ivanti

Endpoint Security

powered by HEAT Software

Air Gap Upgrade Guide

Dec 2020

Contents

Contents 2
Requirements 3
Upgradable Server Versions 4
Supported Server Operating Systems 5
Supported Database Servers 7
Supported Web Browsers 8
Air Gap Software Requirements 9
Air Gap Checklist 10
Air Gap Upgrade 11
Upgrade Overview 12
Upgrading the Air Gap Provider 13
To Upgrade the Air Gap Provider 13
Importing an Air Gap License File 17
To Import an Air Gap License File 17
Upgrading the Air Gap Client 20
Configuring the Air Gap Client 25
To Configure the Air Gap Client 25
Activating the Endpoint Security Agent Installers 29
To Activate The Endpoint Security Agent Installers 29
Glossary 31

Requirements

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

Upgradable Server Versions

Air Gap can only be upgraded if you are running a currently supported version of Endpoint Security.

Additionally, you can only upgrade Endpoint Security if it is installed on:

- "Supported Server Operating Systems" on the next page
- "Supported Database Servers" on page 7

Supported Server Operating Systems

You can install the Ivanti Endpoint Security application server (Endpoint Security) on any of the following operating systems.

New installations of the Endpoint Security Server are only supported on 64-bit operating systems.

- Windows Server 2019
  - Standard
  - Datacenter
- Windows Server 2016
  - Standard
  - Datacenter
- Windows Server 2012 R2[1]
  - Datacenter[2]
  - Foundation
  - Standard[2]
- Windows Server 2012 R2[1]
  - Datacenter[3]
  - Foundation
  - Standard[2]
- Windows Server 2012[1]
  - Datacenter[2]
  - Foundation
  - Standard[2]

---

[1]Initial installation of Endpoint Security on this family of operating systems when Core mode is enabled is not supported; a GUI is required. However, following installation, general operation of Endpoint Security while Core mode is enabled is supported. For more information on enabling and disabling Core mode on Windows 2012 and 2012 R2 servers, see KnowledgeBase Article 1642 (http:// www.lumension.com/kb/1642).
[2]The Hyper-V edition of this operating system edition is supported, however, the Microsoft Hyper-V Server 2012 stand-alone edition is not.
[3]The Hyper-V edition of this operating system edition is supported, however, the Microsoft Hyper-V Server 2012 stand-alone edition is not.

Blank Page

Supported Database Servers

Ivanti Endpoint Security requires an instance of Microsoft SQL Server to store its data. You can either install this database server on the same server as your Endpoint Security application, or your can install the database on a server that's remote from Endpoint Security.

- SQL Server 2019 (64- and 32-bit)
  - Enterprise
  - Express
  - Standard
- SQL Server 2017 (64- and 32-bit)
  - Enterprise
  - Express
  - Standard
- SQL Server 2016 (64- and 32-bit)
  - Enterprise
  - Express
  - Standard
- SQL Server 2014 and later (64- and 32-bit)
  - Business Intelligence
  - Enterprise
  - Express
  - Standard
- SQL Server 2012 and later (64- and 32-bit)
  - Enterprise
  - Express
  - Standard

Ivanti recommends:

- using the latest service pack available for your SQL Server install
- using a 64-bit database

Supported Web Browsers

Following The Ivanti Endpoint Security Server installation, you can view the Endpoint Security Console in one of the following web browsers:

- Google Chrome 53 and higher
- Microsoft Edge EdgeHTML 14 and higher

  Google Chrome and Microsoft Edge are currently incompatible with the following Endpoint Security features:

  - Patch and Remediation Patch Package Editor
  - Device Control Media Hasher
  - Ivanti Installation Manager

- Microsoft Internet Explorer 9 and higher
- Mozilla Firefox Extended Support Release 31 and higher

There are a couple caveats related to web browsers:

- Microsoft Silverlight 5.1.30214.0 is also required to use Ivanti Installation Manager.
- Due to the accelerated release cycle of Mozilla Firefox Rapid Release, support cannot be guaranteed.

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

- An existing Air Gap Provider (an Endpoint Security Server that's connected to the Internet).
- One or more existing Air Gap Clients (an Endpoint Security Server that's disconnected from the Internet).
- 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.

Air Gap Upgrade

Upgrading your Endpoint Security Servers for an air gap setup is a much simpler process than initial installation. Follow the procedures in this chapter, and you'll have your Air Gap Provider and Air Gap Client upgraded quickly.

Upgrade Overview

Upgrading Endpoint Security in an air gap environment is a multi-stage process. It involves upgrading Endpoint Security on multiple servers, and then running utilities that complete the upgrade process.

Review this list to form a basic understanding of each procedure that you'll perform. It will give you a high-level overview of the upgrade process.

Before you start, review the "Air Gap Checklist" on page 10. Make sure you have all the materials you'll need.

1. "Upgrading the Air Gap Provider" on the next page

   Upgrade your Air Gap Provider by opening Installation Manager and completing an upgrade to the latest version of Endpoint Security.

2. "Exporting an Air Gap License File" on page 1

   You only have to complete this procedure if you've renewed your product licensing. If your license isn't near its expiration date, skip this procedure and continue to "Upgrading the Air Gap Client" on page 20.

   Use the License Tool included in the Air Gap Toolkit to export your Endpoint Security security license from your Provider. When setting up your Client later, you'll need this license.

3. "Importing an Air Gap License File" on page 17

   If your Air Gap Client license data hasn't been updated recently and is near expiration, re-import an air gap license file from Ivanti to your Air Gap Client.

4. "Upgrading the Air Gap Client" on page 20

   Run the Air Gap Hotfix on your Client. This utility places all the Endpoint Security system components necessary to complete the Client upgrade. Then, use Installation Manager to complete the upgrade.

5. "Configuring the Air Gap Client" on page 25

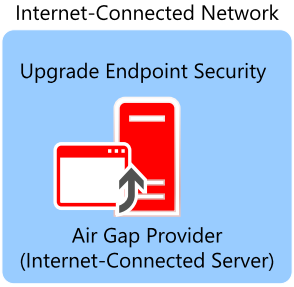
   Each time you upgrade your Air Gap Client, you need to re-run the scripts included in the Air Gap Toolkit.

6. "Activating the Endpoint Security Agent Installers" on page 29

   Because (once again) your Air Gap Client can't access the Internet, the Client cannot download an agent manifest, which is a file that lists the different versions of the Endpoint Security Agent authorized to connect to the Air Gap Client. Use our utility to import the Endpoint Security Agent Manifest on your Air Gap Client.

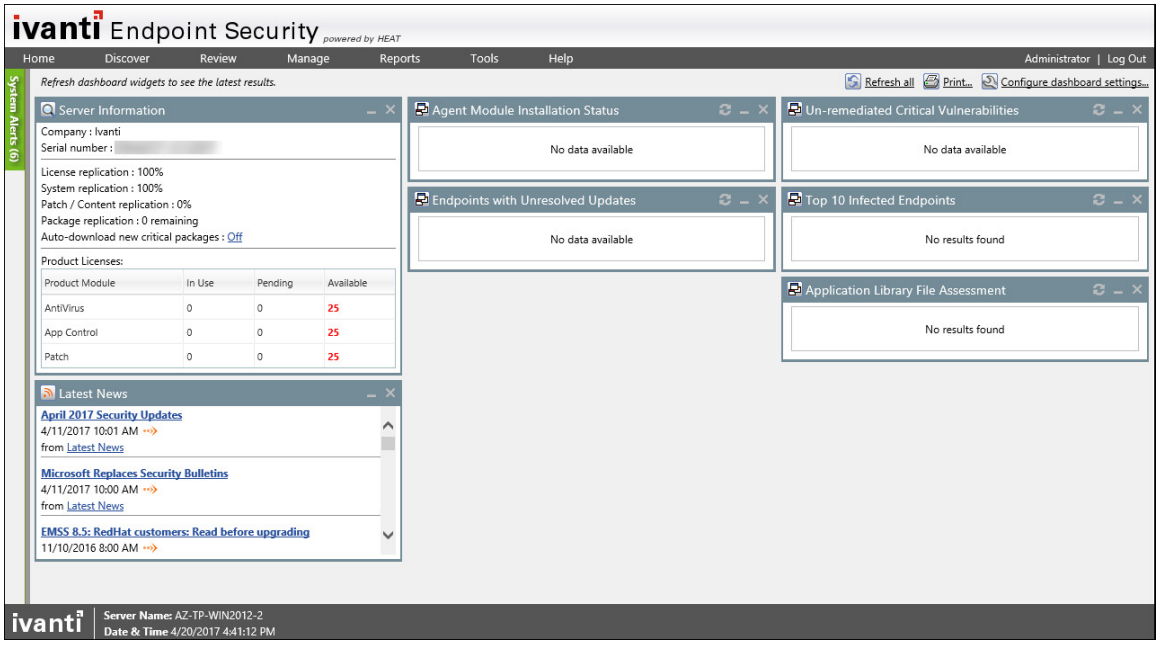
Upgrading the Air Gap Provider

Upgrade your Air Gap Provider by opening Installation Manager and completing an upgrade to the latest version of Endpoint Security.

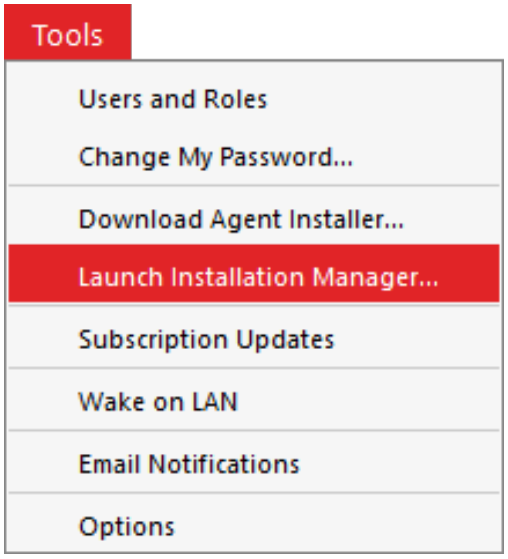


To Upgrade the Air Gap Provider

1. Log in to the Endpoint Security Console for your Air Gap Provider.



2. From the **Navigation Menu**, select **Tools** > **Launch Installation Manager**.

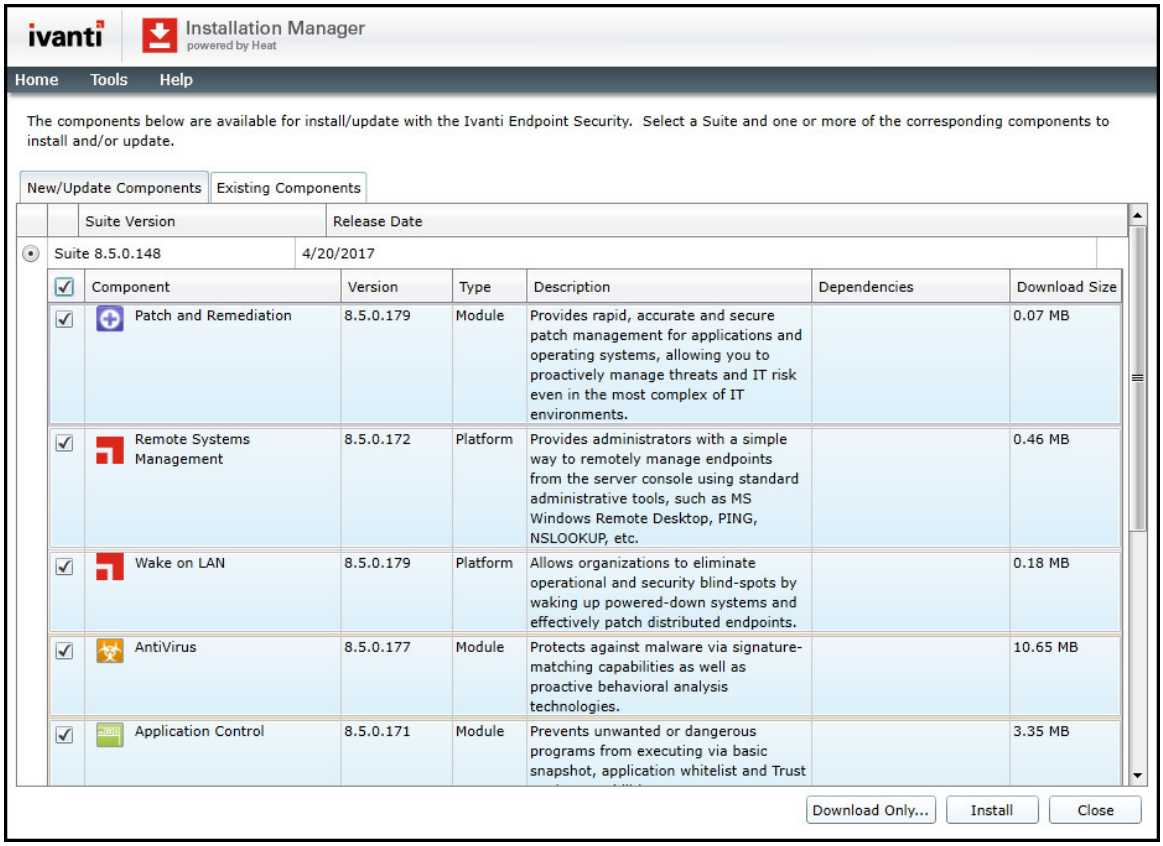


3. Complete Installation Manager's self update.

   Installation Manager requires a reboot and a few other actions to update itself. Complete the reboot as prompted, and then log back into Endpoint Security and Installation Manager after the reboot completes. Then finish the installation by clicking through the prompts.

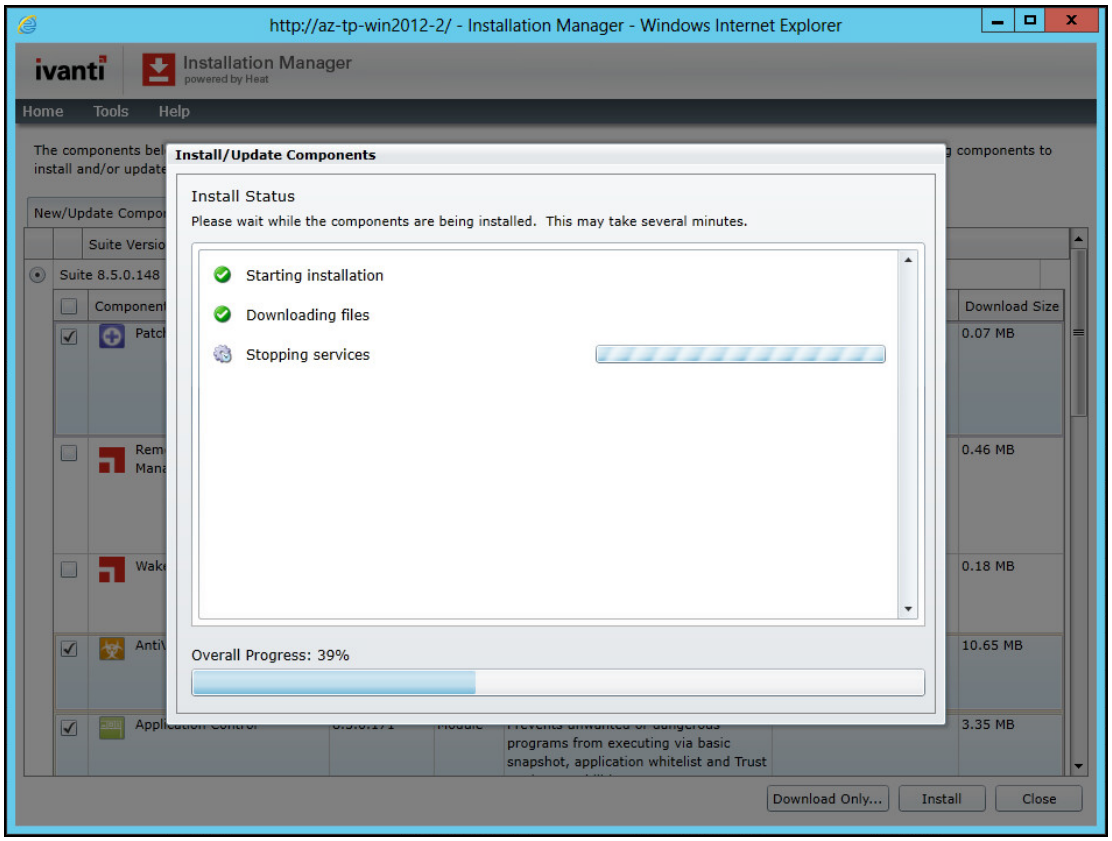
   Having problems here? See Troubleshooting.

4. Upgrade to Endpoint Security latest version. Make the following selections:
    - Select the latest **Suite Version** available
    - Select any additional modules you want to use in your Air Gap network.



5. After you're done making selections, click **Install** to begin the upgrade. Click through any additional prompts that Installation Manager displays (you may need to reboot one more time—if so, log back into Installation Manager when the reboot completes).

Don't ignore the database backup warnings :)



6. After the upgrade completes, close Installation Manager and the Endpoint Security Console.

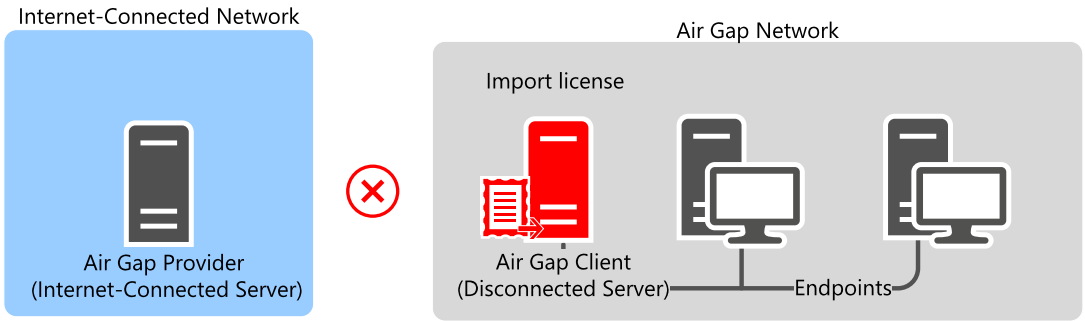
Your Air Gap Provider is upgraded.

Proceed to "Importing an Air Gap License File" on the next page to your Air Gap Client.

Importing an Air Gap License File

You only have to complete this procedure if you've renewed your product licensing. If your license isn't near its expiration date, skip this procedure and continue to "Upgrading the Air Gap Client" on page 20.

If your Air Gap Client license data hasn't been updated recently and is near expiration, re-import an air gap license file from Ivanti to your Air Gap Client.

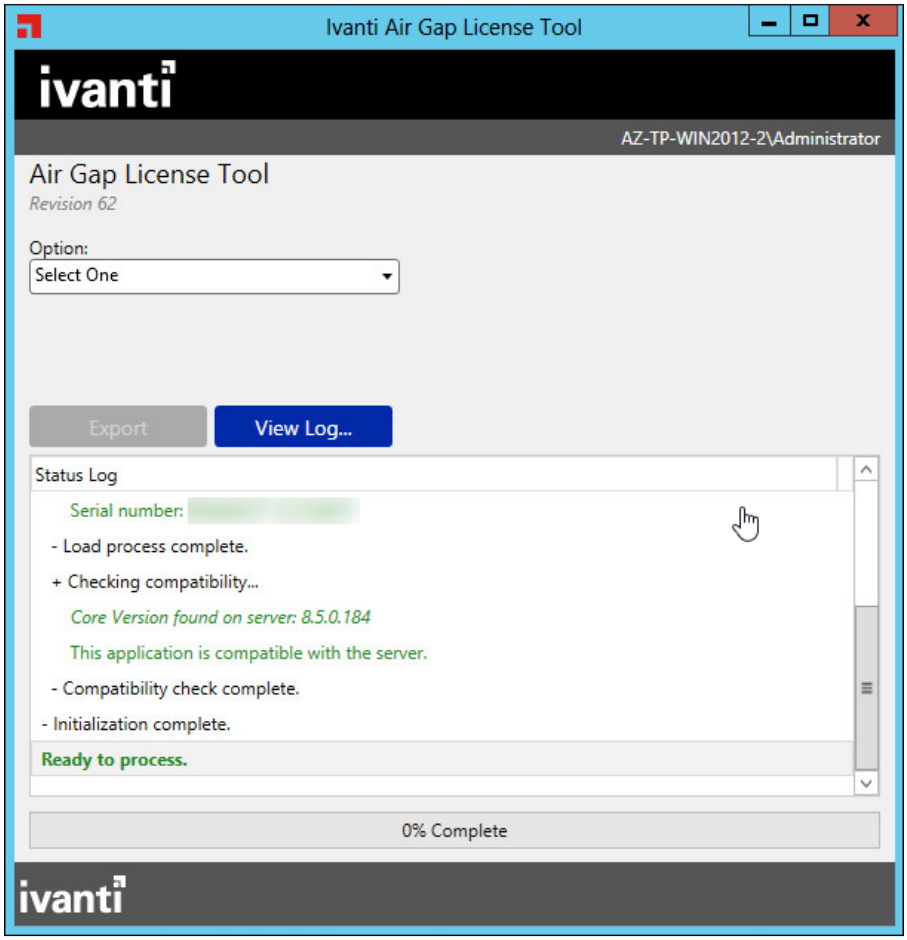


To Import an Air Gap License File

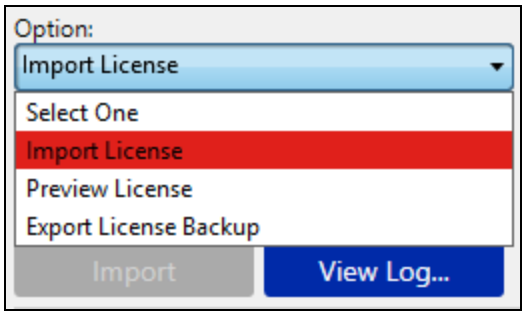
1. On your Air Gap Client, connect the USB thumb drive and browse to it. Navigate to **Ivanti AirGap Toolkit 8.5.0.40\Software**.

2. **Double-click** the Air Gap License Tool (**AirGapLicenseToolUI.exe**).

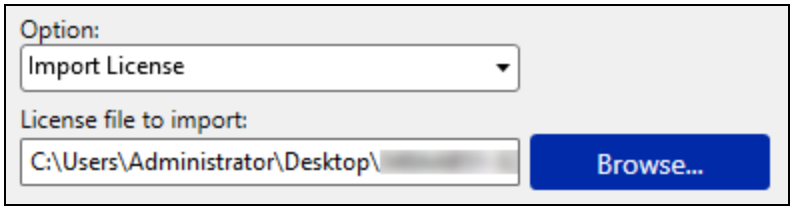
   The Air Gap License Tool opens.



3. From the **Option** drop-down, select **Import License**.

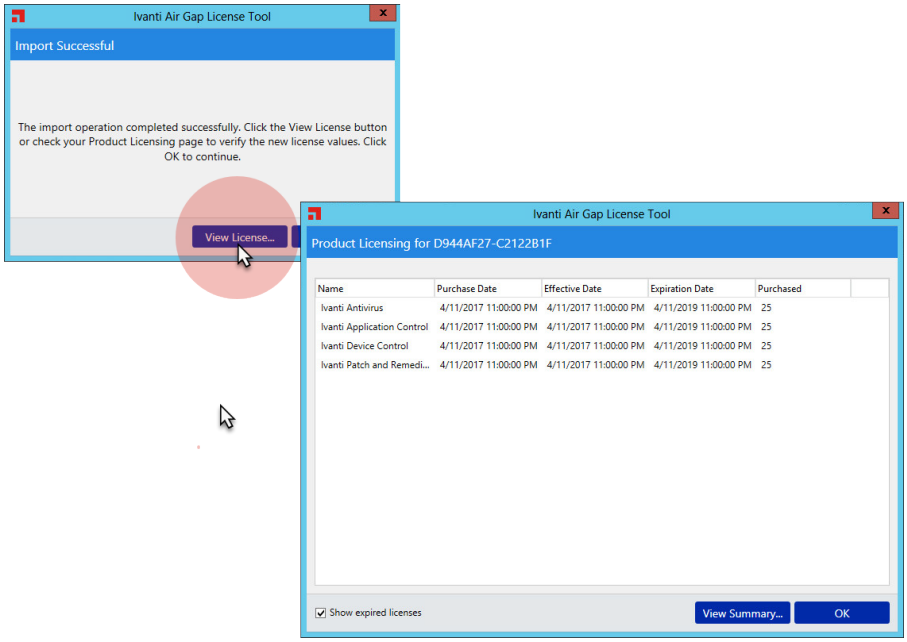


4. Click the **Browse** button and navigate to license file on your USB thumb drive.



5. Click **Import**. Then click **Yes** to proceed with the import.

   After the import completes, click **View Licenses** to see the outcome.



   - Click a product name to display the **Total Purchased (non-expired)** licenses.
   - Expired licenses display as italicized text.
   - Toggle the **Show expired licenses** option to hide or display expired licenses.

6. Click **OK**.

   Before closing the Air Gap License Tool, we recommend selecting **Export** from the **Option** drop-down to create a backup license file.

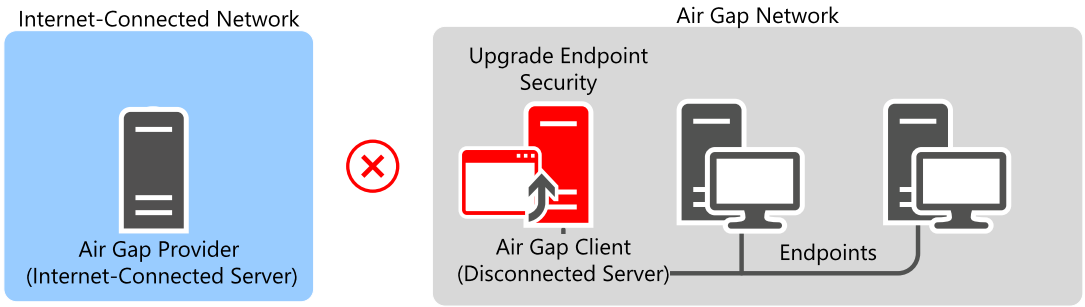
7. Close the Air Gap License Tool.

Your Air Gap Client is updated with licenses. We recommend opening the Endpoint Security Console and selecting **Help > Product Licensing** to verify that your license is correct.

Proceed to "Upgrading the Air Gap Client" on the next page.

Upgrading the Air Gap Client

Run the Air Gap Hotfix on your Client. This utility places all the Endpoint Security system components necessary to complete the Client upgrade. Then, use Installation Manager to complete the upgrade.

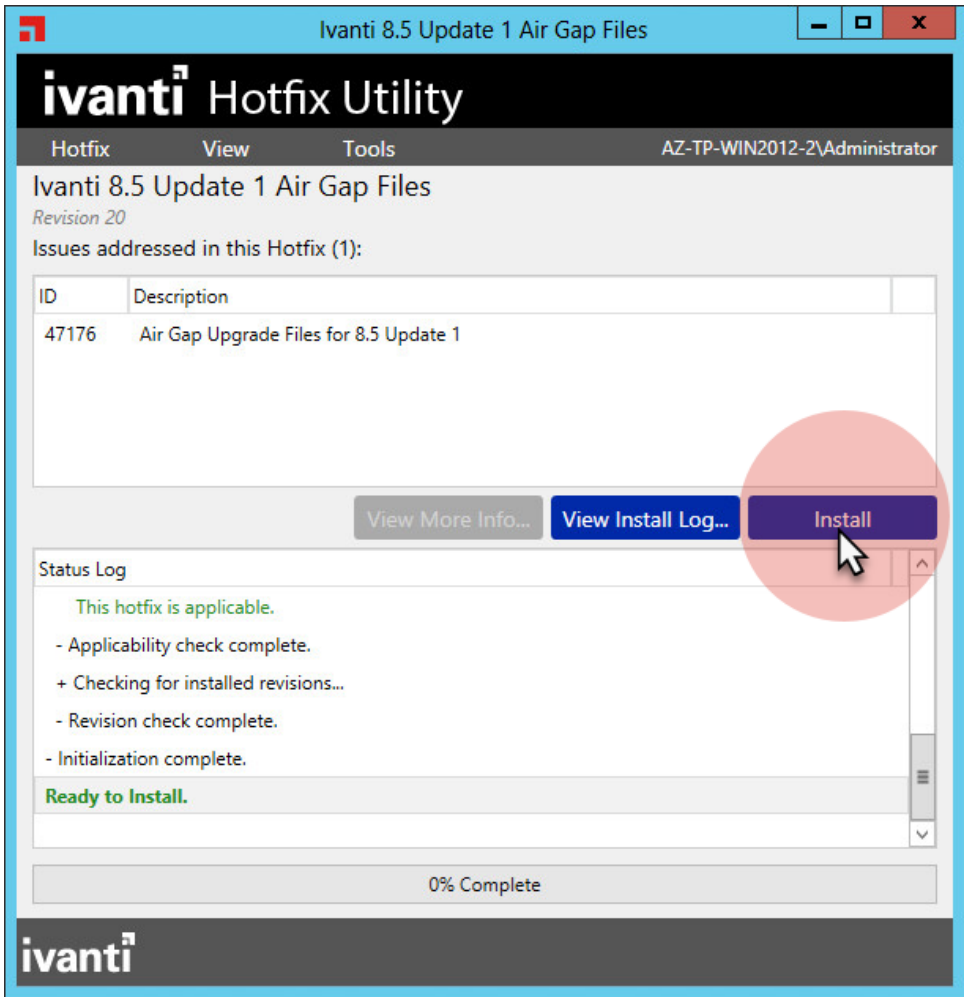


Are you upgrading from Endpoint Security version 8.0? Complete Installing Microsoft Silverlight before you begin this procedure.

1. From your Air Gap Client, browse to your USB thumb drive. Navigate to **HEAT AirGap Toolkit 8.5.0.40\Tools\Pre-Reqs**.
2. Open **8.5 U3 Air Gap Hotfix.exe**.

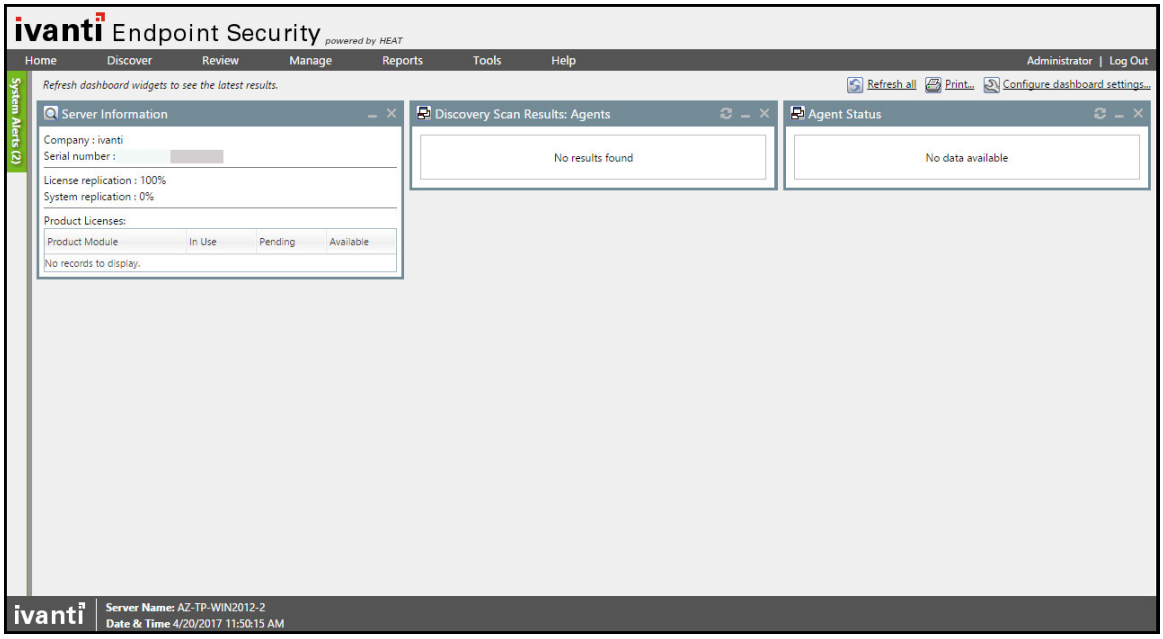
3. Click **Install** to begin.

   The Hotfix takes a couple minutes to complete.

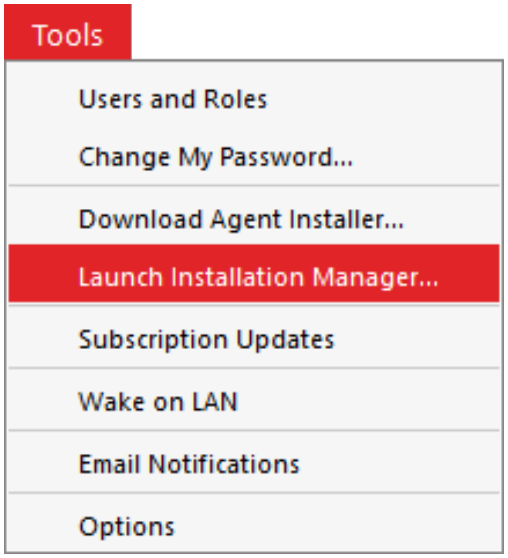


4. After the Hotfix finishes, click **Finish**.

5. Log into the Endpoint Security Console.



6. From the **Navigation Menu**, select **Tools > Launch Installation Manager**.



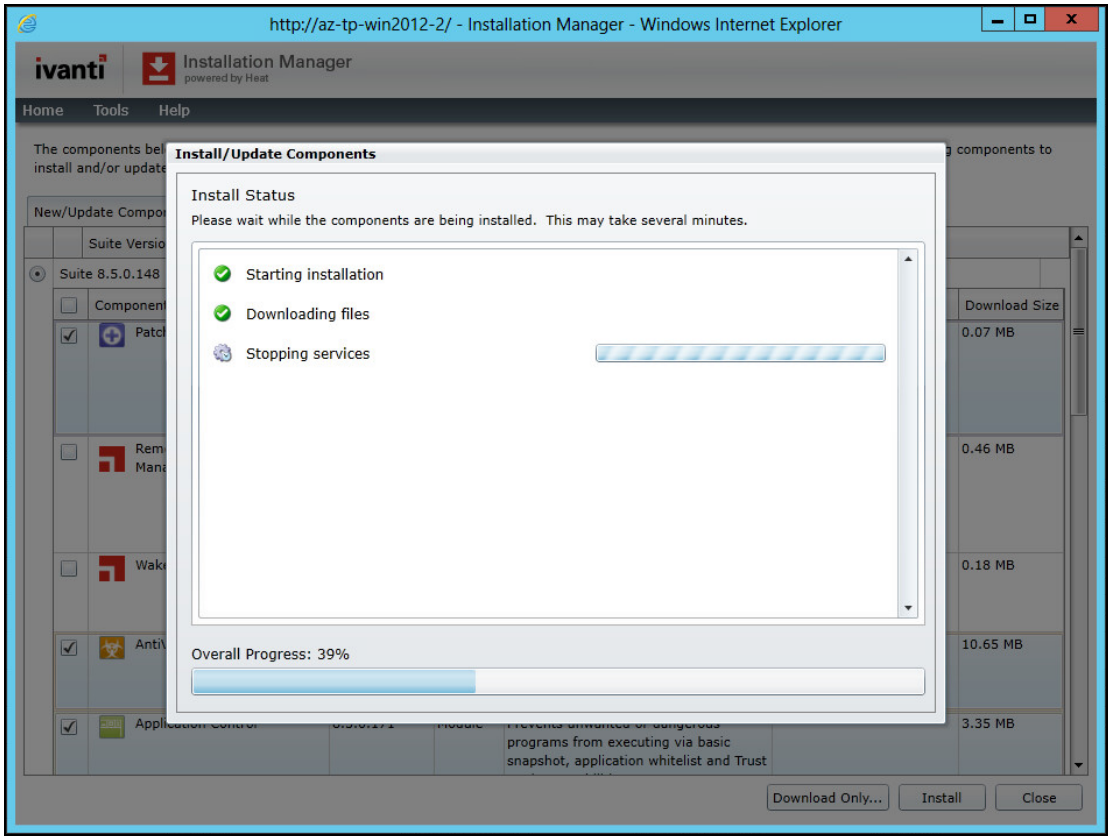
7. Complete Installation Manager's self update.

   Installation Manager requires a reboot and a few other actions to update itself. Complete the reboot as prompted, and then log back into Endpoint Security and Installation Manager after the reboot completes. Then finish the installation by clicking through the prompts.

   Having problems here? See Troubleshooting.

8. Upgrade to the latest version of Endpoint Security. Make the following selections:
   - Select the latest **Suite Version** available.
   - Select any additional modules you want to use in your Air Gap network.
9. After you're done making selections, click **Install** to begin the upgrade. Click through any additional prompts that Installation Manager displays (you may need to reboot one more time—if so, log back into Installation Manager when the reboot completes).

   Don't ignore the database backup warning :)



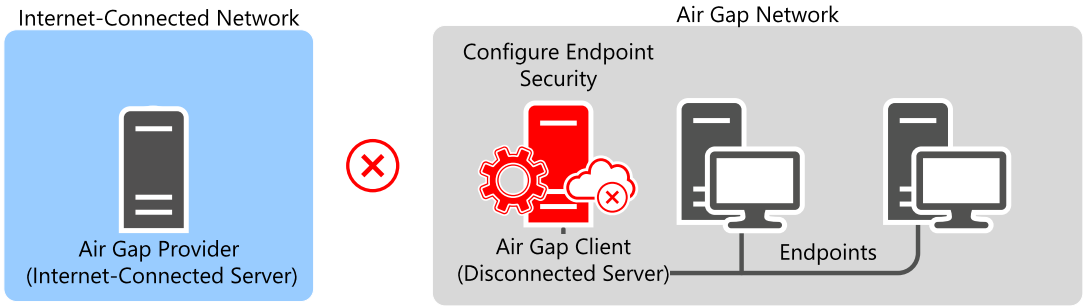
10. After the upgrade completes, close Installation Manager and the Endpoint Security Console.

Your Air Gap Client is upgraded.

Proceed to "Configuring the Air Gap Client" on the next page.

Configuring the Air Gap Client

Each time you upgrade your Air Gap Client, you need to re-run the scripts included in the Air Gap Toolkit.



You can configure the Air Gap Client to be aware of the air gap environment by running scripts that are included in the Toolkit. These scripts deactivate replication and prepare the client to handle Endpoint Security patch content.

To Configure the Air Gap Client

1. From your Air Gap Client, browse to USB thumb drive containing the Air Gap Toolkit. Navigate to **Ivanti AirGap Toolkit 8.5.0.40\Tools\SQL**.

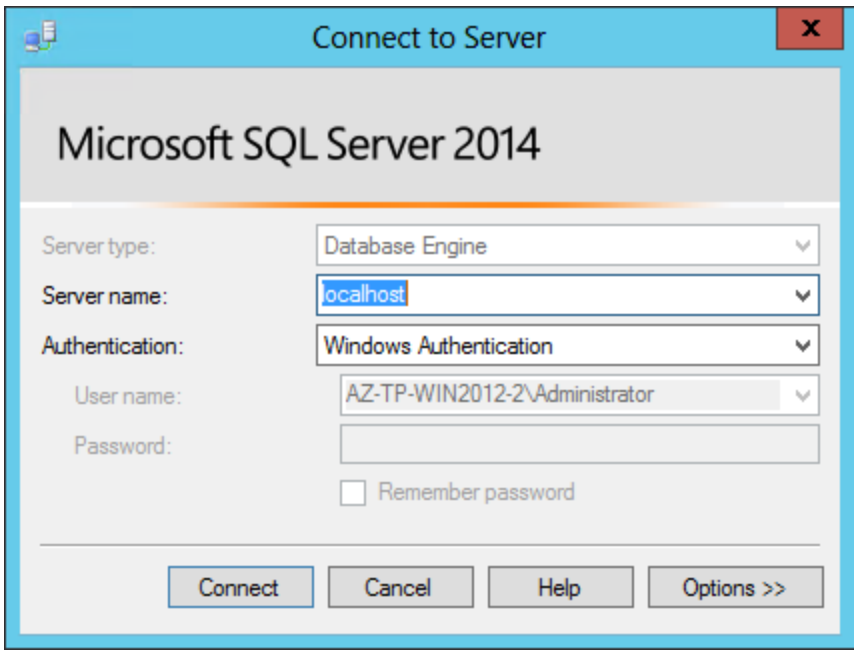
2. Run the following two scripts using SQL Server Management Studio:
   - AirGapScript.sql
   - Dependencies.sql

> Don't have SQL Server Management Studio installed? You can run the scripts without it. See "Configuring the Client from the Command Prompt" on page 1.

Use the following substeps for a walk-through of how to run them.

1. Double-click **AirGapScript.sql**.
2. When prompted, connect to the Endpoint Security database for the Air Gap Client.

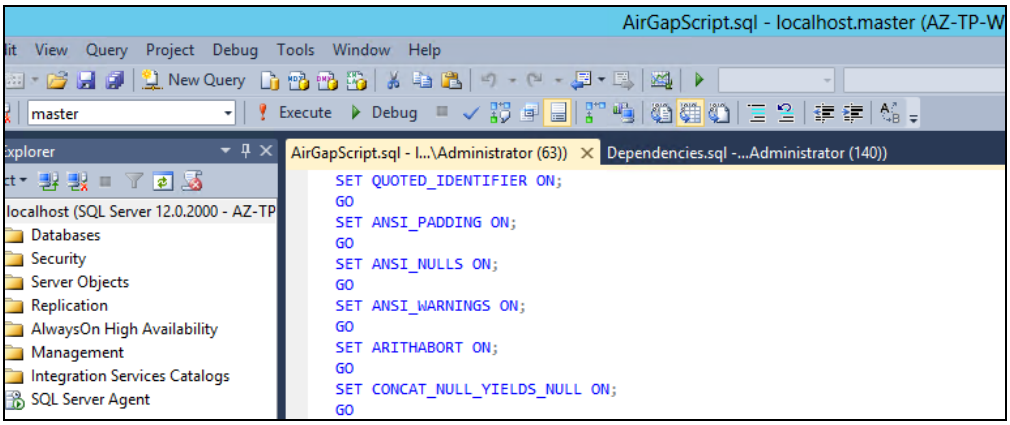
   In our example below, the Endpoint Security database is on the local host. You'll need to adjust the server name if it's on another server in your air gapped network.



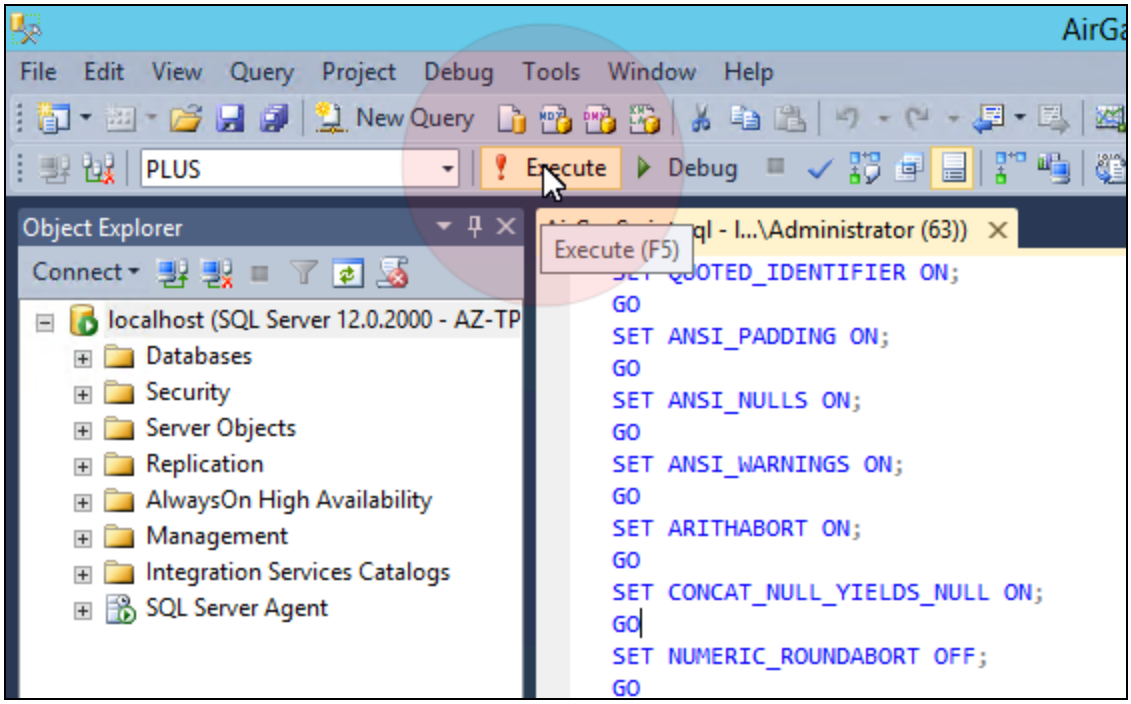
   AirGapScript.sql opens in SQL Server Management Studio.

3. Double click **Dependencies.sql** as well.

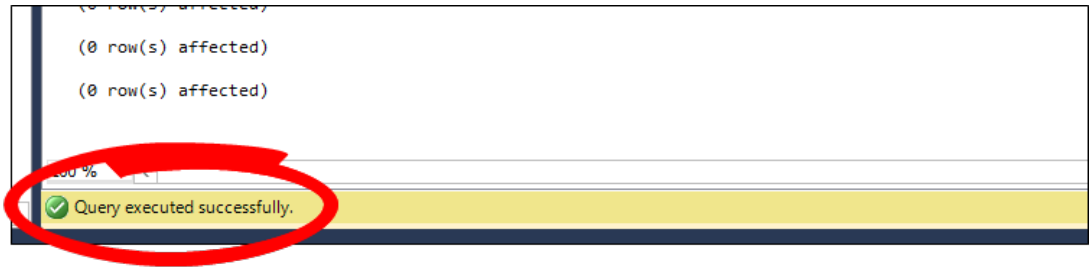
   Dependencies.sql opens in SQL Server Management Studio on a new tab. Both scripts are open.



3. Execute both **AirGapScript.sql** and **Dependencies.sql**. Click **Execute** after selecting each tab.



The scripts are executed. To make sure that each script completed successfully, check the bottom of the main pane.

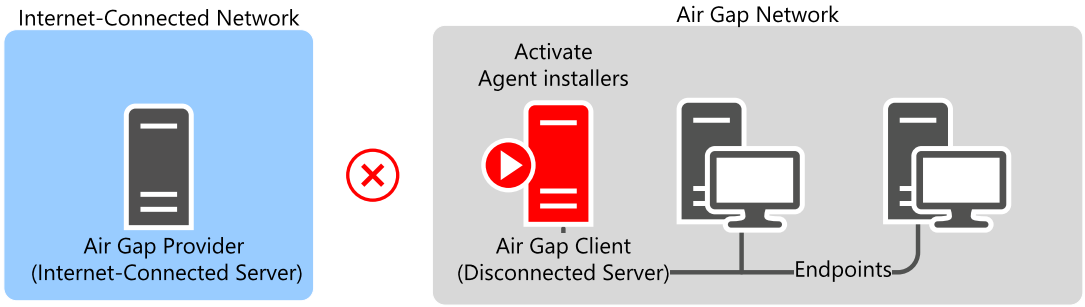


4. Close **SQL Server Management Studio**. You're done.

Proceed to "Activating the Endpoint Security Agent Installers" on the next page

Activating the Endpoint Security Agent Installers

Because (once again) your Air Gap Client can't access the Internet, the Client cannot download an agent manifest, which is a file that lists the different versions of the Endpoint Security Agent authorized to connect to the Air Gap Client. Use our utility to import the Endpoint Security Agent Manifest on your Air Gap Client.



The Air Gap Provider keeps track of all the Endpoint Security Agent versions that are allowed to be installed on your endpoints in a document called the Agent Manifest. Usually, the Endpoint Security Server obtains this document from the Global Subscription Service. However, since your client can't connect to the Internet, you have to update this manifest using a utility, ImportEndpointManifest.exe.

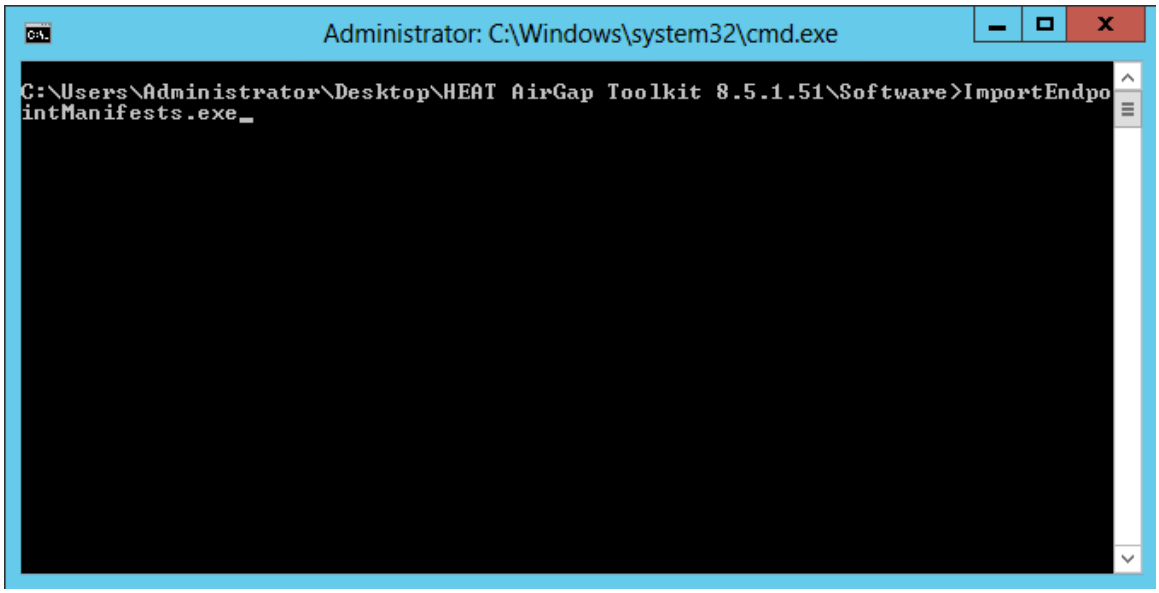
To Activate The Endpoint Security Agent Installers

1. Open a command prompt.
2. Change directories to the **Software** folder in the Air Gap Toolkit. Navigate to the following path within the toolkit:

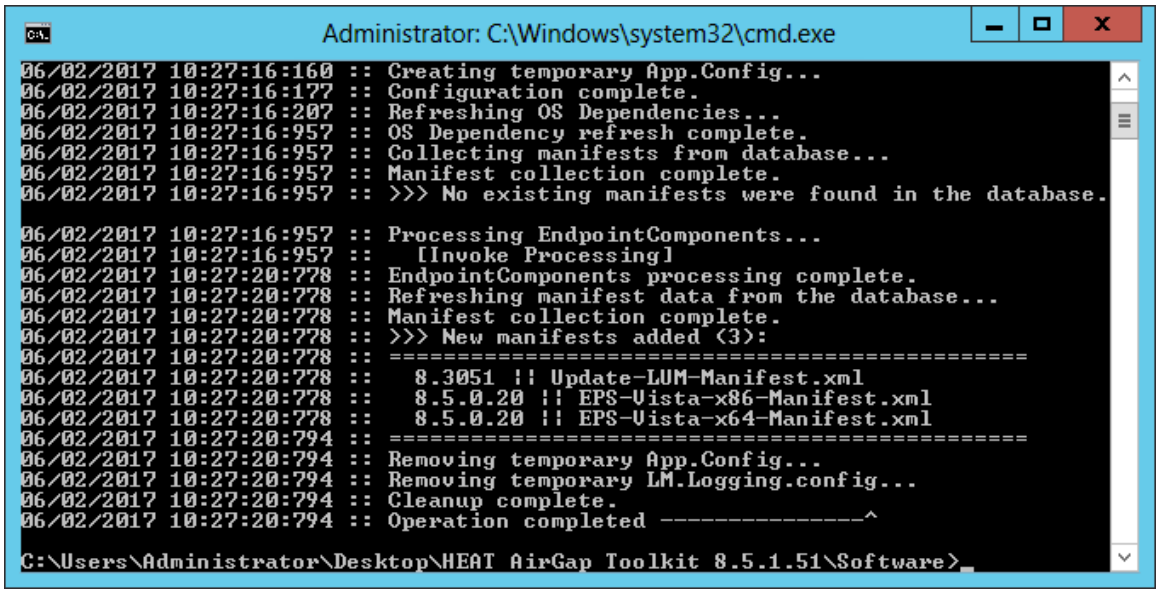
   HEAT AirGap Toolkit 8.5.0.40\Software

3. Enter the following command:

   ImportEndpointManifest.exe



ImportEndpointManifest.exe runs in a command line window. When it completes, that's it!



Your air gap servers are installed and configured. You're ready to start using Endpoint Security in your air gap environment.

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.