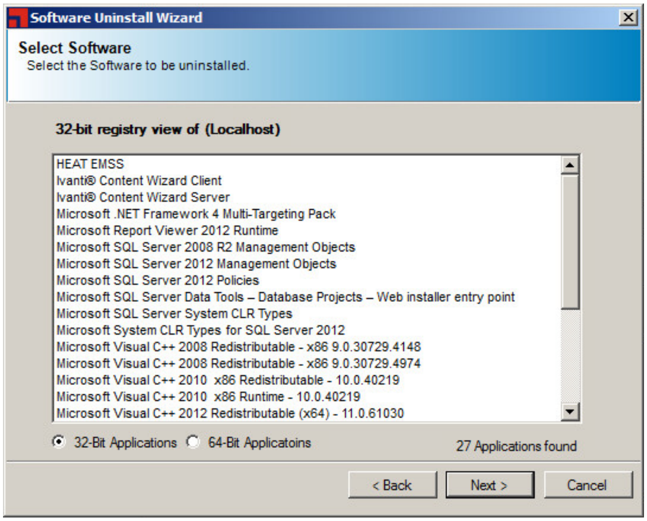
2. Select which device you want to scan for software.

   - Select **Local Device** to scan a locally connected device.
   - Select **Remote Device** to scan a device to which you are allowed remote access.

   **Note:** If you are accessing a remote device, remote registry service must be running on the device, and you should be logged in with workstation administrator or domain administrator credentials.

3. Click **Next**.

   **Step Result:** The ***Select Software*** page opens.



Software Uninstall Wizard

Select Software

Select the Software to be uninstalled.

32-bit registry view of (Localhost)

HEAT EMSS
Ivanti® Content Wizard Client
Ivanti® Content Wizard Server
Microsoft .NET Framework 4 Multi-Targeting Pack
Microsoft Report Viewer 2012 Runtime
Microsoft SQL Server 2008 R2 Management Objects
Microsoft SQL Server 2012 Management Objects
Microsoft SQL Server 2012 Policies
Microsoft SQL Server Data Tools – Database Projects – Web installer entry point
Microsoft SQL Server System CLR Types
Microsoft System CLR Types for SQL Server 2012
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4974
Microsoft Visual C++ 2010  x86 Redistributable - 10.0.40219
Microsoft Visual C++ 2010  x86 Runtime - 10.0.40219
Microsoft Visual C++ 2012 Redistributable (x64) - 11.0.61030

● 32-Bit Applications ○ 64-Bit Applicatoins

27 Applications found

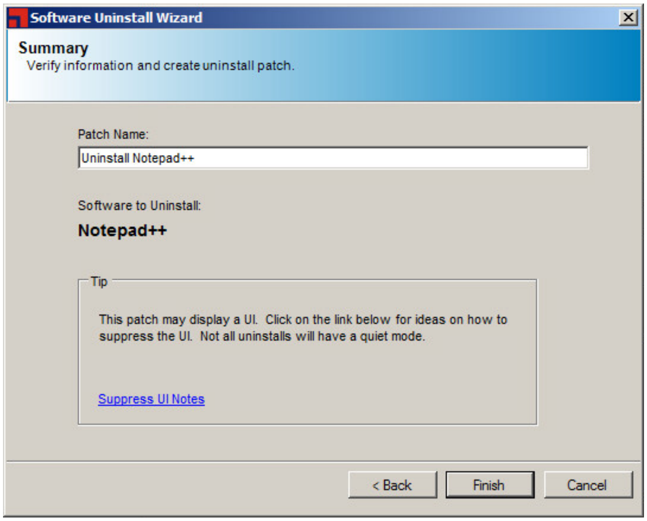
Figure 100: Select Software Page

4. Select either the **32-Bit Applications** or the **64-Bit Applications** radio button, and the select the program you want to uninstall.

   The ***Select Software*** page displays a list of all 32- or 64-bit sub-components that can be uninstalled (based on the radio button that you select).

5. Click **Next**.

   **Step Result:** The ***Summary*** page opens allowing you to verify details.



Software Uninstall Wizard

Summary

Verify information and create uninstall patch.

Patch Name: Uninstall Notepad++

Software to Uninstall:

Notepad++

Tip

This patch may display a UI. Click on the link below for ideas on how to suppress the UI. Not all uninstalls will have a quiet mode.

Suppress UI Notes

Figure 101: Summary

6. [Optional] If applicable modify the name of the patch in the **Patch Name** field.
7. Click **Finish**.

   **Step Result:** The ***Summary*** page closes and the ***Patch Properties*** page displays.

8. [Optional] The ***Patch Properties*** page displays properties associated with the selected patch. Review and edit the patch properties as needed.

   **Note:** For information on ***Patch Properties***, refer to The Patch Properties Page on page 35.

9. Select **File** > **Save**.

   **Step Result:** The patch is stored within the Ivanti Endpoint Security server.

**Result:** A patch is created to uninstall software from a workstation.

> **Note:** Uninstall patches will appear as patched if the software is installed on the device. Not all applications can be uninstalled by default, but users can change the templates as needed.

## The Power Management Wizard

The ***Power Management Wizard*** allows you to create a patch to manage power settings for workstations within a network. Using this simplified power policy creation method, you can manage the enforcement of environmentally friendly policies in distributed environments.

Using the ***Power Management Wizard*** allows you to create a patch to manage power settings. To deploy packages containing power management policies to applicable endpoints you use the ***Deployment Wizard*** within the Ivanti Endpoint Security.

**Note:** Refer to *Creating an Endpoint Deployment* or *Creating a Group Deployment* in the Ivanti Endpoint Security: Patch and Remediation User Guide (https://www.ivanti.com/support/product-documentation) for deployment information.

A package containing a power management policy can have its behavior changed by selecting behavior options. For instance, you may want to completely uninstall a power management policy from an endpoint. The options are found in the ***Package Deployment Behavior Options*** page within the ***Deployment Wizard***.

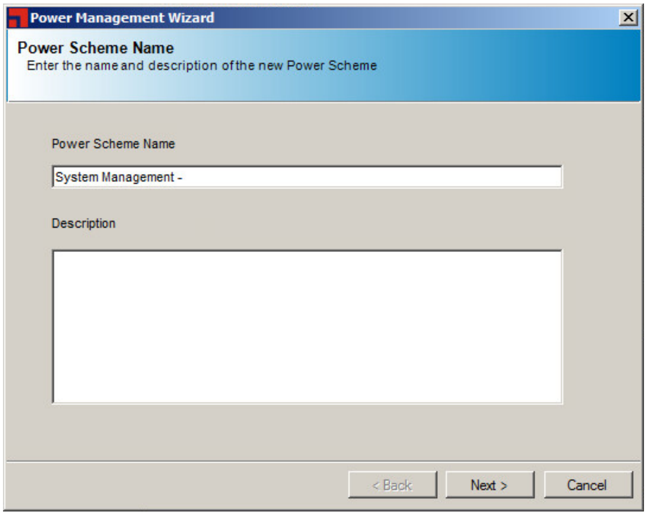
**Important:** To completely remove a power management policy on an endpoint, you would choose **uninstall the package** and **debug mode** behavior options before deploying the package to all applicable endpoints. Refer to the *Package Deployment Behavior Options Page* in the Ivanti Endpoint Security: Patch and Remediation User Guide (https://www.ivanti.com/support/product-documentation) for additional information on changing deployment behavior options.

## Using the Power Management Wizard

The ***Power Management Wizard*** allows the administrator to set local power policy settings on all workstations within the network.

1. Select **Tools** > **Power Management Wizard**.

   **Step Result:** The ***Power Scheme Name*** page of the ***Power Management Wizard*** window opens.



Power Management Wizard

Power Scheme Name

Enter the name and description of the new Power Scheme

Power Scheme Name: System Management -

Description:

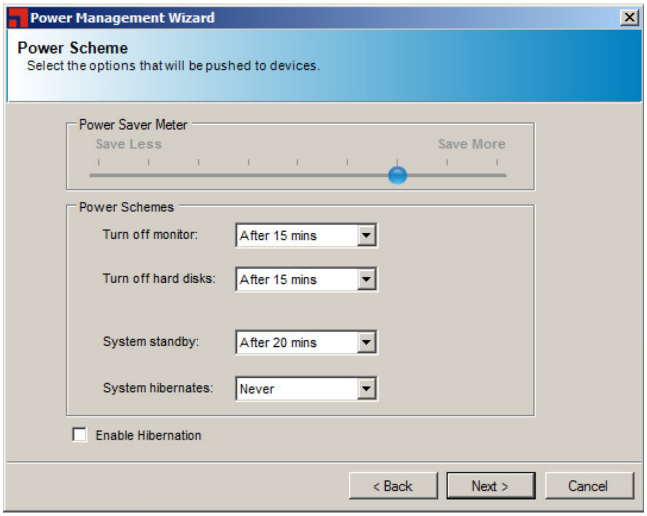
Figure 102: Power Scheme Name Page

2. Type a unique name in the **Power Scheme Name** field.

   The default name is `System Management -`.
3. Type a description of the power scheme in the **Description** field.

4. Click **Next**.

   **Step Result:** The ***Power Scheme*** page opens.



Power Management Wizard

Power Scheme

Select the options that will be pushed to devices.

Power Saver Meter

Power Schemes

Turn off monitor: After 15 mins

Turn off hard disks: After 15 mins

System standby: After 20 mins

System hibernates: Never

□ Enable Hibernation

Figure 103: Power Scheme Page

5. [Optional] Select the **Power Saver Meter** icon and slide it to a desired power saver setting.

   The ***Power Schemes*** settings will automatically adjust based on the slider adjustment level.

6. Select the ***Power Schema*** options.

   a) Select after how long the monitor will be switched off from the **Turn off monitor** drop-down list.

   b) Select after how long the hard disk will be switched off from the **Turn off hard disks** drop-down list.

   c) To force devices into standby mode after a specific period, select the desired time from the **System standby** drop-down list.

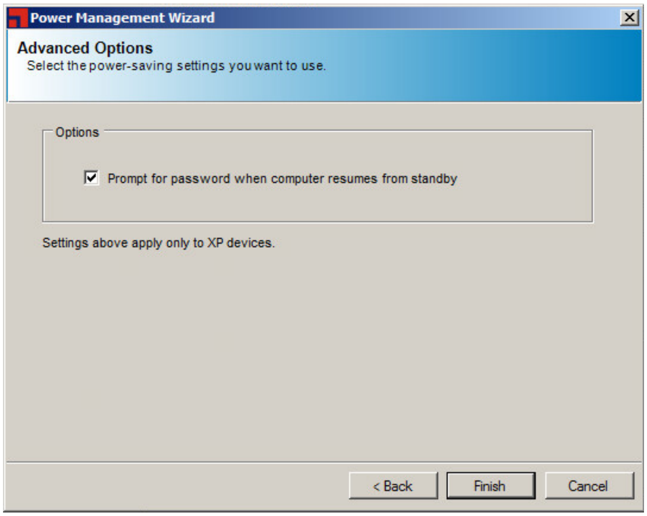
   d) To force devices to go into hibernate mode after a specific period, select the desired time from the **System hibernates** drop-down list.

7. [Optional] To enable hibernation, select the **Enable Hibernation** check box.

**Note:** When a device enters hibernation, a snapshot of the device settings and memory content of the device is taken. The information is saved to a local hard disk prior to the device shutting down. When you restart the device, all the settings and memory content are restored to their original state.

8. Click **Next**.

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



Power Management Wizard

Advanced Options

Select the power-saving settings you want to use.

Options

☑ Prompt for password when computer resumes from standby

Settings above apply only to XP devices.

Figure 104: Advanced Options Page

9. [Optional] To require the user to log into the device when waking it from standby, ensure the **Prompt for password when computer resumes from standby** check box is selected.

   This option is selected by default.

10. Click **Finish**.

    **Step Result:** The ***Advance Option*** page closes and the ***Patch Properties*** page displays.

11. [Optional] The ***Patch Properties*** page displays properties associated with the selected patch. Review and edit the patch properties as needed.

    **Note:** For information on ***Patch Properties***, refer to The Patch Properties Page on page 35.

12. Select **File** > **Save**.

    **Step Result:** The patch is stored within the Ivanti Endpoint Security server.

**Result:** A patch is created to manage power settings for workstations.

To complete the deployment process, you deploy package content using the ***Deployment Wizard*** to applicable endpoints.

**Note:** Refer to *Creating an Endpoint Deployment* or *Creating a Group Deployment* in the Ivanti Endpoint Security: Patch and Remediation User Guide (https://www.ivanti.com/support/product-documentation) for deployment information.

## The Policy Wizard

The ***Policy Wizard*** allows you to create new policy patches that can enforce local Windows security policies on managed devices within your network.

The ***Policy Wizard*** allows you to choose the type of policy you want to create:

- The **Select individual policies** option allows you to choose predefined standard Windows local policy items. For further information, refer to Selecting Standard Windows Local Policy Items on page 177.
- The **Security template file** option allows you to specify your own local security template file defined within the Microsoft Security Template add-on for Microsoft Management Console (MMC). For further information, refer to Creating a Policy Patch Using a Security Template File on page 182.

**Note:** For additional information on the Microsoft Security Template add-on, refer to MSDN Library: Security Templates (http://msdn.microsoft.com/en-us/library/bb521615(v=winembedded.51).aspx).

Once created, the policy patch can be deployed to some or all of the workstations within the network to enforce the default local policy settings. The patch can also be used within a mandatory baseline to enforce compliance to local security policy settings automatically for all devices within that group.

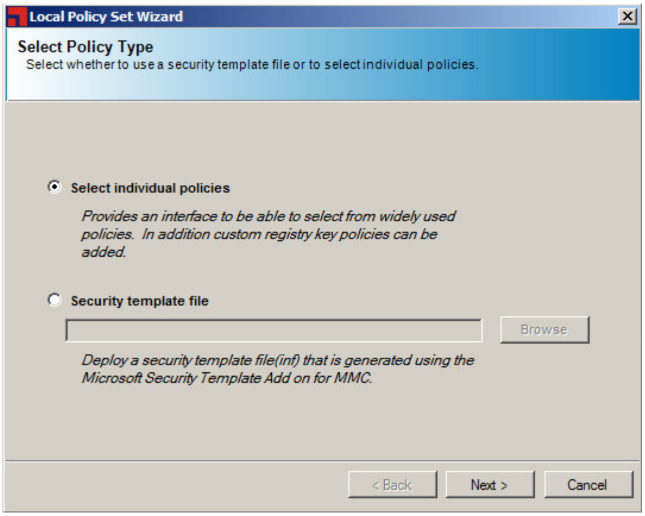
**Note:** If the administrator chooses a domain or active directory managed environment, the policy settings may be overridden by domain policies for users who are logging in with their domain credentials.

## Selecting Standard Windows Local Policy Items

The ***Policy Wizard*** allows you to choose the type of policy you want to create. Choose the **Select individual policies** option to specify a predefined standard Windows local policy item.

1. Select **Tools** > **Policy Wizard**.

   **Step Result:** The ***Select Policy Type*** page of the ***Local Policy Set Wizard*** window opens.



Local Policy Set Wizard

Select Policy Type

Select whether to use a security template file or to select individual policies.

● Select individual policies

*Provides an interface to be able to select from widely used policies. In addition custom registry key policies can be added.*

○ Security template file

*Deploy a security template file(inf) that is generated using the Microsoft Security Template Add on for MMC.*

Figure 105: Select Policy Type Page

2. Ensure the **Select individual policies** option is selected.

3. Click **Next**.

   **Step Result:** The ***Select Policies*** page opens.

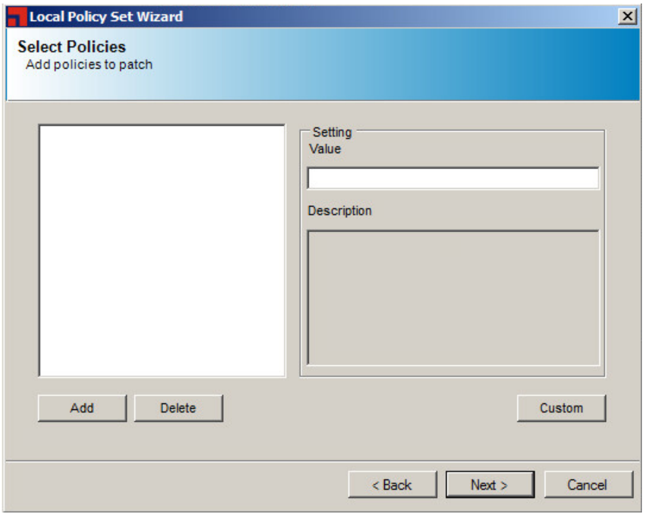
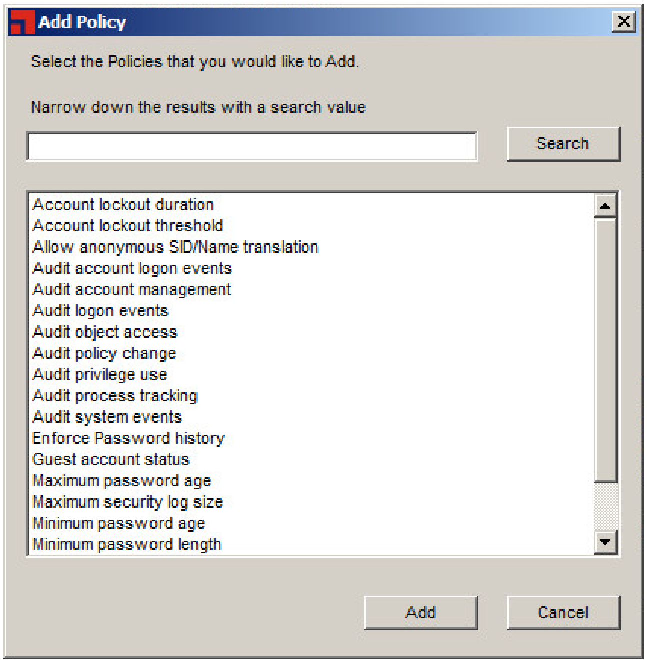


Figure 106: Select Policies Page

**4.** Click **Add**.

**Step Result:** The ***Add Policy*** page opens to a list of predefined standard Windows local policy items.



Add Policy

Select the Policies that you would like to Add.

Narrow down the results with a search value

Account lockout duration
Account lockout threshold
Allow anonymous SID/Name translation
Audit account logon events
Audit account management
Audit logon events
Audit object access
Audit policy change
Audit privilege use
Audit process tracking
Audit system events
Enforce Password history
Guest account status
Maximum password age
Maximum security log size
Minimum password age
Minimum password length

Figure 107: Add Policy Page

**5.** Find the standard Windows local policy item you want.

a) Type a policy name in the **Narrow down the results with a search value** field.
b) Click **Search**.

**Step Result:** The list displays based on your search value.

**6.** Select the policy you want from the available list.

**Note:** You may select multiple, non-concurrent policies by using `CTRL+Click` on the available list.

**7.** Click **Add**.

**Step Result:** The ***Add Policy*** window closes.

**8.** Set the value for each policy.

a) Select the policy.

b) Edit the existing value or select a new value from the **Value** drop-down list.

> **Tip:** The control type is dependent on the selected policy.

**Step Result:** The policy value is defined.

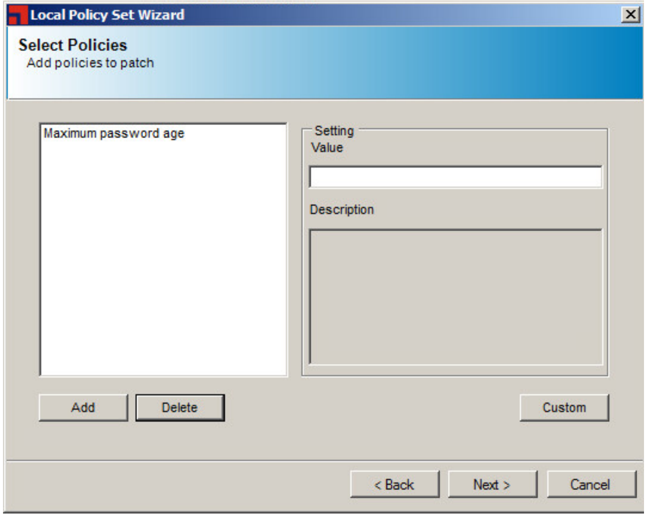


Figure 108: Select Policies Page

**9.** [Optional] Click **Custom** to enter a new registry value for this policy.

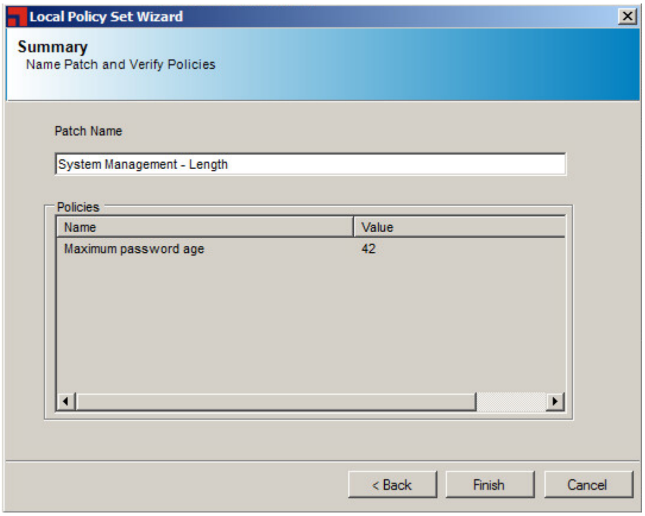
a) Select a key from the **Root Key** drop-down list.
b) Type the sub key in the **Sub Key** field.
c) Type a name in the **Value Name** field.
d) Type a value in the **Value** field.
e) Click **Add**.

**Step Result:** The ***Add Custom Policy*** dialog closes and the value displays in the ***Add Policy*** window.

> **Note:** If an invalid value is entered in the value field for a policy, an error message appears. You cannot proceed until you have entered valid values in the **Value** field.

**10.**Click **Next**.

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



Patch Name

System Management - Length

Policies

| Name | Value |
|---|---|
| Maximum password age | 42 |

Figure 109: Summary Page

**11.**Type a unique name for the patch in the **Patch Name** field.

The default name is `System Management -`.

**12.**Click **Finish**.

**Step Result:** The ***Summary*** page closes and the ***Patch Properties*** page displays.

**13.**[Optional] The ***Patch Properties*** page displays properties associated with the selected patch. Review and edit the patch properties as needed.

**Note:** For information on ***Patch Properties***, refer to The Patch Properties Page on page 35.

**14.**Select **File** > **Save**.

**Step Result:** The patch is stored within the Ivanti Endpoint Security server.

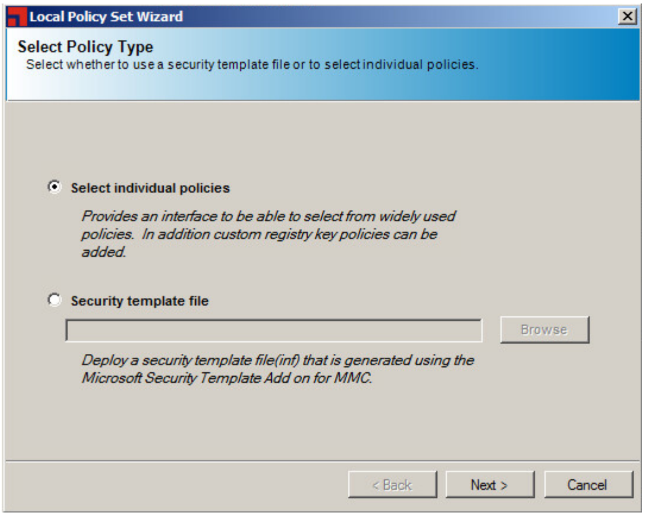
**Result:** The new policy patch is created.

## Creating a Policy Patch Using a Security Template File

The ***Policy Wizard*** allows you to choose the type of policy you want to create. Choose the **Security template file** option to specify your own local security template file defined within the Microsoft Security Template add-on for Microsoft Management Console (MMC).

**1.** Select **Tools** > **Policy Wizard**.

**Step Result:** The ***Select Policy Type*** page of the ***Local Policy Set Wizard*** window opens.



Local Policy Set Wizard

Select Policy Type

Select whether to use a security template file or to select individual policies.

● Select individual policies

*Provides an interface to be able to select from widely used policies. In addition custom registry key policies can be added.*

○ Security template file

*Deploy a security template file(inf) that is generated using the Microsoft Security Template Add on for MMC.*

Figure 110: Select Policy Type Page

**2.** Select the **Security template file** option.

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

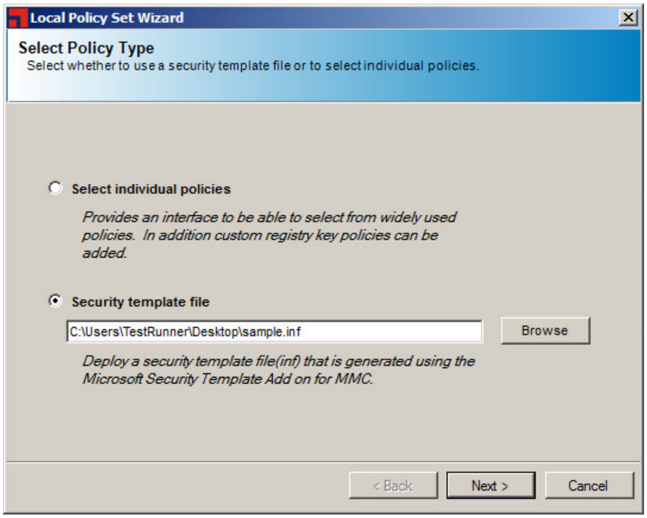
**3.** Click **Browse**.

**Step Result:** The ***Open File*** window opens.

**4.** Navigate to the desired security template file.

5. Click **Open**.

   **Step Result:** The ***Open*** window closes and the template file is added to the ***Select Policy Type*** page.



Select Policy Type

Select whether to use a security template file or to select individual policies.

○ Select individual policies

*Provides an interface to be able to select from widely used policies. In addition custom registry key policies can be added.*

● Security template file

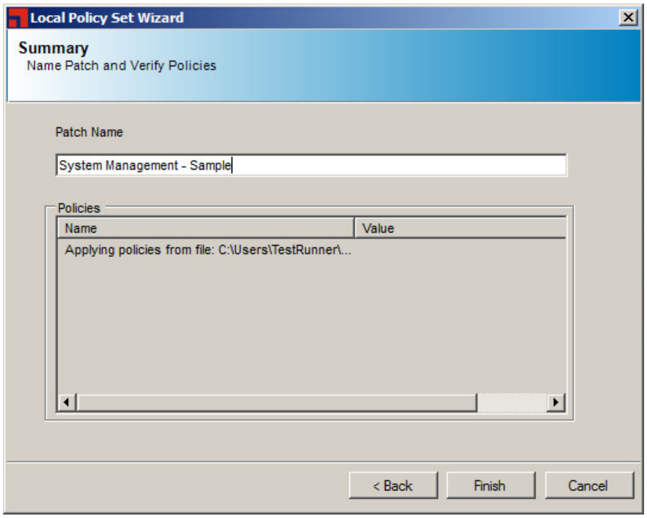
C:\Users\TestRunner\Desktop\sample.inf

*Deploy a security template file(inf) that is generated using the Microsoft Security Template Add on for MMC.*

Figure 111: Select Policy Type Page

6. Click **Next**.

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



Summary

Name Patch and Verify Policies

Patch Name

System Management - Sample

Policies

| Name | Value |
|---|---|
| Applying policies from file: C:\Users\TestRunner\... | |

Figure 112: Summary Page

7. Type a unique name for the patch in the **Patch Name** field.

   The default name is `System Management -`.

8. Click **Finish**.

   **Step Result:** The ***Summary*** page closes and the ***Patch Properties*** page displays.

9. [Optional] The ***Patch Properties*** page displays properties associated with the selected patch. Review and edit the patch properties as needed.

   **Note:** For information on ***Patch Properties***, refer to The Patch Properties Page on page 35.

10. Select **File** > **Save**.

    **Step Result:** The patch is stored within the Ivanti Endpoint Security server.

**Result:** The new policy patch is created.

## The Windows Firewall Wizard

The Ivanti Software Windows Firewall Wizard (Windows Firewall Wizard) allows you to create system management policy content that enforces Windows Firewall policy on managed devices within your network. The Windows Firewall Wizard allows you to use predefined policies or create custom Windows Firewall policies.

Once created, the Windows Firewall policies can provide administrators the ability to define Windows Firewall policies for Windows Vista and higher operating systems.

Ivanti Software recommends using the Windows Firewall Wizard to create a single policy to enforce your Windows Firewall policy settings.

**Note:** Creating multiple firewall patches can cause overlapping policy rules, which may cause conflicting or inadequate Windows Firewall policy settings within your network.

To create Windows Firewall policies using the Windows Firewall Wizard, refer to Creating a Windows Firewall Rule on page 185.

**Important:** The Windows Firewall Wizard cannot override any firewall changes made by Group Policy Objects (GPOs). For additional information on Windows Firewall and GPOs, refer to Managing Windows Firewall with Advanced Security by Using Group Policy (http://technet.microsoft.com/en-us/library/cc753955(v=ws.10).aspx).

After creating the single policy, it can be found in the Ivanti Endpoint Security database.

**Note:** Refer to *Viewing Packages* in the Ivanti Endpoint Security User Guide (https://www.ivanti.com/support/product-documentation) for instruction in finding created patch packages.

As part of a complete package for administrators to define Windows Firewall policies, Ivanti Software provides a patch, that when deployed to applicable endpoints will remove any custom Windows Firewall rules and allow you to restore Windows Firewall settings to system defaults. Refer to Restoring Windows Firewall Defaults on page 204 for additional information.

## Creating a Windows Firewall Rule

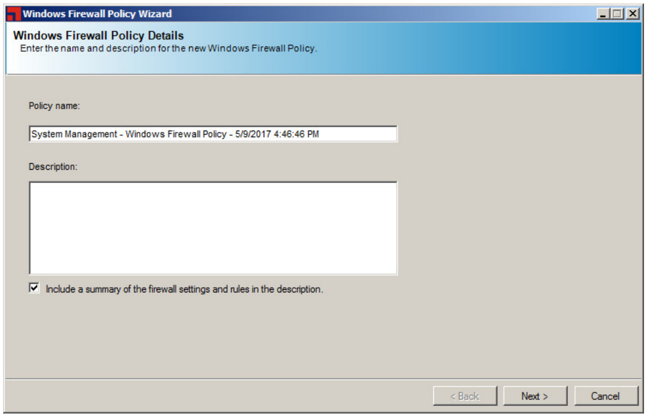
Create a Windows Firewall rule that enforces Windows Firewall policy using the Ivanti Software Windows Firewall Wizard.

**Prerequisites:**

Log in to the Ivanti Endpoint Security server from the Ivanti Content Wizard.

1. Select **Tools** > **Windows Firewall Wizard**.

   **Step Result:** The ***Windows Firewall Policy Details*** page opens.

   Windows Firewall Policy Wizard

   Windows Firewall Policy Details

   Enter the name and description for the new Windows Firewall Policy.

   Policy name:

   System Management - Windows Firewall Policy - 5/9/2017 4:46:46 PM

   Description:

   ☑ Include a summary of the firewall settings and rules in the description.

   Figure 113: Windows Firewall Policy Details Page

2. Type a unique name for the policy in the **Policy Name** field.

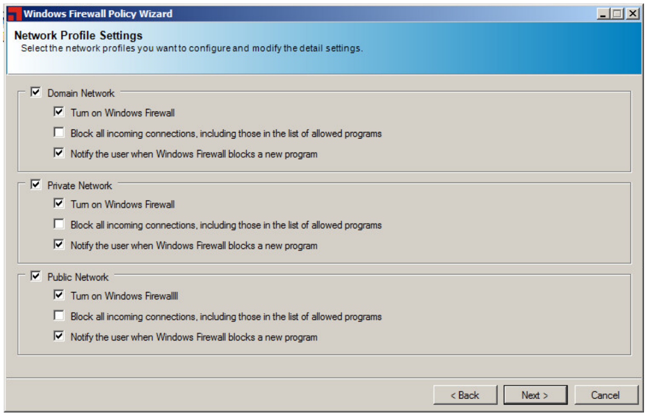
   **Note:** A default name is created automatically and is set to `System Management – Windows Firewall Policy MM/DD/YYYY HH:MM:SS TT`.

3. Type a description of the policy in the **Description** field.
4. Ensure the **Include a summary of the firewall settings and rules in the description** check box is selected.

   This will append to the patch description a summary of the firewall settings and rules.

5. Click **Next**.

   **Step Result:** The ***Network Profile Settings*** page opens.



Network Profile Settings

Select the network profiles you want to configure and modify the detail settings.

☑ Domain Network
- ☑ Turn on Windows Firewall
- ☐ Block all incoming connections, including those in the list of allowed programs
- ☑ Notify the user when Windows Firewall blocks a new program

☑ Private Network
- ☑ Turn on Windows Firewall
- ☐ Block all incoming connections, including those in the list of allowed programs
- ☑ Notify the user when Windows Firewall blocks a new program

☑ Public Network
- ☑ Turn on Windows Firewalll
- ☐ Block all incoming connections, including those in the list of allowed programs
- ☑ Notify the user when Windows Firewall blocks a new program

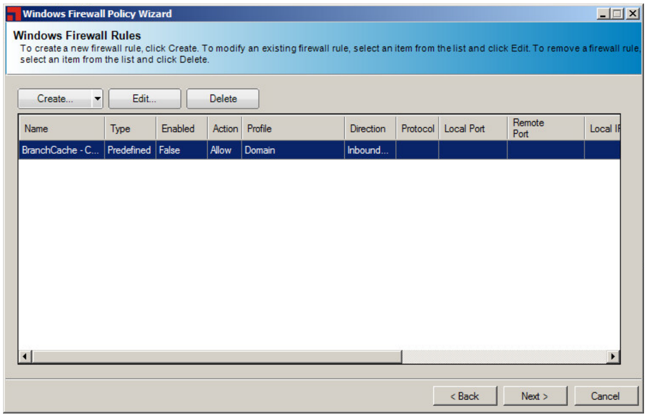
Figure 114: Network Profile Settings Page

> **Note:** The default values are the following:
>
> - All network profiles are checked.
> - `Turn on Windows Firewall` is checked under each profile.
> - `Block all incoming connections, including those in the list of allowed programs` is not checked under each profile.
> - `Notify the user when Windows Firewall blocks a new program` is checked under each profile.

> **Important:** If the **Domain Network** check box is not selected, the patch will not deploy to endpoints within your network.

6. Click **Next**.

   **Step Result:** The ***Windows Firewall Rules*** page opens.



Windows Firewall Policy Wizard

Windows Firewall Rules

To create a new firewall rule, click Create. To modify an existing firewall rule, select an item from the list and click Edit. To remove a firewall rule, select an item from the list and click Delete.

| Name | Type | Enabled | Action | Profile | Direction | Protocol | Local Port | Remote Port | Local IF |
|---|---|---|---|---|---|---|---|---|---|
| BranchCache - C... | Predefined | False | Allow | Domain | Inbound... | | | | |

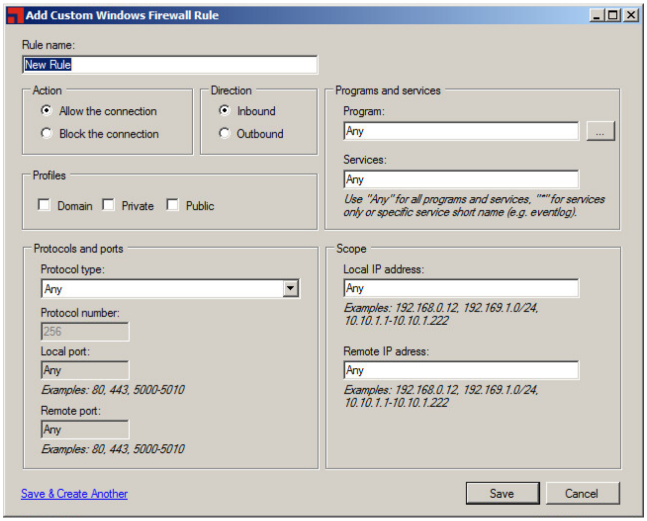
Figure 115: Windows Firewall Rules Page

7. Based on the type of Windows Firewall policy you require, select a menu item from the **Create** menu.

| Menu Item | Step |
|---|---|
| **Custom rule** | Select **Create** > **Custom rule**.<br>The ***Add Custom Windows Firewall Rule*** page opens (See Step 8 for details). |
| **Predefined rule** | Select **Create** > **Defined rule**.<br>The ***Add Predefined Windows Firewall Rule*** page opens (See Step 9 for details). |
| **Delete firewall rule** | Select **Create** > **Delete firewall rule**.<br>The ***Delete Windows Firewall Rule*** page opens (See Step 10 for details). |

**Note:** If you choose to not select a Windows Firewall policy option, your policy content will be based on the settings in the ***Network Profile Settings*** page.

8. If your choice displays the ***Add Custom Windows Firewall Rule*** page, complete the applicable steps.



Add Custom Windows Firewall Rule

Rule name: New Rule

Action
- ● Allow the connection
- ○ Block the connection

Direction
- ● Inbound
- ○ Outbound

Profiles
- □ Domain □ Private □ Public

Programs and services

Program: Any

Services: Any

*Use "Any" for all programs and services, "*" for services only or specific service short name (e.g. eventlog).*

Protocols and ports

Protocol type: Any

Protocol number: 256

Local port: Any

*Examples: 80, 443, 5000-5010*

Remote port: Any

*Examples: 80, 443, 5000-5010*

Scope

Local IP address: Any

*Examples: 192.168.0.12, 192.169.1.0/24, 10.10.1.1-10.10.1.222*

Remote IP adress: Any

*Examples: 192.168.0.12, 192.169.1.0/24, 10.10.1.1-10.10.1.222*

Figure 116: Add Custom Windows Firewall Rule Page

a) Type the name of the custom rule in the **Rule name** field.

b) Select the applicable **Action** option.

The following table describes each option.

Table 14: Action Options

| Option | Description |
|---|---|
| **Allow the connection.**<br>(radio button) | Allows the connection to be inbound or outbound for communication. |
| **Block the connection**<br>(radio button) | Blocks the connection for inbound or outbound communication. |

c) Select the applicable **Direction** option.

The following table describes each option.

Table 15: Direction Options

| Option | Description |
|---|---|
| **Inbound**<br>(radio button) | Inbound communication connection. |
| **Outbound**<br>(radio button) | Outbound communication connection. |

d) Select the **Profiles** option(s) as required by your Windows Firewall needs.

The following table describes each option.

Table 16: Profiles Options

| Option | Description |
|---|---|
| **Domain**<br>(check box) | A policy setting that controls the Windows Firewall whenever the computer is connected to domain networks such as a workplace domain. |
| **Private**<br>(check box) | A policy setting that controls the Windows Firewall whenever the computer is connected to trusted networks such as a home or small office network. |
| **Public**<br>(check box) | A policy setting that controls the Windows Firewall whenever the computer is connected to untrusted networks at a public place such as at coffee shops, hotels or airports. |

**Note:** At least one profile type is required. However you may select multiple profiles as dictated by your Windows Firewall requirements.

e) Define the **Protocols and ports** options:

1. Select the protocol that you want from the **Protocol type** drop-down list.

   Refer to Understanding Protocol Types on page 196 for a description of each protocol type.

   **Note:** The **Protocol number** field is pre-populated with the appropriate number and is read-only.

2. Type the applicable port number in the **Local port** field.
3. Type the applicable port number in the **Remote port** field.

f) Define the **Program and services** needed.

This option is used to specify how Windows Firewall will match criteria based on which program or service on the endpoint is sending the packets to the server.

The following table describes each property.

Table 17: Program and services Properties

| Option | Description |
|---|---|
| **Program**<br>(field and/or button) | You may type the full path to the executable (.exe) file or select the ellipses button (...), which opens the windows explorer browser window to allow a user to locate a file on the local system. The default is `Any`.<br>**Important:** If content is deployed to multiple endpoints, using the browse feature will only work if all of your endpoints contain the program under the same exact path specified. |
| **Services**<br>(field) | You may type the name of the service. The default is `Any`.<br>**Tip:** A system service that runs within its own unique .exe file and is not hosted by a service container is considered to be a program and can be added. Refer to Microsoft Knowledge Base Article 211362 (http://support.microsoft.com/kb/271362) on how to find short names for installed Windows services. |

g) Type the applicable **Scope** addresses.

The following table describes each field.

Table 18: Address Fields

| Option | Description |
|---|---|
| **Local IP address** | The IP address of the network interface on which the connection is made. Type a single IP address, multiple single IP addresses, or an IP address range using a single IP address using CIDR modifiers such as commas, slashes `(/)`, or dashes (–).<br>Examples:<br>• 192.168.0.12<br>• 192.168.0.12, 192.168.0.13<br>• 192.168.0.0/24<br>• 192.170.1.1-192.170.1.222<br>**Note:** Due to a Microsoft bug, you cannot use CIDR modifiers when entering multiple IP addresses. As a workaround, use two IP address ranges instead of two IP addresses with a CIDR modifier. |

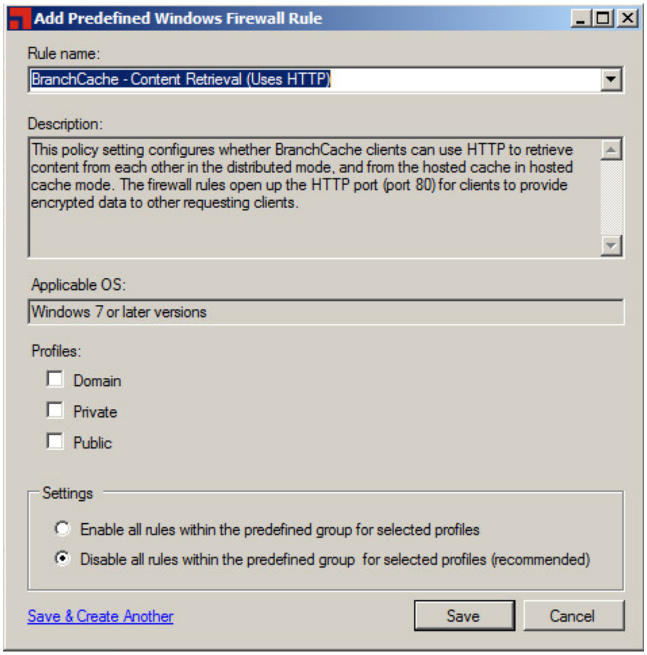
| Option | Description |
|---|---|
| **Remote IP address**<br>(field) | This is the IP address of the remote computer to which the connection is made. Type a single IP address, multiple single IP addresses, or an IP address range using a single IP address using CIDR modifiers such as commas, slashes `(/)`, or dashes (–).<br>Examples:<br>• 192.168.0.12<br>• 192.168.0.12, 192.168.0.13<br>• 192.168.0.0/24<br>• 192.170.1.1-192.170.1.222<br>**Note:** Due to a Microsoft bug, you cannot use CIDR modifiers when entering multiple IP addresses. As a workaround, use two IP address ranges instead of two IP addresses with a CIDR modifier. |

**Note:** The **Save & Create Another** link creates the rule and adds it to the Windows Firewall Rules page window. The page refreshes to allow the user to create another rule.

h) Click **Save**.

**Step Result:** The ***Custom Windows Firewall Rule*** page closes and the rule is displayed in the ***Windows Firewall Rules*** page window.

9. If your choice displays the ***Add Predefined Windows Firewall Rule*** page, complete the applicable steps.



Rule name: BranchCache - Content Retrieval (Uses HTTP)

Description: This policy setting configures whether BranchCache clients can use HTTP to retrieve content from each other in the distributed mode, and from the hosted cache in hosted cache mode. The firewall rules open up the HTTP port (port 80) for clients to provide encrypted data to other requesting clients.

Applicable OS: Windows 7 or later versions

Profiles:

□ Domain

□ Private

□ Public

Settings

○ Enable all rules within the predefined group for selected profiles

● Disable all rules within the predefined group for selected profiles (recommended)

Figure 117: Add Predefined Windows Firewall Rule Page

a) Select a rule from the **Rule name** drop-down list of predefined rules.

**Step Result:** The description, applicable OS, and default options within the ***Add Predefined Windows Firewall Rule*** page reflect the item choice.

**Note:** The **Rule name** drop-down list contains well known services and programs available on endpoints running a Windows operating system.

b) [Optional] Select or change the **Profiles** setting based on your Windows Firewall requirements.

The following table describes each option.

Table 19: Profiles Options

| Option | Description |
|---|---|
| **Domain** | A policy setting that controls the Windows Firewall whenever the computer is connected to domain networks such as a workplace domain. |
| **Private** | A policy setting that controls the Windows Firewall whenever the computer is connected to trusted networks such as a home or small office network. |

| Option | Description |
|---|---|
| **Public** | A policy setting that controls the Windows Firewall whenever the computer is connected to untrusted networks at a public place such as at coffee shops, hotels or airports. |

**Note:** At least one profile type is required. However you may select multiple profiles as dictated by your Windows Firewall requirements.

c) [Optional] Change the **Settings** option, if applicable.

The following table describes each option.

Table 20: Setting Options

| Option | Description |
|---|---|
| **Enable all rules within the predefined group for selected profiles** | This will enable all rules for the predefined group based on the **Profiles** option(s) selected. |
| **Disable all rules within the predefined group for selected profiles (recommended)** | This will disable all rules for the predefined group based on the **Profiles** option(s) selected. |

**Note:** The **Save & Create Another** link creates the rule and adds it to the Windows Firewall Rules page window. The page refreshes to allow the user to create another rule.

d) Click **Save**.

**Step Result:** The ***Predefined Windows Firewall Rule*** page closes and the rule is displayed in the ***Windows Firewall Rules*** page window.

**10.**If your choice displays the ***Delete Windows Firewall Rule*** page, complete the applicable steps.

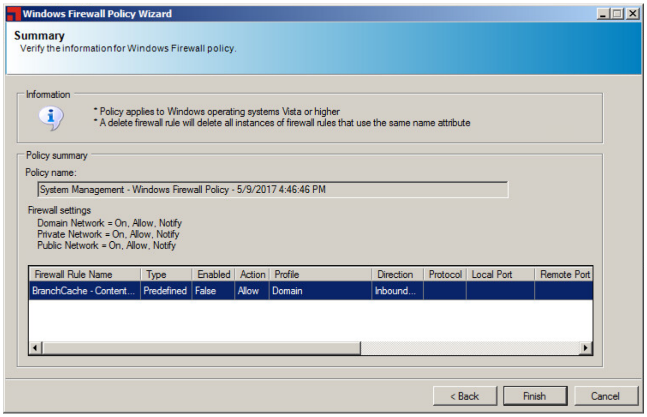
a) Type the name of the rule in the **Rule name** field.

The rule will delete all firewall rules that use the specified rule name.

**Note:** The **Save & Create Another** link creates the rule and adds it to the Windows Firewall Rules page window. The page refreshes to allow the user to create another rule.

b) Click **Save**.

**Step Result:** The ***Delete Windows Firewall Rule*** page closes and the rule is displayed in the ***Windows Firewall Rules*** page window.



Summary

Verify the information for Windows Firewall policy.

Information

- Policy applies to Windows operating systems Vista or higher
- A delete firewall rule will delete all instances of firewall rules that use the same name attribute

Policy summary

Policy name: System Management - Windows Firewall Policy - 5/9/2017 4:46:46 PM

Firewall settings

Domain Network = On, Allow, Notify
Private Network = On, Allow, Notify
Public Network = On, Allow, Notify

| Firewall Rule Name | Type | Enabled | Action | Profile | Direction | Protocol | Local Port | Remote Port |
|---|---|---|---|---|---|---|---|---|
| BranchCache - Content... | Predefined | False | Allow | Domain | Inbound... | | | |

Figure 118: Delete Windows Firewall Rule Page

**11.** The rule displayed in the ***Windows Firewall Rules*** page window reflects the type of Windows Firewall option created.

**12.** Use the ***Windows Firewall Rules*** toolbar options to modify the applicable firewall rule as needed.

The following table describes each toolbar option.

Table 21: Windows Firewall Rules Toolbar

| Name | Description |
|---|---|
| **Create**<br>(menu) | Opens the **Create**  menu. |
| **Custom rule**<br>(**Create** menu item) | Opens the ***Add Custom Windows Firewall Rule*** page. Repeat step 8 to add an additional custom Windows Firewall rule. |
| **Predefined rule**<br>(**Create** menu item) | Opens ***Add Predefined Windows Firewall Rule*** page. Repeat step 9 to add an additional predefined Windows Firewall rule. |
| **Delete rule**<br>(**Create** menu item) | Opens the ***Delete Windows Firewall Rule*** page. Repeat step 10 to add an additional delete Windows Firewall rule. |

| Name | Description |
|---|---|
| **Edit** | Opens one of the following pages based on the rule type selected.<br>1. ***Edit Custom Windows Firewall Rule*** page. Refer to Custom Windows Firewall Rule Options on page 197 for additional information.<br>2. ***Edit Predefined Windows Firewall Rule*** page. Refer to Predefined Windows Firewall Rule Options on page 201 for additional information.<br>3. ***Edit Delete Windows Firewall Rule*** page. Allows you to change the name of the rule in the **Rule name** field. |
| **Deletes** | Deletes the selected rule in the ***Windows Firewall Rules*** page.<br>**Caution:** The firewall rule is deleted automatically. No dialog displays warning you of a pending deletion of the rule. |

**13.**Review your rules within the ***Windows Firewall Rules*** page.

**14.**Click **Next**.

**Step Result:** The ***Summary*** page opens displaying information concerning the Windows Firewall policy.

**Tip:** Select the **Back** button to go back to the ***Windows Firewall Rules*** page.

**15.**Once you have verified the summary information, click **Finish**.

**Step Result:** The ***Summary*** page closes and the ***Patch Properties*** page displays.

**16.**[Optional] The ***Patch Properties*** page displays properties associated with the selected patch. Review and edit the patch properties as needed.

**Note:** For information on ***Patch Properties***, refer to The Patch Properties Page on page 35.

**17.**Select**File** > **Save**.

**Step Result:** The patch is stored within the Ivanti Endpoint Security server.

**Result:** The new custom rule for your Windows Firewall policy is created and ready to use.

**Note:** Refer to *Viewing Packages* in the Ivanti Endpoint Security User Guide (https://www.ivanti.com/support/product-documentation) for instruction in finding created packages.

## Understanding Protocol Types

There are various protocol types used to help filter network traffic. Each protocol type uses a currently assigned IP protocol number.

Protocol types are available as a drop-down list within the ***Add Custom Windows Firewall Rule*** page in the Ivanti Software Windows Firewall Wizard.

**Note:** The **Protocol number** field is pre-populated with the appropriate number and is read-only.

Refer to Creating a Windows Firewall Rule on page 185 for more information on using the Ivanti Software Windows Firewall Wizard.

The following table describes each option.

Table 22: Protocol Types

| Name (Full Name) | Number | Description |
|---|---|---|
| **Any** | 256 | Used for rule settings that apply to any protocol (even those not listed). |
| **HOPOPT**<br>(IPv6 Hop-by-Hop Option) | 0 | Used to alert routers that an IP datagram contains control data that the router will need to handle. When this option is set in the header, the router performs additional parsing on the packets. |
| **ICMPv4**<br>(Internet Control Message Protocol version 4) | 1 | Used to send errors and other messages that are used to analyze networks. |
| **IGMP**<br>(Internet Group Management Protocol) | 2 | Used by IP hosts and multicast routers to establish and manage the membership of IP multicast groups. |
| **TCP**<br>(Transmission Control Protocol) | 6 | Provides a reliable, connection-oriented packet delivery service and is based on point-to-point communication between two network hosts. TCP guarantees delivery and verifies sequencing for any datagrams. |
| **UDP**<br>(User Datagram Protocol) | 17 | Provides a fast reliable way to send and receive data between TCP/IP hosts. Unlike TCP, UDP does not guarantee delivery or verify sequencing for any datagrams. |
| **IPv6**<br>(Internet Protocol version 6) | 41 | This improves on Internet Protocol version 4 (IPv4) by vastly increasing the number of available addresses and by enabling more efficient routing, simpler configuration, built-in IP security, and better support for real-time data delivery. |
| **IPv6-Route** | 43 | This is the Routing Header for IPv6. |

| Name (Full Name) | Number | Description |
|---|---|---|
| **IPv6-Frag** | 44 | This is the Fragment Header for IPv6. |
| **GRE**<br>(Generic Route Encapsulation) | 47 | Used to encapsulate a variety of generic network layer packets. The protocol is designed to be stateless. |
| **ICMPv6**<br>(Internet Control Message Protocol version 6) | 58 | This is to send errors and other messages used to analyze networks. |
| **IPv6-NoNxt**<br>(No Next Header for IPv6) | 59 | Used to communicate that there are no additional headers to process. |
| **IPv6-Opts**<br>(Destination Options for IPv6) | 60 | Used to indicate that the next header is the Destination Options header, which is used to specify processing or delivery parameters to either intermediate or final destinations. |
| **VRRP**<br>(Virtual Router Redundancy Protocol) | 112 | Used to increase the availability of the default gateway for hosts on a subnet. |
| **PGM**<br>(Pragmatic General Multicast) | 113 | Used to improve the reliability of a data stream to multiple network recipients. |
| **L2TP**<br>(Layer 2 Tunneling Protocol) | 115 | Used to facilitate virtual private network (VPN) connections. |

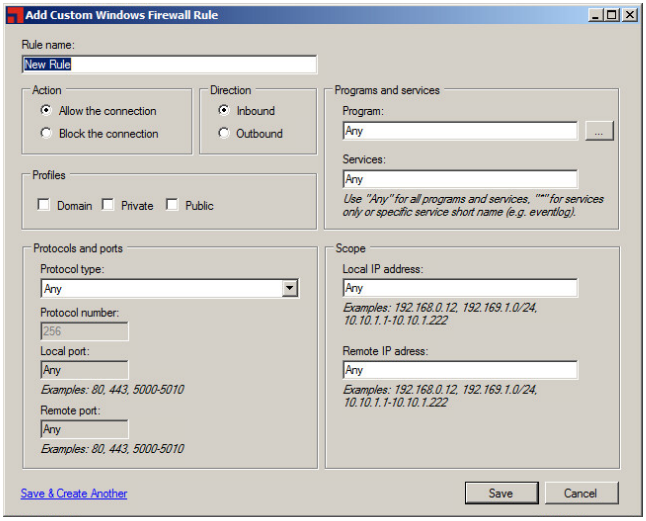
## Custom Windows Firewall Rule Options

You may create or edit a custom Windows Firewall rule using the ***Windows Firewall Policy Wizard***.

The **Custom rule** option is designed so that you create a firewall rule based on criteria not covered by the other types of firewall rules. If your rule requires common Windows programs or services, choose the **Predefined rule** option within the ***Windows Firewall Policy Wizard*** to select a rule from a predefined list based on the Windows operating system.

In addition to the **Custom rule** option, the ***Windows Firewall Policy Wizard*** allows you to create a deletion rule that will delete a rule based on the rule name.

Refer to Creating a Windows Firewall Rule on page 185 for instruction on creating or editing a predefined, custom, or delete firewall rule.



Add Custom Windows Firewall Rule

Rule name: New Rule

Action

● Allow the connection

○ Block the connection

Direction

● Inbound

○ Outbound

Profiles

□ Domain □ Private □ Public

Programs and services

Program: Any

Services: Any

*Use "Any" for all programs and services, "*" for services only or specific service short name (e.g. eventlog).*

Protocols and ports

Protocol type: Any

Protocol number: 256

Local port: Any

*Examples: 80, 443, 5000-5010*

Remote port: Any

*Examples: 80, 443, 5000-5010*

Scope

Local IP address: Any

*Examples: 192.168.0.12, 192.169.1.0/24, 10.10.1.1-10.10.1.222*

Remote IP adress: Any

*Examples: 192.168.0.12, 192.169.1.0/24, 10.10.1.1-10.10.1.222*

Figure 119: Add Custom Windows Firewall Rule Page

The ***Add Custom Windows Firewall Rule*** page contains a number of settings that allow you to create a custom Windows firewall rule to address your Windows Firewall requirements.

The following table describes the fields and options.

Table 23: Custom Windows Firewall Rule Options

| Options | Description |
|---|---|
| **Rule name** | The name of the custom rule. |
| **Action** | |
| **Allow the connection** (option) | Allows the connection to be inbound or outbound for communication. |
| **Block the connection** (option) | Blocks the connection to inbound or outbound communication. |
| **Direction** | |
| **Inbound** (option) | Inbound communication connection. |
| **Outbound** (option) | Outbound communication connection. |
| **Profiles** (required field) | |
| **Note:** At least one profile type is required. However, you may select multiple profiles as dictated by your Windows Firewall needs. | |

| Options | Description |
|---|---|
| **Domain** (check box) | A policy setting that controls the Windows Firewall whenever the computer is connected to domain networks such as a workplace domain. |
| **Private** (check box) | A policy setting that controls the Windows Firewall whenever the computer is connected to trusted networks such as a home or small office network. |
| **Public** (check box) | A policy setting that controls the Windows Firewall whenever the computer is connected to untrusted networks at a public place such as at coffee shops, hotels or airports. |
| **Protocols and ports** | |
| **Protocol type**<br>(drop-down list) | This is a predefined list of protocols whose network traffic you want to filter with a firewall rule.<br>**Note:** The selection defines the default settings within the protocol and port area.<br>Refer to Understanding Protocol Types on page 196. |
| **Protocol number** | The number of the designated protocol.<br>**Note:** The **Protocol number** field is pre-populated with the appropriate number based on the protocol type selected and is read-only. |
| **Local port** | The local port number of the designated protocol.<br>**Note:** The field is pre-populated with the appropriate port number and is read-only with the exception of the `TCP` and `UDP` protocol. If `TCP` or `UDP` is required, then multiple port numbers may be entered. You may separate specific ports with commas and/or specify a range of ports by using a dash (–).<br>Example: `80, 443, 5000-5010` |
| **Remote port** | The port of the remote used by the designated protocol.<br>**Note:** The field is pre-populated with the appropriate port number and is read-only with the exception of the `TCP` and `UDP` protocol. If `TCP` or `UDP` is required, then multiple port numbers may be entered. You may separate specific ports with commas and/or specify a range of ports by using a dash (–).<br>Example: `80, 443, 5000-5010` |
| **Programs and services** | |

| Options | Description |
|---|---|
| **Program** | To add a program to a firewall rule, you must specify the full path to the executable (.exe) file used by the program. The ellipses button (...) opens the windows explorer browser window to allow a user to locate a file on the local system.<br>**Tip:** Type `Any` for all programs.<br>**Important:** Note: If content is deployed to multiple endpoints, using the browse feature will only work if all of your endpoints contain the program under the same exact path specified. |
| **Services** | A system service that runs within its own unique .exe file and is not hosted by a service container is considered to be a program and can be added. The default is `Any`. You may type the name of the service.<br>**Tip:** Type `Any` for all services.<br>**Note:** Refer to Microsoft Knowledge Base Article 211362 (http://support.microsoft.com/kb/271362) on how to find short names for installed Windows services. |
| **Scope** | |
| **Local IP address** | The IP address of the network interface on which the connection is made. Type a single IP address, multiple single IP addresses, or an IP address range using a single IP address using CIDR modifiers such as commas, slashes `(/)`, or dashes (–).<br>Examples:<br>• 192.168.0.12<br>• 192.168.0.12, 192.168.0.13<br>• 192.168.0.0/24<br>• 192.170.1.1-192.170.1.222<br>**Note:**<br>• When Internet Connection Sharing is enabled, your LAN adapter uses the IP address of 192.169.0.1<br>• Due to a Microsoft bug, you cannot use CIDR modifiers when entering multiple IP addresses; the second IP address will not be reognized. As a workaround, use two IP address ranges instead of two IP addresses with a CIDR modifier. |

| Options | Description |
|---|---|
| **Remote IP address** | The IP address of the remote computer on which the connection is made. Type a single IP address, multiple single IP addresses, or an IP address range using a single IP address using CIDR modifiers such as commas, slashes `(/)`, or dashes (–).<br>Examples:<br>• 192.168.0.12<br>• 192.168.0.12, 192.168.0.13<br>• 192.168.0.0/24<br>• 192.170.1.1-192.170.1.222<br>**Note:** Due to a Microsoft bug, you cannot use CIDR modifiers when entering multiple IP addresses. As a workaround, use two IP address ranges instead of two IP addresses with a CIDR modifier. |
| **Links** | |
| **Save & Create Another** | This link creates the rule and adds it to the Windows Firewall Rules page window. The page refreshes to allow a user to create another rule. |
| **Button** | |
| **Save** | This creates the predefined rule, closes the dialog, and adds the new rule to the Windows Firewall Rules list |
| **Cancel** | This closes the wizard dialog without making any changes |

## Predefined Windows Firewall Rule Options

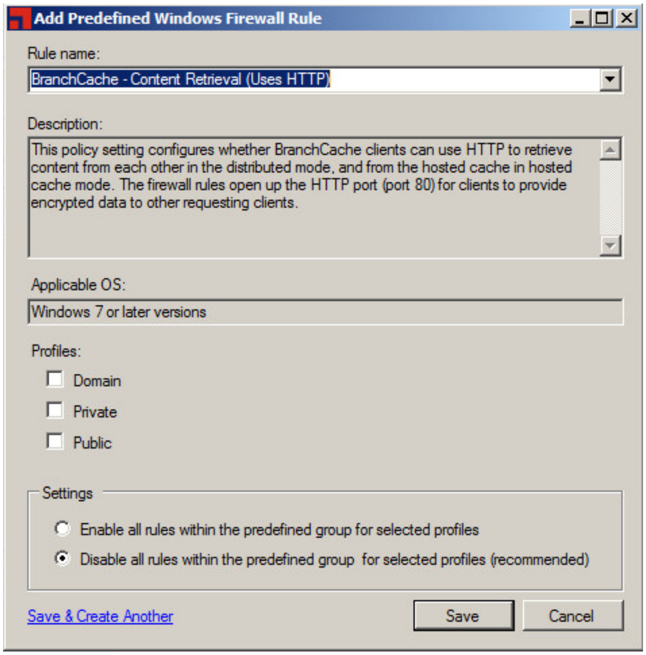
You may create or edit a predefined Windows Firewall rule using the ***Windows Firewall Policy Wizard***.

The **Predefined rule** option allows you to select programs or services from a predefined list. Most well known services and programs available on devices running a version of a Windows operating system appears in the list. The **Predefined rule** option allows you to enable or disable these rules for your selected profile(s).

If your rule requires additional requirements not found in the **Predefined rule** option, then select the **Custom rule** option. The **Custom rule** option is designed so that you may create a firewall rule based on criteria not covered by the other types of firewall rules.

In addition to the **Custom rule** option, the ***Windows Firewall Policy Wizard*** allows you to create a deletion rule that will delete a package based on the rule name.

Refer to Creating a Windows Firewall Rule on page 185 for instruction on creating or editing a predefined, custom, or delete firewall rule.



Rule name:
BranchCache - Content Retrieval (Uses HTTP)

Description:
This policy setting configures whether BranchCache clients can use HTTP to retrieve content from each other in the distributed mode, and from the hosted cache in hosted cache mode. The firewall rules open up the HTTP port (port 80) for clients to provide encrypted data to other requesting clients.

Applicable OS:
Windows 7 or later versions

Profiles:
□ Domain
□ Private
□ Public

Settings
○ Enable all rules within the predefined group for selected profiles
● Disable all rules within the predefined group  for selected profiles (recommended)

Figure 120: Add Predefined Windows Firewall Rule Page

The ***Add Predefined Windows Firewall Rule*** page contains a number of settings that allow you to create a predefined Windows Firewall rule to address your Windows Firewall requirements.

The following table describes the fields and options.

Table 24: Predefined Windows Firewall Rule Options

| Options | Description |
|---|---|
| **Rule name**<br>(drop-down list) | The name of the predefined rule.<br>The rules list well known services and programs available on devices running a Windows operating system. |
| **`Description`** | The description of the policy setting configuration setting. The description information matches the predefined rule name. The field is read-only. |
| **`Applicable OS`** | The applicable operating system the rule applies to. The field is read-only. |
| **Profiles** | |
| **Note:** At least one profile type is required. However, you may select multiple profiles as dictated by your Windows Firewall requirements. | |

| Options | Description |
|---|---|
| **Domain** (check box) | A policy setting that controls the Windows Firewall whenever the device is connected to domain networks such as a workplace domain. |
| **Private** (check box) | A policy setting that controls the Windows Firewall whenever the device is connected to trusted networks such as a home or small office network. |
| **Public** (check box) | A policy setting that controls the Windows Firewall whenever the device is connected to untrusted networks at a public place such as at coffee shops, hotels or airports. |
| **Settings** | |
| **Enable all rules within the predefined group for selected profiles**<br>(radio button) | A policy setting that enables all rules for the predefined group for the profile type(s) selected. |
| **Disable all rules within the predefined group for selected profiles (recommended)**<br>(radio button) | A policy setting that will disable all rules for the predefined group for the profile type(s) selected. |
| **Links** | |
| **Save & Create Another** | This link creates the rule and adds it to the Windows Firewall Rules page window. The page refreshes to allow a user to create another rule. |
| **Button** | |
| **Save** | This creates the predefined rule, closes the dialog, and adds the new rule to the Windows Firewall Rules list. |
| **Cancel** | This closes the wizard dialog without making any changes. |

## Restoring Windows Firewall Defaults

Importing a provided patch is the first step in the process to allow you to remove any custom Windows Firewall rules and restore Windows Firewall settings to system defaults.

**Prerequisites:**

The Ivanti Content Wizard Client has been installed. Refer to Installing the Ivanti Content Wizard Client on page 19 for installation instructions.

**Note:** This patch content is designed to only be applicable to endpoints that have had their firewall policy modified by the Ivanti Software Windows Firewall Wizard.

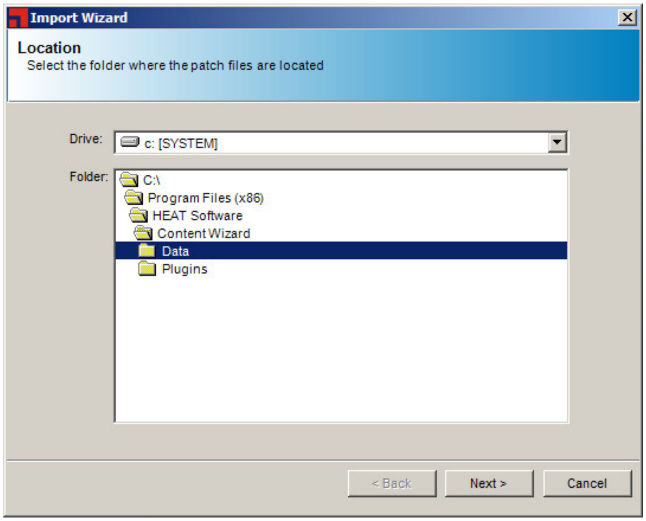
1. Log in to the Ivanti Endpoint Security server from the Ivanti Content Wizard.
2. Select **File** > **Import Wizard**.

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

3. Navigate to the installation location of the provided `SystemMgmtRestoreWindowsFirewallSetting.plfz` patch.

   a) Navigate to the `<Installation Directory>\HEAT Software\Content Wizard\Data` folder.

   **Step Result:**



Import Wizard

Location

Select the folder where the patch files are located

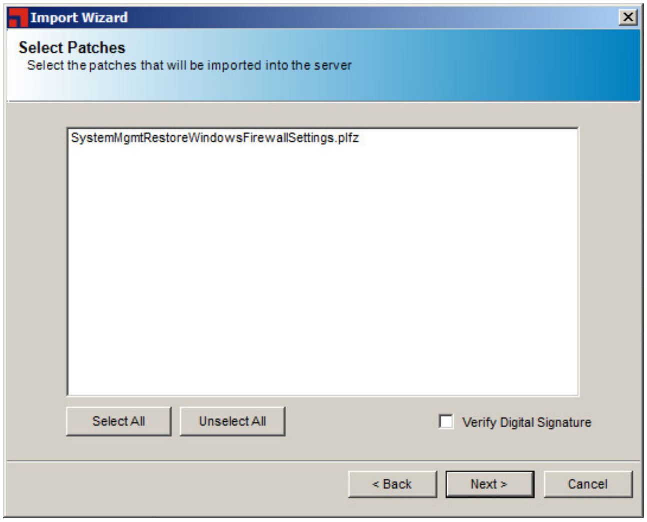
Drive: c: [SYSTEM]

Folder:
C:\
Program Files (x86)
HEAT Software
Content Wizard
Data
Plugins

Figure 121: Location Page

b) Click **Next**.

**Step Result:** The ***Select Patches*** page opens and the `SystemMgmtRestoreWindowsFirewallSetting.plfz` patch displays within the pane.



Import Wizard
Select Patches
Select the patches that will be imported into the server
SystemMgmtRestoreWindowsFirewallSettings.plfz
Select All
Unselect All
□ Verify Digital Signature
< Back
Next >
Cancel

Figure 122: Select Patches Page

c) [Optional] To verify the patch's digital signature, select the **Verify Digital Signature** check box.

**Note:** The `SystemMgmtRestoreWindowsFirewallSetting.plfz` patch is automatically included as part of the Ivanti Content Wizard Client installation. Refer to Installing the Ivanti Content Wizard Client on page 19 for installation details.

**4.** Click **Next**.

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

**5.** [Optional] View the ***Import Summary*** page.

a) Click **Preview** to view the ***Import Summary*** page prior to selecting **Import**.

**Step Result:** The ***Import Summary*** page displays information concerning the patch.

**Note:** For information on patch properties, refer to The Patch Properties Page on page 35.

b) Click **File** > **Exit**.

**Step Result:** The ***Import Summary*** page closes.

6. Click **Import**.

   **Step Result:** The import begins and finishes.

   > **Note:** The ***Import Wizard*** may take several minutes to import the patch.

7. Click **Finish**.

   **Step Result:** The ***Import Wizard*** window closes.

**Result:** The patch is imported into the Ivanti Endpoint Security server.

The package name for this imported patch is `System Management - Restore Windows Firewall settings to system defaults` within the ***Deployment Wizard***.

To complete the removal process, you deploy the package using the ***Deployment Wizard*** to applicable endpoints. Any custom firewall policy modified by the Ivanti Software Windows Firewall Wizard will be removed and Windows Firewall settings will be restored to system defaults on the applicable endpoints.

> **Note:** Refer to *Creating an Endpoint Deployment* or *Creating a Group Deployment* in the Ivanti Endpoint Security: Patch and Remediation User Guide (https://www.ivanti.com/support/product-documentation) for deployment information.

## Community Functionality

The Ivanti Content Wizard incorporates community publishing of patches. This allows you to publish or download patches from an internal patch distribution website within your organization.

The Ivanti Content Wizard community functionality allows you to:

- Select a patch (or set of patches) to be packaged for publication to an online community. For additional information, refer to The Community Subscribe Wizard on page 206.
- Download a patch that has been published an online community. For additional information, refer to The Community Publish Wizard on page 209.

### The Community Subscribe Wizard

The ***Community Subscribe Wizard*** lets you share custom patches with other Ivanti administrators.

Using the ***Community Subscribe Wizard*** you can obtain custom patches posted by other Ivanti administrators from an internal patch distribution website within your organization.

Content downloaded using the ***Community Subscribe Wizard*** is used at your own risk. Even when importing content that has been digitally signed and is from a trusted provider, it is essential that you scrutinize the patch for potential problems before deploying it within your network. It is recommended that you use a staged approach, testing for compatibility with a number of test machines, when deploying patches to your network.

> **Warning:** Importing unsigned `.plfz` files is not recommended.

### Create a Subscription Through an Enterprise Distribution Website

The ***Community Subscribe Wizard*** lets you create custom policies or software patches and then share those items with other network administrators throughout the enterprise.

**Prerequisites:**

Setup an enterprise distribution website for your organization. For more information, refer to the following Creating an Enterprise Patch Distribution Website on page 219.

1. Create a designated folder in the directory `<Installation Directory>\Program Files\Apache Software Foundation\Apache2.2\htdocs`.

   **Example:** A folder named `Patch Files` would be located at `<Installation Directory>\Program Files\Apache Software Foundation\Apache2.2\htdocs\Patch Files`.

   > **Note:** For information on installing an Apache server, refer to Installing the Apache Server on page 219.

2. Populate the designated folder with created custom policies or software patches.

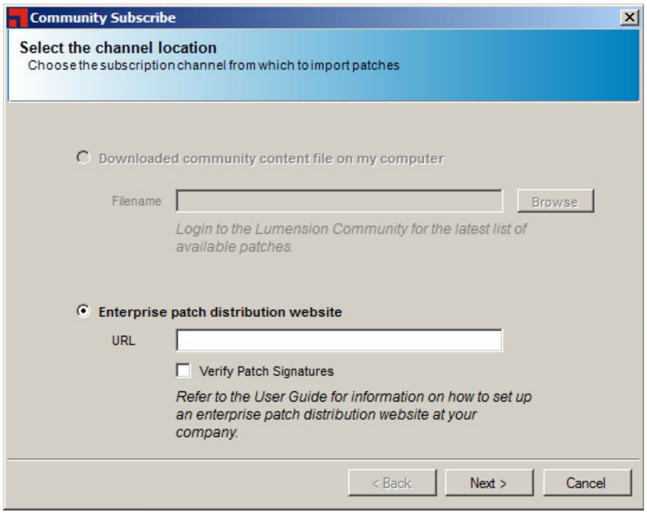
   You must put the patche content file (.plfz) and the channel file (.xml) in the designated folder within the directory `<Installation Directory>\Program Files\Apache Software Foundation\Apache2.2\htdocs`.

   **Example:** Populate the `<Installation Directory>\Program Files\Apache Software Foundation\Apache2.2\htdocs\Patch Files` folder with software patch content.

3. Log in to the Ivanti Endpoint Security server from the Ivanti Content Wizard.
4. Select **Tools** > **Community Subscribe**.

   **Step Result:** The ***Select the channel location*** page of the ***Community Subscribe*** window opens.

5. Select **Enterprise patch distribution website**.



Community Subscribe

Select the channel location

Choose the subscription channel from which to import patches

○ Downloaded community content file on my computer

Filename

Login to the Lumension Community for the latest list of available patches.

● Enterprise patch distribution website

URL

□ Verify Patch Signatures

Refer to the User Guide for information on how to set up an enterprise patch distribution website at your company.

Figure 123: Select the Channel Location Page

6. Type the distribution website URL.

   **Example:** Type `http://localhost:8080/Patch Files`.

   You do not need to specify a filename, just the web directory in which the patch content file (.plfz) and the channel file (.xml) was extracted to. Example: Patch Files.

   **Note:** Patch content and channel files are packed in `.zip` files published from the Ivanti Endpoint Security servers. Both patch content files (.plfz) and channel (.xml) file types are extracted to the designated folder for distribution. To proceed, you must enter a valid web address within your enterprise that contains a web directory folder containing content.

7. [Optional] Select the **Verify Patch Signatures** check box.
8. Click **Next**.

   **Step Result:** The ***Channel Selection*** page opens.

9. Select the channel in the left pane.

   **Note:** The channel selection name and channel content names are a reflection of content found in the channel file (.xml) within the designated folder in the directory. Example: `<Installation Directory>\Program Files\Apache Software Foundation\Apache2.2\htdocs\Patch Files`.

10. Click **Next**.

    **Step Result:** The ***Channel Content*** page opens.

**11.**Select the patch content in the left pane that you wish to import.

**Tip:** To select multiple channel content items, hold down **CTRL** key and then click each item you want to select.

**12.**Click **Next**.

**Step Result:** The ***Importing Content*** page opens.

Figure 124: Importing Content Page

**13.**[Optional] Click **Preview** to view the ***Import Summary*** page prior to selecting **Download**.

The ***Import Summary*** page displays information concerning the patch.

**14.**Click **Download**.

**Step Result:** Ivanti Content Wizard imports the selected content to `<Install Location>\HEAT Software\EMSS\Web\LCW-Work\Cache`.

**Note:** Importation times vary according to patch sizes.

**15.**When the import completes, the status window displays the completion status.

The status will either be success or failure.

Figure 125: Importing Content: Success

**Tip:** The file upload process requires access to both the patch content file (.plfz) and the channel file (.xml). If an error occurs, it is often related to file access. Verify that both files exist within the designated folder. For example, `<Installation Directory>\Program Files\Apache Software Foundation\Apache2.2\htdocs\Patch Files`. Ensure the user has adequate security permissions to access the files and folders within the directory.

**16.**Click **Finish**.

**Step Result:** The ***Importing Content*** page closes.

**Result:** The subscription content is imported to `<Install Location>\HEAT Software\EMSS\Web\LCW-Work\Cache`.

## The Community Publish Wizard

The Ivanti Content Wizard ***Community Publish Wizard*** lets you post the patches you have created to an internal server within your organization.

You can publish your custom patches to an internal patch distribution web site within your organization using the ***Community Publish Wizard***.

When you publish a patch, it must be digitally signed to provide proof as to the organization that created it. Any patches that the administrator has created and published as signed `.cab` files can then be posted to the Content Garden section of the community.

You can also use the ***Community Publish Wizard*** to distribute patches from a Ivanti Endpoint Security server with an Internet connection to other Ivanti Endpoint Security servers within a closed network segment that would otherwise be unable to access the new patches. When a new set of patches are published, the wizard converts the desired set of patches into a channel file that can be quickly extracted to a local web server and shared with other Ivanti Endpoint Security Servers that are running the Ivanti Content Wizard.

### Publishing Content Through an Enterprise Server

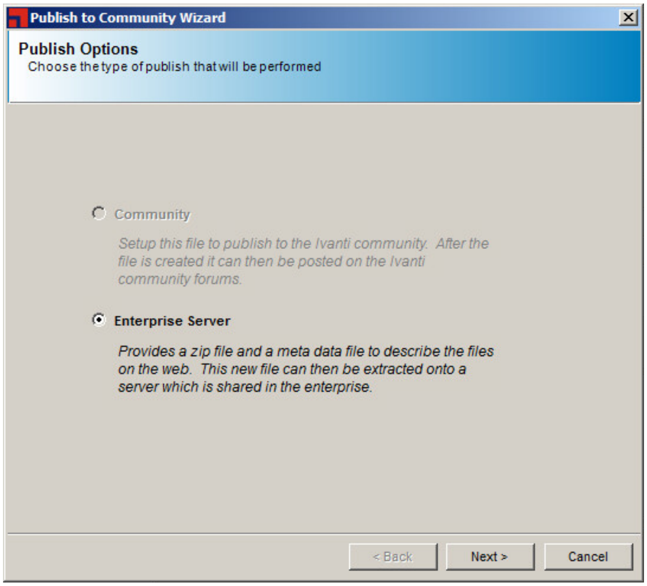
The ***Community Publish Wizard*** lets you use an enterprise server to post user-created patches to the Ivanti Connect Community. Each zip file contains a simple `.xml` file that identifies the channel information (publisher, company, date, graphic, etc.) as well as the exported patches (`.plfz` files) that were created during the publish process.

**Prerequisites:**

Setup an enterprise distribution website for your organization. For more information, refer to Creating an Enterprise Patch Distribution Website on page 219.

1. Log in to the Ivanti Endpoint Security server from the Ivanti Content Wizard.
2. Select **Tools** > **Community Publish**.

   **Step Result:** The ***Publish Options*** page of the ***Community Publish*** window opens.
3. Select **Enterprise Server**.



Publish to Community Wizard

Publish Options

Choose the type of publish that will be performed

○ Community

*Setup this file to publish to the Ivanti community. After the file is created it can then be posted on the Ivanti community forums.*

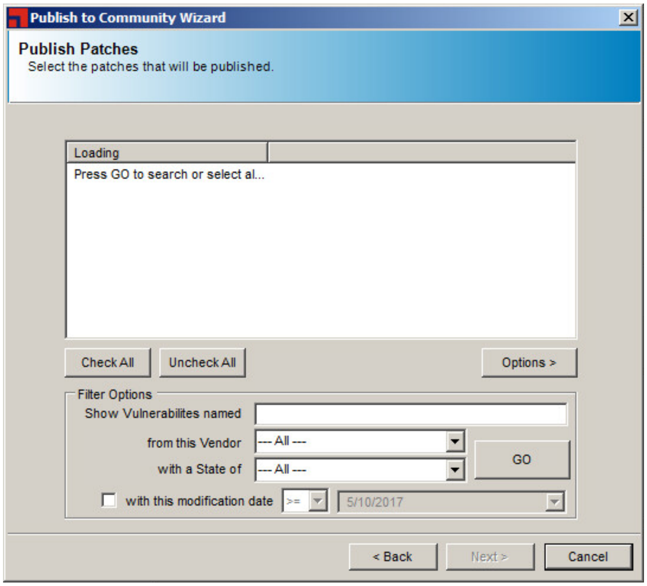
● Enterprise Server

*Provides a zip file and a meta data file to describe the files on the web. This new file can then be extracted onto a server which is shared in the enterprise.*

Figure 126: Publish Options Page

4. Click **Next**.

   **Step Result:** The ***Publish Patches*** page opens.



Publish to Community Wizard

Publish Patches

Select the patches that will be published.

Loading

Press GO to search or select al...

Filter Options

Show Vulnerabilites named

from this Vendor --- All ---

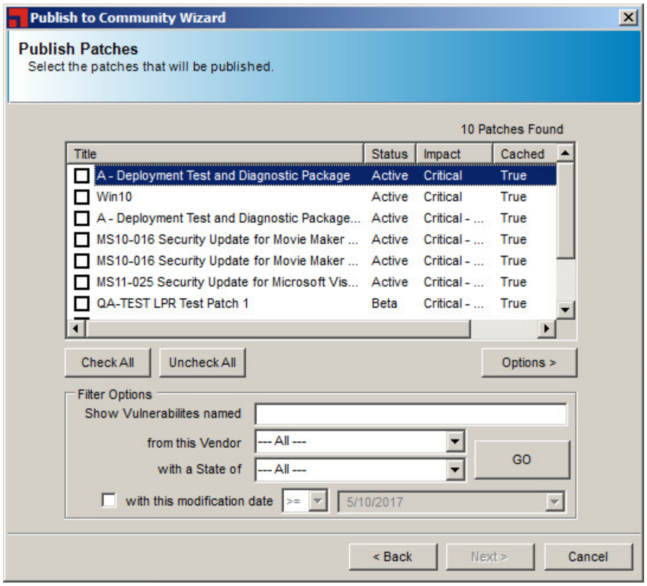
with a State of --- All ---

□ with this modification date >= 5/10/2017

Figure 127: Publish Patches Page

5. Click **GO**.

   **Step Result:** The list is displayed in the ***Publish Patches*** page window.



Publish to Community Wizard

**Publish Patches**

Select the patches that will be published.

10 Patches Found

| | Title | Status | Impact | Cached |
|---|---|---|---|---|
| □ | A - Deployment Test and Diagnostic Package | Active | Critical | True |
| □ | Win10 | Active | Critical | True |
| □ | A - Deployment Test and Diagnostic Package... | Active | Critical - ... | True |
| □ | MS10-016 Security Update for Movie Maker ... | Active | Critical - ... | True |
| □ | MS10-016 Security Update for Movie Maker ... | Active | Critical - ... | True |
| □ | MS11-025 Security Update for Microsoft Vis... | Active | Critical - ... | True |
| □ | QA-TEST LPR Test Patch 1 | Beta | Critical - ... | True |

Filter Options

Show Vulnerabilites named:

from this Vendor: --- All ---

with a State of: --- All ---

□ with this modification date: >= 5/10/2017

Figure 128: Publish Patches Page

6. Select the applicable option for your export needs based on the following table:

| Option | Description |
|---|---|
| **Title (check box)** | Select each individual patch item(s). |
| **Check All (button)** | Selects all patches in the display list. |
| **Uncheck All (button)** | Deselects all patches in the display list. |

7. To filter patches, specify the filter options.

   a) Type the patch name in the **Show Vulnerabilities named** field.

   **Note:** The underscore character (_) is a special character that matches any single character.

   b) If necessary, select ***with this modification date***, select **>=** or **<=**, and the date from the drop-down list.

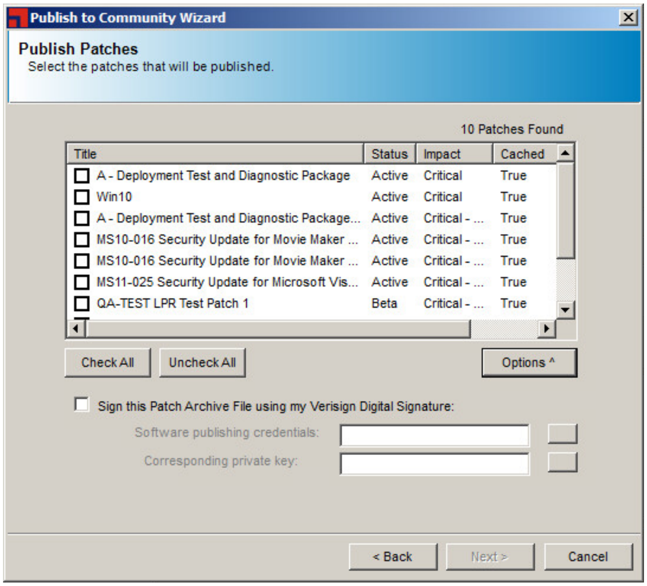
   c) Click **GO**.

   d) Select the patches you want to publish.

   **Step Result:** The sorted list is displayed in the ***Publish Patches*** page window.

8. Click **Options**.

   **Step Result:** The ***Filter Options*** area closes and is replaced by a ***Digital Signature*** area.



Publish to Community Wizard

**Publish Patches**

Select the patches that will be published.

10 Patches Found

| Title | Status | Impact | Cached |
|---|---|---|---|
| □ A - Deployment Test and Diagnostic Package | Active | Critical | True |
| □ Win10 | Active | Critical | True |
| □ A - Deployment Test and Diagnostic Package... | Active | Critical - ... | True |
| □ MS10-016 Security Update for Movie Maker ... | Active | Critical - ... | True |
| □ MS10-016 Security Update for Movie Maker ... | Active | Critical - ... | True |
| □ MS11-025 Security Update for Microsoft Vis... | Active | Critical - ... | True |
| □ QA-TEST LPR Test Patch 1 | Beta | Critical - ... | True |

□ Sign this Patch Archive File using my Verisign Digital Signature:

Software publishing credentials:

Corresponding private key:

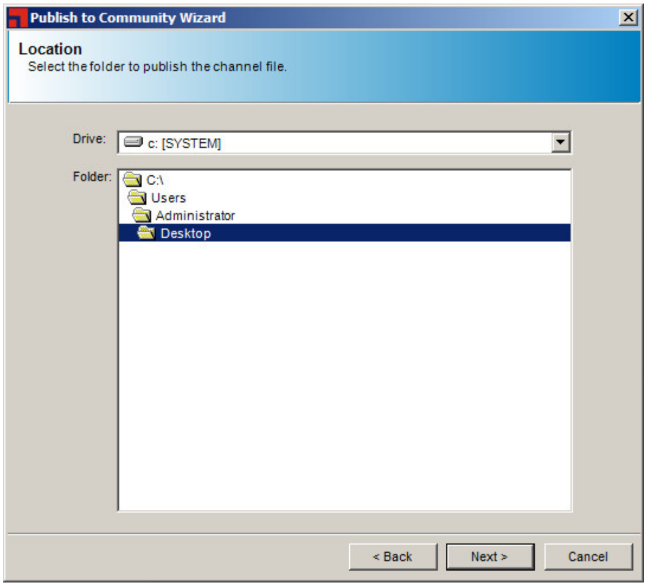
Figure 129: Publish Patches Page: Digital Signature

9. To include a digital signature, select the **Sign this Patch Archive File using My Verisign Digital Signature** check box.

   **Step Result:** The **Software publishing credentials** and the **Corresponding private key** fields become active.

**10.**In the **Software publishing credentials** field, click **Search**.

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



Publish to Community Wizard

Location

Select the folder to publish the channel file.

Drive: c: [SYSTEM]

Folder: C:\ Users Administrator Desktop

Figure 130: Location Page

**11.**Locate the Verisign certificate you want to use.

The certificate will be in the form of a `.spc` file.

**12.**Click **Next**.

**Step Result:** The **Software publishing credentials** field displays the `.spc` file.

**13.**In the **Corresponding private key** field, click **Search**.

**Step Result:** The ***Locate Private Key*** page opens.

**14.**Locate the Verisign private key you want to use.

The key will be in the form of a `.pvk` file.

**15.**Click **Open**.

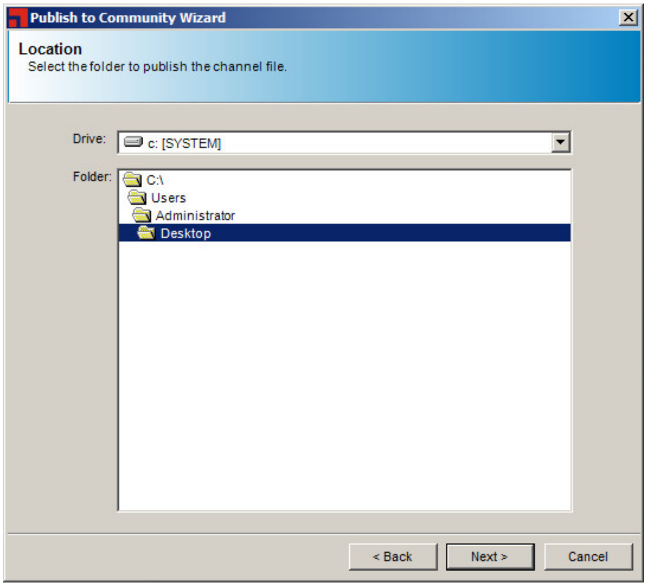
**Step Result:** The **Corresponding private key** field displays the `.pvk` file.

**16.**Verify the patch information is correct.

**Note:** If you want to sign a patch with your Verisign digital signature, you must make sure the internet connection is working. This functionality will not work in an AirGap environment because the timestamp part of the signature requires an internet connection.

**17.**Click **Next**.

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



Publish to Community Wizard

Location

Select the folder to publish the channel file.

Drive: c: [SYSTEM]

Folder: C:\ Users Administrator Desktop

Figure 131: Location Page

**18.**Select the folder where the channel file will be saved.

19. Click **Next**.

    **Step Result:** The ***Community Info*** page opens.

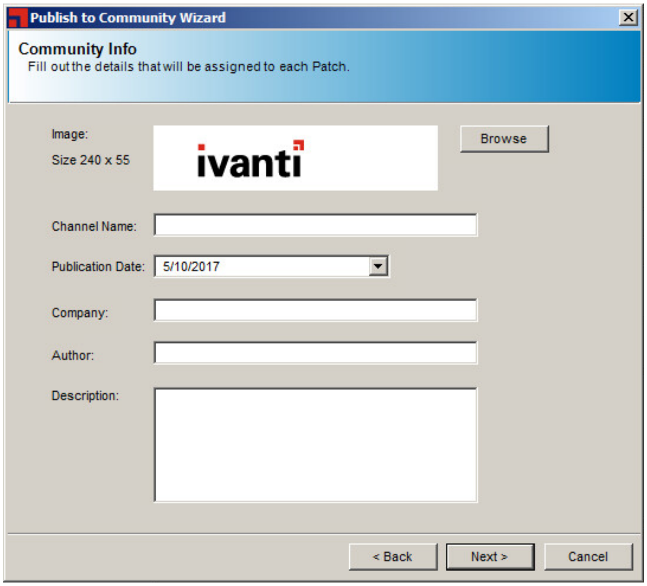


Figure 132: Community Info Page

20. Specify the information associated with the published content.

    a) Click **Browse** to insert an image of your company logo.

    **Tip:** Choose the image from the local machine, rather than a remote machine.

    b) Type a **Channel Name**.

    c) Select a **Publication Date** from the drop-down list.

    d) Type your company name in the **Company** field.

    e) Type the patch author's name in the **Author** field.

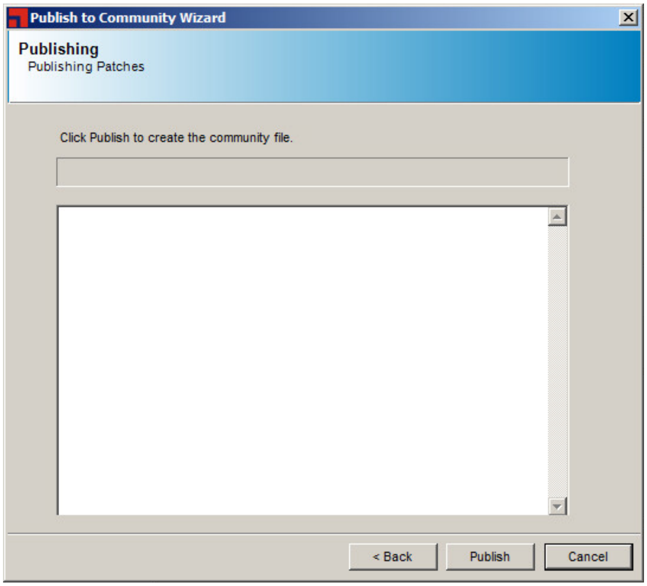
    f) Enter a description of the content in the **Description** field.

    This information will be shown to users importing the channel file.

**Note:** The filename that will be generated will be based on the channel name. The file generated will be a signed `.cab` file holding a `.zip` file of the generated `channel.xml` and `.plfz` file.

**21.**Click **Next**.

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



Click Publish to create the community file.

Figure 133: Publishing Page

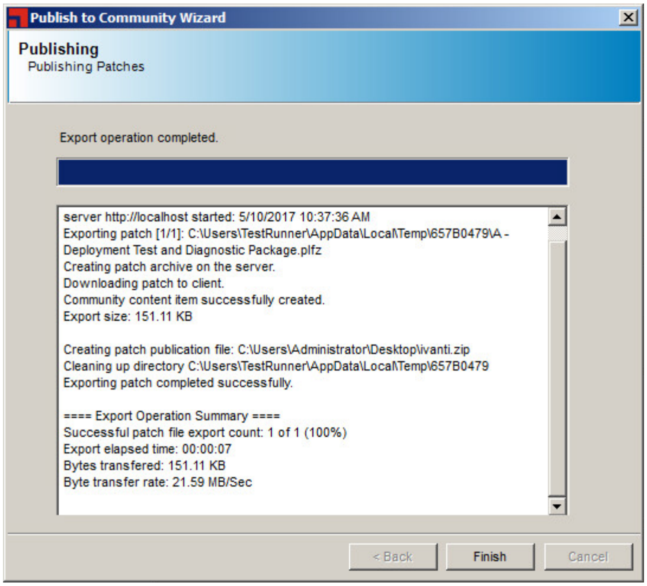
**22.**Click **Publish**.

**Step Result:** Creation of the channel file begins. A progress indicator is displayed during the export process. The lower status window is updated with details as the export is running.

> **Note:** Publish execution varies based upon the size of the patches selected for publishing.

**23.** When the export completes, the status window displays the completion status.

The status will either be success or failure. On successful completion, the status window displays the location of the patch publication file.



Export operation completed.

```
server http://localhost started: 5/10/2017 10:37:36 AM
Exporting patch [1/1]: C:\Users\TestRunner\AppData\Local\Temp\657B0479\A -
Deployment Test and Diagnostic Package.plfz
Creating patch archive on the server.
Downloading patch to client.
Community content item successfully created.
Export size: 151.11 KB

Creating patch publication file: C:\Users\Administrator\Desktop\ivanti.zip
Cleaning up directory C:\Users\TestRunner\AppData\Local\Temp\657B0479
Exporting patch completed successfully.

==== Export Operation Summary ====
Successful patch file export count: 1 of 1 (100%)
Export elapsed time: 00:00:07
Bytes transfered: 151.11 KB
Byte transfer rate: 21.59 MB/Sec
```

Figure 134: Publishing Page: Completion

**24.** Click **Finish**.

**Step Result:** The ***Publishing*** page closes.

**Result:** A channel `.zip` file is generated.

> **Note:** To evaluate this feature, it is important to make sure that you know the URL of your web directory where the content was published and that you can download the `.xml` file and `.plfz` files successfully in a web browser within your company from that website.

**After Completing This Task:**

Extract your channel `.zip` file into a web server (Internet Information Server, Apache Server) and thus make these patches available for use by others within your organization.

# Creating an Enterprise Patch Distribution Website

When using Community Subscribe and Community Publish wizards, a web server (Apache, IIS, etc) is required. Ivanti recommends using an Apache server.

## Installing the Apache Server

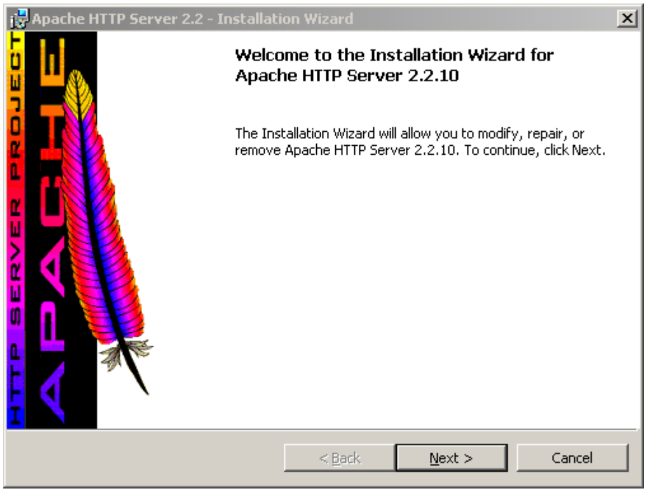
Installing an Apache server is the first step in creating an enterprise patch distribution website. Apache server version 2.2 and higher are supported.

**Prerequisites:**

At least 50MB disk space is required for the Apache server installation. After installation, Apache occupies 10MB of hard disk space. The actual space requirements for Apache depends on the configuration, the third-party module, and the library you select to account for the logs and cache files.

1. Download the latest installation software from the Apache website (http://apache.org/).
2. Double-click the installation file.

   **Step Result:** The ***Apache HTTP Server Installation Wizard*** opens.



Apache HTTP Server 2.2 - Installation Wizard

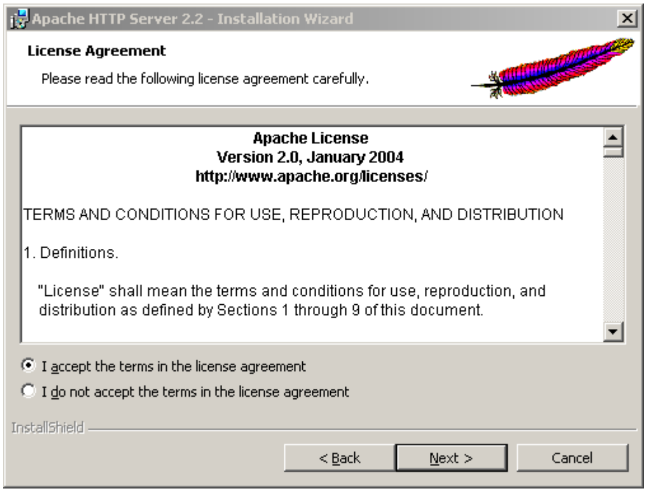
**Welcome to the Installation Wizard for Apache HTTP Server 2.2.10**

The Installation Wizard will allow you to modify, repair, or remove Apache HTTP Server 2.2.10. To continue, click Next.

Figure 135: Apache HTTP Server Installation Wizard

3. Click **Next**.

   **Step Result:** The ***License Agreement*** page opens.



**License Agreement**

Please read the following license agreement carefully.

**Apache License**
**Version 2.0, January 2004**
**http://www.apache.org/licenses/**

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

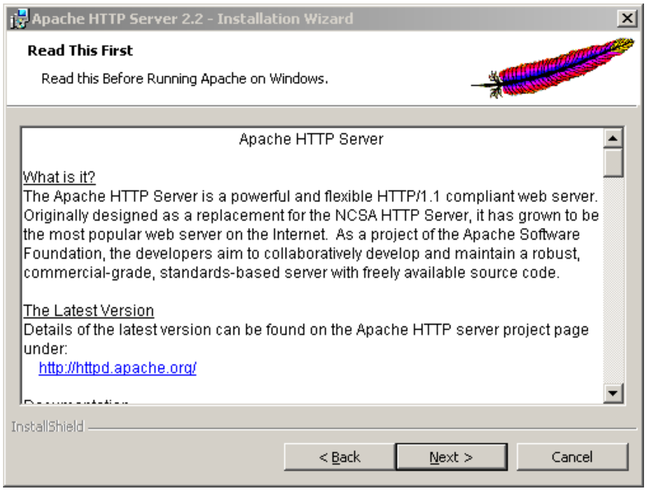
Figure 136: License Agreement Page

4. Accept the terms of the license agreement if you wish to proceed with the installation process.

   a) Select **I accept the terms in the license agreement**.

   b) Click **Next**.

   **Step Result:** The ***Read This First*** page opens.



**Read This First**

Read this Before Running Apache on Windows.

Apache HTTP Server

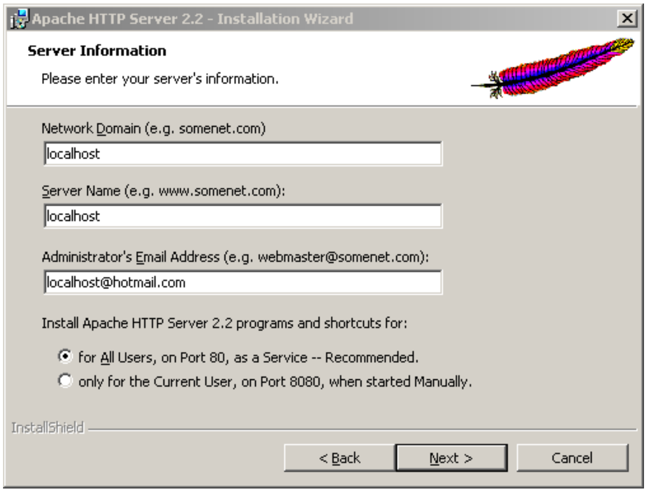
What is it?
The Apache HTTP Server is a powerful and flexible HTTP/1.1 compliant web server. Originally designed as a replacement for the NCSA HTTP Server, it has grown to be the most popular web server on the Internet. As a project of the Apache Software Foundation, the developers aim to collaboratively develop and maintain a robust, commercial-grade, standards-based server with freely available source code.

The Latest Version
Details of the latest version can be found on the Apache HTTP server project page under:
http://httpd.apache.org/

Figure 137: Read This First Page

5. Click **Next**.

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



Apache HTTP Server 2.2 - Installation Wizard

**Server Information**

Please enter your server's information.

Network Domain (e.g. somenet.com)

localhost

Server Name (e.g. www.somenet.com):

localhost

Administrator's Email Address (e.g. webmaster@somenet.com):

localhost@hotmail.com

Install Apache HTTP Server 2.2 programs and shortcuts for:

● for All Users, on Port 80, as a Service -- Recommended.

○ only for the Current User, on Port 8080, when started Manually.

Figure 138: Server Information Page

6. Specify the server information.

   a) Type **localhost** in the **Network Domain** field.

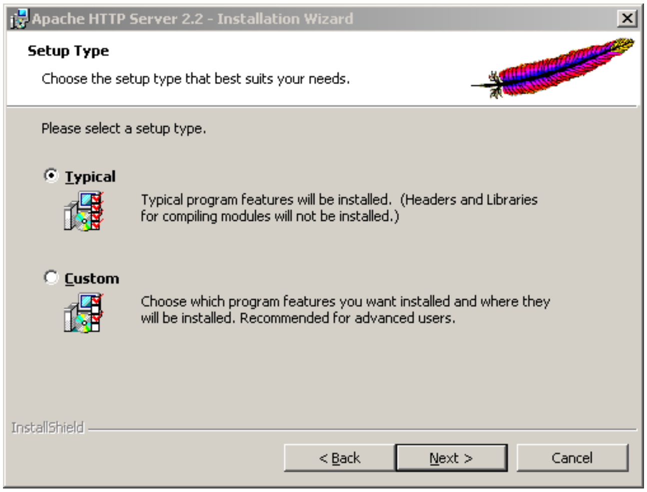
   b) Type **localhost** in the **Server Name** field.

   c) Type the administrator's email address in the **Administrator's Email Address** field.

   d) Select **for All Users, on Port 80 as a Service -- Recommended**.

7. Click **Next**.

   **Step Result:** The ***Setup Type*** page opens.



Apache HTTP Server 2.2 - Installation Wizard

**Setup Type**

Choose the setup type that best suits your needs.

Please select a setup type.

● Typical

Typical program features will be installed. (Headers and Libraries for compiling modules will not be installed.)

○ Custom

Choose which program features you want installed and where they will be installed. Recommended for advanced users.

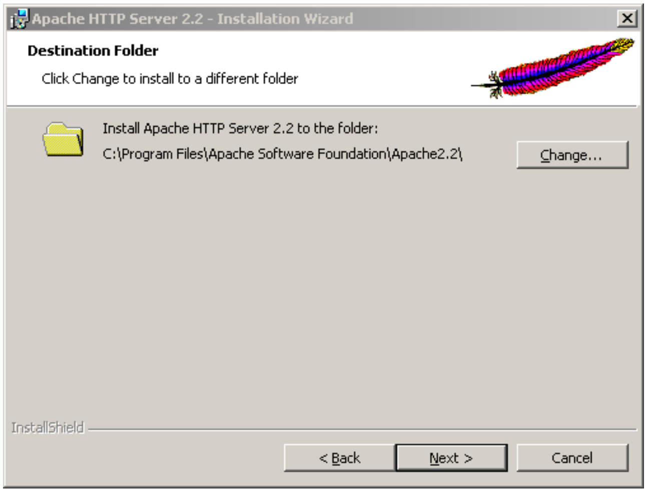
Figure 139: Setup Type Page

8. Select the type of setup that you want to use.

   The default option is **Typical**.

9. Click **Next**.

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



Apache HTTP Server 2.2 - Installation Wizard

**Destination Folder**

Click Change to install to a different folder

Install Apache HTTP Server 2.2 to the folder:
C:\Program Files\Apache Software Foundation\Apache2.2\

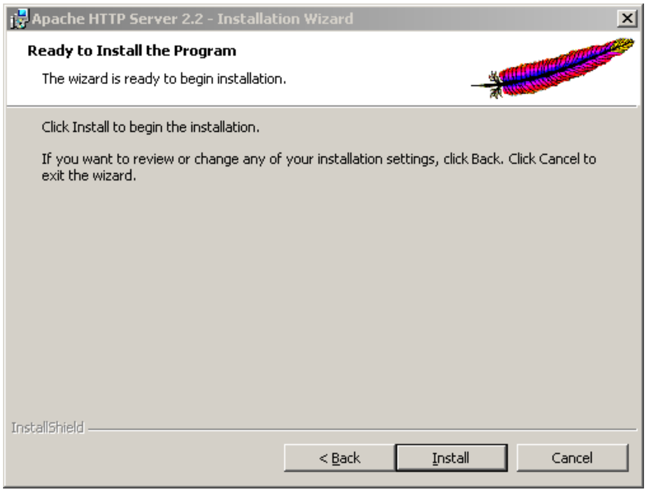
Figure 140: Destination Folder Page

10. Select the installation folder for the server.

    Click **Change** to install the server in a location that you specify.

11. Click **Next**.

    **Step Result:** The ***Ready to Install the Program*** page opens.



Apache HTTP Server 2.2 - Installation Wizard

**Ready to Install the Program**

The wizard is ready to begin installation.

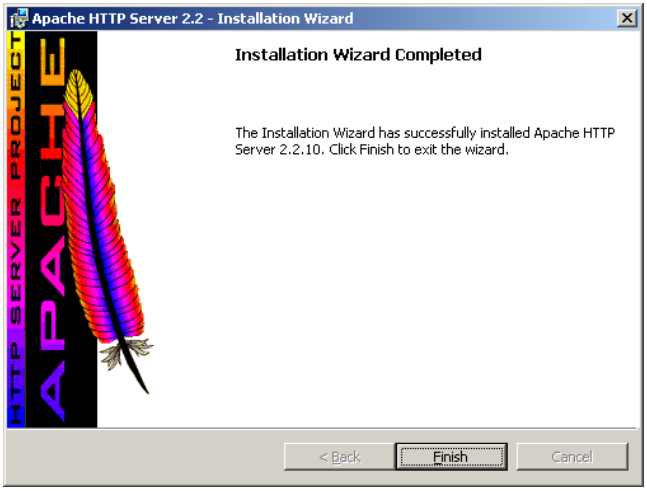
Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

Figure 141: Ready to Install the Program Page

12. Click **Install**.

    **Step Result:** The ***Installation Wizard Completed*** page opens.



Apache HTTP Server 2.2 - Installation Wizard

**Installation Wizard Completed**

The Installation Wizard has successfully installed Apache HTTP Server 2.2.10. Click Finish to exit the wizard.

Figure 142: Installation Wizard Completed Page

13. Click **Finish**.

    **Step Result:** The ***Apache HTTP Server Installation Wizard*** closes.

**Result:** The Apache HTTP server is successfully installed at the selected location.

## Configuring the Apache HTTP Server

You can configure the Apache HTTP server to meet your specific requirements. To configure the server, edit the `httpd.conf` file in a text editor.

1. Create a copy of the `httpd.conf` file for backup.
2. Open the `httpd.conf` file.

   By default, this file is located in `C:\Program Files\Apache Software Foundation\Apache2.2\conf\`.
3. Modify the default port **Listen 80** to any other available port.
4. Select **File** > **Save**.

**Result:** The Apache HTTP server configuration is changed.

## Starting the Apache Server Service

You can start the Apache HTTP server by clicking on the desktop icon or from the Windows **Start** menu.

1. Select **Start** > **Programs** > **Apache HTTP Server 2.2**.

   **Step Result:** The ***Apache HTTP Server*** opens.

2. Click **Monitor Apache Servers**.

   **Step Result:** A small red icon appears in the taskbar.

3. Click the red icon in the taskbar.

   **Step Result:** The ***Apache Server Monitor*** window opens.

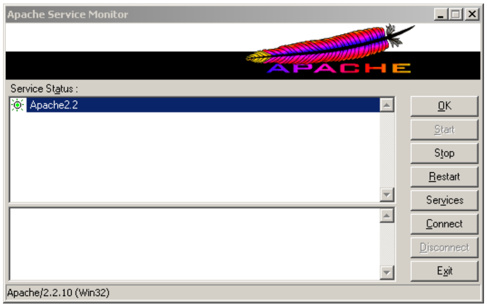


Figure 143: Apache Server Monitor

4. Select a service.

5. Click **Start**.

   **Step Result:** The selected service becomes active.

**Result:** You can begin using the selected Apache service.

## Testing the Apache Server

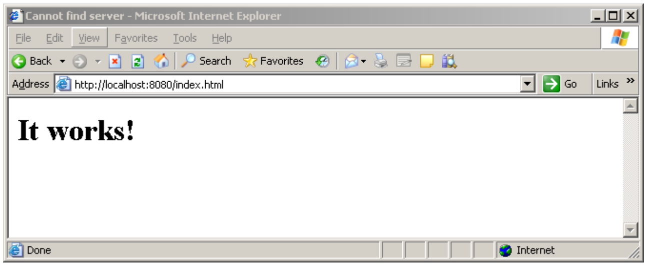
You must test the Apache server that you have installed before creating the enterprise patch distribution website. Testing is performed by trying to get a successful response from the localhost.

1. Open a web browser window.
2. Type `http://localhost:8080/`.

   You can also type `http://localhost:8080/index.html`.

   > **Note:** Using the HTTPS connection type is not recommended. If you must use the HTTPS connection type, the SSL needs to be configured and the keys will need to be imported into the cache on the machines running the Ivanti Content Wizard.

   **Step Result:** A success message is displayed.



Cannot find server - Microsoft Internet Explorer

Address http://localhost:8080/index.html

It works!

Figure 144: Success Message

**Result:** The Apache HTTP server is successfully tested.