



Endpoint Security

powered by HEAT Software

Air Gap Windows Patching Guide

Dec 2020

Contents

Contents	2
Requirements	3
Air Gap Software Requirements	4
Air Gap Checklist	5
Windows Patch Configuration for Air Gap	6
Air Gap Provider: Windows Patch Configuration Overview	7
Installing the ICW Server on the Provider	8
Installing the ICW Client on the Provider	10
Air Gap Client: Windows Patch Configuration Overview	11
Installing the ICW Server on the Client	12
Installing the ICW Client on the Client	14
Windows Air Gap Updates	15
Windows Air Gap Update: Creation Overview	16
Replicating With the Global Subscription Service	17
Caching Windows Patches	20
Exporting Windows Patches	25
Copying Windows Patch Metadata	28
Windows Update Installation Overview	29
Importing Windows Patch Content	30
Installing Windows Patch Metadata	32
Appendix	33
Troubleshooting	33
Glossary	34

Requirements

Before beginning installation, review the requirements to make sure you have all the hardware and software necessary for successful use of Air Gap.

Air Gap Software Requirements

Setting up Ivanti Endpoint Security in an air gap network requires additional software created specifically for air gap.

The Air Gap Toolkit

This toolkit includes several tools, utilities, and scripts needed to configure and maintain an Endpoint Security Server that's disconnected from the Internet.

The Air Gap Toolkit includes:

- Air Gap Hotfix
- Air Gap License Tool
 - AirGapLicenseTool.exe
 - AirGapLicenseToolUI.exe
- ImportEndpointManifest.exe
- A couple of scripts that configure your Endpoint Security Server running in the air gap network:
 - AirGapScript.sql
 - Dependencies.sql
- Ivanti Content Wizard: this tool includes two installable components:
 - A server installer (ICWServer.msi)
 - A client installer (ICWClient.msi)

Air Gap Checklist

Before you begin, make sure you have the following materials on hand:

Hardware

- 1 TB of open disk space on both the Air Gap Provider and Air Gap Client.
- 1 TB USB thumb drive. This portable media is used to move software across the air gap.



As a security best-practice, format the thumb drive to remove any software already on the drive.

Ivanti Software

Download the following software from the [Ivanti Download Page](#).

- The Air Gap Toolkit



After you download the software listed above, move it to your USB thumb drive. You'll be using the software on both the Air Gap Provider and the Air Gap Client.

Windows Patch Configuration for Air Gap

Before you can patch Windows endpoints operating in an air gap network, you must install some additional software on:

- The Air Gap Provider
- The Air Gap Client

These configurations only need to be completed once. After you make these configurations, you likely won't have to complete this process again.

Air Gap Provider: Windows Patch Configuration Overview

If you're going to patch Windows endpoints in your air gap network, extra configuration is required on your Air Gap Provider.

Each procedure listed below is performed from your Air Gap Provider. Review this list to form a basic understanding of each procedure you'll perform (there will be a similar topic later that provides an overview for the Air Gap Client).



Before you start, review the "Air Gap Checklist" on page 5. Make sure you have all the materials you'll need.

1. "Installing the ICW Server on the Provider" on the next page

Install the Ivanti Content Wizard (ICW) Server on your Air Gap Provider. The ICW Server allows you to export patch content from your Endpoint Security Server. You'll use a USB thumb drive to move this patch content to your Air Gap Client later.

2. "Installing the ICW Client on the Provider" on page 10

Install the Ivanti Content Wizard (ICW) Client on your Air Gap Provider. The ICW Client is the console that you use to interact with the ICW Server.

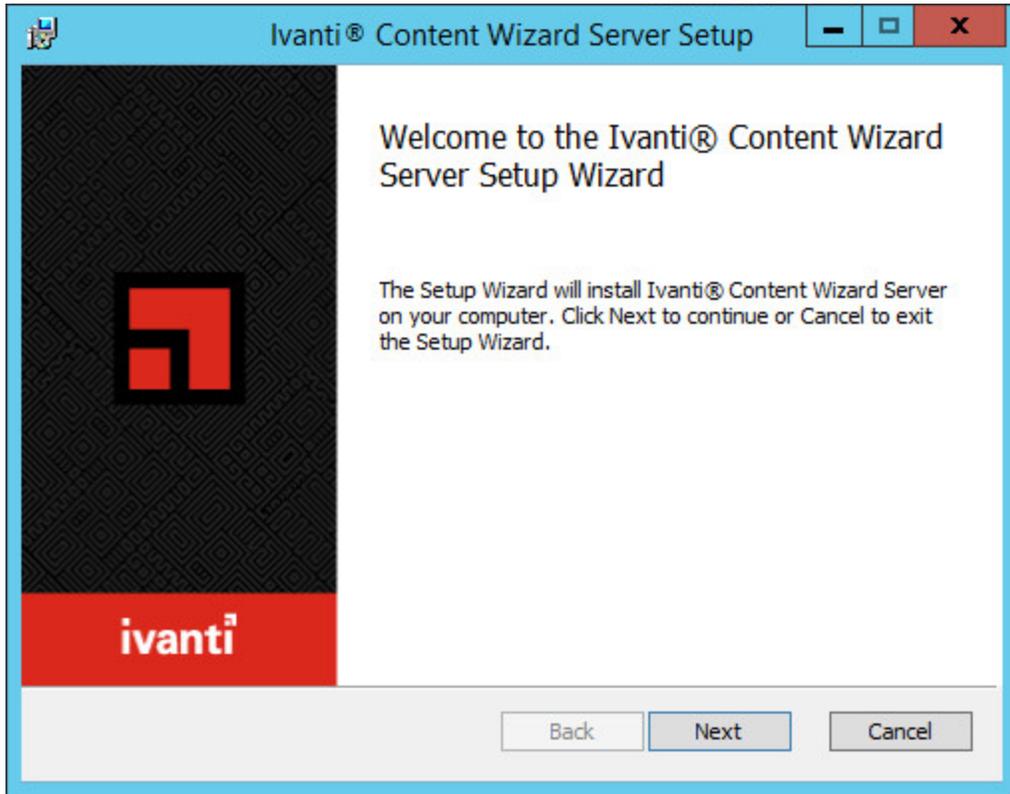
Installing the ICW Server on the Provider

Install the Ivanti Content Wizard (ICW) Server on your Air Gap Provider. The ICW Server allows you to export patch content from your Endpoint Security Server. You'll use a USB thumb drive to move this patch content to your Air Gap Client later.

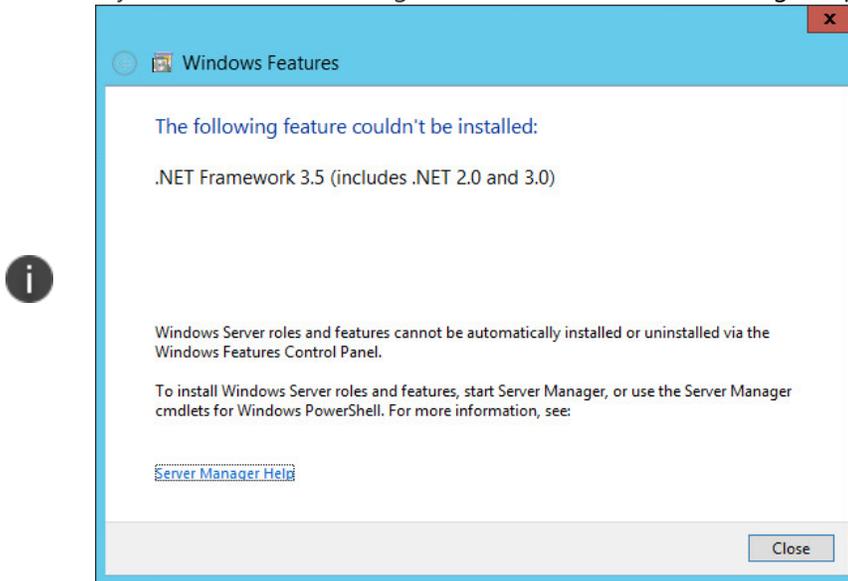
To Install the ICW Server on your Air Gap Provider

1. Make sure that the USB thumb drive containing the Air Gap Toolkit is connected.
2. Open Windows Explorer and browse to the USB thumbdrive.
3. Within the thumb drive, browse to **Ivanti AirGap Toolkit 8.5.0.40\Software**.

4. Open **ICWServer.msi** and complete the Ivanti Content Wizard Server Setup.



If you receive the following error, refer to "Troubleshooting" on page 33:



ICW Server is installed.

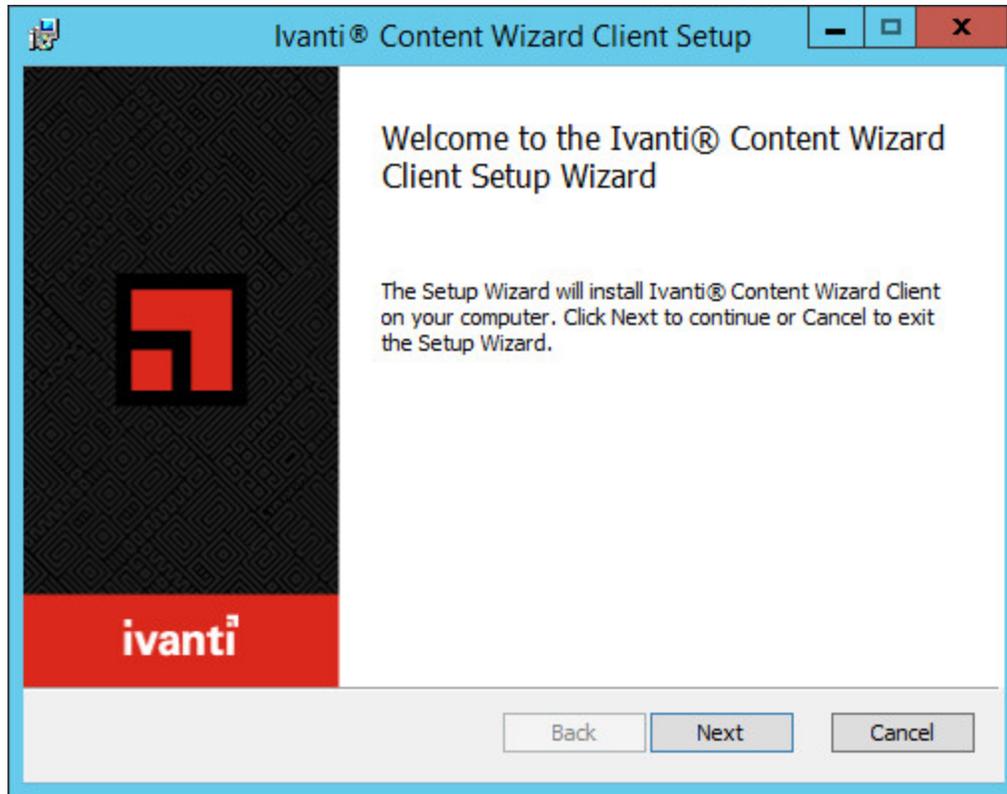
Proceed to "Installing the ICW Client on the Provider" on the next page.

Installing the ICW Client on the Provider

Install the Ivanti Content Wizard (ICW) Client on your Air Gap Provider. The ICW Client is the console that you use to interact with the ICW Server.

To Install the ICW Client on your Air Gap Provider

1. Open Windows Explorer and browse to the USB thumbdrive.
2. Within the thumb drive, browse to **Ivanti AirGap Toolkit 8.5.0.40\Software**.
3. Open ICWClient.msi and complete the Ivanti Content Wizard Client Setup.



ICW Client is installed.

Proceed to "Air Gap Client: Windows Patch Configuration Overview" on the next page.

Air Gap Client: Windows Patch Configuration Overview

To patch Windows endpoints in your air gap network, you must make configurations to your Air Gap Client so that it can receive Windows patches.

Each procedure listed below is performed from your Air Gap Client. Review this list to form a basic understanding of each procedure that you'll perform.



Before you start, review the "Air Gap Checklist" on page 5. Make sure you have all the materials you'll need.

1. "Installing the ICW Server on the Client" on the next page

The Ivanti Content Wizard (ICW) Server is also used on your Air Gap Client to import patch content. Install the ICW Server on your Air Gap Client so it can receive patch content updates.

2. "Installing the ICW Client on the Client" on page 14

Install the Ivanti Content Wizard (ICW) Client on your Air Gap Client so that you can interact with the ICW Server using a console.

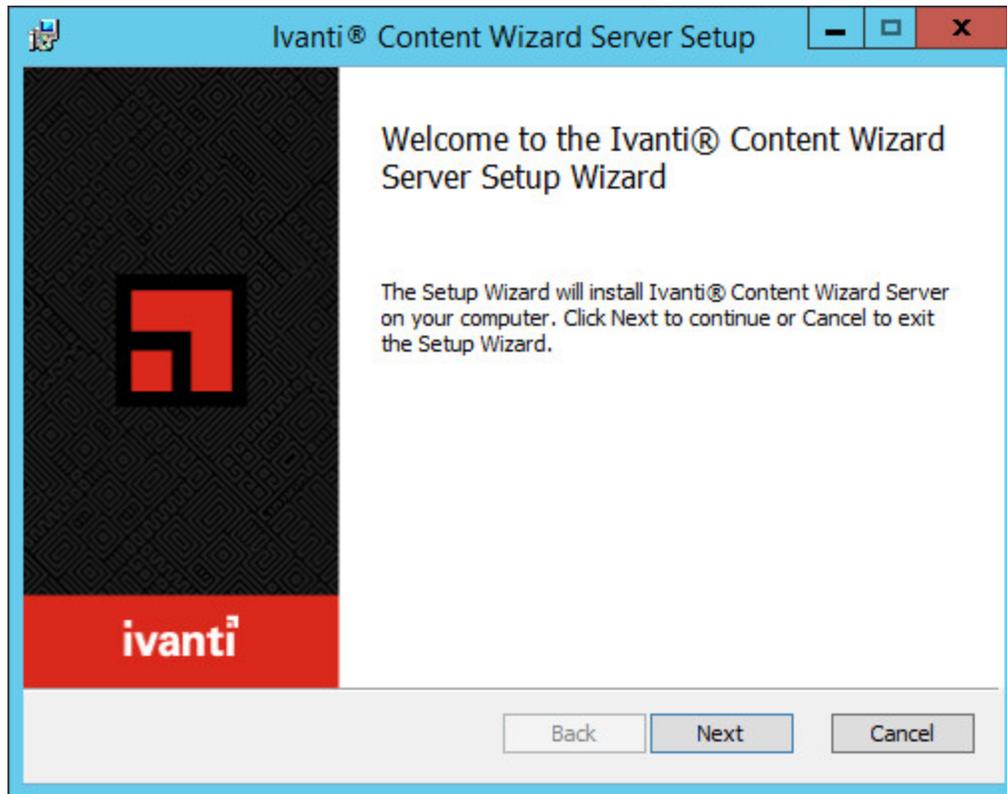
Installing the ICW Server on the Client

The Ivanti Content Wizard (ICW) Server is also used on your Air Gap Client to import patch content. Install the ICW Server on your Air Gap Client so it can receive patch content updates.

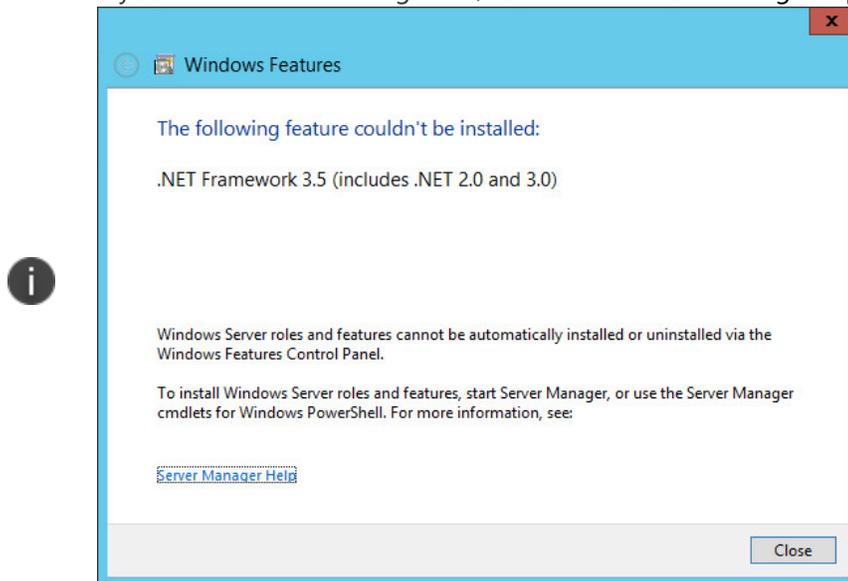
To Install the ICW Server on your Air Gap Client

1. Make sure that the USB thumb drive containing the Air Gap Toolkit is connected.
2. Open Windows Explorer and browse to the USB thumbdrive.
3. Within the thumb drive, browse to **Ivanti AirGap Toolkit 8.5.0.40\Software**.

4. Open **ICWServer.msi** and complete the Ivanti Content Wizard Server Setup.



If you receive the following error, refer to "Troubleshooting" on page 33:



ICW Server is installed.

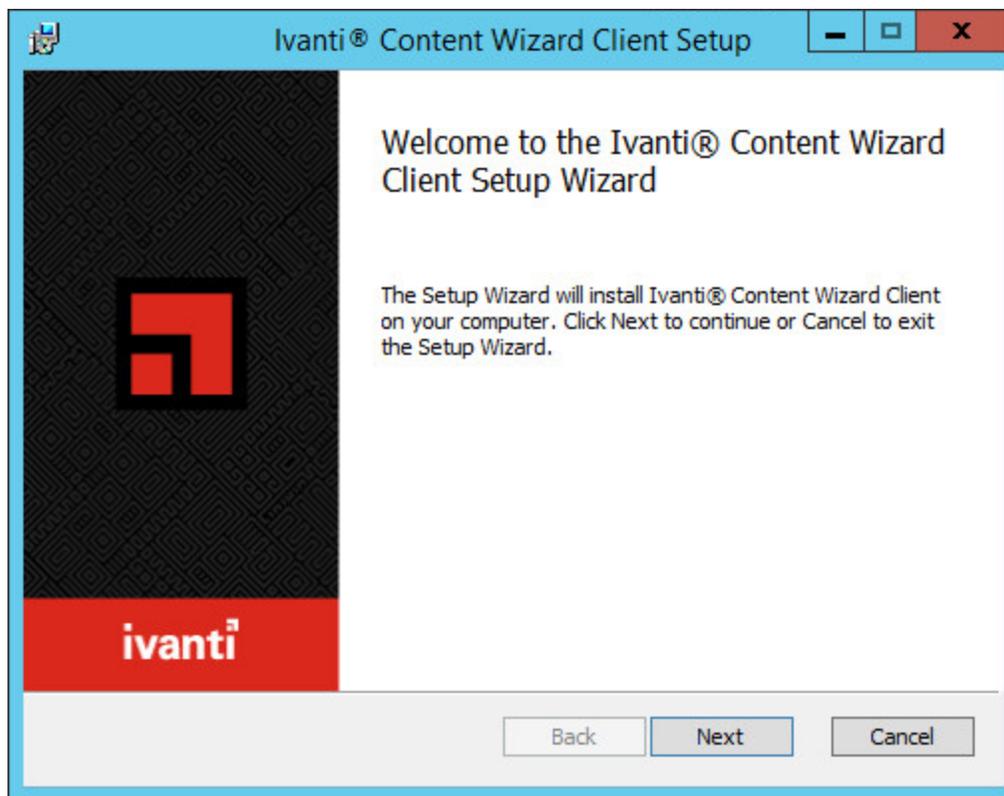
Proceed to Installing the ICW Client on the Client.

Installing the ICW Client on the Client

Install the Ivanti Content Wizard (ICW) Client on your Air Gap Client so that you can interact with the ICW Server using a console.

To Install the ICW Client on your Air Gap Client

1. Open Windows Explorer and browse to the USB thumbdrive.
2. Within the thumb drive, browse to **Ivanti AirGap Toolkit 8.5.0.40\Software**.
3. Open ICWClient.msi and complete the Ivanti Content Wizard Client Setup.



ICW Client is installed.

Proceed to "Windows Air Gap Updates" on page 15.

Windows Air Gap Updates

This chapter guides you through the standard air gap Linux patching workflow.

An Air Gap Update is a bundle of new Endpoint Security content that is moved from the Air Gap Provider to the Air Gap Client. Updates include the software that is used to secure your endpoints in an air gap network. Updates can include any of the following content:

- Windows Patch Content
- Linux Patch Content
- AntiVirus Definitions

Making an Air Gap Update for Windows consists of two parts:

- Creating an Air Gap Update, which takes place on the Air Gap Provider
- Installing an Air Gap Update, which takes place on the Air Gap Client

We recommended making an Air Gap Update every Patch Tuesday, or when a critical security vulnerability is found that needs to be patched immediately.

Windows Air Gap Update: Creation Overview

This overview summarizes each process required to create an Air Gap Update that includes Windows patch content.

All procedures in this overview are performed from the Air Gap Provider. There will be another overview similar to this one for the process of installing the Update on your Air Gap Client.



Before you start, review the "Air Gap Checklist" on page 5. Make sure you have all the materials you'll need.

1. "Replicating With the Global Subscription Service" on the next page

Begin by initiating a replication with the Global Subscription Service (GSS), which is a cloud service for your Endpoint Security Server. You can download the latest:

- License information
- System updates
- Patch content
- AntiVirus definitions

Although this process isn't absolutely required because the Air Gap Provider automatically replicates once daily by default, we recommend replicating before creating an Air Gap Update.

2. "Caching Windows Patches" on page 20

After replicating to download the latest Windows patch metadata, you need to download the patch binaries themselves—a process known as caching.

3. "Exporting Windows Patches" on page 25

Use the Ivanti Content Wizard to export your Windows patches from the Air Gap Provider to your USB thumb drive.

4. "Copying Windows Patch Metadata" on page 28

Bring your Windows patch metadata over the air gap so that you can view the Windows patches on your Air Gap Client and deploy them. Begin this process by copying the Windows patch metadata on your Provider to a USB thumbdrive.

Replicating With the Global Subscription Service

Begin by initiating a replication with the Global Subscription Service (GSS), which is a cloud service for your Endpoint Security Server. You can download the latest:

- License information
- System updates
- Patch content
- AntiVirus definitions

Although this process isn't absolutely required because the Air Gap Provider automatically replicates once daily by default, we recommend replicating before creating an Air Gap Update.

To Replicate With the GSS

1. From the Air Gap Provider, log into the Endpoint Security Console.

The screenshot displays the Ivanti Endpoint Security console interface. At the top, the navigation bar includes 'Home', 'Discover', 'Review', 'Manage', 'Reports', 'Tools', and 'Help'. The user is logged in as 'Administrator'. The dashboard features several widgets:

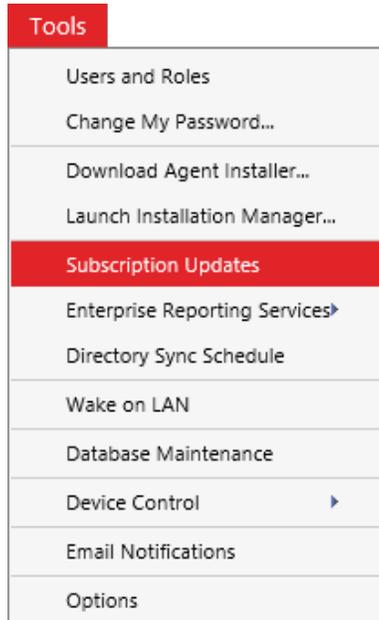
- Server Information:** Shows company details (Ivanti), license replication (100%), system replication (100%), patch/content replication (0%), and package replication (0 remaining). It includes a table for Product Licenses:

Product Module	In Use	Pending	Available
AntiVirus	0	0	25
App Control	0	0	25
Patch	0	0	25

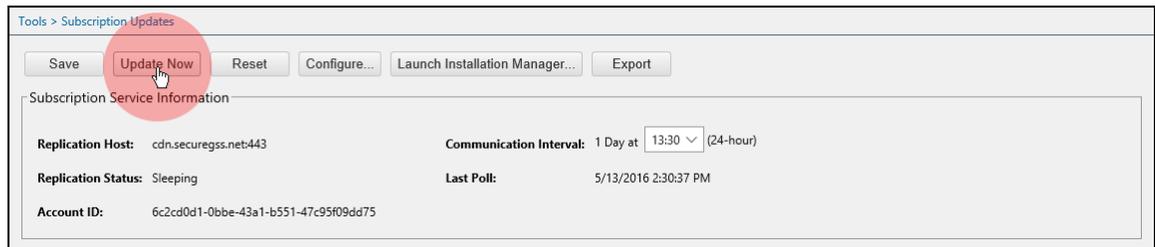
- Agent Module Installation Status:** No data available.
- Un-remediated Critical Vulnerabilities:** No data available.
- Endpoints with Unresolved Updates:** No data available.
- Top 10 Infected Endpoints:** No results found.
- Application Library File Assessment:** No results found.
- Latest News:** Lists security updates such as 'April 2017 Security Updates' and 'Microsoft Replaces Security Bulletins'.

The footer shows the server name 'AZ-TP-WIN2012-2' and the date/time '4/20/2017 4:41:12 PM'.

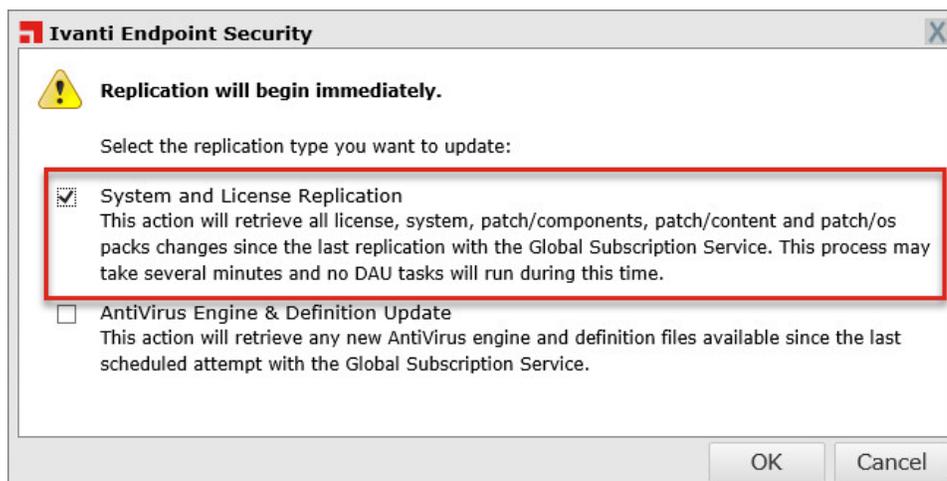
2. From the Navigation Menu, select **Tools > Subscription Updates**.



3. Click **Update Now**.



4. Make sure **System and License Replication** is selected and then click **OK**.



5. Watch the window and wait for patch replication to complete.

Patch / OS Packs	Completed
Patch / Content	Completed
Patch / Components	Completed

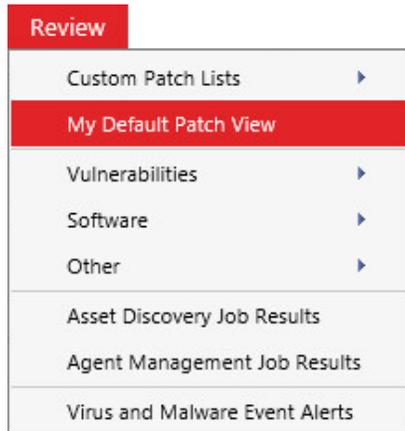
Continue to "Caching Windows Patches" on the next page.

Caching Windows Patches

After replicating to download the latest Windows patch metadata, you need to download the patch binaries themselves—a process known as caching.

To Cache Windows Content

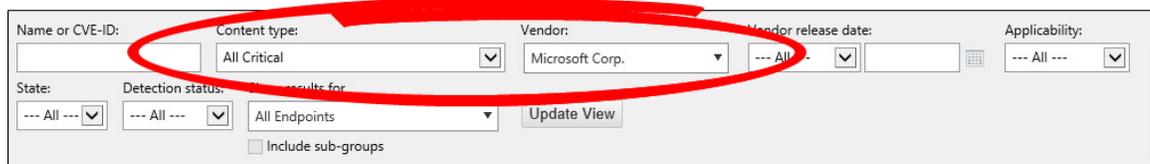
1. Navigate to **Review > My Default Patch View**.



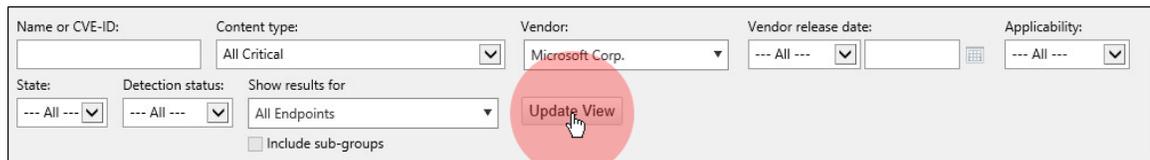
2. Use the page filters to find the Windows patches that you want to move to your Air Gap Client (in other words, the patches that you're going to cache).

For your initial Air Gap Update, we recommend the following filter settings at a minimum to cache all critical content:

- **Content type: All Critical**
- **Vendor: Microsoft Corp.**
- **All remaining options: ---All---**

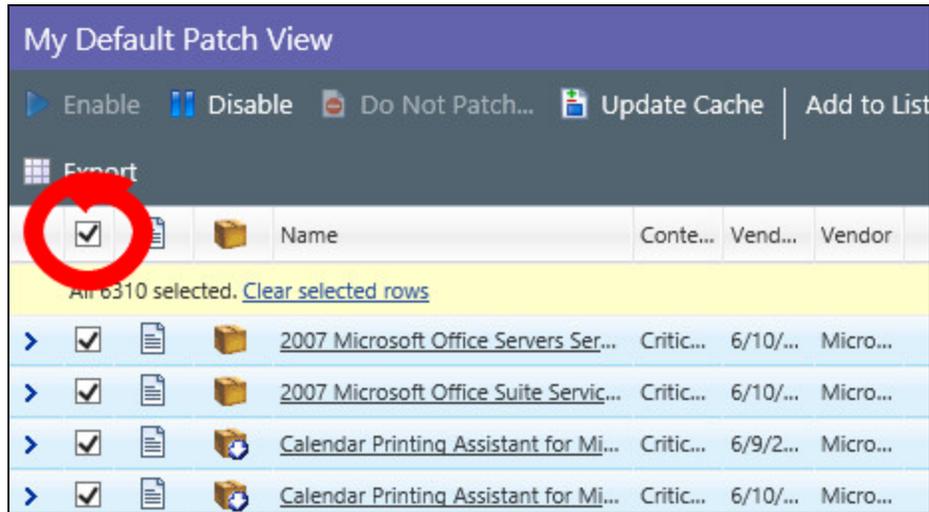


3. Click **Update View**.

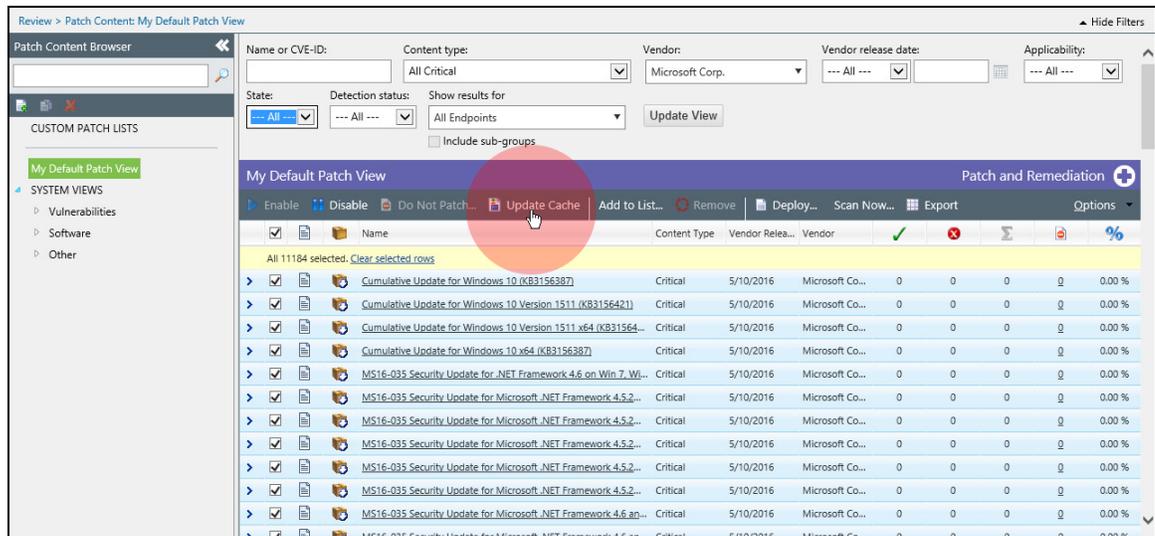


- Select the patches you want to move to your Air Gap Client.

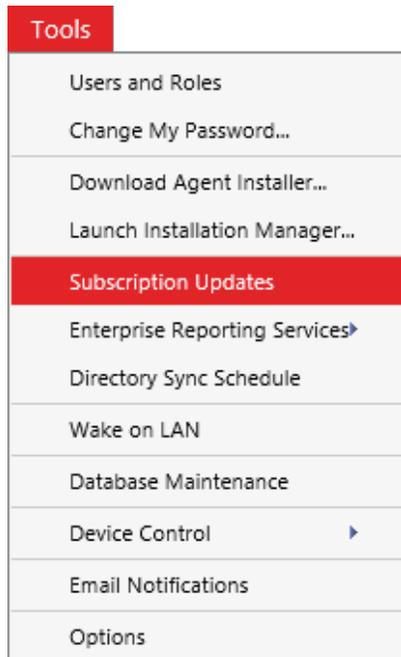
For your initial Air Gap Update, use the **Select All** checkbox to choose all patches.



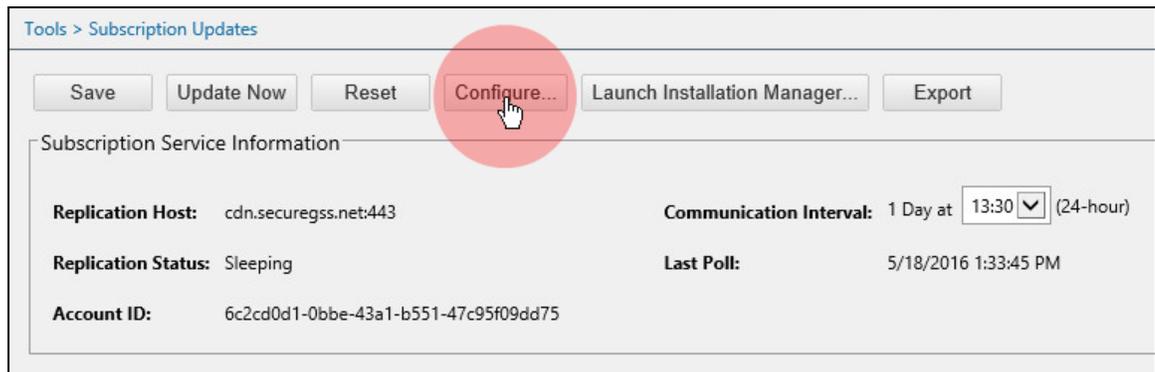
- Click **Update Cache** to download the patch binaries. Confirm the download when prompted.



6. Navigate to **Tools > Subscription Updates**.



7. Click **Configure**.



8. Make sure that the **Auto-download new critical packages** option is selected.

Save and close the dialog when you're done.

This option configures Endpoint Security to automatically cache critical patches released in the future so that you don't have to cache them yourself.

Subscription Service Configuration

Service Languages Content AntiVirus

Status

Service Status: Running

Last Checked: 5/18/2016 1:33 PM

Next Check: 5/19/2016 1:30 PM

Package Caching

Auto-download new critical packages

Proxy

Address:

Port:

Authenticated

User Name:

Password:

Confirm Password:

Communication

Logging Level: Error

Enable Bandwidth Throttling

Kbytes per second

Retry Limit: 3

Retry Wait: 300 (secs)

Connect Timeout: 1800 (secs)

Command Timeout: 1800 (secs)

RSA BSAFE

Save Cancel Apply

9. Monitor the **Subscription Service History**. When the most-recent **Packages** entry Completes, your Windows patches are cached.

Subscription Service History

Type	Status
Packages	In Progress
Patch / OS Packs	Completed
Patch / Content	Completed

Continue to "Exporting Windows Patches" on the next page.

Exporting Windows Patches

Use the Ivanti Content Wizard to export your Windows patches from the Air Gap Provider to your USB thumb drive.

To Export Windows Patches

1. Make sure you have a USB thumb drive connected to your Air Gap Provider.
2. Open ICW Client and connect to the ICW Server.



Connect to Server

ivanti Content Wizard
powered by Heat

Login Proxy

Server URL:
http://<ContentWizardServer>

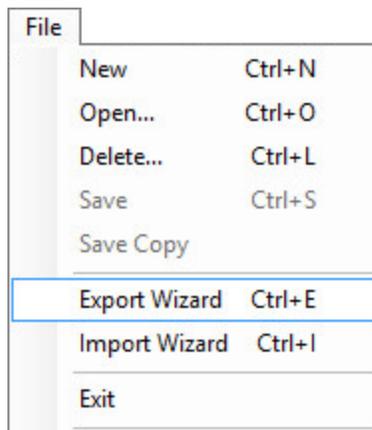
Username:
Administrator

Password:

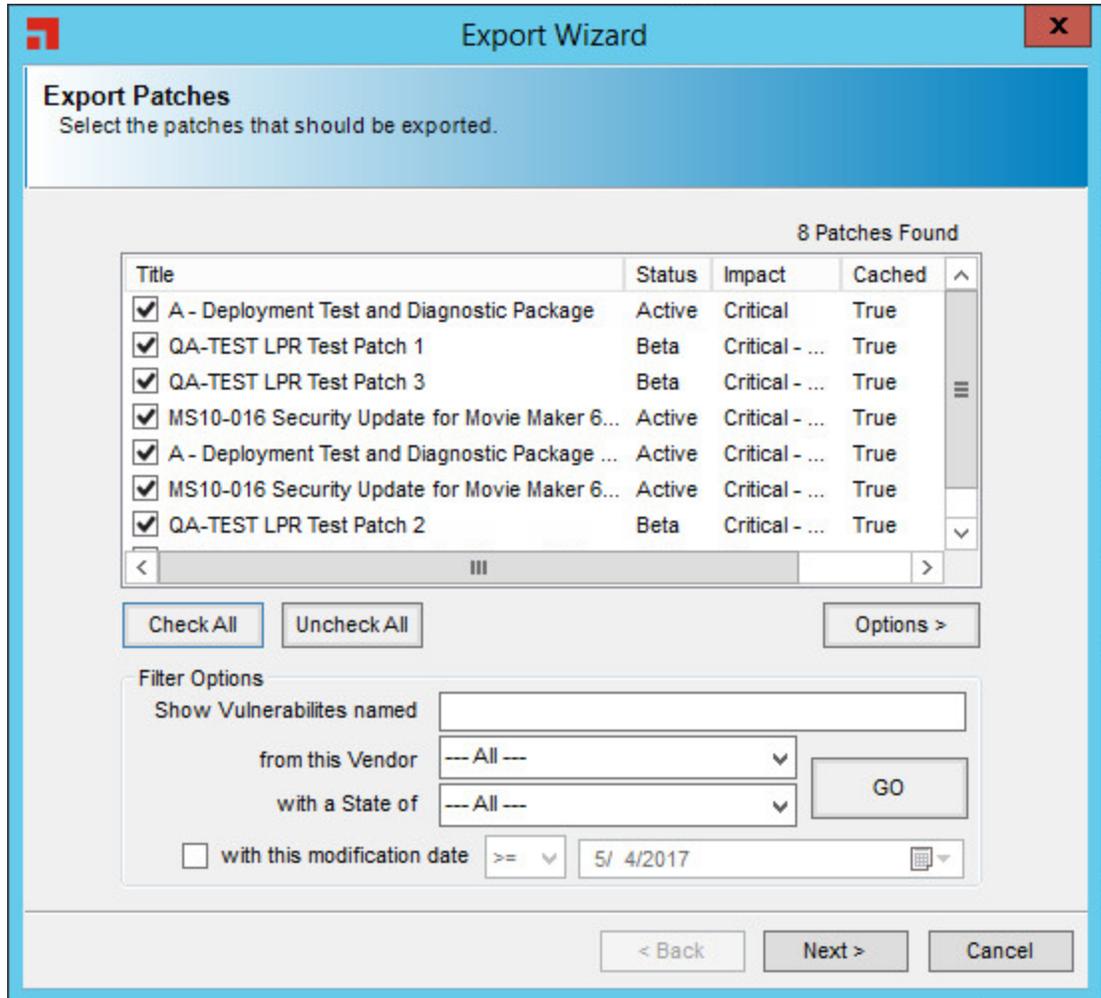
Remember my password

OK Cancel

3. Select **File > Export Wizard**.



4. Use the Export Wizard to export your Windows patches to your USB thumb drive.
 - For the first Air Gap Update you create, don't select any filter option. Just Click **Go**.
 - If you're making a follow up Air Gap Update, use the modification date filter to find only patches that have been cached since your previous Air Gap Update.



5. Close the Ivanti Content Wizard Client.

Your Windows patch content is transferred to the USB thumb drive.

Continue to "Copying Windows Patch Metadata" on the next page.

Copying Windows Patch Metadata

Bring your Windows patch metadata over the air gap so that you can view the Windows patches on your Air Gap Client and deploy them. Begin this process by copying the Windows patch metadata on your Provider to a USB thumbdrive.

To Copy Windows Metadata

1. Open Windows Explorer and browse to **C:\Program Files (x86)\HEAT Software\EMSS\Content**.
2. Open a second instance of Windows Explorer. Browse to your USB thumb drive.
3. Copy the following folders from **Content** to your USB thumb drive:
 - **PatchComponents**
 - **00000000-0000-0000-0000-000000000000\GssComponents**
4. Close both instances of Windows Explorer and disconnect your USB thumb drive.

Your Windows metadata is copied to the USB thumb drive and your Air Gap Update is created.

Continue to "Windows Update Installation Overview" on the next page.

Windows Update Installation Overview

This overview summarizes each process required to install a Windows Air Gap Update on your Client.

All procedures in this overview are performed from the Air Gap Client.



Before you start, review the "Air Gap Checklist" on page 5. Make sure you have all the materials you'll need.

1. "Importing Windows Patch Content" on the next page

On your Air Gap Client, import the Windows patches that are on your USB thumb drive.

2. "Installing Windows Patch Metadata" on page 32

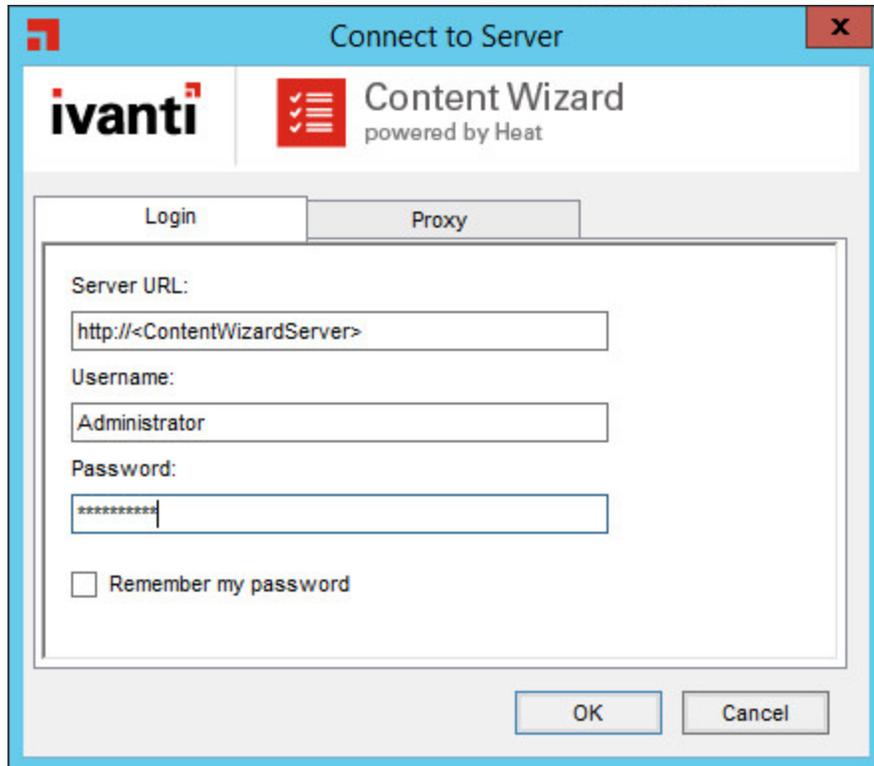
Install the Windows patch metadata that you copied to your USB thumb drive earlier so that you can view your patches on the Air Gap Client.

Importing Windows Patch Content

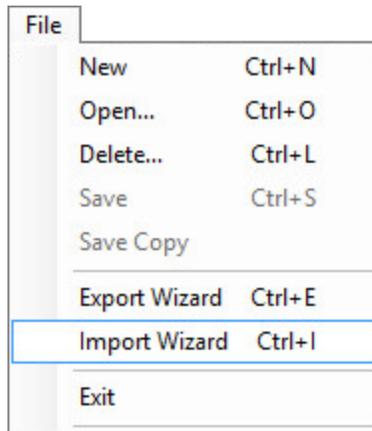
On your Air Gap Client, import the Windows patches that are on your USB thumb drive.

To Import Windows Patch Content

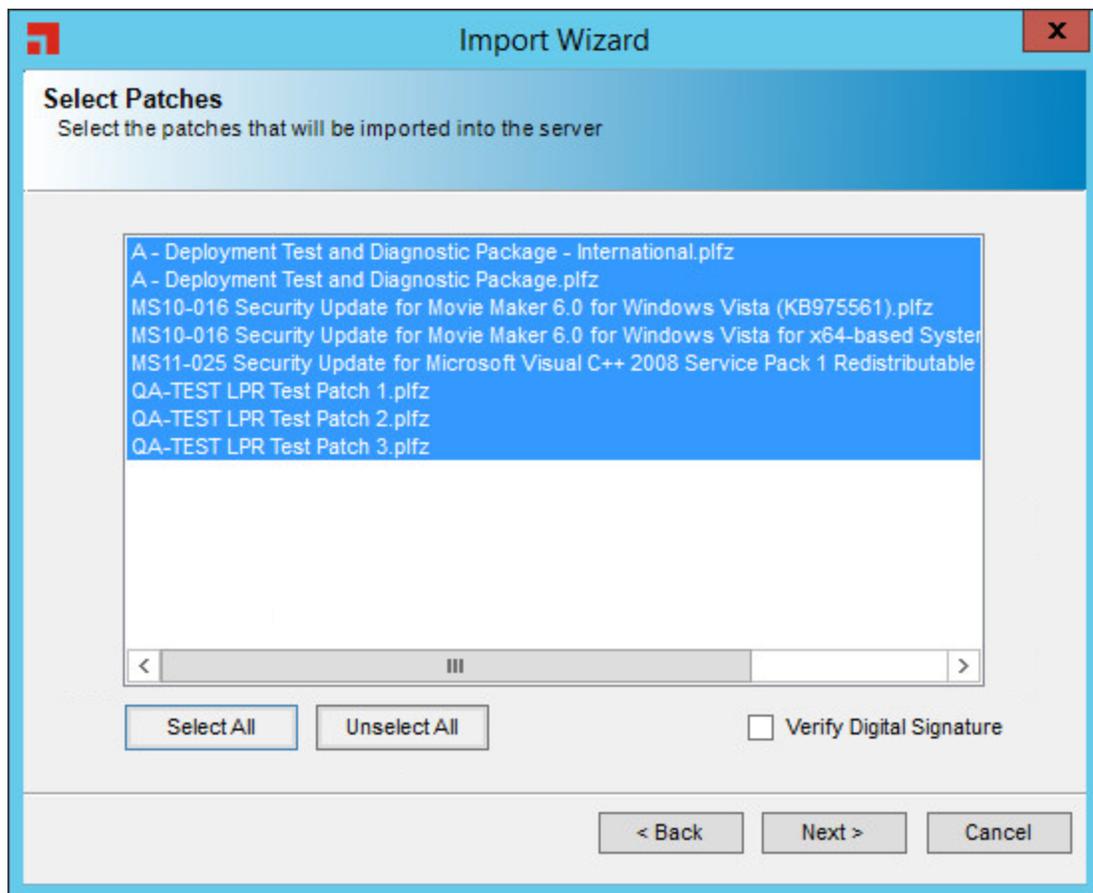
1. Log in to your Air Gap Client.
2. Make sure that the USB thumb drive containing your Windows patches is connected to the Air Gap Client.
3. Open ICW Client and connect to the ICW Server.



4. Select **File > Import Wizard**.



5. Use the Import Wizard to import the Windows patches on your USB thumb drive.



6. When you're done, close the ICW Client.

Your Windows patch content is imported to your Air Gap Client.

Continue to "Installing Windows Patch Metadata" on the next page.

Installing Windows Patch Metadata

Install the Windows patch metadata that you copied to your USB thumb drive earlier so that you can view your patches on the Air Gap Client.

To Install Windows Patch Metadata

1. Open Windows Explorer and browse to your USB thumb drive.
2. Open a second instance of Windows Explorer. Browse to **C:\Program Files (x86)\HEAT Software\EMSS\Content**.
3. Copy the following folders from your USB thumb drive and paste them to **Content**:
 - **PatchComponents**
 - **00000000-0000-0000-0000-000000000000\GssComponents**
4. Close both instances of Windows Explorer and disconnect your USB thumb drive.

You've moved the Air Gap Update that includes Windows patch content across the air gap. You can now begin deploying it to air gap endpoints.

Appendix

This appendix contains reference information for edge-case scenarios and troubleshooting related to your air gap Endpoint Security installation.

Troubleshooting

There are a few parts during air gap configuration that are prone to trouble. Hopefully this help topic can get you through them :)

Glossary

A

Air Gap

A highly secure computing environment where a network of computers is isolated from other networks, and most often, from the Internet. This practice significantly reduces the attack surface of endpoints within the air gap, and is used most often in industries that handle sensitive information, such as the defense industry.

Air Gap Client

An Endpoint Security Server in an air gap environment that secures the endpoint in your air gapped network. The Air Gap Client is not connected to the Internet. Since the Client has no Internet connection, it relies on the Air Gap Provider to move system updates and content over the air gap.

Air Gap Hotfix

A utility that moves Endpoint Security binaries and modules on to an Air Gap client. This utility copies all the files necessary to complete an air gap install or upgrade, and then the user opens Installation Manager to complete the module installation.

Air Gap License Tool

A utility used to import a license for an Endpoint Security Server operating in an air gap network.

Air Gap Provider

An Endpoint Security Server that's connected to the Internet in an air gap environment. This server downloads Endpoint Security system components and content from the Internet. These components and content is then moved across the air gap to the Air Gap Client, which then uses this content to secure your air gap endpoints.

Air Gap Toolkit

A bundle of software that includes tools, utilities, and scripts needed to configure and maintain an Endpoint Security Server that's disconnected from the Internet.

AirGapScript.sql

A script that disables the replication process on an air gap Endpoint Security Server (also known as an Air Gap Provider). The script prevents the Air Gap Provider from trying to communicate and download content from the cloud.

C

caching

The process of downloading patch content binaries from the Global Subscription Service. You can cache either Windows or Linux content.

Credentials Manager

A utility that connects to different Linux vendors and passes on the credentials that you've purchased from the vendor. When you replicate with the Global Subscription Service or cache Linux content, Endpoint Security passes your credentials to the vendors so that Endpoint Security download Linux patch metadata and binaries.

D

Dependencies.sql

A script that installs Endpoint Security prerequisites on a server that doesn't have Internet access.

G

Global Subscription Service

A cloud server that hosts Endpoint Security system data, patch content, and antivirus content.

I

ImportEndpointManifest.exe

A utility used to enable new versions of the Endpoint Security Agent included in an air gap update. Use this tool after installing or upgrading an air gap Endpoint Security Server (also known as an Air Gap Client).

Ivanti Content Wizard

A utility used to create your own patches for Endpoint Security. This tool lets you add patches and additional files that check for prerequisites. In air gap networks, Ivanti Content Wizard is used to bundle patches and then move them into your air gap network.

R

Replication

The synchronization process between the Endpoint Security Server and the Global Subscription Server. During this process, Endpoint Security downloads the latest Endpoint Security system updates, patch content, and antivirus content. Depending on how much content you are licensed for, initial replication can take as long as an hour. Subsequent replications are much faster.