ivanti

Endpoint Security

powered by HEAT Software

Air Gap AntiVirus Guide

Dec 2020

Contents

Contents 2
Requirements 3
Air Gap Software Requirements 4
Air Gap Checklist 5
AntiVirus Configuration for Air Gap 6
Air Gap AntiVirus Configuration Overview 7
Creating AntiVirus Files and Folders 8
Updating IIS for AntiVirus 12
Updating the AntiVirus Storage Location 18
AntiVirus Air Gap Updates 21
Air Gap AntiVirus Update Overview 22
Replicating With the Global Subscription Service 23
Creating an AntiVirus Air Gap Update 26
Installing an AntiVirus Air Gap Update 27
Glossary 30

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 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.

AntiVirus Configuration for Air Gap

Before you can protect air gap endpoints from viruses, you must make special configurations to your Air Gap Client.

These configurations only need to be completed once. After you make them, you won't need to complete this process again until the next Endpoint Security Air Gap release.

Air Gap AntiVirus Configuration Overview

Before you can use Ivanti AntiVirus in your air gap network, you need to configure a few things on your Air Gap Client. This overview contains a high-level summary of each configuration you'll complete.

All AntiVirus configuration takes place on 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. "Creating AntiVirus Files and Folders" on the next page

   Begin AntiVirus configuration by creating files and folders that will be used to store AntiVirus definitions on your Air Gap Client.

2. "Updating IIS for AntiVirus" on page 12

   Use Internet Information Services (IIS) Manager to create virtual directories of the files and folders you created in the previous procedure. These virtual directories are where your air gap endpoints will access the latest AntiVirus definitions.

3. "Updating the AntiVirus Storage Location" on page 18

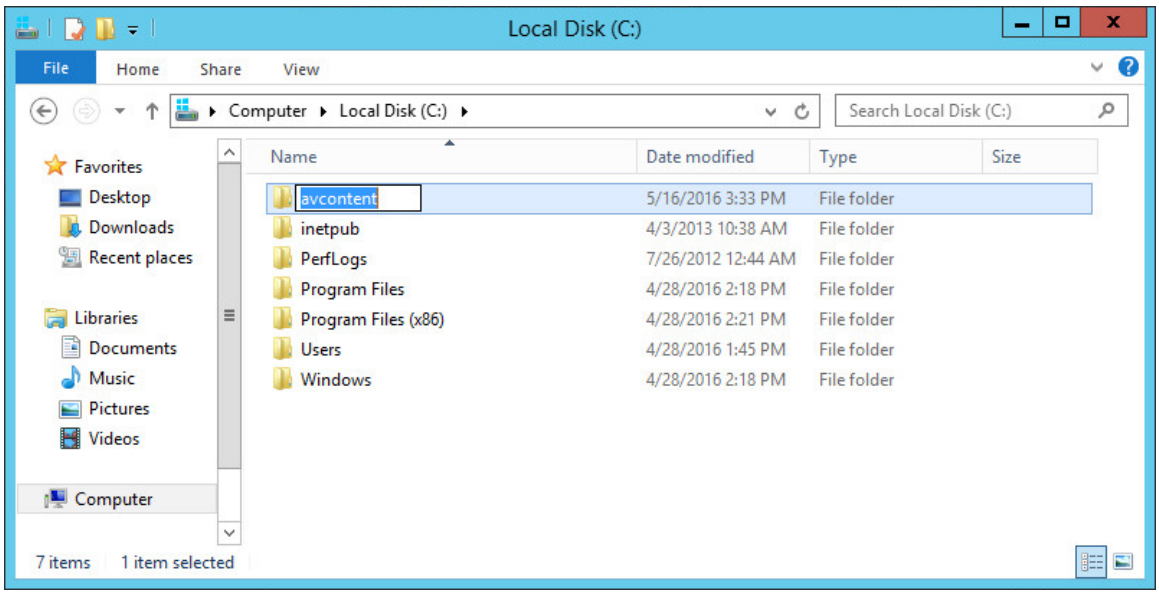
   Use the Endpoint Security Console on the Air Gap Client to direct Endpoint Security to your virtual directories.

Creating AntiVirus Files and Folders

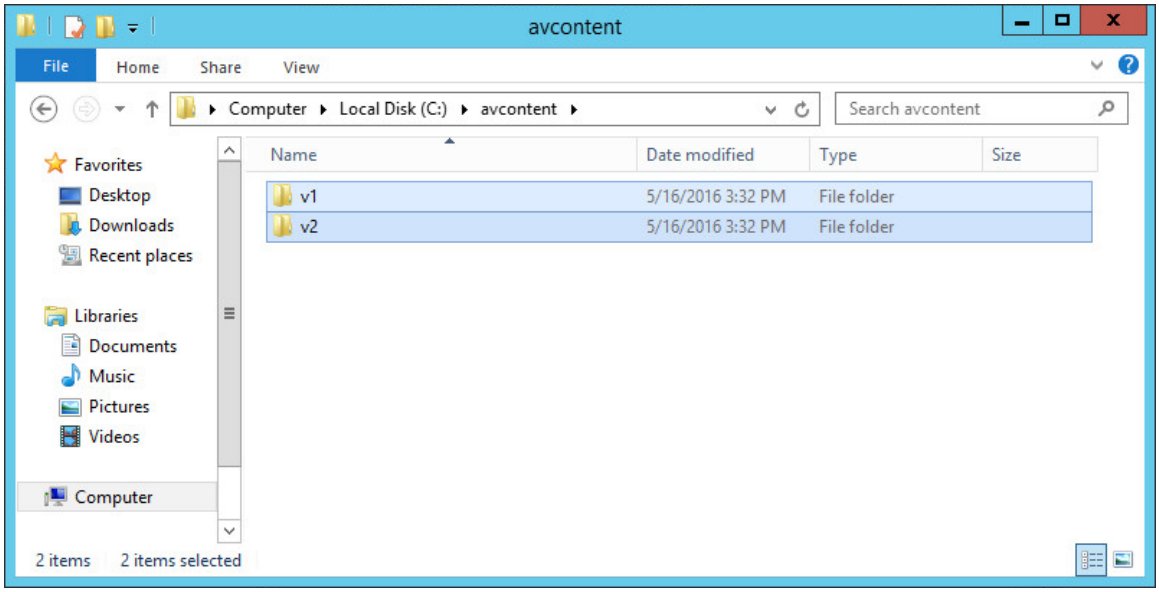
Begin AntiVirus configuration by creating files and folders that will be used to store AntiVirus definitions on your Air Gap Client.

To Create AntiVirus Files and Folders

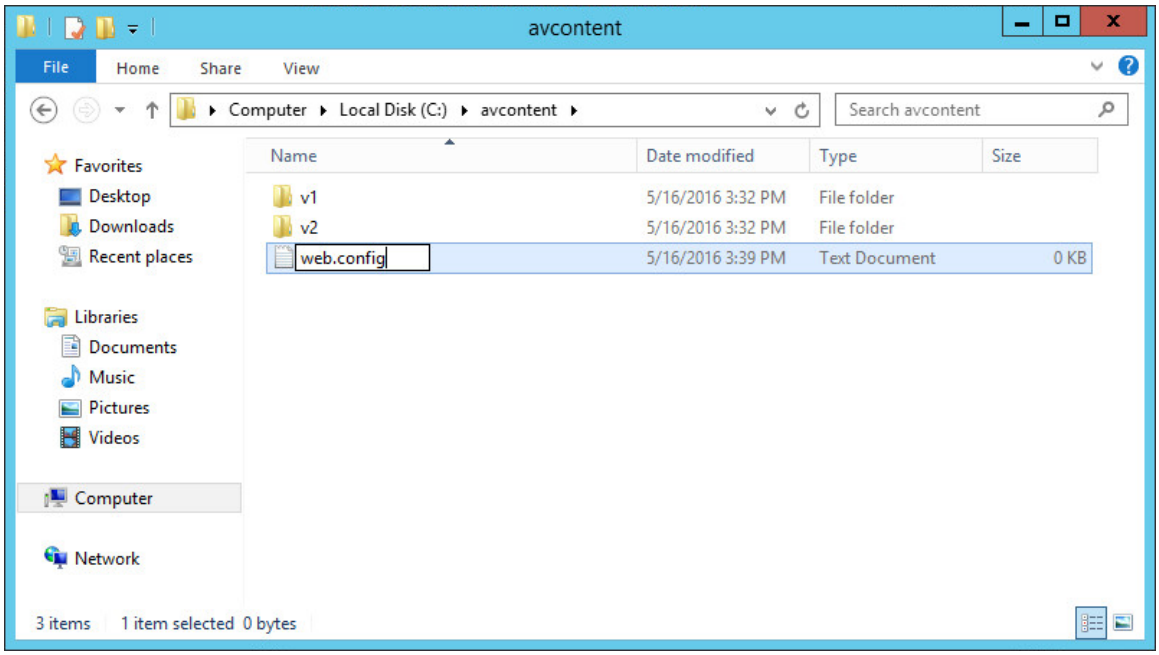
1. Log into the Air Gap Client.
2. From the root of your hard disk, create a folder named **C:\avcontent**.



3. Within the new **avcontent** folder, create the following folders:
   - **v1**
   - **v2**



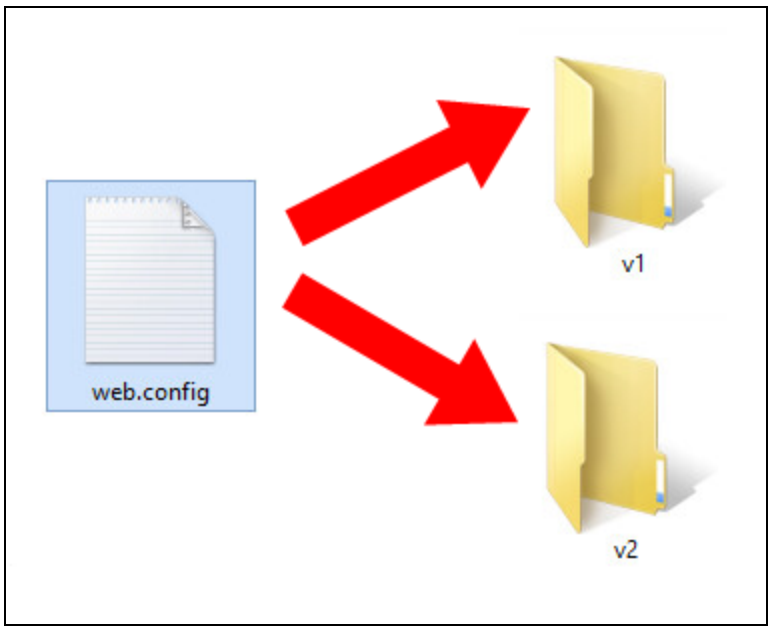
4. From the **avcontent** folder, create a text file named **web.config**.



5. Open **web.config**. Paste the following code sample in the file:

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
        <system.webServer>
                <staticContent>
                        <mimeMap
                                fileExtension=".*"
                                mimeType="application/octet-stream"
                        />
                        <mimeMap
                                fileExtension=".*."
                                mimeType="application/binary"
                        />
                </staticContent>
                <directoryBrowse enabled="true" />
        </system.webServer>
</configuration>
```

6. Save and close the config file.
7. Copy the **web.config** file and paste it in the following folders.
   - **v1**
   - **v2**



8. Close Windows Explorer.

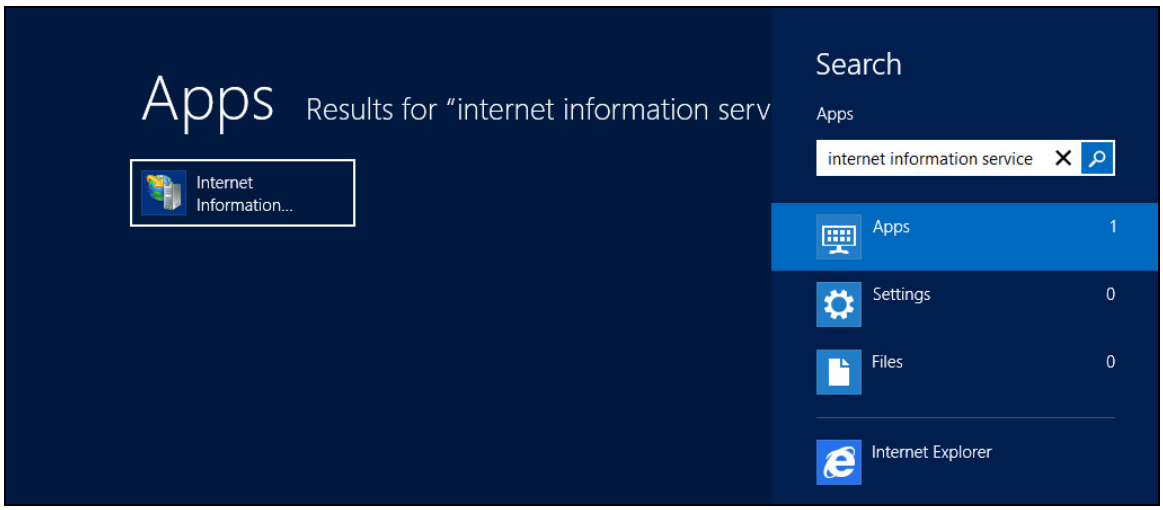
The files and folders required to use AntiVirus in the air gap are created.

Continue to "Updating IIS for AntiVirus" on the next page.

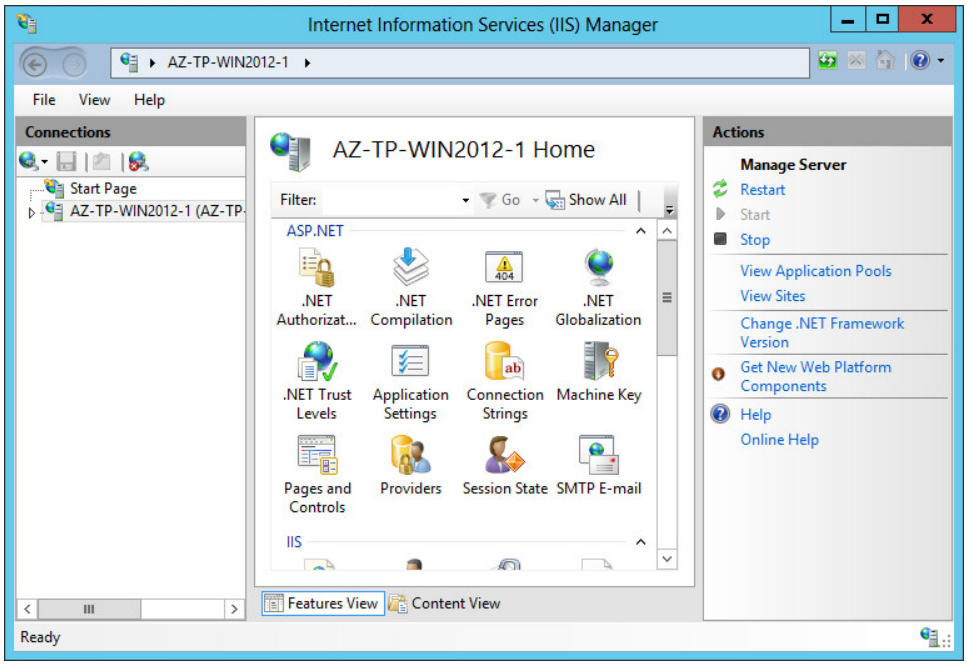
Updating IIS for AntiVirus

Use Internet Information Services (IIS) Manager to create virtual directories of the files and folders you created in the previous procedure. These virtual directories are where your air gap endpoints will access the latest AntiVirus definitions.

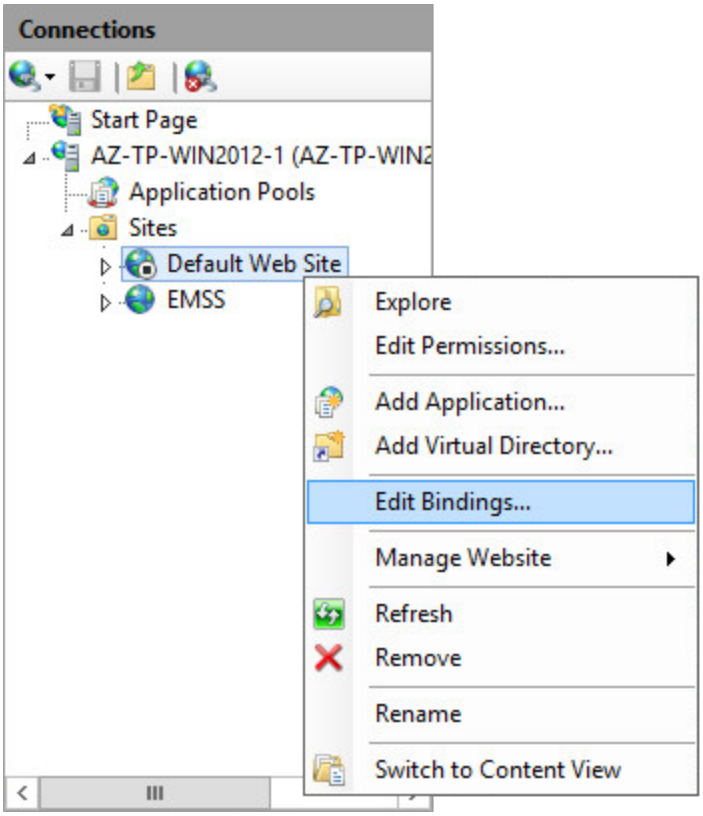
1. From the **Start Page** or **Start Menu**, search for **Internet Information Services**. Open it.



Internet Information Services (IIS) Manager opens.

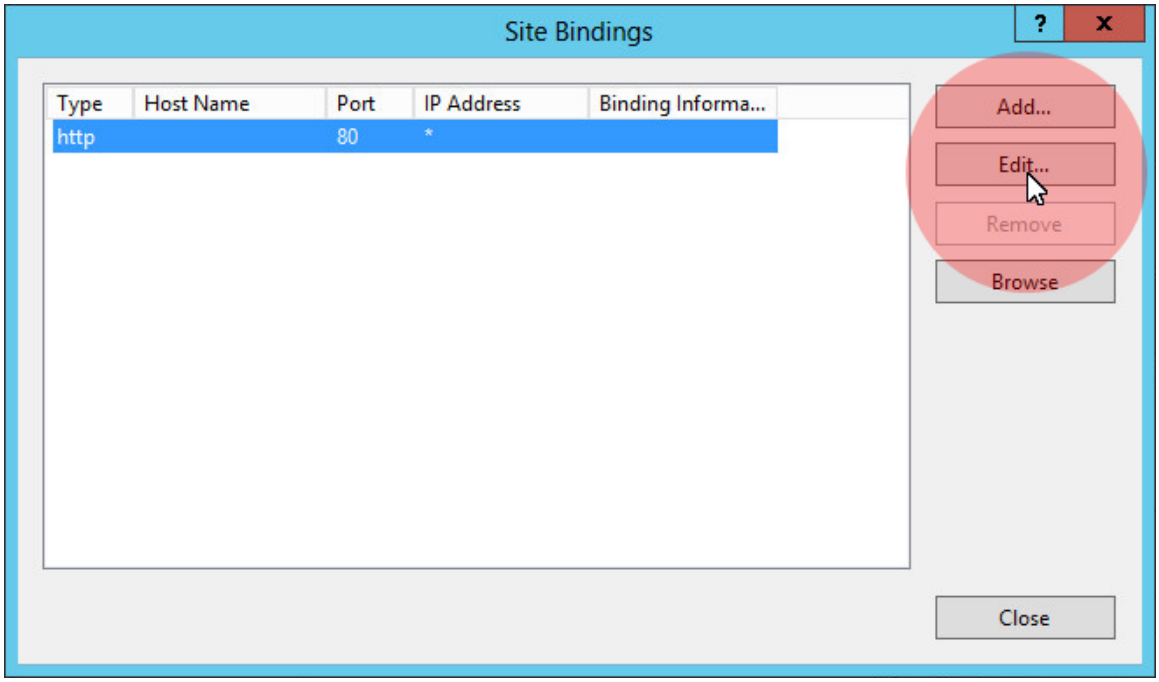


2. In the **Connections** pane, click on your **Air Gap Client machine name** > **Sites** > **Default Web Site**. Right-Click **Default Web Site** and select **Edit Bindings**.

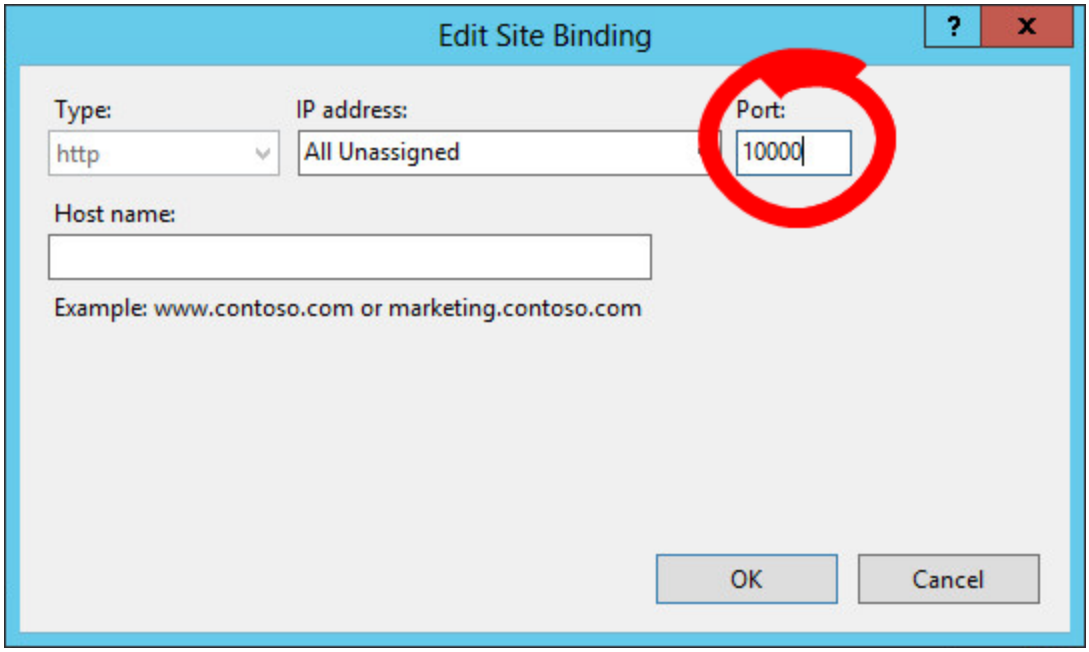


The Site Bindings dialog opens.

3. Select the **http** item from the list and click **Edit**.

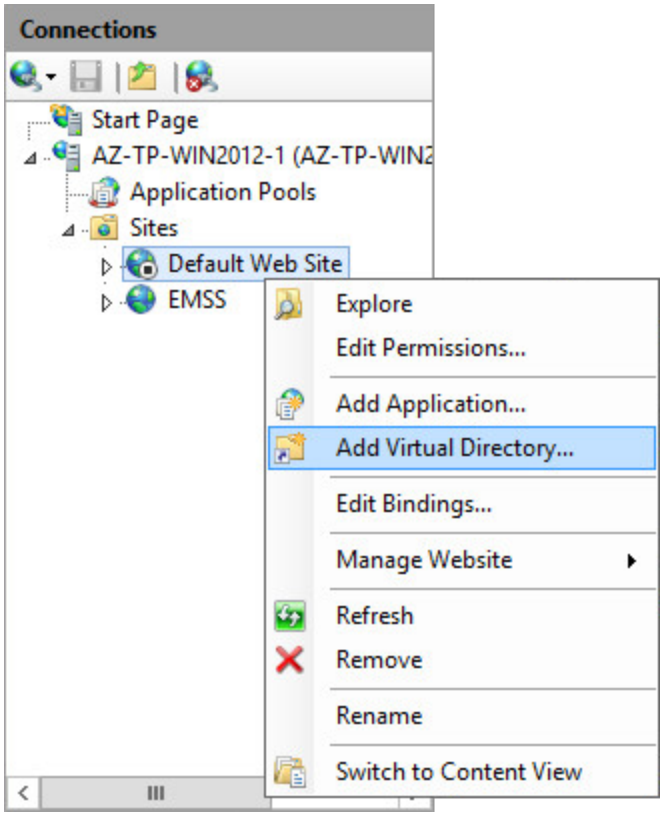


4. Change the Port value to 10000 and click OK.



5. Close the Site Bindings dialog.

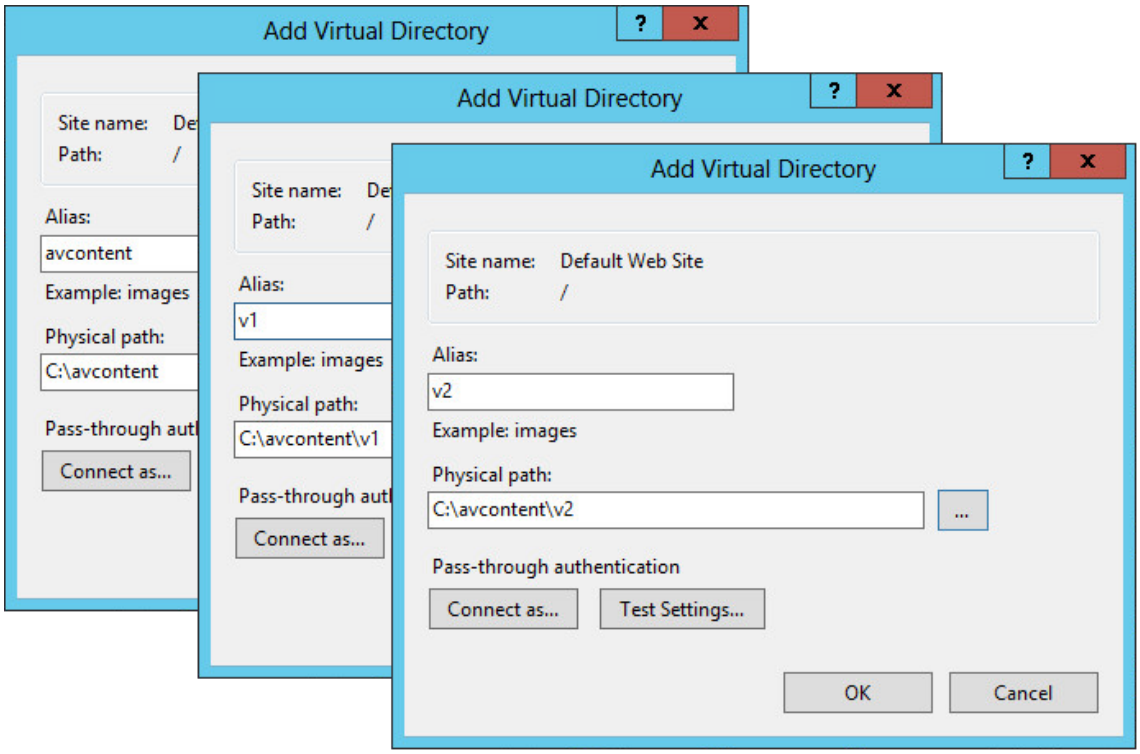
6. From the tree, right-click **Default Web Site** and select **Add Virtual Directory**.



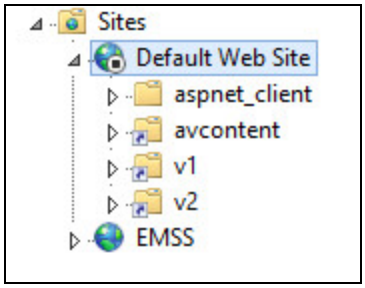
7. Add a virtual directory for each of the folders you created in "Creating AntiVirus Files and Folders" on page 8. Give each virtual directory the same alias as the folder name. Create a virtual directory for each of the following folders:

   - **avcontent**
   - **v1**
   - **v2**

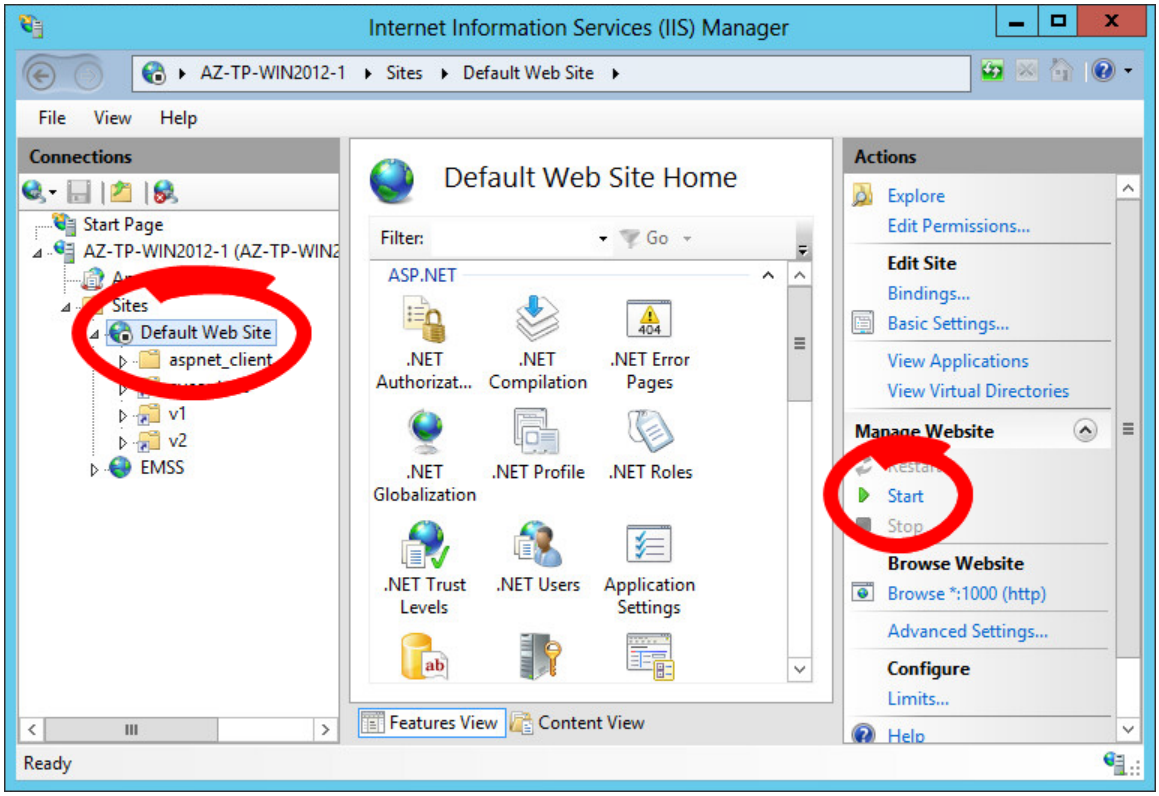
Repeat steps 6 and 7 for each folder.



When you're done, the tree should look like this:



8. Start the Default Web Site. Select **Default Web Site** from the tree and then click **Start**.



You've created the virtual directories that are used to store your AntiVirus definitions.

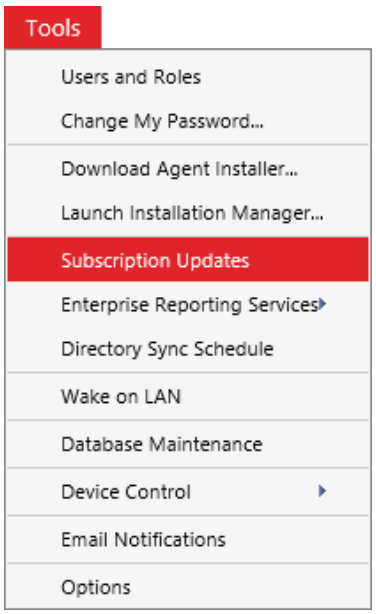
Continue to "Updating the AntiVirus Storage Location" on the next page.

Updating the AntiVirus Storage Location

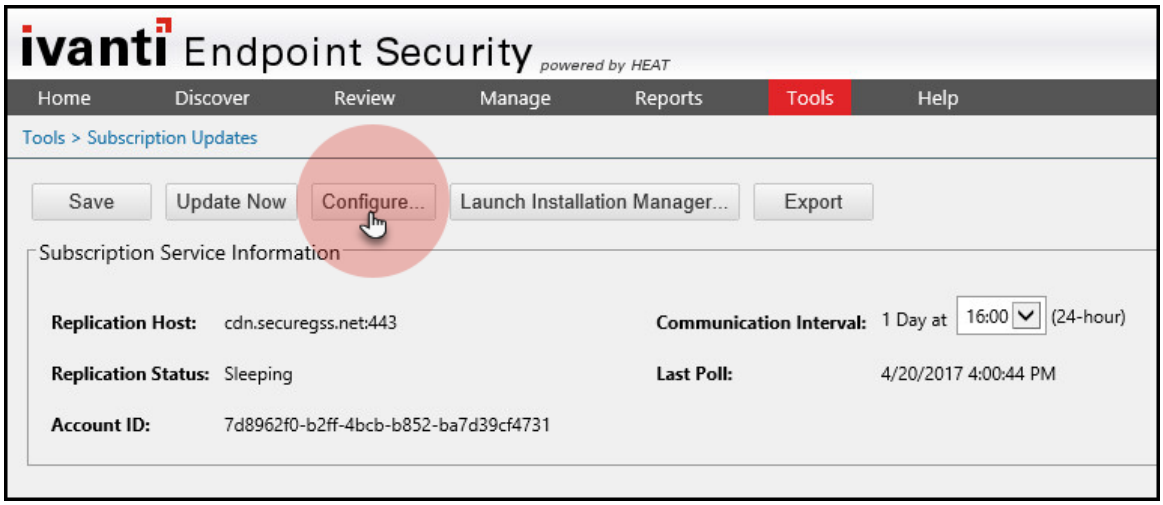
Use the Endpoint Security Console on the Air Gap Client to direct Endpoint Security to your virtual directories.

To Update the AntiVirus Store Location

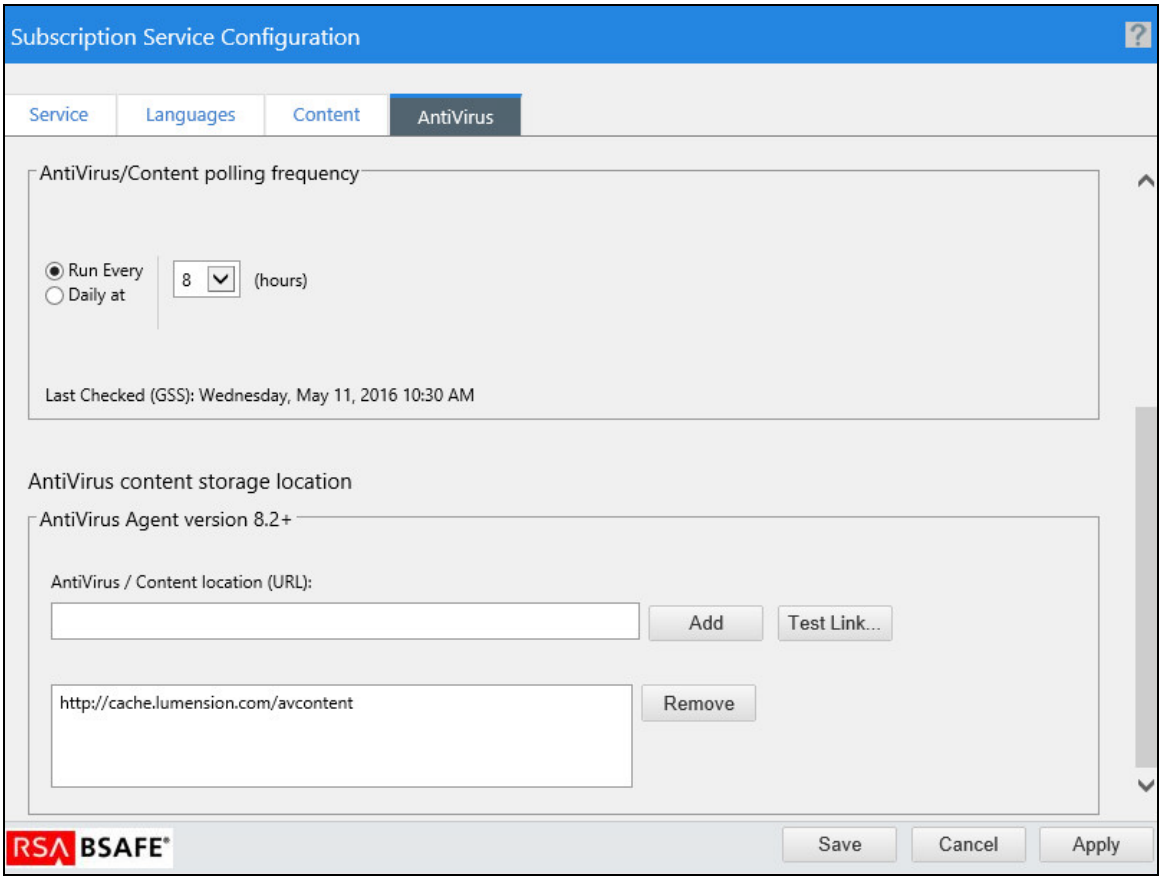
1. Log into the Endpoint Security Console for your Air Gap Client.
2. From the Navigation Menu, select **Tools > Subscription Updates**.



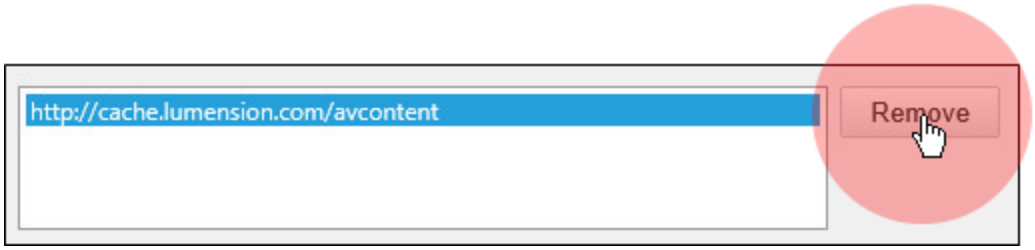
3. Click **Configure**.



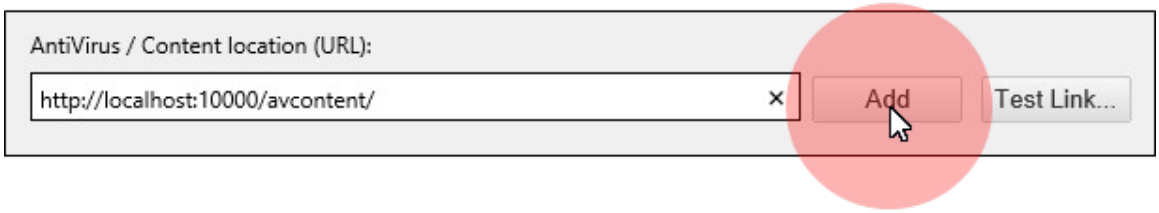
4. Select the **AntiVirus** tab and scroll down to **AntiVirus content storage location.**



5. Remove all URLs listed.



6. Add the following URL as a storage location: **http://localhost:10000/avcontent/**



7. Click **Save** to close the Subscription Updates dialog. Close the Endpoint Security Console.

Your Air Gap Client is configured for AntiVirus. You can begin creating Air Gap Update with AntiVirus content.

Continue to "Air Gap AntiVirus Update Overview" on page 22.

AntiVirus Air Gap Updates

This chapter guides you through the standard Air Gap AntiVirus 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

We recommend making Air Gap Updates that include AntiVirus definitions at least once a week, or when particularly dangerous malware is discovered.

Air Gap AntiVirus Update Overview

The usual air gap AntiVirus workflow consists of creating an Air Gap update from your Provider and then installing it 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.

   Complete this procedure from the Air Gap Provider.

2. "Creating an AntiVirus Air Gap Update" on page 26

   Creating an Air Gap Update for AntiVirus is as simple as copying a few files and folders to a USB thumb drive.

   Complete this procedure from the Air Gap Provider.

3. "Installing an AntiVirus Air Gap Update" on page 27

   Install the AntiVirus Air Gap Update by connecting your USB thumb drive to the Air Gap Client and copying over your AntiVirus definitions.

   Complete this procedure from the Air Gap Client.

Replicating With the Global Subscription Service

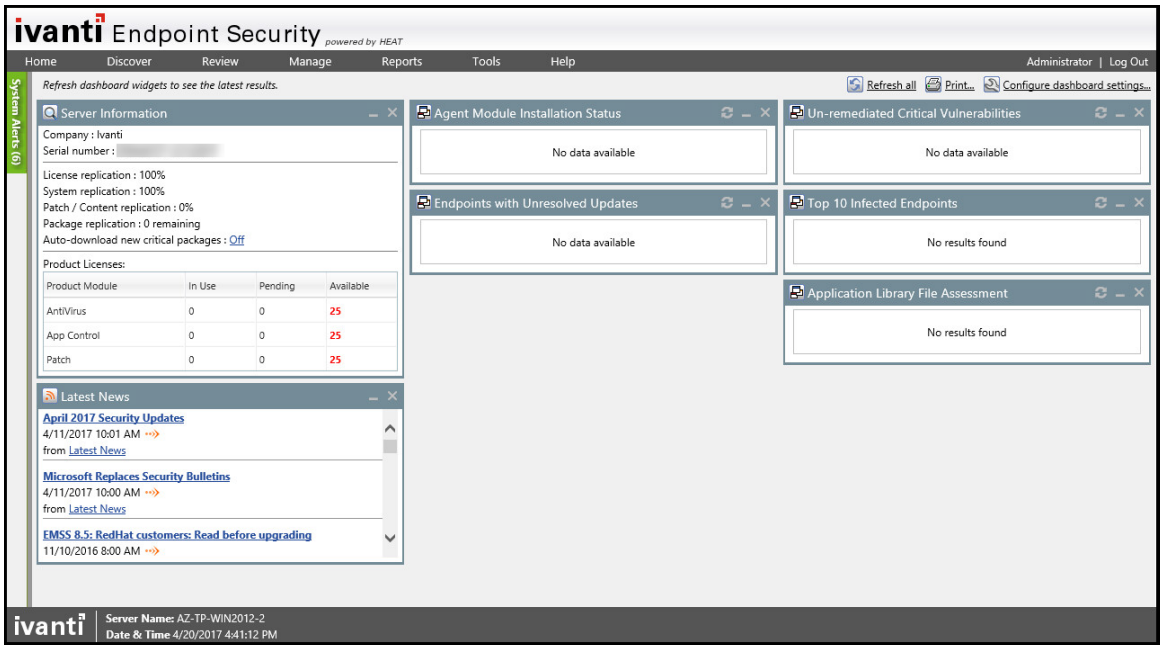
Begin by initiating a replication with the Global Subscription Service (GSS), which is a cloud service for your Endpoint Security Server. You can download the latest:

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

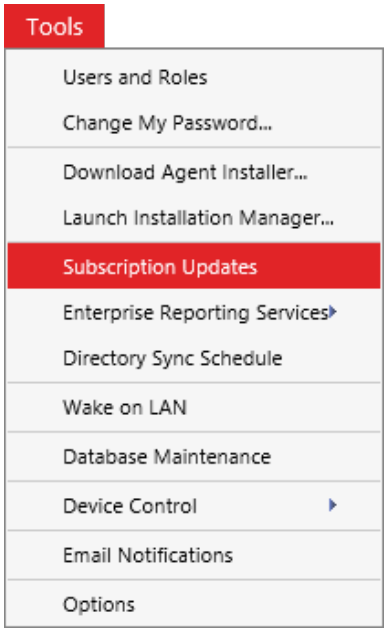
Although this process isn't absolutely required because the Air Gap Provider automatically replicates once daily by default, we recommend replicating before creating an Air Gap Update.

To Replicate With the GSS

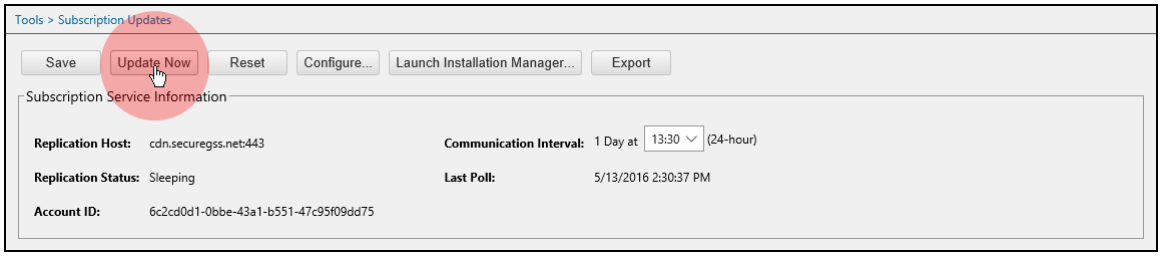
1. From the Air Gap Provider, log into the Endpoint Security Console.



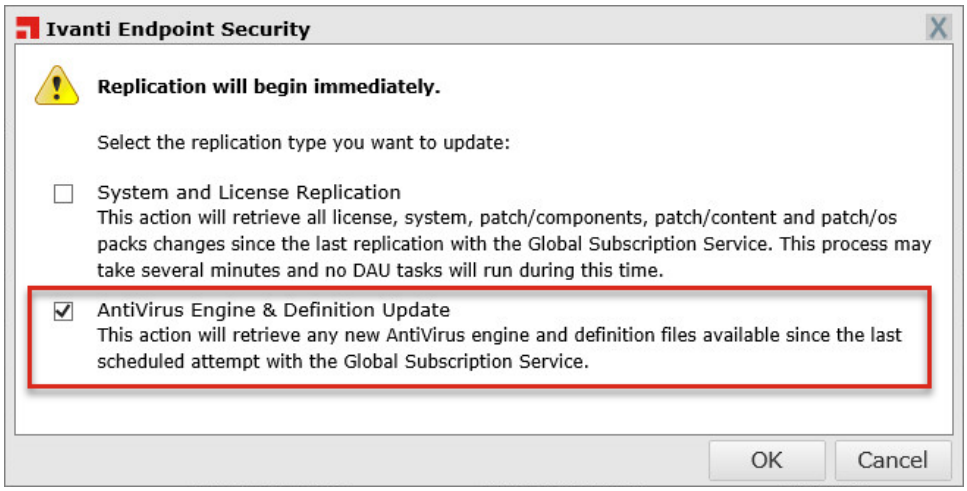
2. From the Navigation Menu, select **Tools > Subscription Updates**.



3. Click **Update Now**.



4. Make sure **AntiVirus Engine & Definition Update** is selected and then click **OK**.



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

AntiVirus / Content (32-bit)	Completed
AntiVirus / Content (64-bit)	Completed

Continue to "Creating an AntiVirus Air Gap Update" on the next page.

Creating an AntiVirus Air Gap Update

Creating an Air Gap Update for AntiVirus is as simple as copying a few files and folders to a USB thumb drive.

Complete this procedure from the Air Gap Provider.

1. Make sure that your USB thumb drive is connected to the Air Gap Provider.
2. Open Windows Explorer and browse to **C:\Program Files (x86)\HEAT Software\EMSS\Content\AntiVirus\Definitions**
3. Open a second instance of Windows Explorer and browse to the USB thumb drive.
4. Copy the following folders from the **Definitions** folder and paste them in your USB thumb drive.
   - **av32bit**
   - **av64bit**
   - **v1**
   - **v2**
   - **av32bit_*HighVersionNumber***
   - **av64bit_*HighVersionNumber***
5. Close Windows Explorer.

The AntiVirus Air Gap Update is created.

Continue to "Installing an AntiVirus Air Gap Update" on the next page.

Installing an AntiVirus Air Gap Update

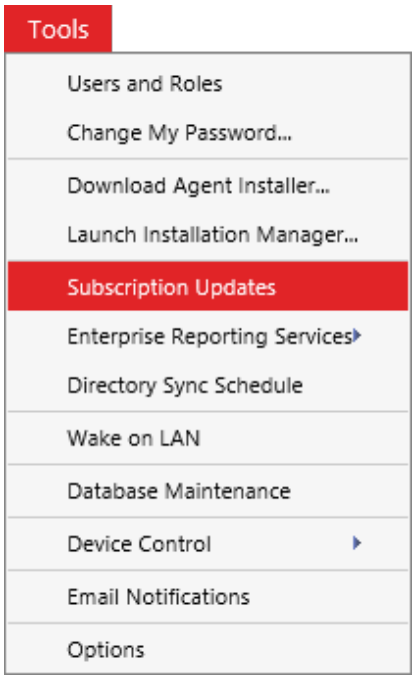
Install the AntiVirus Air Gap Update by connecting your USB thumb drive to the Air Gap Client and copying over your AntiVirus definitions.

Complete this procedure from the Air Gap Client.

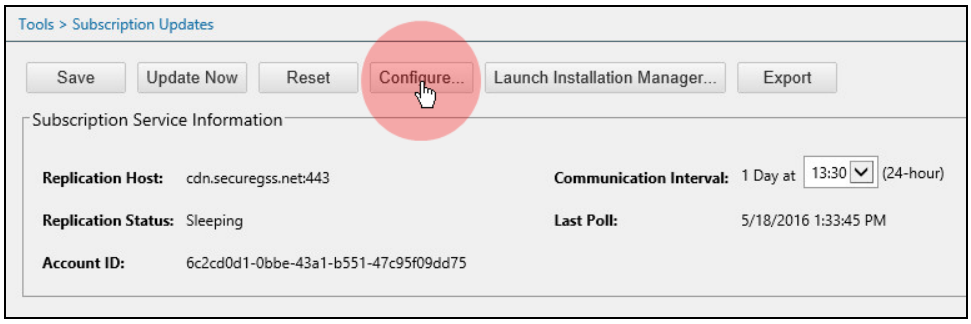
1. Make sure that your USB thumb drive is connected to the Air Gap Client.
2. Open Windows Explorer and browse to your USB thumb drive.
3. Open a second instance of Windows Explorer and browse to **C:\avcontent**.
4. Copy the following folders to **C:\avcontent**.
    - **av32bit**
    - **av64bit**
    - **v1**
    - **v2**
    - **av32bit_*HighVersionNumber***
    - **av64bit_*HighVersionNumber***
5. Close Windows Explorer.

6. Confirm that the latest AntiVirus definitions are installed.

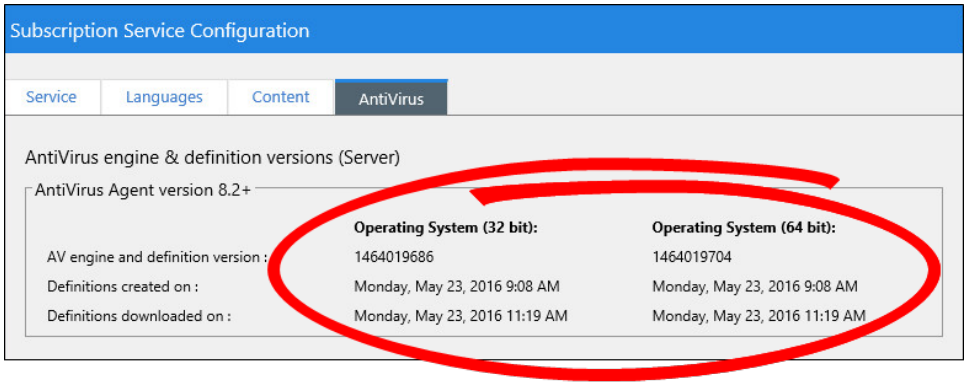
   a. Navigate to **Tools > Subscription Updates**.



   b. Click **Configure**.



c. Select the **AntiVirus** tab. Verify that **AntiVirus engine and definition versions** are updated.



The latest AntiVirus definitions are installed on your Air Gap Client. You can now install them on your air gap endpoints.

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 bundles 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.