Preparing for Migration

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. After you read Understanding the Migration Process, page 2-1 and outline how and in which order you will migrate your appliances, you can begin preparing your appliances for the migration.

Note Cisco® Security Migration Services can help you migrate from their current security environment to a more innovative security infrastructure that provides proactive ongoing protection. Contact your Cisco representative to learn more or order Cisco Security Migration Services. See Cisco® Security Migration Services, page 1-2.

Although Cisco recommends that you perform the migration in a maintenance window or at a time when the interruption will have the least impact on your deployment, the migration process can take a significant amount of time. You can minimize disruption by thoroughly preparing, but it is unlikely you will be able to avoid it completely.

For physical appliances that you reimage to Version 5.2, you should make sure that once you start the reimage process, you have the resources and information you need to finish quickly and add the appliance to your new deployment.

If you replace a physical appliance or re-create a virtual appliance, you should **fully** set up the new appliance and **completely** prepare it to become part of your Version 5.2 deployment **before** you begin running migration scripts, changing cabling, or performing any other action that could disrupt your current deployment.

Caution Failure to correctly prepare your appliances for migration could cause a longer than expected disruption to your deployment during the migration.

For more information on preparing appliances for migration, see:

- Appliance, Version, and License Requirements, page 3-2 details the prerequisites that appliances must meet for you to perform successful migration.
- Time and Physical Access Requirements, page 3-5 explains the importance of setting aside enough time for the migration and obtaining physical access to any appliances that require it for reimage, installation, or recabling.
- Traffic Flow and Inspection During the Migration, page 3-6 explains how migrating your deployment can affect your organization's inspection capabilities and traffic flow.

- Addressing Configuration Incompatibilities, page 3-7 explains which Version 4.10.3 configurations cannot be migrated, cleanly or otherwise, to Version 5.2, and how you can fix many of these incompatibilities before you begin the process.
- Obtaining and Installing Migration Packages, page 3-12 explains how and where to obtain and install the migration scripts.

Appliance, Version, and License Requirements

Part of planning and preparing to migrate your deployment is to ensure that your current appliances and configurations are supported in Version 5.2. If they are not, your plan must account for any necessary adjustments, including hardware or virtual appliance hypervisor host replacements. For information on replacing your appliances, including an evaluation of your current and future performance needs, contact Sales.

Before you begin, you must also make sure that any existing or replacement appliances are running migration-compatible versions of the system, you have the correct licenses, and so on. Finally, you must download and install the migration scripts.

For more information on preparing your appliances for migration, see:

- Supported Appliances, page 3-2
- Supported Source and Destination Versions for the Migration, page 3-3
- SEU and Intrusion Rule Update Requirements, page 3-3
- Version 5.2 License Requirements, page 3-4
- Disk Space Requirements, page 3-5
- Configuration and Event Backup Guidelines, page 3-5

Supported Appliances

Version 5.2 is supported on all physical appliances that support Version 4.10.3. In addition, you can host 64-bit virtual appliances on VMware vSphere Hypervisor 5.0 and 5.1 as well as VMware ESX/ESXi 4.1.

The following configurations and appliances are **not** supported with Version 5.2:

- DC3000 and DC3500 appliances deployed as Master Defense Centers
- 32-bit virtual appliances or the Xen Hypervisor or RHEV hosting environments
- Crossbeam (Cisco NGIPS for Blue Coat X-Series) devices

Tip Although Version 5.2 does not support Crossbeam (Cisco NGIPS for Blue Coat X-Series) devices, support for these devices returned with the release of Version 5.3. If your Version 4.10.3 deployment includes a Crossbeam software sensor, and you plan to upgrade to Version 5.3 or later after completing the migration, remove the sensor from the network, reimage it to Version 5.3 or later, and redeploy it in the migrated and upgraded network. For information on installing Version 5.3 or later on Cisco NGIPS for Blue Coat X-Series devices, see the *Crossbeam Installation and Configuration Guide* and the *Sourcefire 3D System Release Notes* for the version you install.

A migrated Version 5.2 deployment will function nearly equivalently to the corresponding Version 4.10.3 deployment, depending on the configurations you migrate. However, depending on the specific models of those appliances, you may not be able to take advantage of all the new features in Version 5.2 due to resource and architecture limitations.

Supported Capabilities by Appliance Model, page 1-26 matches the major capabilities of the Version 5.2 system with the appliances that support those capabilities, assuming you have the correct licenses installed and applied. For information on replacing your appliances, contact Sales.

Tip Although you must recreate all your virtual appliances in a 64-bit hosting environment, you can migrate legacy configurations and events to those new Version 5.2 appliances. For information on creating a new virtual appliance, including operating environment prerequisites and other details, see the Version 5.2 *Sourcefire 3D System Virtual Installation Guide*.

Supported Source and Destination Versions for the Migration

You can use the **export scripts** to export configurations and events from any physical or virtual appliance running **Version 4.10.3.x (patch 4.10.3.5 or later)**.

You can use the **import scripts** to import configurations and events onto any physical or virtual Defense Center running **Version 5.2.0.x** of the system.

You can run the **sensor migration script** from any physical or virtual **Version 5.2.0.x** Defense Center to migrate any physical **Version 4.10.3 (or a later patch)** Series 2 or Series 3 sensor on your network to Version 5.2; this includes standalone sensors, unregistered sensors, and sensors registered to physical or virtual Defense Centers.

Tip You can run the sensor migration script from a Version 5.3 Defense Center if you update the Defense Center from Version 5.2.0.x after installing the script. You cannot install the script directly on a Version 5.3 Defense Center. For example, if you want to manage Version 5.3 devices while migrating sensors, you must install the sensor migration package on your Version 5.2.0.x Defense Center before updating it to Version 5.3.

For information on updating appliances to the correct version of the system see the release notes. If you are replacing physical appliances or if your deployment includes virtual appliances (which you must re-create), see the Version 5.2 *Sourcefire 3D System Installation Guide* or the Version 5.2 *Sourcefire 3D System Virtual Installation Guide* for information on setting up new appliances.

SEU and Intrusion Rule Update Requirements

The Vulnerability and Research Team (VRT) releases Security Enhancement Updates (SEUs) to update intrusion rules and other features for Version 4.10.3. For Version 5.2, the VRT releases corresponding and comparable intrusion rule updates, also called SRUs.

The documentation accompanying each SEU identifies the corresponding rule update, and vice versa. For example, documentation for rule update 2013-08-21-001 includes the text:

```
Corresponding SEU number: 943
```

and documentation for SEU 943 includes the text:

```
Corresponding SRU number: 2013-08-21-001
```

To complete a successful migration, the SEU on the exporting Version 4.10.3 appliance **must** match the rule update on the importing Version 5.2 Defense Center. If you try to import configurations or events onto a Version 5.2 Defense Center using a package created on a Version 4.10.3 appliance running a non-matching SEU, the import fails. Note that if the documentation for your SEU or rule update does not list the corresponding partner, you **cannot** use that SEU or rule update and must import a newer one.

To ensure that the SEU and rule update match and are up-to-date, Cisco recommends that you install the latest SEU/rule update on the appliances involved in your migration, that is, on:

- **all** Version 4.10.3 standalone 3D Sensors and Defense Centers from which you plan to export configurations and events; make sure you reapply all affected intrusion policies after you update the SEU
- **all** Version 5.2 Defense Centers onto which you plan to import

For detailed instructions on importing SEUs and rule updates, see the Updating System Software chapter in the Version 5.2 *Sourcefire 3D System User Guide*.

Version 5.2 License Requirements

Version 5.2 uses a different licensing scheme than Version 4.10.3. In Version 5.2, you use the Defense Center to control licenses for itself and the devices it manages, and most licenses from previous releases are **not** supported; see Licensing, page 1-4.

At the time determined by your migration plan, add any new licenses to the appropriate Defense Centers. If you are setting up a new or reimaged physical Defense Center or a re-created virtual Defense Center, you can add licenses as part of the Version 5.2 appliance's setup process. Otherwise, you can use the Defense Center's web interface to add licenses. For more information on reimaging and setting up a new appliances, see the Version 5.2 *Sourcefire 3D System Installation Guide* or the Version 5.2 *Sourcefire 3D System Virtual Installation Guide*; for information on adding licenses to the Defense Center after initial setup, see the Version 5.2 *Sourcefire 3D System User Guide*.

Note Your migration plan should include adding the appropriate licenses to your Version 5.2 Defense Center **before** you begin importing configurations, events, or devices. This means that **before** you begin the migration process, contact Sales for the licenses you need so that your Version 5.2 deployment can behave equivalently to your Version 4.10.3 deployment.

The following table describes which new licenses you need, if any, to migrate your deployment. Depending on your appliances, you can license additional capabilities after you complete the migration process.

Table 3-1 Licenses Required for Successful Migration

Type	Appliance	Required Licenses in Version 5.2
any	3D Sensor with RNA (managed)	none
Series 2	3D Sensor with IPS, either managed or standalone	none
Series 3 virtual	3D Sensor with IPS (managed)	Contact Sales for **new** model-specific **Protection** licenses to install on the managing Version 5.2 Defense Center.

Table 3-1 Licenses Required for Successful Migration (continued)

Type	Appliance	Required Licenses in Version 5.2
Series 2 Series 3	**replacement** Defense Center	Contact Sales for a **new FireSIGHT** license.
Series 2 Series 3	**reimaged** Defense Center	You can use legacy RNA Host and RUA User licenses instead of a FireSIGHT license.
virtual	**replacement 64-bit** Defense Center	Contact Sales for a **new FireSIGHT** license, unless you can assign the same MAC address to the new Defense Center's management interface that you used in Version 4.10.3. In that case, 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

Disk Space Requirements

Event packages created by the migration can be large. When you run the export event script, the export fails if there is not enough space on a Version 4.10.3 appliance to create the package. Before trying again, you should free space on the appliance by deleting extraneous events, saved backup files, and so on.

Similarly, when you import events onto a Version 5.2 Defense Center, the import script warns you if you do not have enough disk space on the Defense Center to import the events in the package. Do **not** proceed if there is not enough disk space for the import; the import will fail. Before trying again, you should free space on the appliance.

Configuration and Event Backup Guidelines

Before you begin the migration process, Cisco **strongly** recommends that you back up current event and configuration data for your Version 4.10.3 deployment to an external location. Reimaging an appliance to Version 5.2 results in the loss of almost **all** configuration and event data on the appliance

When possible, use the Defense Center to back up event and configuration data for itself and the sensors it manages. For more information on the backup and restore feature, see the Version 4.10.3 *Sourcefire 3D System User Guide*.

Time and Physical Access Requirements

Depending on the size of your deployment and the scope of your plan, the migration process can take a significant amount of time, especially if you need to reimage multiple appliances.

You can minimize disruption by thoroughly preparing, but it is unlikely you will be able to avoid it completely. Cisco **strongly** recommends you perform the update in a maintenance window or at a time when the interruption will have the least impact on your deployment.

Caution Failure to plan and prepare could cause a longer than expected disruption to your deployment during the migration.

Additionally, it is possible that you will need physical access to some or all of the appliances in your deployment during the migration process, depending on your appliance models, locations, and method of migration.

If you are replacing physical appliances, you must be able to install the new appliances and remove the old ones. If you are using the sensor migration script to reimage sensors, physical access is not required. If you are manually reimaging any appliances, all Series 2 appliances require physical access, as described in the following table.

Table 3-2 Manual Reimage Requirements by Appliance Model

Models	Physical Access Required to Manually Reimage?
DC1000 DC3000	**yes**, to boot from and load a restore CD that contains the ISO image
DC500 all Series 2 devices	**yes**, to boot from a USB drive that contains the restore utility
Series 3 appliances	**no**; if you have a remote KVM switch (all) or LOM (Series 3), you can remotely reimage by booting from an internal flash drive

Additionally, reimaging an inline sensor that is not configured to fail open causes it to fail closed until you register the reimaged devices to a Defense Center and reconfigure the device's interfaces. Disconnecting inline sensors that are not configured to fail open from your critical network path during a reimage—which can take a significant amount of time—allows traffic to continue to flow, albeit uninspected.

Also, keep in mind that some migration methods require more extended physical access to your appliances than others. For example, if you have a spare device to act as a swap, you can perform a "rolling" migration that replaces each Version 4.10.3 sensor in turn. 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.

By giving you an overview of the migration process for a basic scenario, then describing common variations that may apply to your deployment, Understanding the Migration Process, page 2-1 can help you choose a migration method, and therefore the kind and duration of physical access you need to your appliances during the process.

Traffic Flow and Inspection During the Migration

The migration process can also affect your organization's inspection capabilities and traffic flow, especially if your plan involves reimaging your physical devices. In most cases, your available resources will dictate your course of action. You can minimize disruption by thoroughly preparing and carefully choosing a migration process, each of which has pros and cons. For more information on these and other strategies, see Understanding the Migration Process, page 2-1.

Reimaging Physical Devices: More Interruption

Reimaging physical devices 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.

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.

Replacing Devices: Less Interruption

Replacing physical devices minimizes 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.

Because you must re-create virtual devices, traffic flow in a virtual deployment should only be interrupted while you redirect traffic to your new virtual devices.

Rolling Migration: Compromise

A "rolling" migration represents a compromise that replaces each sensor in turn. You 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 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.

Addressing Configuration Incompatibilities

The goal of the migration is that your Version 5.2 migrated deployment behaves equivalently to your Version 4.10.3 deployment. However, there are some configurations that cannot be migrated to Version 5.2 because of deprecated functionality or functionality changes.

For your convenience, the configuration export script analyzes the exportable configurations on the appliance and lists the issues it finds. For each incompatibility, the script indicates the consequences of continuing without resolving the issue, and also lists possible solutions or workarounds. Note that you may be able to resolve some—but not all—incompatibilities when you import configurations onto the Version 5.2 Defense Center.

Note If the script identifies issues, exit and resolve all critical incompatibilities before you perform a final configuration export.

Your final export from Version 4.10.3 should list only those issues that you have decided not to correct, because:

- you want to recreate specific configurations in Version 5.2,
- you do not want to migrate specific configurations, or
- you plan to resolve specific configuration conflicts when you import the package onto the Version 5.2 Defense Center (not an option for all incompatibilities)

Then, when you import a configuration package into Version 5.2, the import script again warns you of configurations in the package that cannot be migrated. If you cannot or do not want to restart the process to fix any unanticipated issues, you should have a thorough understanding of which configurations will not be migrated and why, so that you can recreate them later if necessary.

The scripts can identify, and sometimes resolve, the following migration issues:

Multiple Same-Type Detection Engines Using One Interface Set

In Version 4.10.3, you could monitor one interface set with multiple IPS (or RNA or RUA) detection engines. This would allow you to, for example, analyze the same traffic with multiple intrusion policies.

Version 5.2 does not support this capability. Now, you apply one access control policy to a device. In that access control policy, if traffic matches an access control rule you can analyze it with one intrusion policy; if it matches no rules, you can analyze it with a different intrusion policy (the default action policy).

To resolve this issue before you export Version 4.10.3 configurations, modify your deployment so that only one of each type of detection engine uses each interface set. For instructions, see the Using Detection Engines and Interface Sets chapter in the Version 4.10.3 *Sourcefire 3D System User Guide*.

If you export Version 4.10.3 configurations where more than one IPS or RNA detection engine monitored the same interface, the configuration import script prompts you to choose one; for more information, see Assigning One Detection Engine of Each Type to Interface Sets, page 4-10.

Choosing an RNA or IPS detection engine uses the policy that was applied to that detection engine as a basis for your Version 5.2 configurations. Although it is unlikely that you were using more than one RUA detection engine to monitor the same traffic (because there was no advantage to doing so), the script automatically chooses just one of them to use for Version 5.2.

Intrusion Policy Proliferation Due To Custom Variables

In the Sourcefire 3D System a variable is a representation of a port or network value that is commonly used in intrusion rules. Rather than hard-coding these values in multiple rules, to tailor a rule to accurately reflect your network environment, you can change the variable value.

In Version 4.10.3 you could configure custom variables for IPS detection engines, which had priority over intrusion policy-specific variables which, in turn, had priority over system variables. With Version 5.2, you no longer explicitly configure detection engines or detection engine variables; however, you still can configure policy-specific variables, which still have priority over system variables. However, this means that you cannot cleanly migrate a Version 4.10.3 intrusion policy applied to IPS detection engines that use custom variables.

To replicate Version 4.10.3 functionality and migrate custom detection engine variables, the import script can create a copy of the intrusion policy for each detection engine that uses custom variables. These copies use the original intrusion policy as the base policy; each one has different policy-specific variables that correspond to one of the Version 4.10.3 custom variable sets.

Because this can result in a proliferation of intrusion policies, the import script prompts you whether to create the copies; see Creating Intrusion Policies For Custom Detection Engine Variables, page 4-11. For details on how custom detection engine variables appear after they are migrated, see Migrating Detection Engine Variables Into Policy Variables, page 5-7.

To resolve this issue before you export Version 4.10.3 configurations, make sure you do not use IPS detection-engine variables. Your solution may be to create a copy of the intrusion policy for each detection engine that uses custom variables, just as the import script would. Or, you can delete detection engine variables if you do not plan to need them in your Version 5.2 deployment. For instructions, see the Using Detection Engines and Interface Sets chapter in the Version 4.10.3 *Sourcefire 3D System User Guide*.

Errors Due to Unavailable Policies

You can only migrate intrusion policies that were created on (or imported onto) a Version 4.10.3 appliance, that currently exist on the appliance, and that are currently applied to IPS detection engines. Similarly, you can only migrate settings from RNA detection policies, RNA-related settings in system policies, and PEP policies if they exist (and if necessary, are applied) on an exporting Version 4.10.3 Defense Center.

You **cannot** migrate the following:

- a remotely-authored intrusion policy, that is, an intrusion policy that is applied to an IPS detection engine from an appliance other than the one from which you are exporting configurations
- applied-then-deleted intrusion polices
- settings from applied-then-deleted policies: PEP, system, and RNA detection policies
- occasionally, settings from applied-then-modified system policies

Both the configuration export and import scripts warn you that these policies and settings will not be migrated, and give you a chance to exit the script. Not importing these configurations can cause the omission of rules and other important settings from the new access control policy and the network discovery policy on the Version 5.2 Defense Center.

Note, however, that the migration attempts to resolve unavailable and conflicting system policy settings in the following ways:

- If another version of the currently applied system policy exists on the Version 4.10.3 Defense Center (for example, you modified the policy since you last applied it and a saved revision exists), the migration uses the settings in the saved revision.
- If you deleted the currently applied system policy, the migration uses the existing settings on the Version 5.2 Defense Center that the configuration import script would otherwise overwrite; see Understanding How RNA and RUA Settings Are Migrated, page 5-13.

To resolve this issue before you export Version 4.10.3 configurations, apply the policies that you want to migrate to the appropriate sensors, detection engines, or interface sets. Note that you do not have to apply compliance policies. For instructions, see the Version 4.10.3 *Sourcefire 3D System User Guide*.

RNA Port Exclusion Issues

In Version 4.10.3, you configured host discovery and flow data logging in RNA detection policies, and could easily exclude a port associated with a specific IP address from having its sessions logged.

In Version 5.2, logging and monitoring functionality is split: the access control policy governs which connections (flows) are logged on a per-access-control-rule basis, but the network discovery policy governs host discovery. Access control rules also define the traffic that you allow, and only traffic that you allow (as opposed to outright block or trust) can be monitored with discovery or subject to an intrusion policy.

To exclude traffic to and from a specific host from connection logging while preserving logging and inspection for other hosts, the script must create multiple access control rules for combinations of intrusion inspection and port exclusion preferences; see Migrating RNA Settings into Rules and Logging Preferences, page 5-7.

If your Version 4.10.3 RNA detection policies specified **Source/Destination** ports to exclude, the import scripts prompts you to choose whether to create these extra rules in the new access control policy, for example. To avoid a confusing proliferation of rules, the default option is to create the access control policy without them.

However, you cannot migrate source-only or destination port exclusions. If your Version 4.10.3 RNA detection policies specifies either **Source** or **Destination** ports to exclude, the script warns you that these configurations will not be migrated.

To resolve these issues before you export Version 4.10.3 configurations, modify the port exclusions in your RNA detection policies, then reapply the polices. For instructions, see the Introduction to Sourcefire RNA chapter in the Version 4.10.3 *Sourcefire 3D System User Guide*.

Tip For information on configuring port exclusions in Version 5.2 using discovery rules, see the Introduction to Network Discovery chapter in the Version 5.2 *Sourcefire 3D System User Guide*.

Unsupported RNA and RUA Fast-Path PEP Rules

Version 4.10.3 PEP rules with an action of **Fast Path** are migrated to Version 5.2 as access control rules that trust the specified traffic. For information on how other types of PEP rule are migrated, see Migrating PEP Rules into Access Control Rules, page 5-3.

Because of the way Version 5.2 access control rules handle traffic, you cannot configure traffic to bypass discovery (RNA or RUA) but still be analyzed by an intrusion policy (IPS). Therefore, Version 4.10.3 RNA and RUA fast-path PEP rules **cannot** be migrated unless you also fast-path IPS.

To resolve this issue before you export Version 4.10.3 configurations, delete or modify unsupported PEP rules. For instructions, see the *Using PEP to Manage Traffic* chapter in the Version 4.10.3 *Sourcefire 3D System User Guide*.

If you export these Version 4.10.3 PEP rules, the configuration import script prompts you to resolve the issue by either deleting the configuration, bypassing intrusion inspection only, or bypassing all inspection. You **cannot** migrate the PEP rule as-is. For more information, see Resolving Unsupported RNA and RUA Fast-Path PEP Rules, page 4-12.

Unsupported Conditions in Compliance Rules and Traffic Profiles

In Version 5.2, the Policy & Response and compliance features are known as *correlation features*. You can successfully migrate most compliance policies and rules to Version 5.2 correlation policies and rules; see Understanding Migrated Compliance Policies and Rules, page 5-18. Most traffic profiles also migrate successfully.

The Policy & Responses configurations that you **cannot** migrate are detailed in the following table. Both the configuration export and import scripts warn you that these configurations will not be migrated, and give you a chance to exit the script.

Table 3-3 Unsupported Conditions in Compliances Rules and Traffic Profiles

You cannot migrate a...	Where...	Because...
compliance rule	**an RNA event occurs** using a **Detection Engine** constraint	the migration script cannot create a Version 5.2 discovery-based correlation rule using a **Device** constraint until you add devices to the Defense Center, which you do after you run the import script.
compliance rule	**an RNA event occurs** or **a flow event occurs** using an **Application Type** or **Payload Type** constraint	in Version 5.2, you cannot trigger correlation rules based on application categories and tags, which are the Version 5.2 analogs for application and payload types.
traffic profile	a host profile qualification using a **Client Application** constraint where you specify one or more **Application Type** (other than **any**)	in Version 5.2, you cannot track connections based on application categories and tags, which are the Version 5.2 analogs for application and payload types.
traffic profile	a host profile qualification using a **Client Application** constraint where you specify an **Application** of **any**	in Version 5.2, you cannot track connections based on a **Client** of any; you must explicitly choose one or more client applications.

To resolve these issues before you export Version 4.10.3 configurations, you must modify your compliance rules and traffic profiles so that they no longer use the unsupported conditions. For instructions, see the Configuring Compliance Policies and Rules and Working With Flow Data and Traffic Profiles chapters in the Version 4.10.3 *Sourcefire 3D System User Guide*.

Tip You can re-create discovery-based device-specific correlation rules on your Version 5.2 Defense Center after you complete the migration process.

Intrusion Rules with Ports Have No Service Metadata

In Version 4.10.3, local intrusion rules that inspect traffic only on specified ports do so regardless of the application detected in the traffic. In Version 5.2, for an intrusion rule to inspect application traffic, that rule **must** include a service metadata option for the identified application.

The configuration import script identifies local intrusion rules that have port constraints but no corresponding service metadata, and generates one or more service metadata recommendations based on the rule content. Then, the script prompts you to accept, review, or reject the recommendations; see Adding Service Metadata to Intrusion Rules, page 4-11. Note that you **cannot** use the script to add more than eight metadata entries; the script presents the first eight, alphabetically. You can add additional metadata before or after the migration.

Note Skipping (rejecting) the addition of service metadata will stop the affected intrusion rules from firing until you add service metadata after the migration. For more information, see the Understanding and Writing Intrusion Rules chapter in the Version 5.2 *Sourcefire 3D System User Guide*.

Note that the script does not allow you to review or automatically add service metadata to local intrusion rules that inspect traffic based on port negations; this would be too complex. For these rules to fire, you **must** manually add service metadata after the migration. The script warns you which rules need this manual update.

To resolve these issues before you export Version 4.10.3 configurations, add service metadata to all local intrusion rules that have port constraints, including port negations. For instructions, see the Understanding and Writing Intrusion Rules chapter of your Version 4.10.3 *Sourcefire 3D System User Guide*.

Obtaining and Installing Migration Packages

Cisco delivers migration scripts in appliance-specific packages. To install the scripts, you must install the correct package for your appliance type. The packages include the following scripts:

- An appliance-specific **export package** contains the configuration export script and the event export script.

  You must download and install the export package on every **Version 4.10.3.x (patch 4.10.3.5 or later)** Defense Center or standalone sensor where you want to run the configuration and event export scripts.

- An appliance-specific **import package** contains the configuration import script and the event import script.

  You must download and install the import package on every **Version 5.2.0.x** Defense Center where you want to run the configuration and event import scripts.

- A Defense Center series-specific **sensor migration package** contains the sensor migration script.

  You must download and install the sensor migration package on every **Version 5.2.0.x** Defense Center where you want to run the sensor migration script.

Tip In a high availability deployment, you only need to install the import package on the primary Defense Center, unless you want to import events onto both Defense Centers in the pair.

The following table lists the packages you must install to use the migration scripts on each appliance:

Table 3-4 Migration Script Packages by Appliance

Package Type	Appliance	Package
export	Series 2 Defense Center 32-bit virtual Defense Center	`Sourcefire_3D_DC_Migration_Export_Package-4.10.3.999-`*`build`*`.sh`
export	Series 3 Defense Center	`Sourcefire_3D_Defense_Center_S3_Migration_Export_Package-4.10.3.999-`*`build`*`.sh`
export	standalone Series 2 3D Sensors	`Sourcefire_3D_Sensor_Migration_Export_Package-4.10.3.999-`*`build`*`.sh`

Table 3-4 Migration Script Packages by Appliance (continued)

Package Type	Appliance	Package
export	standalone 3D9900 3D Sensors Note that the 3D9900 is no longer supported; however, you can use this script to export configurations and events from a Version 4.10.3 standalone 3D9900.	`Sourcefire_3D_Sensor_9900_Migration_Export_Package-4.10.3.999-`*`build`*`.sh`
import	Series 2 Defense Center	`Sourcefire_3D_DC_Migration_Import_Package-5.2.0.999-`*`build`*`.sh`
import	Series 3 Defense Center 64-bit virtual Defense Center	`Sourcefire_3D_Defense_Center_S3_Migration_Import_Package-5.2.0.999-`*`build`*`.sh`
sensor	physical Series 2 Defense Center	`Sourcefire_3D_DC_Sensor-Migration-Hotfix-5.2.0.999-`*`build`*`.sh`
sensor	physical Series 3 Defense Center 64-bit virtual Defense Center	`Sourcefire_3D_Defense_Center_S3_Sensor-Migration-Hotfix-5.2.0.999-`*`build`*`.sh`

To install migration packages:

Access: Admin

Step 1 Using the user name and password for your support account, log into the Support Site.

Step 2 Download the appropriate script package from the Support Site.

For information on which package to download, see Table 3-4 on page 3-12.

Caution Download each script package directly from the Support Site. If you transfer a script package by email, it may become corrupted.

Step 3 On each appliance where you need to run a migration script, upload the appropriate script package:

- to upload the export package to a Version 4.10.3 (patch 4.10.3.5 or later) Defense Center or standalone sensor, select **Operations > Update**, then click **Upload Update**. Browse to the package and click **Upload**.
- to upload the import or sensor migration package to a Version 5.2 Defense Center, select **System > Updates**, then click **Upload Update** on the Product Updates tab. Browse to the package and click **Upload**.

Step 4 Click **Install** next to the package you are installing.

The package is installed and the script or scripts are ready to be run. For information on running each script, see Performing the Migration, page 4-1.