Understanding the Migration Process

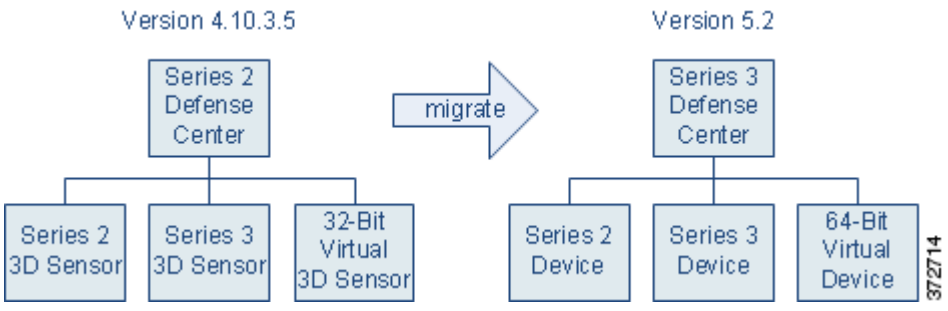
Cisco provides scripts that allow you to migrate vital configurations and events to a Version 5.2 Defense Center from either a Version 4.10.3.x Defense Center or standalone 3D Sensors with IPS. Additionally, you can run a sensor migration script from your Version 5.2.0.x Defense Center to remotely reimage one or more Series 2 and Series 3 sensors in parallel from Version 4.10.3 (or a later patch) to Version 5.2.

The migration process you design for your deployment will be unique and will depend on multiple factors, including (but not limited to) the models of your appliances and your physical access to them, whether you have spare or replacement appliances to use, the number and complexity of configurations you want to migrate, whether you want to migrate events, and so on.

Before you begin to migrate any deployment, thoroughly read this guide and understand the requirements, steps involved, and expected results of the migration. Then, create a detailed plan tailored to your organization.

Note Before you begin the migration process you **must** make sure you have a detailed plan and that you have fully prepared your appliances, including obtaining and installing the new licenses, resolving issues that could prevent a clean migration, setting up replacement appliances, installing the migration utilities, and so on. For detailed information, see Preparing for Migration, page 3-1.

To help you understand the basic migration process, this chapter presents a scenario where you migrate a simple deployment of a Defense Center managing three 3D Sensors from Version 4.10.3 to Version 5.2, while also replacing the Defense Center.



Tip For simplicity, examples use individual managed sensors. However, you can also simultaneously replace or reimage groups of sensors.

Note that this scenario retains all of the physical devices in the deployment, choosing to reimage them to Version 5.2. This is cost effective, but you lose the inspection capabilities of each Series 2 and Series 3 sensor while they are being reimaged to Version 5.2. Additionally, reimaging an inline sensor without the sensor migration script, or with the script when the sensor is not configured to fail open, causes the sensor to fail closed until it is registered to a Version 5.2 Defense Center and its interfaces are reconfigured. In these cases, you may want to disconnect inline sensors from your critical network path during the reimage and configuration portion of the migration process.

There are, however, alternatives, including replacing one or more devices. One-for-one replacements minimize inspection downtime because you can set up a parallel Version 5.2 deployment, migrate configurations, then simply switch cabling over when you are ready. However, this can be costly and requires careful planning to make sure you have the licenses, resources, and physical access to deploy multiple replacement appliances.

With at least one spare device, there is a compromise: a "rolling" migration that replaces each sensor in turn: use the replacement Defense Center to apply equivalent configurations from a Version 4.10.3 sensor to a replacement Version 5.2 device, switch cabling over from sensor to device, then reimage the now-disconnected sensor to Version 5.2 to act as the replacement device for the next Version 4.10.3 sensor. This type of rolling migration minimizes inspection downtime, because for each sensor-to-device migration you only need to interrupt traffic for the recabling. However, this scenario also requires extended physical access and moving of appliances.

Keep the alternatives in mind as you plan your migration. The following sections give you an overview of the migration process for the basic scenario shown above, and describe common variations that may apply to your deployment:

Tip This chapter provides an overview of the migration process to help you plan, but does not go into detail about the steps involved. For detailed information on those steps, see the next chapters: Preparing for Migration, page 3-1 and 4, page 4-1.

CAUTION: Do Not Interrupt the Reimage Process

Supported Devices: Any

Supported Defense Centers: Series 2, Series 3

When your migration involves reimaging (a process that is also commonly referred to as *restoring*) a Defense Center or sensor from Version 4.10.3 to Version 5.2, you must allow time for the process to complete. Interrupting the process can result in an unrecoverable error.

You reimage a Defense Center using the same basic process that you would use to reimage from one version to another. There is no special reimage process for Defense Centers.

Version 5.2 managed devices were more commonly referred to as *sensors* with Version 4.10.x. You can reimage managed devices either manually or using a sensor migration script.

Defense Centers and Managed Devices: Manual Reimage

The time required to reimage a Defense Center, or a sensor when you do not use the sensor migration script, depends on the model. It is reasonable to assume that the minimum time for reimaging a Defense Center would be at least 45 minutes. There is no specific data giving an average or minimum time when you reimage a managed device and do not use the migration script.

Interrupting the reimage process for either - by pressing Ctrl + C, rebooting, or otherwise - can result in an unrecoverable error. Contact Support if you experience any issue with the process. It is imperative that you do not quit, reboot, or otherwise interrupt the process.

Managed Devices: Migration Script Reimage

It is imperative that you not interrupt the reimage process while reimaging a managed device using the migration script. This includes not stopping the Defense Center where you run the script, by rebooting or otherwise. Contact Support if you experience any issue with the process.

You can use Ctrl + C to stop the migration script before the reimage starts. However, the script disables Ctrl + C when you have entered all commands and the reimage begins.

The following table provides average times by model encountered when reimaging either in a single location or in different locations with large bandwidth connections between locations.

Table 2-1 Average Managed Device Reimage Times in Favorable Environments

Device	Time
3D1000	1 hour 40 minutes
3D2000	1 hour 40 minutes
3D2500	1 hour 28 minutes
3D3500	1 hour 28 minutes
3D4500	1 hour 25 minutes
3D6500	1 hour 25 minutes
3D7030	1 hour 35 minutes
3D500	2 hours 5 minutes
3D7110	1 hour 35 minutes
3D7120	1 hour 35 minutes
Series 3 (3D8140, 3D8250)	1 hour 35 minutes

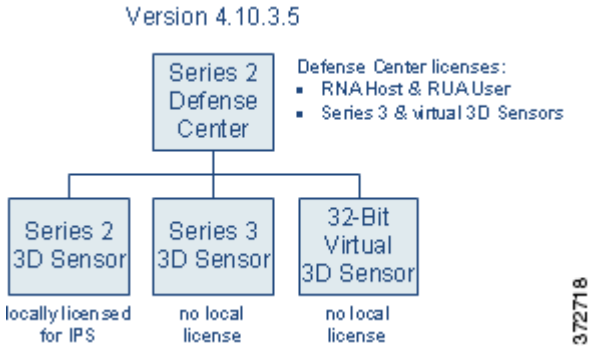
Connection bandwidth can have a significant impact on reimage time, and must be considered so you can anticipate issues. Contact Support before reimaging if you are not sure that you can complete the process without interrupting it.

Migrating a Simple Multi-Sensor Deployment

Supported Devices: Any

Supported Defense Centers: Series 2, Series 3

Although every organization is unique, to help you understand the basic migration process, consider the following simple Version 4.10.3 deployment.



In this deployment, a Series 2 Defense Center manages three 3D Sensors deployed inline: a Series 2 sensor, a Series 3 sensor, and a 32-bit virtual sensor.

So all the sensors can collect both network (RNA) and user (RUA) data, as well as act as an intrusion prevention system (IPS), this deployment includes the following licenses:

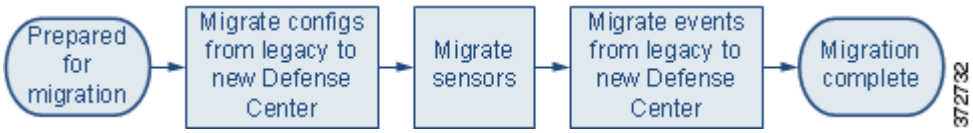
- RNA Host and RUA User feature licenses installed on the Defense Center
- licenses for the Series 3 and virtual sensors, also installed on the Defense Center
- a local IPS license installed on the Series 2 sensor

Now, you want to migrate your deployment to Version 5.2. In this scenario, you are replacing the Series 2 Defense Center with a Series 3 Defense Center, but are not replacing the physical sensors. Instead, you will reimage those sensors to Version 5.2. You must replace the virtual device; Version 5.2 supports only 64-bit virtual appliances.

Tip When you replace an appliance, consider your current and future performance needs. For assistance, contact Sales.

Cisco recommends that you replace your Defense Center for ease of migration and to minimize downtime. If you are not replacing your existing Defense Center; see Migrating By Reimaging the Existing Defense Center, page 2-14.

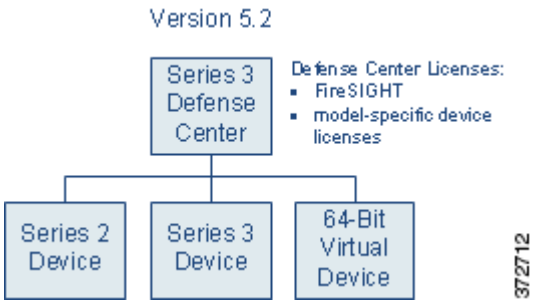
With a replacement, both Defense Centers running at the same time means that you can first copy configuration and event packages directly from Defense Center to Defense Center, then migrate the devices from one active deployment to another. Finally, if you want to migrate events, you can do it at the end of the process when it causes the least disruption.



Caution Always migrate configurations before events. Migrating events before configurations can result in unpredictable event display and behavior.

Note that you do not need to export any configurations or events from the sensors; these are migrated as part of the Defense Center process.

When this migration is complete, a new Series 3 Defense Center will manage three devices deployed inline: your reimaged Series 2 device, your reimaged Series 3 device, and a newly created 64-bit virtual device.



In Version 5.2, which uses a different licensing scheme than Version 4.10.3, you use the Defense Center to control licenses for itself and the devices it manages, and devices are never licensed locally. So that this migrated deployment can behave equivalently with your Version 4.10.3 deployment, you must install the following licenses on the Version 5.2 Defense Center:

- a FireSIGHT license, which replaces the RNA Host and RUA User licenses

  If you reimage the Defense Center instead of replacing it, you may be able to use your legacy licenses; see Host and User Licenses, page 1-4.

- model-specific Protection licenses for both the Series 3 and the virtual devices

You do not need a license for the Series 2 device; these devices automatically have most Protection capabilities. However, you do need a Threat & App (TA) subscription.

After you have fully prepared, you can begin the migration process, which has the following phases:

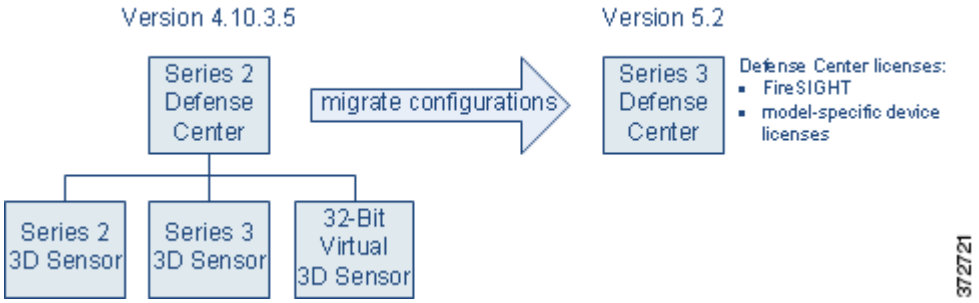
- Migrating Configurations to a Replacement Defense Center, page 2-5
- Migrating 3D Sensors, page 2-6
- Migrating Events from Defense Center to Defense Center, page 2-10

Migrating Configurations to a Replacement Defense Center

Supported Defense Centers: Series 2, Series 3

In this scenario, the Version 4.10.3 Series 2 Defense Center is replaced with a new Version 5.2 Series 3 Defense Center. If you do not have a replacement and must reimage your existing Defense Center, export legacy events before you reimage if you want to retain them; see Migrating By Reimaging the Existing Defense Center, page 2-14.

After you finish this phase, your Version 4.10.3 configurations are imported onto the Version 5.2 Defense Center. However, the Version 4.10.3 deployment is still intact and operating normally.



To migrate configurations between Defense Centers:

Access: Admin

Step 1 On the Version 4.10.3 Defense Center, run the configuration export script to create a package of supported configurations; see Exporting Configurations from a Version 4.10.3 Appliance, page 4-3.

The export script analyzes the configurations and lists those that cannot be migrated (cleanly or otherwise) to Version 5.2.

Note Cisco recommends exiting the script to resolve any issues with configurations essential to your deployment. If you continue without resolving the issues, some configurations will not be migrated, though you may be able to resolve specific issues during the import process. For more information, see Addressing Configuration Incompatibilities, page 3-7.

Step 2 Copy the export package to the Version 5.2 Defense Center.

Step 3 On the Version 5.2 Defense Center, run the configuration import script to import the configurations in the package; see Importing Configurations onto a Version 5.2 Defense Center, page 4-7.

The import script analyzes the configurations and, like the export script, lists those that cannot be migrated. It also gives you the opportunity to resolve any correctable issues with the imported configurations, such as detection engine-specific settings that do not migrate cleanly to Version 5.2. You also must specify some basic information for your Version 5.2 deployment, such as security zones and basic access control settings.

Step 4 Verify the successful migration of your configurations.

For information on what to expect from migrated and new configurations, see Understanding Migrated Configurations and Events, page 5-1.

Step 5 To migrate your sensors to the Version 5.2 Defense Center, continue with the next section, Migrating 3D Sensors.

Migrating 3D Sensors

Supported Devices: Any

Because Version 5.2 Defense Centers cannot manage Version 4.10.3 3D Sensors, after you migrate the Defense Center, you must update the devices it will manage. Because there is no direct update process, you must replace or reimage your 3D Sensors.

When migrating a physical 3D Sensor, you can use your existing appliance (reimage) or you can replace it. In this scenario, we are reusing both the Series 2 and Series 3 devices, and do not have a spare. You must replace the virtual device; Version 5.2 supports only 64-bit virtual appliances.

You do not need to migrate any configurations or events between sensors. You simply use the sensor migration script to update the software on the sensor. The script copies the sensors' interface configurations, reimages the sensors, registers them to the Defense Center, and applies the interface configurations. If you do not use the script, you must complete these tasks manually. Regardless of whether you use the sensor migration script, you must manually apply the configurations imported by the configuration import script.

For more information, see:

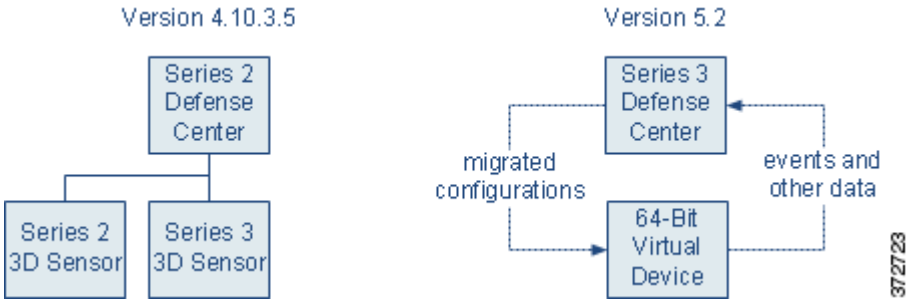
- Migrating Virtual Sensors by Replacement, page 2-7
- Migrating Series 2 and Series 3 Sensors by Reimage, page 2-8

Migrating Virtual Sensors by Replacement

Supported Devices: virtual

Migrating virtual 3D Sensors is straightforward: because there is no hardware to reimage; you simply create a replacement virtual device, register it to the new Defense Center, and apply migrated configurations to it.

At that point, the new device is handling network traffic and reporting events to the Version 5.2 Defense Center. The physical Version 4.10.3 sensors are still handling their own network traffic, and are still reporting to the Version 4.10.3 Defense Center.



To replace a virtual sensor:

Access: Admin

Step 1 Create a new 64-bit virtual device using the VMware vSphere Client. Use the device's CLI to perform its initial setup, including registration (that is, specifying your new Version 5.2 Defense Center as its manager).

Version 5.2 packages 64-bit virtual appliances only for the VMware ESX/ESXi hosting environment. For more information on the requirements for the hypervisor host, as well as information on creating and setting up virtual appliances, see the Version 5.2 *Sourcefire 3D System Virtual Installation Guide*.

Step 2 Using its hypervisor host, remove the inline Version 4.10.3 virtual device from the network path so that traffic can continue to flow while you bring up the replacement device.

For more information, see the documentation for the hypervisor host you are using to run Version 4.10.3 virtual appliances.

Step 3 Using the Version 4.10.3 Defense Center's web interface, remove the device from management.

Tip After you remove the Version 4.10.3 device from your deployment, uninstall it to free resources on your 32-bit hypervisor host.

Step 4 Use the Version 5.2 Defense Center's web interface to add and configure the Version 5.2 device, including applying a license, adding its interfaces to zones, and applying the policies created and updated by the migration.

For more information, see Completing Your Version 5.2 Deployment, page 4-33.

Step 5 Using the VMware vSphere Client on your 64-bit hypervisor host, place the new Version 5.2 device inline.

Step 6 Continue with the next section, Migrating Series 2 and Series 3 Sensors by Reimage, to migrate your physical sensors to the Version 5.2 Defense Center.

Migrating Series 2 and Series 3 Sensors by Reimage

Supported Devices: Series 2, Series 3

When migrating a physical 3D Sensor, you can use your existing appliance (reimage) or you can replace it. In this scenario, we are reusing both physical sensors, and do not have a spare.

Tip If you have spare sensors, you can perform one-for-one replacements or plan a rolling migration that swaps out each sensor in turn. These strategies can minimize downtime but may not be practical given the size of your deployment and physical access to the sensors; see Performing a Multi-Sensor Rolling Migration, page 2-11.

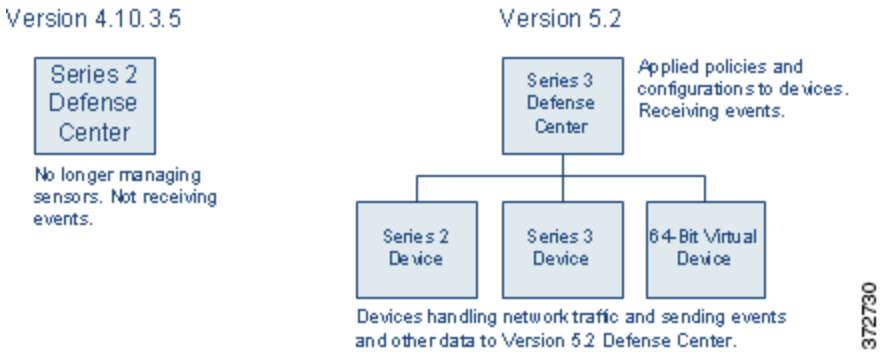
To use an existing sensor, you must reimage it to Version 5.2 and apply migrated configurations to it. If you do not use the sensor migration script, you must manually register the sensor before applying configurations.

Reimaging results in the loss of almost all configuration and event data on the sensor. Reimaging can retain the sensor's network, console, and Series 3 Lights-Out Management (LOM) settings, and the sensor migration script registers sensors and preserves interface configurations. However, you must perform all other setup tasks after the restore process completes.

Note Inline interfaces **fail closed** during the reimage when you do not use the sensor migration script or you use the script and the interfaces are not configured to fail open. In these cases you may want to remove the sensors from your critical network path during reimage, which may require physical access to the sensors.

When you do not use the sensor migration script, physical access is required to reimage Series 2 sensors, even those deployed passively; the standard Series 2 restore utility is distributed on an external USB drive. Also, when you do not use the sensor migration script, you can remotely reimage Series 3 sensors using either a remote KVM or, if enabled, LOM.

After you migrate your Version 4.10.3 sensors to Version 5.2 managed devices, the reimaged devices are handling network traffic and reporting events to the Version 5.2 Defense Center. The Version 4.10.3 Defense Center is no longer managing any sensors or receiving new events. However, it may have stored events that you want to view, so leave it powered on and connected to the management network for now.



To migrate a Series 2 or Series 3 3D Sensor using the sensor migration script:

Access: Admin

Step 1 If any Version 4.10.3 Series 2 or Series 3 inline sensor will be configured to fail closed when you reimage it, remove it from the network path so that traffic can continue to flow while you reimage it.

Step 2 On the Defense Center, run the sensor migration script to reimage your physical sensors; see Reimaging and Registering Devices with the Sensor Migration Script, page 4-22.

The script copies the Series 2 and Series 3 interface configurations, reimages the sensors, registers the reimaged sensors to the Defense Center, and applies the interface configurations. For more information, see Reimaging and Registering Devices with the Sensor Migration Script, page 4-22.

Step 3 Use the Version 5.2 Defense Center's web interface to configure each device, including applying a license, adding its interfaces to zones, and applying the policies created and updated by the migration.

For more information, see Completing Your Version 5.2 Deployment, page 4-33.

Step 4 If you previously removed any inline sensors that were configured to fail closed from the network path prior to reimaging them, place the freshly set up Version 5.2 devices inline.

Step 5 Continue with the next section, Migrating Events from Defense Center to Defense Center, to migrate legacy events.

To migrate a Series 2 or Series 3 3D Sensor manually:

Access: Admin

Step 1 Remove either inline Version 4.10.3 sensor from the network path so that traffic can continue to flow while you reimage it.

Whether you reimage your sensors at once or serially depends on your migration plan. In this case, we are reimaging one sensor after the other.

Step 2 Using the Version 4.10.3 Defense Center's web interface (**Operations > Sensors**), remove the sensor from management.

Step 3 Reimage the Version 4.10.3 sensor to a Version 5.2 device and perform the initial setup on the device.

For more information, see the Version 5.2 *Sourcefire 3D System Installation Guide*.

Step 4 Use the Version 5.2 Defense Center's web interface to add and configure the device, including applying a license, adding its interfaces to zones, and applying the policies created and updated by the migration.

For more information, see Completing Your Version 5.2 Deployment, page 4-33.

Step 5 Place the freshly set up Version 5.2 device inline.

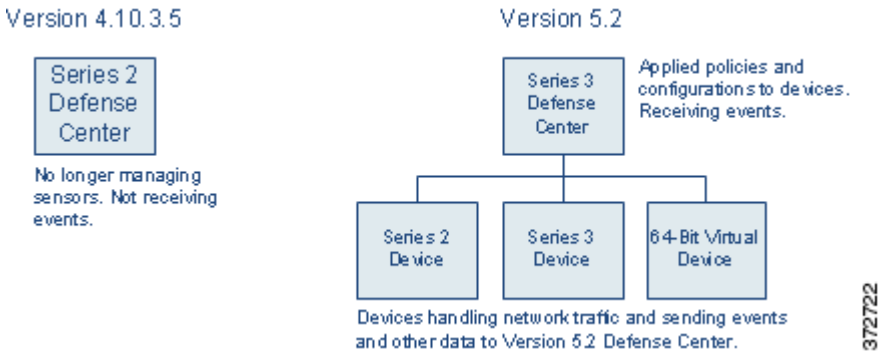
Step 6 Repeat this procedure for the other physical sensor.

Step 7 Continue with the next section, Migrating Events from Defense Center to Defense Center, to migrate legacy events.

Migrating Events from Defense Center to Defense Center

Supported Defense Centers: Any

This scenario includes the optional migration of legacy intrusion and audit events from the Version 4.10.3 Defense Center to the Version 5.2 Defense Center. If you replaced your Defense Center as in this scenario, it is no longer managing any sensors or receiving new events, but you can migrate stored events to the Version 5.2 Defense Center.



If you are not interested in events generated before the migration, you can skip this step.

Note If you are reimaging your existing Defense Center to Version 5.2 and want to migrate legacy events, you must perform this step **before** you reimage the appliance and migrate the sensors. For more information, see Migrating By Reimaging the Existing Defense Center, page 2-14.

Note that the fields in intrusion events generated by Version 4.10.3 are different than the fields in Version 5.2 intrusion events. For information on how legacy events appear in the Version 5.2 web interface, see Understanding Migrated Intrusion and Audit Events, page 5-18.

Also keep in mind that when you migrate events, the timestamps on those events will be "behind" newly generated events on the Version 5.2 Defense Center. Because the database is pruned by event timestamp, your migrated events will be pruned before those events.

After you migrate events, you can shut down and remove the Version 4.10.3 Defense Center from your deployment (or, if you are reusing the Defense Center, reimage it to Version 5.2).

To migrate events between Defense Centers:

Access: Admin

Step 1 On the Version 4.10.3 Defense Center, run the event export script to create a package of intrusion and audit events; see Exporting Events from a Version 4.10.3 Appliance, page 4-6.

Step 2 Copy the event package to the Version 5.2 Defense Center.

Step 3 On the Version 5.2 Defense Center, run the import events script to import the events in the package; see Importing Events onto a Version 5.2 Defense Center, page 4-20.

The script analyzes the package and displays the disk space required to import the events. You can abort the import if the events require too much space Otherwise, continue to import the events.

Performing a Multi-Sensor Rolling Migration

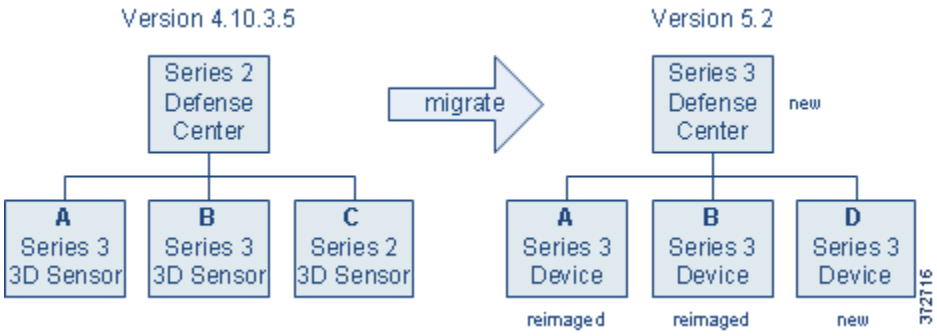
Supported Devices: Series 2, Series 3

A "rolling" migration from Version 4.10.3 to Version 5.2 replaces each sensor in a deployment in turn to minimize inspection downtime. The basic strategy is to use a replacement Defense Center to apply equivalent configurations from a Version 4.10.3 sensor to a replacement Version 5.2 device, switch cabling over from sensor to device, then reimage the now-disconnected sensor to Version 5.2 to act as the replacement device for the next Version 4.10.3 sensor.

This means that for each sensor-to-device migration you only need to interrupt traffic flow for the recabling. However, this scenario also requires extended physical access to and moving of appliances, as well as a replacement physical or virtual Defense Center.

Note If you are reimaging your existing Defense Center, there is no advantage to a rolling migration. See Migrating By Reimaging the Existing Defense Center, page 2-14.

Now, consider a scenario similar to that in Migrating a Simple Multi-Sensor Deployment, page 2-3, except in this case the Version 4.10.3 Defense Center is managing two Series 3 sensors (A and B) and one Series 2 (C). When you migrate this deployment to Version 5.2, you want to replace both the Defense Center and the Series 2 sensor with Series 3 appliances.



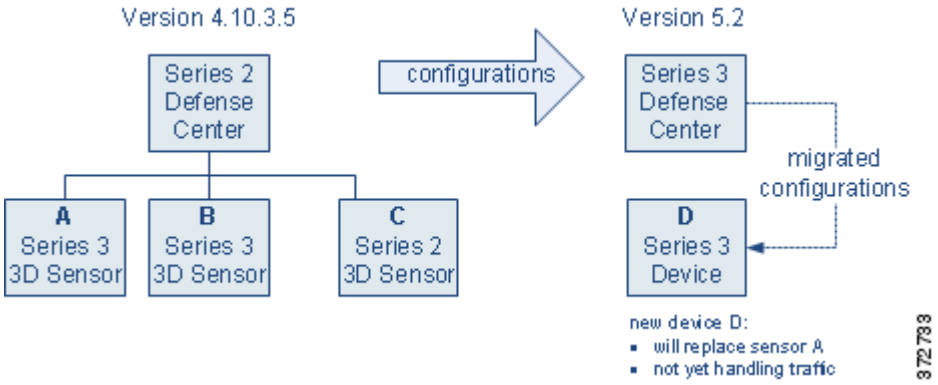
Preparing for this migration includes fully setting up the Version 5.2 replacement Defense Center as well as the new Series 3 device (D) that will replace your Series 2 sensor. Then, you can migrate configurations from Defense Center to Defense Center, as described in Migrating Configurations to a

Replacement Defense Center, page 2-5.

After the replacement Defense Center has the configurations it needs to manage your migrated deployment, you can use the Defense Center to add and configure the new device D as described in Completing Your Version 5.2 Deployment, page 4-33. Make sure you enable a Protection license, apply the access control policy created by the migration, and apply a device configuration that adds the device's interfaces to the appropriate zones (also created by the migration).

Note Add interfaces to zones based on which Version 4.10.3 sensor you are replacing right now. In this example, where you are replacing sensor A with device D, assign the interfaces on D to the zones that represent network traffic monitored by the interfaces on A. For a detailed explanation, see Configuring and Verifying Sensing Interfaces and Inline Sets, page 4-33.

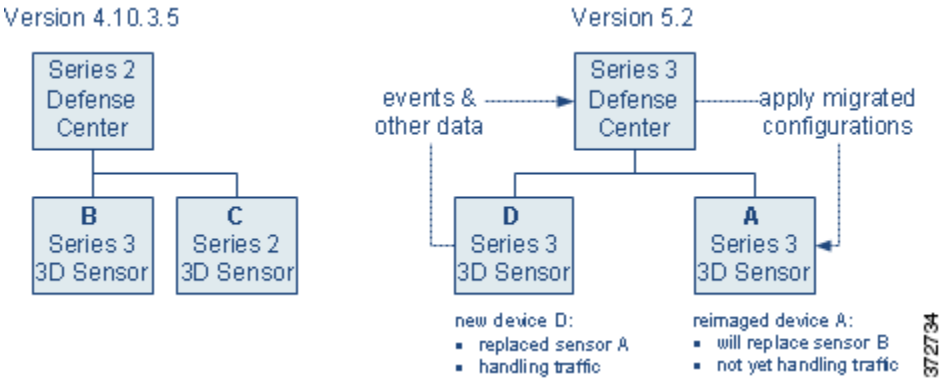
At this point, the Version 4.10.3 deployment is still intact. The Version 5.2 replacement Defense Center is managing replacement device D, which is ready to be placed inline and take over for sensor A.



Now, you can switch the cabling from sensor A to device D to have your Version 5.2 deployment begin handling network traffic previously inspected by sensor A.

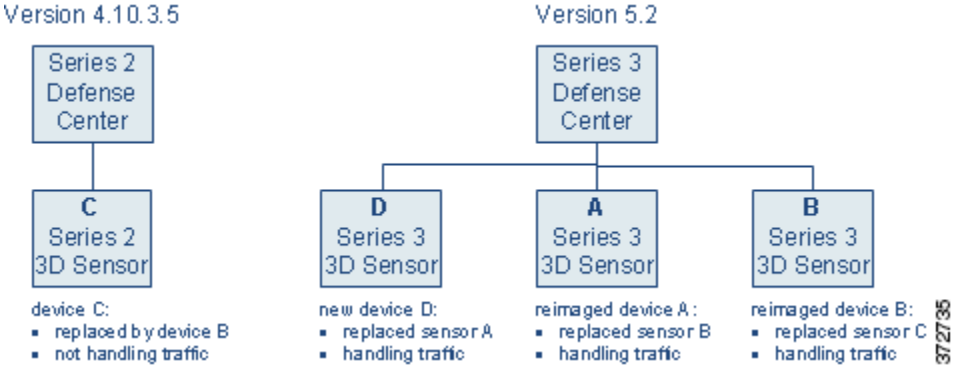
You now have a new spare sensor, A, and can repeat the process. Use the Version 4.10.3 Defense Center to delete sensor A from management, reimage it to Version 5.2, and add it to the Version 5.2 Defense Center as a replacement for the next sensor to be migrated: B. Optionally, you can use the sensor migration script to reimage sensor A and register it to the Version 5.2 Defense Center. As before, enable a Protection license, apply a device configuration that adds the device's interfaces to the appropriate zones, and apply the access control policy created by the migration.

At this point, the Version 4.10.3 deployment includes sensors B and C. The Version 5.2 sensor D has taken over for Version 4.10.3 sensor A, which has been reimaged to Version 5.2 and is ready to take over for sensor B.



Now, you can switch the cabling from sensor B to reimaged device A to have your Version 5.2 deployment begin handling network traffic previously inspected by sensor B. Your spare sensor is now sensor B, which you can use to replace sensor C.

After you replace sensor C, your Version 5.2 deployment has fully replaced your Version 4.10.3 deployment.



The Version 4.10.3 Defense Center is now managing only sensor C, which is not inspecting any traffic. You can power down and disconnect the sensor. However, If the Defense Center has stored events that you want to migrate, leave it powered on and connected to the management network until you perform the steps in Migrating Events from Defense Center to Defense Center, page 2-10.

Migrating Stacked 3D Sensors

Supported Devices: 8000 Series

When you reimage a 3D Sensor, you lose almost all configuration and event data on the appliance, including stacking configurations. Because reimaging a sensor automatically breaks the stack, migrating stacked sensors is not significantly different from migrating single sensors.

If your Version 4.10.3 deployment includes stacked sensors, first delete the stack from the managing Version 4.10.3 Defense Center, then reimage the stacked sensors. Re-establish the stack after adding the devices to the Version 5.2 Defense Center.

Note You must obtain a model-specific Protection license for each Series 3 device you plan to stack.

Migrating By Reimaging the Existing Defense Center

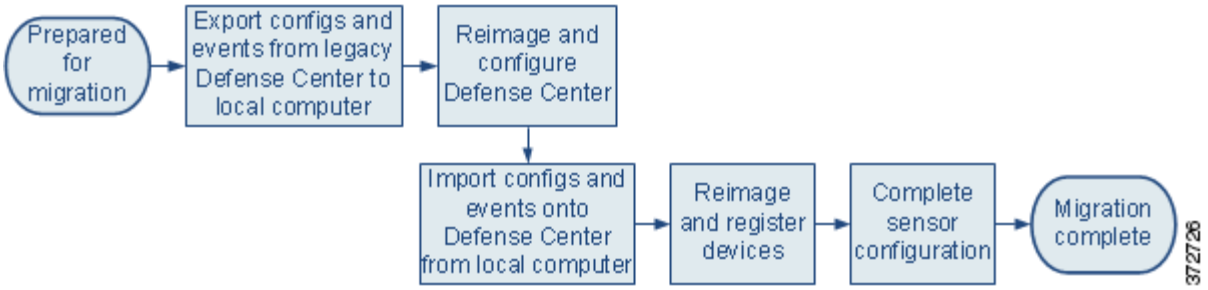
Supported Devices: migration method dependent

Supported Defense Centers: Series 2, Series 3

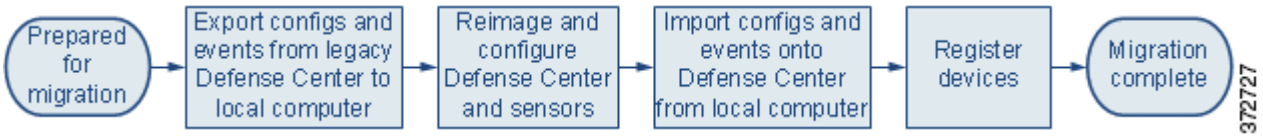
In the simple scenario presented earlier in this chapter (see Migrating a Simple Multi-Sensor Deployment, page 2-3), you replaced the Series 2 Defense Center in your deployment with a Series 3 Defense Center running Version 5.2. Replacing the Defense Center is convenient and can minimize downtime, but if you do not have the resources to replace the Defense Center, you must reimage your existing Defense Center to Version 5.2.

In this reimage scenario, when you export configurations and events from the Version 4.10.3 Defense Center you must copy them to a local computer so they are not lost while you reimage and reconfigure your appliances. After you reimage the Defense Center, you must set it up and prepare it for migration, then import the configurations and events and, finally, if you do not use the sensor migration script, re-register the migrated sensors, configure sensor interfaces, and apply the interface configurations.

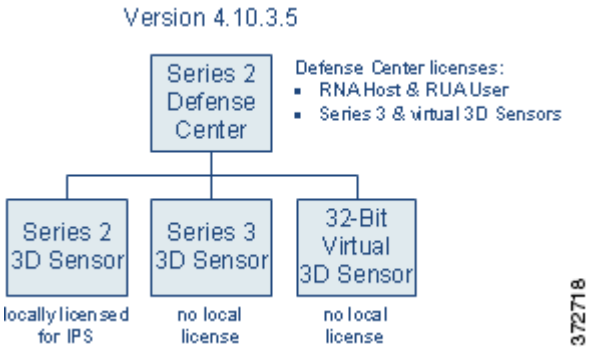
Whether you use the sensor migration script depends on your migration plan. The migration scenario in the following diagram assumes that you use the sensor migration script. When you use the script, Cisco recommends that you reimage devices **after** reimaging the Defense Center and importing configurations, so policies are in place and ready to apply.



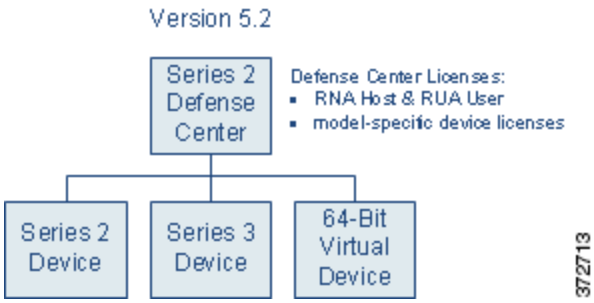
The following diagram shows an alternative migration sequence where you do **not** use the sensor migration script. In this case, you might find it convenient to reimage your sensors and the Defense Center before importing configurations, but you should register your devices after importing configurations and events so your configurations and events are in place.



Once again, consider the following simple Version 4.10.3 deployment, where a Series 2 Defense Center manages three 3D Sensors deployed inline: a Series 2 sensor, a Series 3 sensor, and a 32-bit virtual sensor:



Now, you want to migrate your deployment to Version 5.2 **without** replacing any of the physical appliances. In your Version 5.2 deployment, a reimaged Series 2 Defense Center will manage three devices deployed inline: your reimaged Series 2 device, your reimaged Series 3 device, and a newly created 64-bit virtual device.



So that this migrated deployment can behave equivalently with your Version 4.10.3 deployment, install the following licenses on the reimaged Version 5.2 Defense Center:

- your RNA Host and RUA User licenses from Version 4.10.3

  These legacy licenses function identically to the newer FireSIGHT license. You can obtain a FireSIGHT license for your reimaged Defense Center, but it is not required. For more information, see Host and User Licenses, page 1-4.

- model-specific Protection licenses for both the Series 3 and the virtual devices

You do not need a license for the Series 2 device; these devices automatically have most Protection capabilities. However, you do need a Threat & App (TA) subscription.

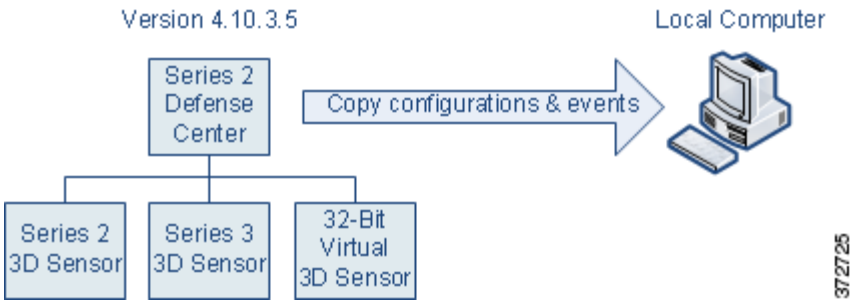
For more information on the phases in this migration process, see:

- Exporting Configurations and Events from the Defense Center, page 2-15
- Completing the Migration Using the Sensor Migration Script, page 2-16
- Completing the Migration Manually, page 2-21

Exporting Configurations and Events from the Defense Center

Supported Defense Centers: Series 2, Series 3

After you fully prepare for migration, the first step when migrating a deployment where you are going to reimage the Defense Center is to create configuration and export packages on the Version 4.10.3 Defense Center, then copy them to a local computer.



To export configurations and events from a Defense Center you are going to reimage:

Access: Admin

Step 1 On the Defense Center, run a configuration export script to create a package of supported configurations; see Exporting Configurations from a Version 4.10.3 Appliance, page 4-3.

The export script analyzes the configurations and lists those that cannot be migrated (cleanly or otherwise) to Version 5.2.

Note Cisco recommends exiting the script to resolve any issues with configurations essential to your deployment. If you continue without resolving the issues, some configurations will not be migrated, though you may be able to resolve specific issues during the import process. This is especially important because you are reimaging the Defense Center. For more information, see Addressing Configuration Incompatibilities, page 3-7.

Step 2 On the Defense Center, run an events export script to create a package of intrusion and audit events; see Exporting Events from a Version 4.10.3 Appliance, page 4-6.

Step 3 So they are not lost while you reimage and reconfigure the Defense Center, copy the configuration and event packages to a local computer.

Step 4 Choose one of the following options:

- If you plan to use the sensor migration script to reimage and register physical devices, continue with Completing the Migration Using the Sensor Migration Script.
- If you do not plan to use the sensor migration script to reimage and register physical devices, continue with Completing the Migration Manually, page 2-21.

Completing the Migration Using the Sensor Migration Script

Supported Devices: Series 2, Series 3

Supported Defense Centers: Series 2, Series 3

After exporting configurations and events from the Defense Center, you are going to reimage the Defense Center and then import your configurations. Finally, you can use the sensor migration script to reimage one or more Series 2 and Series 3 sensors, register reimaged sensors, and copy your interface configurations. If your sensors are configured to fail open, network traffic flow is not interrupted during the reimaging and configuration process.

The following sections describe the steps for completing the migration when you use the sensor migration script to reimage sensors:

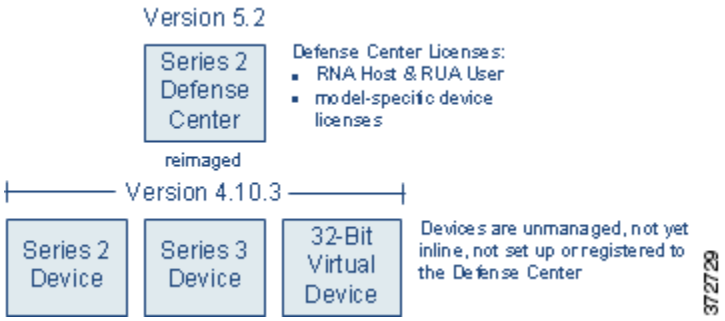
- Reimaging the Defense Center, page 2-17.
- Importing Configurations and Events onto the Defense Center, page 2-18.
- Adding Devices to the Defense Center Using the Sensor Migration Script, page 2-19.
- Completing Device Configuration After Using the Sensor Migration Script, page 2-21.

Reimaging the Defense Center

Supported Defense Centers: Series 2, Series 3

After you copy the packaged configurations and events from the Defense Center onto a local computer, you are ready to install Version 5.2 on your Defense Center. Reimaging results in the loss of almost all configuration and event data on the appliance. Although the restore utility can retain license, network, console, and Series 3 Lights-Out Management (LOM) settings, you must perform all other setup tasks after the restore process completes.

When you finish reimaging and setting up the Defense Center (including licensing), the Defense Center is ready to import configurations and events exported from Version 4.10.3.



Optionally, because you cannot reimage a virtual device (manually or by using the sensor migration script), you can also recreate the virtual sensor at this time.

To reimage your Defense Center:

Access: Admin

Step 1 Using the Version 4.10.3 Defense Center's web interface (**Operations > Sensors**), remove all sensors from management.

Step 2 Remove the virtual sensor in this scenario from the network path, and also remove any physical sensor with an inline interface that is not configured to fail open, so that traffic can continue to flow while you recreate your deployment.

Step 3 Reimage the physical Version 4.10.3 Defense Center to Version 5.2 and perform the initial setup.

Caution Make sure you allow sufficient time for the restore process to complete. If you interrupt the process (for example, by pressing Ctrl + C or rebooting), you could cause an unrecoverable error. If you think the restore is taking too long or you experience any other issues with the process, **do not** quit, reboot, or otherwise interrupt the process. Instead, contact Support. For more information, see CAUTION: Do Not Interrupt the Reimage Process, page 2-2.

For more information, see *Restoring a Sourcefire Appliance to Factory Defaults* in the Version 5.2 *Sourcefire 3D System Installation Guide*.

Step 4 Prepare the freshly reimaged Defense Center for the import of configurations and events, as described in Preparing for Migration, page 3-1.

Step 5 Optionally, create a new 64-bit virtual device using the VMware vSphere Client. Use the device's CLI to perform its initial setup.

Version 5.2 packages 64-bit virtual appliances only for the VMware ESX/ESXi hosting environment. For more information on the requirements for the hypervisor host, as well as information on creating and setting up virtual appliances, see the Version 5.2 *Sourcefire 3D System Virtual Installation Guide*.

Step 6 Continue with Importing Configurations and Events onto the Defense Center.

Importing Configurations and Events onto the Defense Center

Supported Defense Centers: Series 2, Series 3

After you reimage and set up the Defense Center, import the configurations and events you exported earlier. After you finish importing your configurations, you are ready to reimage your devices and add them to the Defense Center.

To import configurations and events onto the Defense Center:

Access: Admin

Step 1 From a local computer, copy the configuration and events export packages you exported earlier to the Version 5.2 Defense Center.

Step 2 On the Defense Center, run a script to import configurations; see Importing Configurations onto a Version 5.2 Defense Center, page 4-7.

The script analyzes the configurations and, like the export script, lists those that cannot be migrated. It also gives you the opportunity to resolve any correctable issues with the imported configurations, such as detection engine-specific settings that do not migrate cleanly to Version 5.2. You also must specify some basic information for your Version 5.2 deployment, such as security zones and basic access control settings.

Step 3 Verify the successful migration of your configurations.

For information on what to expect from migrated and new configurations, see Understanding Migrated Configurations and Events, page 5-1.

Step 4 On the Defense Center, run a script to import events; see Importing Events onto a Version 5.2 Defense Center, page 4-20.

The script analyzes the event package and displays the disk space required to import the events. You can abort the import if the events require too much space, otherwise continue to import the events.

Step 5 Continue with Adding Devices to the Defense Center Using the Sensor Migration Script.

Adding Devices to the Defense Center Using the Sensor Migration Script

Supported Devices: Series 2, Series 3

Supported Defense Centers: Series 2, Series 3

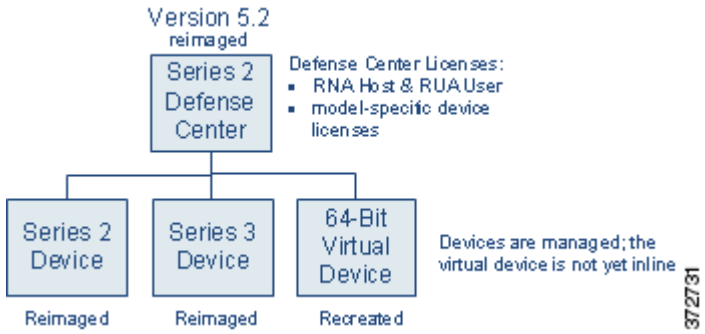
After you import the configurations and events onto the reimaged Defense Center, you must install the sensor migration package. You are then ready to use the sensor migration script to reimage your sensors to Version 5.2. The sensor migration script copies the sensors' interface configurations, reimages the sensors, registers them to the Defense Center, and applies the interface configurations.

The script reimages and registers physical appliances, but you must recreate and register the virtual sensor in this scenario which, optionally, you could do earlier in the process (for example, while reimaging the Defense Center; see Reimaging the Defense Center, page 2-17).

Reimaging results in the loss of almost **all** configuration and event data on the sensors. Although reimaging can retain the sensor's network, console, and Series 3 Lights-Out Management (LOM) settings, and the sensor migration script can register devices and preserve interface configurations, you must perform all other setup tasks after the restore process completes; for example, if applicable, you must reconfigure LDAP authentication.

Note Inline interfaces **fail closed** during the reimage when you do not use the sensor migration script, or you use the script and the interfaces are not configured to fail open. In these cases, you may want to remove the sensors from your critical network path during reimage, which may require physical access to the sensors.

When you finish this phase of the migration, all sensors in your deployment are running Version 5.2 and registered. Physical devices are automatically registered and ready to establish communications. You must manually register the virtual device and, in the next phase, put it inline.



To reimage and register your sensors using the sensor migration script:

Access: Admin

Step 1 If any Version 4.10.3 Series 2 or Series 3 inline sensor will be configured to fail closed when you reimage it, remove it from the network path so that traffic can continue to flow while you reimage it.

On the Defense Center, run the sensor migration script to reimage your physical sensors; see Reimaging and Registering Devices with the Sensor Migration Script, page 4-22.

The script copies the Series 2 and Series 3 interface configurations, reimages the sensors, registers the reimaged sensors to the he Defense Center, and applies the interface configurations.

Caution Make sure you allow sufficient time for the restore process to complete. If you interrupt the process (for example, by pressing Ctrl + C or rebooting), you could cause an unrecoverable error. If you think the restore is taking too long or you experience any other issues with the process, **do not** quit, reboot, or otherwise interrupt the process. Instead, contact Support. For more information, see CAUTION: Do Not Interrupt the Reimage Process, page 2-2.

Tip You can specify IP addresses or host names of any physical Version 4.10.3 sensors on your network that you want to reimage and register to the Version 5.2 Defense Center, including sensors not originally registered to the Version 4.10.3 Defense Center.

Step 2 If you did not create a new 64-bit virtual device while reimaging the Defense Center, create one now using the VMware vSphere Client. Use the device's CLI to perform its initial setup.

Version 5.2 packages 64-bit virtual appliances only for the VMware ESX/ESXi hosting environment. For more information on the requirements for the hypervisor host, as well as information on creating and setting up virtual appliances, see the Version 5.2 *Sourcefire 3D System Virtual Installation Guide*.

Step 3 If you previously removed any inline sensors that were configured to fail closed from the network path prior to reimaging them, place the freshly set up Version 5.2 devices inline.

Step 4 Continue with Completing Device Configuration After Using the Sensor Migration Script.

Completing Device Configuration After Using the Sensor Migration Script

Supported Devices: Any

Supported Defense Centers: Series 2, Series 3

After you use the sensor migration script to reimage and register the physical sensors, and you manually recreate the virtual sensor, the final phase is to register the virtual sensor and configure all managed devices so they can begin to handle network traffic and report events to the Defense Center.

First, use the Version 5.2 Defense Center's web interface to register the virtual device, configure its interfaces, and apply the interface configurations. Then, verify the interface configurations applied by the sensor migration script. Finally, for all devices, apply the policies created and updated by the migration. For more information, see Completing Your Version 5.2 Deployment, page 4-33.

Finally, place the recreated virtual device inline so it can begin handling traffic.

Completing the Migration Manually

Supported Devices: Any

Supported Defense Centers: Series 2, Series 3

Optionally, you can reimage sensors manually without using the sensor migration script. For example, you might choose to reimage manually if you have a small or low-bandwidth deployment. When you manually reimage sensors, inline sensors fail closed and physical access is often required.

The following sections describe the steps for completing the migration when you manually reimage sensors.

- Manually Reimaging and Configuring Appliances, page 2-21.
- Importing Configurations and Events onto the Defense Center, page 2-22.
- Manually Adding Devices to the Defense Center, page 2-23.

Manually Reimaging and Configuring Appliances

Supported Devices: Any

Supported Defense Centers: Series 2, Series 3

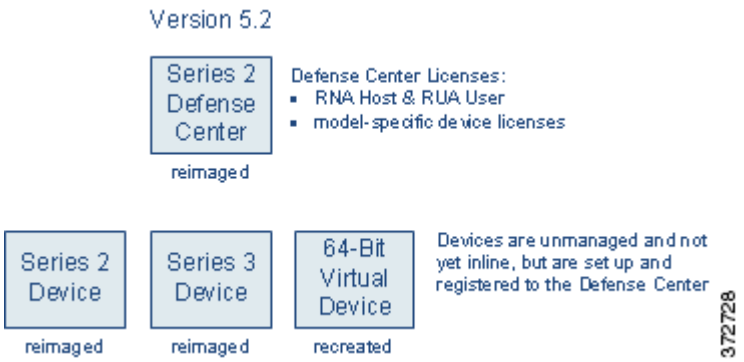
After you copy the packaged configurations and events from the Defense Center onto a local computer, you are ready to install Version 5.2 across your deployment. You can reimage the physical appliances, but you must recreate the virtual sensor.

Reimaging results in the loss of almost **all** configuration and event data on the appliance. Although the restore utility can retain the appliance's license, network, console, and Series 3 Lights-Out Management (LOM) settings, you must perform all other setup tasks after the restore process completes.

Note Manually reimaging a sensor causes inline interfaces to fail closed until you: register the sensor to a Defense Center, and reconfigure and apply its interface configurations. You may want to disconnect inline sensors from your critical network path during the reimage. This may require physical access to the sensors.

When you do not use the sensor migration script, physical access is required to reimage Series 2 sensors, even those deployed passively; the standard Series 2 restore utility is distributed on an external USB drive. Also, when you do not use the sensor migration script, you can remotely reimage Series 3 sensors using either a remote KVM or, if enabled, LOM.

When you finish this phase of the migration, all appliances in your deployment are running Version 5.2, set up (including licensing), and ready to establish communications. The Defense Center is ready to import configurations and events exported from Version 4.10.3.



To manually reimage your deployment:

Access: Admin

Step 1 Create a new 64-bit virtual device using the VMware vSphere Client. Use the device's CLI to perform its initial setup.

Version 5.2 packages 64-bit virtual appliances only for the VMware ESX/ESXi hosting environment. For more information on the requirements for the hypervisor host, as well as information on creating and setting up virtual appliances, see the Version 5.2 *Sourcefire 3D System Virtual Installation Guide*.

Step 2 Using the Version 4.10.3 Defense Center's web interface (**Operations > Sensors**), remove all sensors from management.

There is no advantage to migrating appliances one by one in this scenario.

Step 3 Remove the sensors (including the virtual sensor) from the network path so that traffic can continue to flow while you recreate your deployment.

Step 4 Reimage the physical Version 4.10.3 appliances to Version 5.2, and perform the initial setup.

For more information, see the Version 5.2 *Sourcefire 3D System Installation Guide*.

Step 5 Prepare the freshly reimaged Defense Center for the import of configurations and events, as described in Preparing for Migration, page 3-1.

Step 6 Continue with Importing Configurations and Events onto the Defense Center.

Importing Configurations and Events onto the Defense Center

Supported Defense Centers: Series 2, Series 3

After you reimage and set up the Defense Center, import the configurations and events you exported earlier. It is important to perform this import before you manually add devices so you can have policies and zones in place. After you finish this phase, you are ready to put devices inline and add them to the Defense Center.

To import configurations and events onto the Defense Center:

Access: Admin

Step 1 From a local computer, copy the configuration and events export packages you exported earlier to the Version 5.2 Defense Center.

Step 2 On the Defense Center, run a script to import configurations; see Importing Configurations onto a Version 5.2 Defense Center, page 4-7.

The script analyzes the configurations and, like the export script, lists those that cannot be migrated. It also gives you the opportunity to resolve any correctable issues with the imported configurations, such as detection engine-specific settings that do not migrate cleanly to Version 5.2. You also must specify some basic information for your Version 5.2 deployment, such as security zones and basic access control settings.

Step 3 Verify the successful migration of your configurations.

For information on what to expect from migrated and new configurations, see Understanding Migrated Configurations and Events, page 5-1.

Step 4 On the Defense Center, run a script to import events; see Importing Events onto a Version 5.2 Defense Center, page 4-20.

The script analyzes the event package and displays the disk space required to import the events. You can abort the import if the events require too much space, otherwise continue to import the events.

Step 5 Continue with Completing Device Configuration After Using the Sensor Migration Script.

Manually Adding Devices to the Defense Center

Supported Devices: Any

Supported Defense Centers: Series 2, Series 3

After you import configurations onto your migrated Version 5.2 Defense Center, the final step is to add and configure its managed devices so they can begin to handle network traffic and report events to the Defense Center.

First, use the Version 5.2 Defense Center's web interface to add and configure the devices, including applying licenses, adding interfaces to zones, and applying the policies created and updated by the migration. For more information, see Completing Your Version 5.2 Deployment, page 4-33.

Then, place the freshly set up Version 5.2 devices (including the virtual device) inline so they can begin handling traffic.

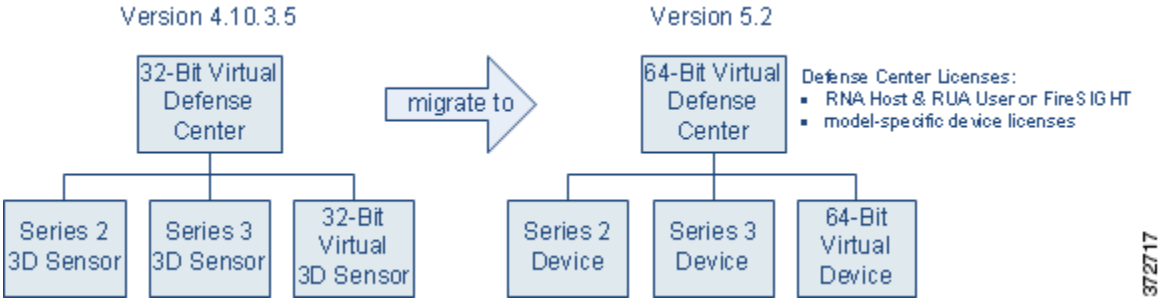
Migrating a Deployment with a Virtual Defense Center

Supported Devices: Any

Supported Defense Centers: virtual

In the scenario described in Migrating a Simple Multi-Sensor Deployment, page 2-3, we replace a Version 4.10.3 Series 2 Defense Center with a Version 5.2 Series 3 Defense Center. Now, change the scenario to include a Version 4.10.3 virtual Defense Center.

The migration process is almost identical, because you must replace virtual appliances. If you want to use a virtual Defense Center to manage your Version 5.2 deployment, you must create a new 64-bit virtual Defense Center just as you must create a new virtual device.



Keep in mind that Version 5.2 packages 64-bit virtual appliances only for the VMware ESX/ESXi hosting environment. For more information on the requirements for the hypervisor host, as well as information on creating and setting up virtual appliances, see the Version 5.2 *Sourcefire 3D System Virtual Installation Guide*.

So that this migrated deployment can behave equivalently with your Version 4.10.3 deployment, you must install the following licenses on the Version 5.2 virtual Defense Center:

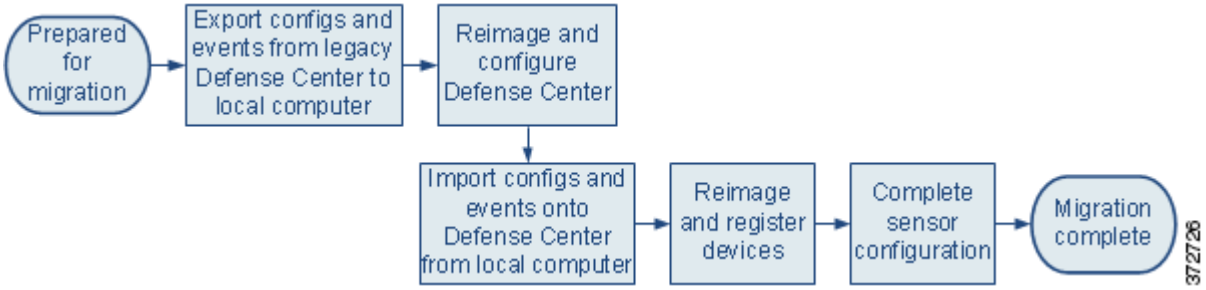
- a FireSIGHT license, which replaces the RNA Host and RUA User licenses

Tip If you assign the same MAC address to the Defense Center's management interface that you used in Version 4.10.3, you can use your existing RNA Host and RUA User licenses. If you cannot use the same MAC address for the management interface (for example, the Version 4.10.3 Defense Center's MAC was dynamically assigned), you must obtain a new FireSIGHT license.

- model-specific Protection licenses for both the Series 3 and the virtual devices

You do not need a license for the Series 2 device; these devices automatically have most Protection capabilities. However, you do need a Threat & App (TA) subscription.

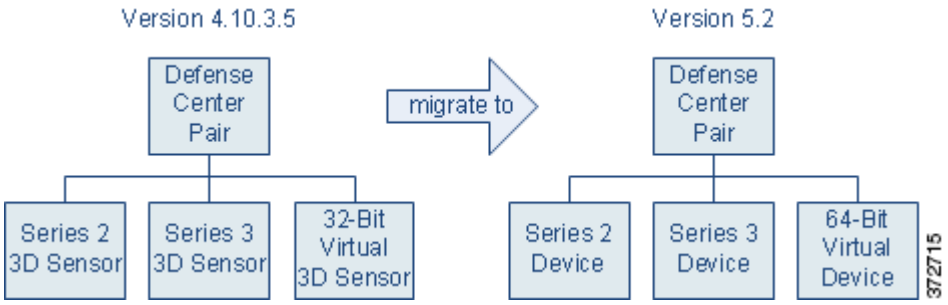
After you create and configure the replacement virtual Defense Center, you can copy configuration and event packages directly from one Defense Center to the other, then migrate the devices from the Version 4.10.3 deployment to the Version 5.2. Finally, if you want to migrate events, you can do it at the end of the process when it causes the least disruption.



Migrating High Availability Defense Center Pairs

Supported Defense Centers: DC1000, DC1500, DC3000, DC3500

Consider the simple scenario at the beginning of the chapter, Migrating a Simple Multi-Sensor Deployment, page 2-3, where you migrated a simple deployment of a Defense Center managing three 3D Sensors from Version 4.10.3 to Version 5.2, while also replacing the Defense Center. Now, replace the Version 4.10.3 Defense Center with a high availability pair of Defense Centers.



How you migrate a deployment that includes a high availability pair of Defense Centers depends on whether you have a replacement Defense Center or Defense Centers. Replacing both Defense Centers in the pair is the bast way to minimize downtime, and the only way to ensure that you maintain Defense Center redundancy at all times. If you do not have the resources to replace both Defense Centers, you can minimize downtime while sacrificing redundancy by using one of the pair as a temporary replacement Defense Center.

Note Cisco **strongly** recommends that both Defense Centers in a high availability pair be the same model. Do **not** replace only one member of a pair with a different model.

Regardless of your method, keep in mind that Defense Centers in a high availability pair do not share licenses. You must obtain equivalent licenses for each member of the pair. So that this migrated high availability deployment can behave equivalently with your Version 4.10.3 deployment, you must install the following licenses on **both** Version 5.2 Defense Centers in the high availability pair:

- either a new FireSIGHT license (replacing the Defense Centers), or your RNA Host and RUA User licenses from Version 4.10.3 (using the same Defense Centers)

The RNA and RUA licenses function identically to the newer FireSIGHT license. You can obtain a FireSIGHT license for reimaged Defense Centers, but it is not required. For more information, see Host and User Licenses, page 1-4.

- model-specific Protection licenses for both the Series 3 and the virtual devices

You do not need a license for the Series 2 device; these devices automatically have most Protection capabilities. However, you do need a Threat & App (TA) subscription.

For more information, see the following sections:

- Replacing Paired Defense Centers, page 2-26
- Migrating an Existing High Availability Pair of Defense Centers, page 2-26

Replacing Paired Defense Centers

Supported Defense Centers: DC1000, DC1500, DC3000, DC3500

To replace both Defense Centers, use the same basic process described in Migrating a Simple Multi-Sensor Deployment, page 2-3, except instead of a single replacement Defense Center, configure a high availability pair of Version 5.2 Defense Centers.

After you prepare for the migration, create the exportable configuration package on the Version 4.10.3 primary Defense Center and copy it to the Version 5.2 primary where you can import them. The system automatically synchronizes the configurations after import. After you migrate configurations, migrate sensors, again from primary to primary.

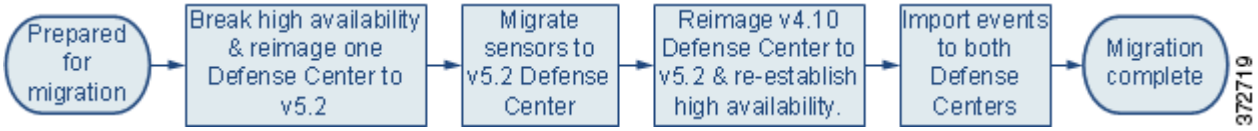
Note In most cases, when you reimage sensors for a high availability deployment, you can register and add the freshly configured Version 5.2 devices to only the primary Defense Center, and the system will synchronize. However, in some high availability deployments where network address translation (NAT) is used, you may need to explicitly register the device to the secondary. For more information, contact Support.

Optionally, migrate events. Unlike configurations, events are not synchronized between Defense Centers. If you want to migrate legacy events as part of your process, make sure you install the event migration scripts on both Version 5.2 Defense Centers in the replacement pair so that you can import legacy events to each one.

Migrating an Existing High Availability Pair of Defense Centers

Supported Defense Centers: DC1000, DC1500, DC3000, DC3500

If you do not have the resources to replace both Defense Centers, you can complete the migration of a high availability pair using the same basic process described in Migrating a Simple Multi-Sensor Deployment, page 2-3, and using one of the pair as the replacement Defense Center, as shown in the following diagram. Note that the drawback to this scenario is that redundancy is not maintained during the process.



First, before you begin migrating configurations, disable high availability while leaving the management of the sensors active on one of the Defense Centers. Then, reimage the Defense Center that is no longer managing sensors to Version 5.2 and migrate all the sensors to that freshly reimaged Defense Center.

Reimaging results in the loss of almost all configuration and event data on the appliance. Although the restore utility can retain the appliance's license, network, console, and Series 3 Lights-Out Management (LOM) settings, you must perform all other setup tasks after the reimage process completes.

Tip Reimage the Defense Center that you want to act as your primary Defense Center first. If you want to continue using the same Defense Center as your primary, switch your Version 4.10.3 Defense Centers' roles before you disable high availability. This allows the secondary Defense Center to manage the Version 4.10.3 deployment while you reimage the primary to Version 5.2.

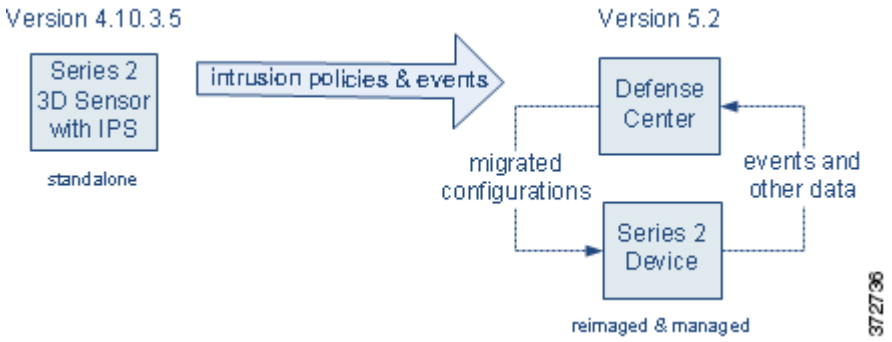
After you migrate all the sensors to the Version 5.2 Defense Center, you can reimage the remaining Version 4.10.3 Defense Center and re-establish the high availability pair using the Version 5.2 web interface. After the migrated configurations automatically synchronize, you can import legacy events onto both Defense Centers (events are not synchronized).

Migrating Standalone 3D Sensors with IPS

Supported Devices: Series 2

Standalone Series 2 3D Sensors used as an intrusion detection and prevention system (IPS) are not supported in Version 5.2. All devices must be managed by a Defense Center, and almost all configuration and analysis functions are restricted to the Defense Center. Only essential administrative and monitoring functions are available on the managed device's web interface.

If you have a standalone Version 4.10.3 3D Sensor, you can migrate its intrusion policies and events to a Version 5.2 Defense Center. After you reimage the 3D Sensor to Version 5.2, either manually or using the sensor migration script, you can manage it with that Defense Center.



In Version 5.2, intrusion detection and prevention is integrated with access control. Instead of using the local web interface to manage a 3D Sensor with IPS and apply intrusion policies directly to detection engines, in Version 5.2 you use the Defense Center to apply access control policies to managed devices. Access control policies contain rules that determine which intrusion policy handles which traffic.

The migration process for a standalone sensor creates an access control policy on the managing Defense Center that, when applied to the migrated device, handles traffic in the same way (with a very few exceptions) as it did in Version 4.10.3.

Reimaging results in the loss of almost all configuration and event data on the sensor. The restore utility can retain the sensor's network and console settings, and the sensor migration script registers sensors and copies (but does not apply) interface configurations. However, you must perform all other setup tasks after the restore process completes.

Note Inline interfaces **fail closed** during the reimage when you do not use the sensor migration script, or you use the script and the interfaces are not configured to fail open. In these cases, you may want to remove the sensors from your critical network path during reimage, which may require physical access to the sensors.

When you do not use the sensor migration script, physical access is required to reimage Series 2 sensors, even those deployed passively; the standard Series 2 restore utility is distributed on an external USB drive.

You do not need any additional licenses to manage previous standalone 3D Sensors with IPS; sensors with that capability are all Series 2, which automatically have most Protection capabilities in Version 5.2.

Tip After migration, former standalone Series 2 devices can also report network discovery information to their managing Defense Center.

To migrate a standalone 3D Sensor:

Access: Admin

Step 1 Make sure you have a Version 5.2 Defense Center prepared to manage the sensor and import configurations and events.

The Defense Center can be part of your existing deployment, or can be purchased new and freshly configured. For more information, see Preparing for Migration, page 3-1.

Step 2 On the sensor, run an export script to create a package of supported configurations; see Exporting Configurations from a Version 4.10.3 Appliance, page 4-3.

The export script analyzes the configurations and lists those that cannot be migrated (cleanly or otherwise) to Version 5.2.

Note Cisco recommends exiting the script to resolve any issues with configurations essential to your deployment. If you continue without resolving the issues, some configurations will not be migrated, though you may be able to resolve specific issues during the import process. This is especially important because you are reimaging the sensor. For more information, see Addressing Configuration Incompatibilities, page 3-7.

Step 3 On the sensor, run an export script to create a package of intrusion and audit events; see Exporting Events from a Version 4.10.3 Appliance, page 4-6.

Step 4 Copy the configuration and event packages from the Version 4.10.3 3D Sensor to the Version 5.2 Defense Center.

Step 5 On the Defense Center, run a script to import configurations; see Importing Configurations onto a Version 5.2 Defense Center, page 4-7.

The script analyzes the configurations and, like the export script, lists those that cannot be migrated. It also gives you the opportunity to resolve any correctable issues with the imported configurations, such as detection-engine specific settings that do not migrate cleanly to Version 5.2. You also must specify some basic information for your Version 5.2 deployment, such as security zones and basic access control settings.

Step 6 On the Defense Center, run a script to import events; see Importing Events onto a Version 5.2 Defense Center, page 4-20.

The script analyzes the package and displays the disk space required to import the events. You can abort the import if the events require too much space, otherwise continue to import the events.

Step 7 Verify the successful migration of your configurations and events.

For information on what to expect from migrated and new configurations, see Understanding Migrated Configurations and Events, page 5-1.

Step 8 If the Version 4.10.3 sensor is inline and is not configured to fail open, remove it from the network path so that traffic can continue to flow while you reconfigure your deployment.

Step 9 Reimage the sensor to a Version 5.2 managed device, either manually or using the sensor migration script and, if you did not use the sensor migration script, perform the initial setup.

For more information on manually reimaging sensors, see the Version 5.2 *Sourcefire 3D System Installation Guide*. For more information on reimaging and registering sensors using the sensor migration script, see Reimaging and Registering Devices with the Sensor Migration Script, page 4-22.

Step 10 If you manually reimaged the device, use the Version 5.2 Defense Center's web interface to manually add the device, configure its interfaces, and apply the interface configurations.

For more information, see Manually Adding Version 5.2 Devices to the Defense Center, page 4-31.

Step 11 For all devices, use the Version 5.2 Defense Center's web interface to apply the policies created and updated by the migration.

For more information, see Completing Your Version 5.2 Deployment, page 4-33.

Step 12 If you removed the device from the network path before reimaging it, place it inline so it can begin handling traffic.