
# Performing the Migration

Obtaining and installing migration packages is the last step in preparing for your deployment's migration, as described in Obtaining and Installing Migration Packages, page 3-12. After you install these packages, you can run each script included in the packages at the appropriate time.

**Note** The order in which and appliances where you run migration scripts depends on your migration plan, which is unique to your deployment. Make sure you adhere to your plan by running the migration scripts and performing related tasks in the correct order. In particular: migrating events before you migrate configurations can result in unpredictable event display and behavior; also, the order in which you reimage and register devices depends on whether you reimage using the sensor migration script. For more information on the order in which you should migrate configurations and events in your situation, see Understanding the Migration Process, page 2-1.

The following table lists each script and its function.

***Table 4-1 Migration Scripts***

| Use this script... | To... |
|---|---|
| configuration export: `config_export.pl` | create an exportable package of configurations on a Version 4.10.3 Defense Center or standalone 3D Sensor |
| event export: `event_export.pl` | create an exportable package of intrusion and audit events on a Version 4.10.3 Defense Center or standalone 3D Sensor |
| configuration import: `config_import.pl` | import configurations onto a Version 5.2 Defense Center |
| event import: `event_import.pl` | import events onto a Version 5.2 Defense Center |
| display interfaces: `display_interfaces.pl` | display interface configurations after running the configuration import script; this script is not necessary when you use the sensor migration script, but is useful when you must manually configure interfaces on physical devices that you manually reimaged or virtual devices that you created |
| migrate sensors: `migration_script.pm` | copy Version 4.10.3 (or a later patch) Series 2 and Series 3 physical sensor interface configurations, reimage the sensors to Version 5.2, register them to the Version 5.2 Defense Center where you run the script, and apply the interface configurations |

To run any migration script, you must be logged into the appliance's shell. You must have Administrator access to the appliance and run the script as the root user. For most appliances, you can use SSH to connect to the appliance; for virtual appliances you can also use the virtual console. You can also connect to the Series 3 appliance shell via Lights-Out Management (LOM).

Depending on the script and the options you use to invoke it, you may need to provide input as the script runs. When prompted, either type the requested information or the number corresponding to your choice and press Enter to continue. You can also just press Enter to accept the default, which is displayed in brackets.

For example, the configuration import script asks you to provide a name for the new access control policy created by the import:

```
Enter the new Access Control policy name [Migrated policy]:
```

In this case, you can either type a name for the new policy, or press Enter to accept the default name of `Migrated policy`. Invalid input causes the scripts to re-prompt you for valid input.

**Tip** This chapter explains in detail how to run each of the migration scripts, but you can get basic instructions and syntax by running any of the scripts with the `--help` option; for example: `config_export.pl --help`.

This chapter also provides details on reimaging appliances as part of the migration, and performing the initial setup on those and any replacement appliances you are using in your new Version 5.2 deployment.

For more information, see:



# Logging Into an Appliance to Run Migration Scripts

To run any migration script, you must be logged into the appliance's shell. You must have Administrator access to the appliance and run the script as the root user. For most appliances, you can use SSH to connect to the appliance; for virtual appliances you can also use the virtual console. You can also connect to the Series 3 appliance shell via Lights-Out Management (LOM).

**Note** Before you can run migration scripts using LOM, you must enable the feature on the appliance and install an IPMI utility on your computer. Keep in mind that the syntax of LOM commands depends on the utility you are using. For more information on LOM, including a full list of available commands,

**To log into a Series 3 appliance using Lights-Out Management:**

**Access:** Admin

**Step 1** At your computer's command prompt, enter the IPMI command to start a Serial over LAN (SOL) session and display the prompt for the appliance:

- For IPMItool, type: `ipmitool -I lanplus -H IP_address -U username sol activate`
- For ipmiutil, type: `ipmiutil sol -a -V4 -J3 -N IP_address -U username -P password`

  Where *IP_address* is the IP address of the management interface on the appliance, *username* is the user name of an authorized LOM account, and *password* is the password for that account.

  Note that IPMItool prompts you for the password after you issue the `sol activate` command.

# Exporting Configurations from a Version 4.10.3 Appliance

**Supported Devices:** Series 2

**Supported Defense Centers:** Any

After you prepare for migration, the next step is to export vital configurations from your Version 4.10.3 Defense Centers and standalone 3D Sensors. To export configurations from an appliance, log into its shell and run a script that creates an export package:

- On a standalone 3D Sensor, the package contains information on applied intrusion policies and their associated variables.
- On a Defense Center, the package contains information on applied intrusion policies and their associated variables for all managed sensors, RNA and RUA settings and policies, PEP rules, as well as compliance policies, rules, and traffic profiles.

For more information on exactly what is migrated, see Understanding Migrated Configurations and Events, page 5-1.

When you start the configuration export script, it analyzes the exportable configurations on the appliance and lists any configurations that cannot be migrated, cleanly or otherwise, to Version 5.2. For each incompatibility, the script indicates the consequences of continuing without resolving the issue, and also lists possible solutions or workarounds.

The following table displays the issues the script can detect, and directs you to documentation where you can learn about why the problem exists and what you can do to correct it.

***Table 4-2 Migration Issues Identified by the Configuration Export Script***

| Issue | For more information, see... |
|---|---|
| `Multiple DE_type detection engines are using interface set 'set_name' from sensor sensor_name.` | Multiple Same-Type Detection Engines Using One Interface Set, page 3-8 |
| `Intrusion Policies with customized variable definitions must be created in order to accurately migrate Detection Engine variables.` | Intrusion Policy Proliferation Due To Custom Variables, page 3-8 |

*Table 4-2 Migration Issues Identified by the Configuration Export Script (continued)*

| Issue | For more information, see... |
|---|---|
| The following remotely authored intrusion policies are applied to IPS detection engines:<br><br>These intrusion policies have been deleted but are applied to IPS detection engines:<br><br>The RNA policy applied to '*detection_engine*' on sensor *sensor_name* was deleted and cannot be migrated.<br><br>The PEP policy applied to '*interface_set*' on sensor *sensor_name* was deleted and cannot be migrated.<br><br>The applied System Policy revision cannot be found. The latest revision will be used.<br><br>The applied System Policy cannot be found. Network Discovery settings will use the installed defaults. | Errors Due to Unavailable Policies, page 3-9 |
| These RNA port exclusions are not compatible with network discovery in 5.2.0 because they target either a source network or a destination network (not both source and destination): | RNA Port Exclusion Issues, page 3-10 |
| PEP rules have been found that have an action of 'DE-specific' and are configured to fast path RNA or RUA: | Unsupported RNA and RUA Fast-Path PEP Rules, page 3-10 |
| These compliance rules are not compatible with 5.2.0 because they contain a '*condition_type*' condition.<br><br>These traffic profiles are not compatible with 5.2.0 because they contain a '*condition_type*' condition. | Unsupported Conditions in Compliance Rules and Traffic Profiles, page 3-11 |

If the script identifies issues, Cisco recommends that you exit and resolve all critical incompatibilities before you perform a final export. Your final export should list only those issues that you have decided not to correct, because either you want to recreate the configurations in Version 5.2, or you do not want to migrate those configurations. Note that in some cases, you may be able to resolve some issues during the import process.

Every time you run the script without exiting, it creates a new export package— unless you specify otherwise, a timestamped compressed archive (.tgz) file in the migration directory on the appliance. For example, a file created at 1:14:15 PM on January 1, 2014 would be located at:

```
/var/sf/migration/migration_config_20140101_131415.tgz
```

**Note** Before you run the configuration export script on a Version 4.10.3 Defense Center, make sure that the appliances in your deployment are communicating successfully. If the Defense Center cannot contact one of its managed sensors, it cannot include its interface information in the package.

The following table describes the options you can use with the configuration export script.

*Table 4-3 Configuration Export Script Options*

| Option | Description |
|---|---|
| `--file` | Create a new export package with a specified file name and location, instead of the default. You can use an absolute or relative path, for example:<br>`--file ./export_1/my_export.tgz`<br>`--file /var/sf/migration/export_1/my_export.tgz`<br>If the directory you specify does not exist, the script automatically creates it. Note that if you specify the same name and location as an existing export package, the older package is overwritten. |
| `--help` | Display basic instructions and syntax for running the script. |

**To create an export package of configurations:**

**Access:** Admin

**Step 1** Log into the appliance's shell using an account with Administrator privileges.

For more information, see Logging Into an Appliance to Run Migration Scripts, page 4-2.

**Step 2** Navigate to the migration folder:

```
cd /var/sf/migration
```

**Step 3** Run the export script as the root user, providing your password when prompted:

```
sudo ./config_export.pl
```

Use the `--file` option to specify an alternate location or file name for the export package. For more information on the other options you can use, see Configuration Import Script Syntax and Options, page 4-17.

After you provide your password, the script starts and lists any configuration incompatibilities with the migration:

```
Migration Export Assistant v1.0
SOURCEfire, inc.
============================================================
Analyzing configuration.....................................
The following issues were detected:
```

**Step 4** Read and understand the list of issues, if any.

To cross reference an issue displayed with information on how to correct it, see Table 4-2 on page 4-3.

**Step 5** When prompted, type `y` to continue or `n` to exit the export process, then press Enter.

Cisco recommends exiting the script to resolve any issues with configurations essential to your deployment. If you continue, the script gathers data from the appliance (and, for a Defense Center, its managed sensors), creates the export package, and exits, for example:

```
Do you want to continue the export process? (y/n) [n]: y
Collecting data from sensors...
Gathering data for My_4.10.3_Defense_Center...
Creating migration backup...
Migration export complete!
migration_config_20140101_131415.tgz created.
```

**Step 6** Continue with the next step in your migration plan.

For more information on planning your migration, see Understanding the Migration Process, page 2-1.

# Exporting Events from a Version 4.10.3 Appliance

**Supported Devices:** Series 2

**Supported Defense Centers:** Any

If you are interested in intrusion and audit events generated in your Version 4.10.3 deployment before the migration, you can migrate these legacy events from Version 4.10.3 Defense Centers and standalone 3D Sensors.

To export events from an appliance, log into its shell and run a script that creates an export package, which contains all intrusion events and audit events on the appliance at the time. You can then copy and import the event package onto a Version 5.2 Defense Center.

When you start the script on a Defense Center, it first determines whether you are still managing any sensors and, if so, allows you to exit. Depending on your migration plan, you may actually want to export events and then remove sensors from management (for example, if you are reimaging an existing Defense Center that is managing sensors that you plan to remove from the network path because they would fail closed). However, keep in mind that events reported to the Defense Center after you start the export process are not included in the package. For more information on planning your migration, see Understanding the Migration Process, page 2-1.

Every time you run the script without exiting, it creates a new export package— unless you specify otherwise, a timestamped compressed archive (.tgz) file in the migration directory on the appliance. For example, a file created at 1:14:15 PM on January 1, 2014 would be located at:

```
/var/sf/migration/migration_event_20140101_131415.tgz
```

The following table explains the options you can use with the event export script.

*Table 4-4 Event Export Script Options*

| Option | Description |
|---|---|
| `--file` | Create a new export package with a specified file name and location. You can use an absolute or relative path, for example:<br>`--file ./export_1/my_export.tgz`<br>`--file /var/sf/migration/export_1/my_export.tgz`<br>If the directory you specify does not exist, the script automatically creates it. Note that if you specify the same name and location as an existing export package, the older package is overwritten. |
| `--test` | Runs the script but does not create the event package. This allows you to preview what will happen when you run the final export. |
| `--help` | Display basic instructions and syntax for running the script. |

Note that if there is not enough space on the appliance to create the export package, the export fails. Before you try again, free space on the appliance by deleting extraneous events, saved backup files, and so on.

Also, keep in mind that some fields in intrusion events generated by Version 4.10.3 are different from the fields in Version 5.2 intrusion events, and that the timestamps on migrated events will be “behind” newly generated 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.

**To create an export package of intrusion and audit events:**

**Access:** Admin

**Step 1** Log into the appliance's shell using an account with Administrator privileges.

For more information, see Logging Into an Appliance to Run Migration Scripts, page 4-2.

**Step 2** Navigate to the migration folder:

```
cd /var/sf/migration
```

**Step 3** Run the export script as the root user, providing your password when prompted:

```
sudo ./event_export.pl
```

Use the `--file` option to specify an alternate location or file name for the export package. For more information on the other options you can use, see Table 4-4Event Export Script Options, page 4-6.

After you provide your password, the script starts:

```
Migration Event Export Assistant v1.0
SOURCEfire, inc.
============================================================
```

**Step 4** On a Defense Center that is still managing 3D Sensors, if prompted whether you want to continue the export process, enter `y` to continue or `n` to exit.

```
This DC has at least one sensor attached.
Are you sure you want to export events now? (y/n) [y]:
```

**Step 5** Wait until the export script completes and creates the export package, for example:

```
Dumping mysql tables...
Archiving audit events...
Archiving IS events...
Creating event migration backup...
migration_event_20140101_131415.tgz created.
```

**Step 6** Continue with the next step in your migration plan.

For more information on planning your migration, see Understanding the Migration Process, page 2-1.

# Importing Configurations onto a Version 5.2 Defense Center

**Supported Devices:** None

**Supported Defense Centers:** Any

After you export configurations from your Version 4.10.3 deployment and ready your Version 5.2 Defense Center, your next step is to import the configurations. First, copy a Version 4.10.3 configuration package (see Exporting Configurations from a Version 4.10.3 Appliance, page 4-3) to the new Defense Center. Then, run an interactive script that steps you through the import of the configurations in the package, using a series of checks and requests for input.

You should run the import script once for each configuration package you need to import:

- If you are migrating from a single Version 4.10.3 Defense Center to a single Version 5.2 Defense Center, you should only have one configuration package to import.
- If you are replacing two or more Version 4.10.3 Defense Centers with one Version 5.2 Defense Center, or are adding several former standalone 3D Sensors to a new Defense Center, you must import each configuration package individually.

Before you commit to importing configurations from a specific exported package, you can run the import script using the `--manifest` option to display a detailed list of the Version 4.10.3 configurations in that package. If a review of the manifest reveals anything unexpected, Cisco recommends that you fix critical issues and export a new package from the Version 4.10.3 appliance, if possible. For more information on reviewing the manifest, see Reviewing the Manifest of Exported Configurations, page 4-9.

Also note that when you run the import script, it cleans up information from any previous invocations. If you import multiple configuration packages, each import deletes useful information on how to configure migrated devices associated with previously imported packages. For more information, see Importing Multiple Unique Configuration Packages, page 4-18.

The following sections explain how to run and follow the prompts in the configuration import script:



The following sections provide additional information about the import script:



# Starting the Configuration Import Script

When you start the configuration import script on a Version 5.2 Defense Center, it first compares the intrusion rule update on the Defense Center to the SEU on the Version 4.10.3 appliance where you exported the package. If the rule update and SEU do not match, the script exits without importing any configurations. Cisco **strongly** recommends that you update the SEUs and rule updates in your deployment and restart the migration process. For more information, see SEU and Intrusion Rule Update Requirements, page 3-3.

If you cannot restart the migration process because you have already reimaged the appliance where you exported the package, you can force the script to skip the equivalence check by invoking the script with the `--force` option. In most cases, the resulting imported intrusion configurations will work as expected. If you cannot edit or apply policies after forcing a configuration import, contact Support.

**Note** If this is the second time you plan to run the import script on this Defense Center, **regardless** of whether you are re-importing configurations from the same package or you are importing new configurations from a different package, read the warnings in Importing Configurations Multiple Times, page 4-18.

**To begin importing migrated configurations onto a Version 5.2 Defense Center:**

**Access:** Admin

**Step 1** Copy the package you plan to import to the Version 5.2 Defense Center.

Cisco recommends that you copy all packages to the `/var/sf/migration` directory.

**Step 2** Log into the Defense Center's shell using an account with Administrator privileges.

For more information, see Logging Into an Appliance to Run Migration Scripts, page 4-2.

**Step 3** Navigate to the migration directory:

```
cd /var/sf/migration
```

**Step 4** Run the import script as the root user, providing your password when prompted:

```
sudo ./config_import.pl exported_config_package.tgz
```

where *exported_config_package*.tgz is the package you copied to the Defense Center. If you did not copy the package to the migration directory, make sure you provide a relative or absolute path to the package.

After you provide your password, the script starts. If the Defense Center passes the rule update equivalence check, the script collects data from the package and performs any necessary cleanup, for example:

```
Migration Import Assistant v1.0
SOURCEfire, inc.
============================================================
Validating backup.......OK
Collecting data from backup...
(This may take a few minutes)
Removing old sensor file sensor_interface_001E672061D8.json
```

**Step 5** Continue with Reviewing the Manifest of Exported Configurations.

# Reviewing the Manifest of Exported Configurations

After the SEU/rule update equivalence check passes (or if you forced a skip of the check), the script further analyzes the package and displays a Version 4.10.3 configuration manifest:

```
4.10.3.5 Configuration Manifest
Use the arrow keys to navigate this view. Press 'q' when finished.
============================================================
```

This manifest is a detailed list of the Version 4.10.3 configurations that the script will either directly import or use to create new Version 5.2 configurations:

- If you exported from a standalone 3D Sensor, the script lists the intrusion policies and local rules that were applied at export time, as well as which IPS detection engines they were applied to.
- If you exported from a Defense Center, the script lists the applied intrusion policies, rules, and detection engines for all sensors managed by that Defense Center. In addition, it also lists any RNA detection engine and policy information, interface sets associated with PEP rules, compliance policies, compliance rules, and traffic profiles.

For more information on which Version 4.10.3 configurations you can migrate to Version 5.2, see Understanding Migrated Configurations and Events, page 5-1.

The manifest is displayed using the `less` utility. Use the arrow keys and space bar to scroll through the manifest, then press `q` when you are done. Then, continue with Verifying Configuration Incompatibilities, page 4-9.

# Verifying Configuration Incompatibilities

After you review the manifest, the script then displays a list of any Version 4.10.3 configurations in the package that will not be imported onto the Version 5.2 Defense Center. These are some of the same issues that were identified by the export script. For information on each of the issues that the configuration import script cannot resolve, see the following sections:

- Errors Due to Unavailable Policies, page 3-9
- RNA Port Exclusion Issues, page 3-10

- Unsupported Conditions in Compliance Rules and Traffic Profiles, page 3-11

If you planned correctly, the only issues listed should be those that you decided not to correct, because either you want to recreate the configurations in Version 5.2, or you do not want to migrate those configurations.

If the script identifies any unanticipated issues, Cisco recommends that you exit and resolve all critical incompatibilities, then restart the migration process. If you cannot or do not want to restart the process, you should have a thorough understanding of which configurations will not be migrated and why, so that you can recreate them later if necessary.

If the script finds issues, you must confirm your intent to continue the import:

```
Do you wish to continue with the migration? (y/n) [y]:
```

The default is to continue. Unless you exit the migration, continue with the next section, Resolving Configuration Conflicts, page 4-10.

# Resolving Configuration Conflicts

After you review the configurations that will not be migrated, the script gives you an opportunity to resolve additional issues. These are some more of the issues that were identified by the export script and discussed in Addressing Configuration Incompatibilities, page 3-7. If you planned correctly, the only issues listed by the import script at this point should be those you decided to resolve during import.

For more information on each of the conflicts that the script can prompt you to resolve, see the following sections:

- Assigning One Detection Engine of Each Type to Interface Sets, page 4-10
- Creating Intrusion Policies For Custom Detection Engine Variables, page 4-11
- Adding Service Metadata to Intrusion Rules, page 4-11
- Resolving Unsupported RNA and RUA Fast-Path PEP Rules, page 4-12
- Limiting Access Control Rules Associated with RNA Port Exclusions, page 4-13

## Assigning One Detection Engine of Each Type to Interface Sets

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

If you exported Version 4.10.3 configurations where more than one IPS or RNA detection engine monitored the same interface, the script prompts you to choose one, for example:

```
Multiple ids detection engines are using interface set 'passive_interfaces' from
Sensor_B.
Please select the detection engine to use for 'passive interfaces':
1: Default IPS Detection Engine (Sensor_B)
2: Second IPS Detection Engine (Sensor_B)
Enter a number [1]:
```

Choosing a detection engine in this case associates the intrusion policy that was applied to that detection engine in Version 4.10.3 with a rule in the new Version 5.2 access control policy. This access control rule is configured so that it analyzes the traffic in a security zone that you will later create. The default is the first option.migrate

Choosing an RNA detection engine uses the RNA detection policy that was applied to that detection engine as a basis for your Version 5.2 discovery and logging 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.

## Creating Intrusion Policies For Custom Detection Engine 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; 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 used 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, for example:

```
Intrusion Policies with customized variable definitions must be created in order to
accurately migrate Detection Engine variables. These policies will use the Intrusion
Policy that is applied to the Detection Engine as the base policy.
Policy_A (copy for variables from 'DE_Alpha')
Policy_B (copy for variables from 'DE_Beta')
Do you want to create these policies? (y/n) [y]:
```

The default is to create the copies. If you decline, the script does not migrate custom detection engine variables and your Version 5.2 configurations will use only the parent intrusion policy.

## Adding Service Metadata to Intrusion Rules

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 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, for example:

```
3 Intrusion rules were found that may require service metadata options in order to
function properly in 5.2.0.
Do you want to review the suggestions, accept all suggestions, or skip adding service
metadata? (accept/review/skip) [accept]:
```

The default is to `accept` all recommendations.

If you choose to `review` recommendations, the script displays each service metadata-rule combination recommendation individually, which you can accept or reject, for example:

```
Rule: 1:1000000 "http-all"
Source port: any
Destination port: 80
```

```
Protocol: tcp
Service recommendations: http
Add 'service http' metadata? (y/n) [y]:
```

If there is one metadata recommendation for a rule, the script prompts you once; if there are eight applications that commonly use that port, the script prompts you eight times. While reviewing, the default is to accept each recommendation.

Note that you **cannot** use the script to add more than eight service metadata entries; the script presents the first eight, alphabetically. You can add additional metadata after the migration.

If you have a large number of local rules to import, you can also `skip` adding service metadata rather than reviewing each rule individually.

**Note** Skipping 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 basic on port negations. For these rules to fire, you **must** manually add service metadata after the migration. The script warns you which rules need this manual update, for example:

```
The following Intrusion rules contain port negations and cannot be automatically
updated. These rules may require service metadata options to be added manually after
migration is complete:
1:1000001 "port_negation_rule"
```

## Resolving Unsupported RNA and RUA Fast-Path PEP Rules

The import script migrates Version 4.10.3 PEP rules with an action of **Fast Path** by creating 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 have traffic 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.

The import script warns you of these rules, for example:

```
A PEP rule applied to 'passive interfaces' has an action of 'DE-specific' and is set
to fast path IPS and RNA. This rule cannot be migrated as-is to 5.2.0:
FASTPATH ips, rna 0.0.0.0/0 > 0.0.0.0/0 vlan: 122
Delete, fast path only IPS, or fast path all traffic? (del/ips/all) [del]: del
```

You have three choices:

- If you delete (`del`) the configuration, the default, the traffic associated with the Version 4.10.3 PEP rule will be subject to analysis by the new access control policy. The system will **not** trust, or fast path, any of that traffic.
- If you fast path only IPS traffic (`ips`), the script creates an access control rule for with an action of **Allow**, but no associated intrusion policy, to inspect matching traffic. This permits traffic to be inspected by discovery, but not an intrusion policy.
- If you fast path `all` traffic, the script creates an access control rule with an action of **Trust** for matching traffic. This allows traffic to pass without further inspection.

## Limiting Access Control Rules Associated with RNA Port Exclusions

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 preference; 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 configuration import script prompts you to choose whether to create these extra rules in the new access control policy, for example:

```
There are 2 "Ports to Exclude" entries in applied RNA detection policies. Creating
access control rules to avoid logging sessions on these ports can significantly
increase the complexity of the new access control policy.
Do you want to create these extra rules? (y/n) [n]:
```

To avoid a confusing proliferation of rules, the default option is to create the access control policy without them.

**Note** You cannot migrate source-only or destination port exclusions at all.

# Creating Security Zones Based on Interface Sets

The Version 4.10.3 concept of interface sets is replaced by Version 5.2 *security zones*, which are groupings of one or more interfaces that you can use to manage and classify traffic flow in various policies and configurations. The interfaces in a single zone may span multiple devices; you can also configure multiple zones on a single device. Using zones allows you to divide the network into segments where you can apply various policies. You must assign at least one interface to a security zone to match traffic against that security zone, and each interface can belong to only one zone. Note that the sensor migration script automatically assigns migrated passive interfaces, but not inline or inline with failopen interfaces, to security zones. See Completing Your Version 5.2 Deployment, page 4-33.

**Tip** In Version 5.2, an *inline set* refers to one or more pairs of inline interfaces that you group to streamline the applying of various networking settings. Inline sets are unrelated to security zones; not all the ingress interfaces in an inline set must belong to the same zone.

In addition to using security zones to group interfaces, you can use zones in various places in the system's web interface, including access control policies, network discovery rules, and event searches. For example, you could write an access control rule that applies only to a specific source or destination zone, or restrict network discovery to traffic to or from a specific zone.

For each active Version 4.10.3 detection engine in the package you are importing (detection engines that do not have a policy applied are not migrated), the configuration import script prompts you to create a security zone on the Defense Center. Later, after you add your migrated Version 5.2 devices to the Defense Center, you can assign their interfaces to these zones.

**Note** Although the import script can create security zones, you must **manually** assign the interfaces on migrated Version 5.2 devices to those zones if you want to match traffic against those zones. Note that the sensor migration script automatically assigns passive, but not inline or inline with failopen, interfaces to zones. For more information, see Configuring and Verifying Sensing Interfaces and Inline Sets, page 4-33.

For example, consider the following scenario:

- you are importing a configuration package onto a 5.2.0 Defense Center that has an existing security zone named *passive_zone*, which groups interfaces that you want to monitor passively
- the package was exported from a Version 4.10.3 Defense Center that managed two Version 4.10.3 sensors: Sensor_A and Sensor_B
- Sensor_A had a detection engine that monitored an inline-with-failopen interface set named *failopen_interfaces*
- Sensor_B had a detection engine that monitored a passive interface set named *passive_interfaces*

First, the script prompts you to select a security zone for the failopen_interfaces set on Sensor_A:

```
Security Zone Creation
============================================================
Which security zone should be used for interface set 'failopen_interfaces' from the
sensor 'Sensor_A'?
1: passive_zone (passive)
Enter a number or a new zone name [failopen_interfaces]:
```

Accepting the default option creates a new zone that shares the name of the migrated detection engine—in this case, *failopen_interfaces*. You can also type a different name at the prompt.

The import configuration script then prompts you to select a zone for the interfaces in the passive_interfaces set on Sensor_B. Notice how the zone you just created appears in the list:

```
Which security zone should be used for interface set 'passive_interfaces' from the
sensor 'Sensor_B'?
1: failopen_interfaces (inline)
2: passive_zone (passive)
Enter a number or a new zone name [passive_interfaces]: 2
```

In this example, you could type `2` (or *passive_zone*) and press Enter. In this case, the script will not create a new security zone on the Defense Center.

**Tip** When configuring a migrated device's interfaces and inline sets, you are **not** required to assign all the interfaces in an inline set to zones created by the import script, although you may want to for the initial configuration and policy apply steps. Zones are meant to group multiple interfaces for security purposes; in practice you might, for example, group all ingress interfaces in the same zone regardless of their inline set. For more information on how interfaces, inline sets, and zones interact in Version 5.2, see the *Sourcefire 3D System User Guide*.

After you select or create security zones for your Version 5.2 deployment, continue with Providing Basic Access Control Settings, page 4-15.

# Providing Basic Access Control Settings

Access control is a new policy-based feature that allows you to specify, inspect, and log the traffic that can traverse your network. An *access control policy* determines how the system handles traffic on your network, including which intrusion policies are used and when. Because access control policies define the traffic that you permit, they also define the traffic you can monitor with the discovery feature (previously *RNA* and *RUA*).

### Naming the Policy

The script prompts you to choose a name for the new policy, for example:

```
Access Control Policy Creation
============================================================
In 5.2, the access control policy allows you to specify, inspect, and log the traffic
that can traverse your network. To migrate IPS, RNA, and PEP configurations, an access
control policy must be created. What do you want to call this policy?
Enter a name [Migration from My_4.10.3_Defense_Center]:
```

Accepting the default option creates a new policy named after the appliance that exported the configuration package. You can also type a different name at the prompt.

**Tip** Do **not** create an access control policy with the same name as an existing access control policy on the Defense Center, because this can be confusing. If you are re-importing configurations from an appliance, accepting the default name offered by the script automatically creates a second, identically named access control policy. Therefore, Cisco recommends that you delete the older policy or choose a different name when re-importing configurations. For more information, see Re-Importing Configurations from the Same Appliance, page 4-18.

### Associating an Intrusion Policy with the Default Action

In Version 5.2, the access control policy's *default action* specifies how the system handles traffic that does not meet the conditions of any access control rule in an access control policy.

The script prompts you to select an intrusion policy to associate with the default action and thus use to inspect all default-action traffic. You can choose any intrusion policy that exists on the Version 5.2 Defense Center, or you can choose one from the configuration package you are importing. The script lists both system -provided and user-created policies, for example:

```
The default action of the access control policy determines how to handle traffic that
does not match any rule in the policy. What intrusion policy do you want to use to
inspect traffic handled by the default action?
Sourcefire authored policies
1: Balanced Security and Connectivity
2: Connectivity Over Security
3: Experimental Policy 1
4: Network Discovery Only
5: Security Over Connectivity
User created policies
6: Initial Inline Policy My_4.10.3_Defense_Center
7: Initial Passive Policy My_4.10.3_Defense_Center
Enter a number [1]:
```

The default is to associate the system-provided Balanced Security and Connectivity intrusion policy with the default action. You can specify a different policy by typing its name or number at the prompt.

Note that choosing option `4: Network Discovery Only` creates a default action that is **not** associated with an intrusion policy at all, but that allows all default-action traffic to be inspected by network discovery. This is useful in discovery-only (RNA-only) deployments.

**Caution** Do **not** use Experimental Policy 1 unless instructed to do so by a Cisco representative. Cisco uses this policy for testing.

After you provide basic access control settings, continue with Verifying the Migrated Configuration.

# Verifying the Migrated Configuration

As a final step, the script displays what the results of the migration will be if you continue with the import. It lists:

- the security zones that the script will create or modify
- any intrusion policies and local intrusion rules the script will import
- the access control policy the script will create, including a detailed list of the access control rules in the policy and their associated conditions, actions, and intrusion policies
- any rules that the script will add to the network discovery policy, and their associated networks-to-monitor and other discovery options
- any correlation policies, correlation rules, and traffic profiles that the script will import and activate

Although not listed by the script, the import script will also update various discovery-related settings in the system policy and network discovery policy on the Version 5.2 Defense Center. For details on how your Version 4.10.3 configurations translate to Version 5.2, and for information on the new configurations that the migration process creates, see Understanding Migrated Configurations and Events, page 5-1.

The script displays the migrated configuration using the `less` utility. Use the arrow keys and space bar to scroll through the configuration, then press `q` when you are done. Continue with Confirming the Import and Resolving Configuration Collisions, page 4-16.

# Confirming the Import and Resolving Configuration Collisions

After you review the proposed results of the migration, the import script asks you whether you want to proceed:

```
Are you sure you want to import this backup? (y/n) [y]:
```

If you exit the script at this point no changes are made to the Version 5.2 Defense Center, except the cleanup of various files from any previous migrations. If you continue, which is the default, the script begins to import the configurations in the package to the Defense Center.

At this point, if a configuration in the package directly conflicts with an existing configuration on the Defense Center, the script prompts you to resolve the conflict.

This occurs because certain configurations, sometimes called objects, are uniquely identified by the system. Multiple versions of the same object cannot exist on a Defense Center. For example, the script might display the following prompt for a conflicting intrusion policy:

```
The object My_Intrusion_Policy (IntrusionPolicy) already exists. Overwrite? (y/n/all)
[y]:
```

The script displays similar prompts for conflicting local intrusion rules, correlation policies and rules, and traffic profiles. The default is to overwrite the older configuration with the one in the package you are importing. You can also keep the older configuration, or specify `all` to overwrite all remaining conflicting configurations.

**Tip** This type of conflict occurs only if you are re-importing configurations. For more information on why configurations conflict and what you can do to prevent collisions, see Re-Importing Configurations from the Same Appliance, page 4-18.

After you resolve any object conflicts, the script saves the new configurations to the Version 5.2 Defense Center. The script also activates any correlation policies and traffic profiles that were active in your Version 4.10.3 deployment:

```
Writing configuration.....................................
Activating 0 correlation policies and 1 traffic profiles...
```

You can now log out of the Defense Center and continue with the next step in your migration plan. Depending on your deployment, it may be time to perform additional configuration imports, or import events, or reimage your Version 4.10.3 3D Sensors into Version 5.2 devices. For more information on planning your migration, see Understanding the Migration Process, page 2-1.

# Configuration Import Script Syntax and Options

You must run the configuration import script as the root user. Cisco recommends that you copy the configuration package to the migration directory (`/var/sf/migration`) and run the script from that directory using `sudo`, providing your password when prompted.

After you log in to the appliance's shell as an Administrator (see Logging Into an Appliance to Run Migration Scripts, page 4-2), the syntax for running the script is as follows:

```
sudo ./config_import.pl exported_config_package.tgz options
```

where *`exported_config_package.tgz`* is the package you copied to the Defense Center and *`options`* represents one or more script options, as described in the table below. Note that if you are not running the script from the migration directory, or you did not copy the package to the migration directory, make sure you provide relative or absolute paths to the script and package.

***Table 4-5 Configuration Import Script Options***

| Option | Description |
|---|---|
| `none` | Performs the import beginning with the SEU/rule update equivalence check, as described in Starting the Configuration Import Script, page 4-8. |
| `--manifest` | Display a detailed list of the Version 4.10.3 configurations in the specified package. If a review of the manifest reveals anything unexpected, Cisco recommends that you fix critical issues and export a new package from the Version 4.10.3 appliance. For more information, see Reviewing the Manifest of Exported Configurations, page 4-9. |
| `--force` | Forces the script to skip the SEU/rule update equivalence check.<br><br>Do **not** use this option unless you have already reimaged the appliance where you exported the package. Otherwise, Cisco recommends that you update the SEUs and rule updates in your deployment and restart the migration process; for more information see SEU and Intrusion Rule Update Requirements, page 3-3.<br><br>In most cases, the resulting imported intrusion configurations will work as expected. However, contact Support if you cannot edit or apply policies after forcing a configuration import. |

*Table 4-5 Configuration Import Script Options (continued)*

| Option | Description |
|---|---|
| `--usedefaults` | Run the script without providing any user input, using the default answer for all prompts, including conflict resolution, security zone creation, and access control policy settings. See the previous sections for more information on the default choices the import script makes.<br><br>Do **not** use this option unless you fully understand which Version 4.10.3 configurations will be migrated and what the resulting Version 5.2 configurations will be. |
| `--help` | Display basic instructions and syntax for running the script. |

# Importing Configurations Multiple Times

In a properly planned migration, you run the import script once for each configuration package you need to migrate to Version 5.2. For example, in a simple single Defense Center-to-single Defense Center migration, you would run the configuration import script only once during the whole migration process. However, there are a few situations where you must run the configuration import script more than once.

### Importing Multiple Unique Configuration Packages

If you are replacing two or more Version 4.10.3 Defense Centers with one Version 5.2 Defense Center, or if you are adding several former standalone 3D Sensors to a new Defense Center, you must import multiple unique configuration packages onto the Version 5.2 Defense Center.

Running the import script cleans up information from any previous invocations. Also, although the sensor migration script copies and applies interface configurations, importing configurations with the import script **does not** configure interfaces to reimaged Version 5.2 devices. Therefore, when you have multiple unique packages to import, and you do not intend to use the sensor migration script to migrate some or all sensors, you should run the display interfaces script **immediately** after each import, and save that script's output to a file that will not be overwritten. In cases where you do not use the sensor migration script, this preserves the information on how to configure the interfaces on the migrated devices associated with each package after you add the devices to the Defense Center. Alternately, add and configure all devices referenced in the imported package before you perform the next import.

For information on using the display interfaces script, see Configuring and Verifying Sensing Interfaces and Inline Sets, page 4-33.

### Re-Importing Configurations from the Same Appliance

If you have planned your migration correctly, you should only run the configuration import script one time for each exported configuration package. However, you may decide that the results of your migration are not what you want, and that your issues can be resolved by another import.

You can either:

- re-import the same package but choose different options during import, or
- re-import a different package.

  For example, if the Version 4.10.3 appliances whose configurations you are migrating have not already been reimaged, you can update those configurations then create a new package for re-import.

In either case, there are consequences to a re-import that can affect the migrated configurations on the Defense Center, as described in the following list.

#### security zones

For each active Version 4.10.3 detection engine in the package you are importing (detection engines that do not have a policy applied are not migrated), the script prompts you to choose or create a security zone on the Defense Center. Later, after you add your migrated Version 5.2 devices to the Defense Center, you can assign their interfaces to these zones.

In a package re-import, Cisco recommends that you choose the same zones you created in the first import. If you did not rename any interface sets in the Version 4.10.3 deployment before you re-exported, accepting the default answers, no new security zones will be created. However, if you changed the name of an interface set in the exported package, accepting the script defaults can create a new zone.

#### access control policy

Every time you run the import script, the script creates a **new** access control policy. If you are re-importing configurations, accepting the default name offered by the script automatically creates a second, identically named access control policy.

Because it is confusing to have two policies with the same name, Cisco recommends that you delete the older policy before you begin the import, or choose a different name on re-import.

#### unique configurations (objects)

The system uniquely identifies the following migrated configurations, sometimes called objects:

- intrusion policies and local intrusion rules
- correlation policies and rules
- traffic profiles

Multiple versions of the same object **cannot** exist on a Defense Center. If you import a package that contains an object that already exists on the Version 5.2 Defense Center, you must choose which to keep: the existing object or the object in the package. Note that this conflict occurs even if either object has been renamed or otherwise modified.

As an example, consider a scenario where you import a configuration package onto a Version 5.2 Defense Center, then decide that the results are not what you want. You return to your Version 4.10.3 deployment, modify some configurations, then export an updated package. When you import that updated package onto the Version 5.2 Defense Center, all intrusion policies and local intrusion rules, correlation policies and rules, and traffic profiles that were imported the first time and that still exist on the Defense Center now conflict with their counterparts in the updated package.

For your convenience, the import script prompts you to make a decision for each conflicting object; the default is to overwrite the existing configuration with the one from the configuration package. For more information, see Confirming the Import and Resolving Configuration Collisions, page 4-16.

**Tip** To avoid object collision, before you begin a configuration re-import delete any existing objects that will conflict.

#### network discovery policy, rules, and other discovery settings

The import script translates some of the RNA network monitoring settings in your Version 4.10.3 deployment to Version 5.2 discovery rules in the network discovery policy.

Because there is only one network discovery policy on a Version 5.2 Defense Center, the script merges (instead of overwrites) the network monitoring settings on the Defense Center with those in the import package. This could result in duplicate discovery rules. Therefore, Cisco recommends that you delete any network discovery rules created by the first import before you begin the re-import.

In addition, a re-import can overwrite other settings in the network discovery policy.

# Importing Events onto a Version 5.2 Defense Center

**Supported Devices:** None

**Supported Defense Centers:** Any

As an optional and usually one of the final steps in a migration process, you can import the intrusion and audit events that you exported from your Version 4.10.3 appliances.

First, copy a Version 4.10.3 event package (see Exporting Events from a Version 4.10.3 Appliance, page 4-6) to the appropriate Version 5.2 Defense Center. Then, run a script that imports the events. You should run the import script once for each event package you need to import:

- If you are migrating from a single Version 4.10.3 Defense Center to a single Version 5.2 Defense Center, you should only have one event package to import.
- If you are replacing two or more Version 4.10.3 Defense Centers with one Version 5.2 Defense Center, or are adding several former standalone 3D Sensors to a new Defense Center, you must import each event package individually.

When you run the script, it 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 you try again, free space on the appliance by deleting extraneous events, saved backup files, and so on.

Note that some fields in intrusion events generated by Version 4.10.3 are different from 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, the timestamps on migrated 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.

Finally, keep in mind that importing events can take a significant amount of time.

**Tip** If imported events do not display after you complete the import process, clear your browser cache and try again.

**To import a package of intrusion and audit events:**

**Access:** Admin

**Step 1** Copy the package you plan to import to the Version 5.2 Defense Center.

Cisco recommends that you copy all packages to the `/var/sf/migration` directory.

**Step 2** Log into the Defense Center’s shell using an account with Administrator privileges.

For more information, see Logging Into an Appliance to Run Migration Scripts, page 4-2.

**Step 3** Navigate to the migration folder:

```
cd /var/sf/migration
```

**Step 4** Run the export script as the root user, providing your password when prompted:

```
sudo ./event_import.pl exported_event_package.tgz
```

where *exported_config_package*.tgz is the package you copied to the Defense Center. If you did not copy the package to the migration directory, make sure you provide a relative or absolute path to the package.

After you provide your password, the script starts. It compares the disk space required to complete the import with the space available on the Defense Center and asks if you want to proceed, for example:

```
Migration Event Import Assistant v1.0
SOURCEfire, inc.
=====================================================
Validating backup...
Importing these events will take approximately 125MB.
There is approximately 15G free.
Are you sure you want to import this backup? (y/n) [y]: y
```

**Step 5** Choose whether you want to proceed by typing `y` or `n` and pressing Enter.

Do **not** proceed if there is not enough disk space for the import; the import will fail. Before you try again, free space on the appliance by deleting extraneous events, saved backup files, and so on. If you confirm that you want to proceed, the script begins importing the events:

```
Importing events...
Migration event import complete!
```

**Step 6** Continue with the next step in your migration plan.

For more information on planning your migration, see Understanding the Migration Process, page 2-1.

# Rebuilding Version 4.10.3 Appliances

As part of the migration to Version 5.2, you must either replace, reimage, or re-create your Version 4.10.3 appliances. The method and timing depend on the type of appliances in your deployment and on your migration plan.

If you are **replacing** a physical appliance or **re-creating** a virtual appliance, perform the initial setup on the new Version 5.2 appliance and prepare it for configuration import **before** you take its Version 4.10.3 counterpart out of band or begin running any migration scripts. After you set up the new Version 5.2 appliance, you can add it to your deployment seamlessly at the time determined by your migration plan.

If you are **reimaging** a physical appliance **during** the migration, your migration plan must account for the time it will take to perform the reimage. Because reimaging results in the loss of almost **all** configuration and event data on the appliance, including special configurations such as LDAP authentication, your plan must also account for setup and import preparation.

To reimage sensors, you can install the sensor migration script on the Version 5.2 Defense Center and remotely reimage one or more standalone or managed Series 2 or Series 3 3D Sensors. The script automatically copies the sensors' interface configurations, reimages the sensors, registers the reimaged sensors to the Defense Center, and applies the interface configurations.

**Caution** Contact Support before using the sensor migration script to migrate a 3D500 3D Sensor.

You must manually reimage Version 4.10.3 Defense Centers to Version 5.2. In some cases (for example, in a small or low-bandwidth deployment) you might also prefer to manually reimage Series 2 and Series 3 3D Sensors.

When you replace or manually reimage a physical sensor, or re-create a virtual sensor, you must also manually add it to the Version 5.2 Defense Center and configure its interfaces.

**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.

Use the following resources to complete appliance replacements, re-creations, or manual reimages:

- See the appropriate Version 5.2 *Installation Guide* for instructions on replacing, recreating, and manually reimaging appliances,
- See Understanding the Migration Process, page 2-1 for information on:
  - migration- and deployment-specific information on manual reimaging
  - reimaging using the sensor migration script
  - replacing and recreating appliances
  - details on when or whether to take Version 4.10.3 appliances out of band
  - when to start using Version 5.2 appliances
- See Preparing for Migration, page 3-1 for migration-specific information on preparing a new or freshly reimaged Version 5.2 Defense Center or standalone sensor for configuration import, including:
  - intrusion rule update requirements
  - license requirements
  - instructions for installing the migration script

Additionally, see the following sections for more information on using the sensor migration script and manually adding devices:

- Reimaging and Registering Devices with the Sensor Migration Script.
- Manually Adding Version 5.2 Devices to the Defense Center, page 4-31.

# Reimaging and Registering Devices with the Sensor Migration Script

**Supported Devices:** Series 2, Series 3

You can use the sensor migration script to remotely reimage one or more Version 4.10.3 (or a later patch) 3D Sensors to Version 5.2. First, you install the script on your Version 5.2.0.x Defense Center using the Defense Center's web interface. Then you run the script as the root user from the Defense Center's shell, typically via SSH. Alternately, you can also connect to the Series 3 Defense Center shell via Lights-Out Management (LOM). Status messages display migration progress.

**Caution** Contact Support before using the sensor migration script to migrate a 3D500 3D Sensor.

You install one of two script packages depending on whether you run the script from a Series 2 or Series 3 Defense Center. See Table 3-4 on page 3-12 for more information. The script from either package can reimage multiple Series 2 and Series 3 sensors in parallel.

You **cannot** use the script to migrate virtual devices. You **can** use the script to migrate any eligible physical sensor on your network, regardless of whether you first import configurations or events. The script copies your Version 4.10.3 sensor interface configurations to the Defense Center, reimages the sensors, registers the sensors to the Version 5.2.0.x Defense Center where you run the script, and applies the interface configurations. During the migration, sensor interfaces that were configured to fail open remain open, allowing network traffic to pass without interruption.

**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.

The script automatically reboots reimaged sensors at the appropriate migration stage. As a precautionary measure, it disables the use of Ctrl+C when you have responded to all prompts and the migration process begins.

**Caution** **Do not** interrupt the migration or reboot your 3D Sensors or Defense Center during the sensor migration. This could corrupt the rebooted system or negatively affect migrated configurations.

You can run the script multiple times. For example, you might want to test the migration on a few sample sensors before migrating remaining sensors, or migrate sensors in groups to avoid performance issues. If a sensor fails to migrate, the script skips the failed sensor and continues migrating the other sensors. If you migrate a single sensor and it fails, or you migrate multiple sensors and all sensors fail, the script aborts. In most cases, you can include failed sensors in a subsequent migration.

Although you can migrate up to twenty sensors at a time, Cisco recommends for performance reasons that you migrate no more than ten sensors at a time. The script cautions you before you add another sensor when you have already added ten or more sensors.

Reimaging results in the loss of almost **all** configuration and event data on the sensor. Although reimaging can retain the sensor's network, console, and Series 3 Lights-Out Management (LOM) settings, and the sensor migration script can register sensors and preserve interface configurations, you must perform all other setup tasks after the restore process completes. See Completing Your Version 5.2 Deployment, page 4-33 for more information.

In the event of an unavoidable migration interruption such as a power outage, you can manually reimage interrupted sensors to Version 5.2 in most cases. However, you lose the script's advantages of allowing sensors to fail open, copying interface configurations, registering sensors, and providing remote access. If the interruption occurs at a critical stage of the migration and you to lose access to the sensor, contact Support. For instructions on manually reimaging a sensor, see the appropriate Version 5.2 *Installation Guide*.

**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.

Note that a Version 4.10.3.x Defense Center where a migrated sensor was originally registered still shows configured interfaces and detection engines for the sensor after the migration; these non-functional *ghost images* are merely artifacts of the migration.

See the following sections for more information:

- Running the Sensor Migration Script, page 4-24
- Understanding the Status Display, page 4-27
- Understanding End-of-Run Error Messages, page 4-29
- Resolving SSH Key Conflicts, page 4-31

## Running the Sensor Migration Script

After you import and install the sensor migration package using the Version 5.2.0.x Defense Center web interface, run the script from the Defense Center command line as the root user. The script prompts you for the following information:

- the user name and password of an account with `sudo` privileges on the Version 5.2 Defense Center where you run the script.

  The script typically pauses approximately three minutes to verify this account information, and aborts if you provide invalid information.

- the IP address or host name for each sensor you want to migrate, and a user name and password of an account with `sudo` privileges for each.

  The script pauses three to five minutes to verify communication between the sensor and the Defense Center each time you provide the user name and password for a sensor; if the script must resolve invalid SSH keys, the pause can be up to approximately eight minutes. See Resolving SSH Key Conflicts, page 4-31 for more information.

Cisco recommends that you use the `admin` account for the Version 5.2 Defense Center where you run the script and for each sensor you specify.

**Caution** **Do not** use an LDAP or Radius account for sensor migration. External authentication configurations are not migrated. The reimaged software could exhibit unpredictable behavior, and the script cannot register migrated sensors to the Version 5.2.0.x Defense Center.

The script uses the authentication information you provide to facilitate SSH communication over port 22 between migrating 3D Sensors and the Defense Center. If you provide an invalid sensor IP address, host name, user name, or password, the script reprompts you.

Finally, the script lists the sensors you have identified and asks if you want to proceed. If you proceed, the script disables Ctrl+C as a precautionary measure and begins the migration.

The following table explains the options you can use with the sensor migration script.

***Table 4-6 Sensor Migration Script Options***

| Option | Description |
|---|---|
| `--timeout=`*`value`* | Configures the script to run for *`value`* minutes before timing out, where *`value`* is a number greater than the default value of 120 minutes. |
| `--help` | Describes the options you can use when running the script. |

**To reimage and register Version 4.10.3 Sensors:**

**Access:** Admin

**Step 1** Obtain the sensor migration package and install it on your Version 5.2.0.x Defense Center. See Obtaining and Installing Migration Packages, page 3-12 for more informations.

**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.

**Step 2** Log into the Defense Center's shell using an account with `sudo` privileges.

For more information, see Logging Into an Appliance to Run Migration Scripts, page 4-2.

**Step 3** Switch to the root user and provide the password when prompted. For example:

```
sudo su
Password:
```

**Step 4** Navigate to the sensor migration directory:

```
cd /Volume/migration_tmp
```

**Step 5** Enter either of the following commands, depending on whether you want to modify the default timer setting:

- To run the script using the default timeout value of 120 minutes, enter:

  ```
  ./migration_script.pm
  ```

- To run the script using a different timeout value, enter:

  ```
  ./migration_script.pm --timeout=value
  ```

  where *value* is the number of minutes (120 or greater) before the timer expires.

The script displays a welcome message, then prompts you for the Defense Center's user name and password. For example:

```
###########################################################
#                                                         #
#  Welcome to the Sourcefire Sensor Migration Script      #
#                                                         #
###########################################################

This script is intended to be run on a 5.2 Defense Center and will upgrade 4.10.3
devices to 5.2.

In order for migration to complete successfully, the following conditions must be met:
 * This Defense Center must be running version 5.2 or greater
 * The Sensors to be migrated must be running version 4.10.3 or greater
 * Communication between Defense Center and Sensor(s) must be possible

Please also note that once the migration process is begun, it must be allowed to
run to completion.

Sensors to be migrated will need to contact this Defense Center for update
information. Please provide a username (with sudo privileges and password for this
Defense Center.
```

```
Username:admin
Password:
```

**Step 6** Enter the user name and password for an account with `sudo` privileges on the Version 5.2 host Defense Center. Cisco recommends that you use the `admin` account.

**Caution** **Do not** use an LDAP or Radius account for sensor migration. External authentication configurations are not migrated. The reimaged software could exhibit unpredictable behavior, and the script cannot register migrated sensors to the Version 5.2.0.x Defense Center.

These credentials facilitate communication between migrating 3D Sensors and the Defense Center. The script validates the credentials and aborts if the information is invalid:

```
Verifying credentials (this may take several minutes)...     Authentication failure.

Unable to continue.
```

If the information is valid, the script prompts you for the host name or IP address of the first sensor you want to migrate:

```
Verifying credentials (this may take several minutes)...     Success

Please specify name or IP address of sensor:
```

**Step 7** Enter the host name or IP address of a Series 2 or Series 3 sensor on your network.

The script asks if you want to identify another sensor.

```
Specify additional sensors? (y/n) [n]:
```

**Step 8** Enter `y` to add another sensor or press Enter when you have added the last sensor.

When you indicate that you have added the last sensor, the script lists each sensor and prompts you for the user name and password for the first sensor you specified. For example:

```
The following devices were specified:
  192.168.13.12
  kilroy (192.168.13.13)
  killjoy (192.168.13.14)
  192.168.13.15
Please supply a username with sudo privileges
 for use with system 192.168.13.12: admin
Please supply the password for user 'admin':
```

**Step 9** Enter the user name and password for a user who has `sudo` privileges for the sensor. Cisco recommends that you use the `admin` account for each sensor.

**Caution** **Do not** use an LDAP or Radius account for sensor migration. External authentication configurations are not migrated. The reimaged software could exhibit unpredictable behavior, and the script cannot register migrated sensors to the Version 5.2.0.x Defense Center.

For each sensor you specified, the script tests the credentials and, if more sensors remain, prompts you for the next user name and password. For example.

```
Testing ssh connection to the sensor, and from the sensor back to
 the Defense Center (this may take several minutes)...      Success
Please supply a username with sudo privileges
 for use with system 192.168.13.13: admin
```

```
Please supply the password for user 'admin':
...
```

Note that testing the SSH connection can take three to five minutes per sensor, and up to eight minutes if the script must resolve invalid SSH keys. The script reprompts if you enter invalid information.

After successfully testing the last sensor, the script warns you that reimaging permanently deletes data from all migrated sensors and asks if you want to begin the migration process.

```
Warning: Migration will reimage sensors,
permanently deleting data on those systems.

Start the migration process for selected devices? (y/n) [n]:
```

**Step 10** Enter `y` to start the migration process and the migration timer, or press Enter to exit the script.

The script displays progress information during the migration. See Understanding the Status Display, page 4-27.

When the migration completes or the timer expires, messages:

- provide the result of the migration for each sensor
- remind you to inspect your interface configurations
- remind you to apply your access control policy.

For example:

```
Migration script complete.

MySensor1.example.com (192.168.13.11)
     Success: Migration and registration completed successfully.
MySensor2.example.com (192.168.13.12)
     Failure: Unable to upload new data to sensor.
Please inspect interface configurations and apply policy to migrated systems.
```

See Understanding End-of-Run Error Messages, page 4-29 for more information.

**Step 11** Continue with Completing Your Version 5.2 Deployment, page 4-33.

## Understanding the Status Display

The sensor migration begins after you have identified the sensors to migrate, provided the requested information (see Running the Sensor Migration Script, page 4-24), and confirmed that you want to proceed with the migration. At this point the script prohibits you from using Ctrl+C, begins the migration process, and informs you that it is preparing status information:

```
Preparing to Display Progress...
```

The script displays updated migration progress approximately every five seconds:

```
 ############################################################
 #                                                          #
 #        Sourcefire Sensor Migration Underway              #
 #                                                          #
 #      Please do not reboot this Defense Center!           #
 #      Your terminal will refresh as progress is updated   #
 #                                                          #
 ############################################################

Backup Legacy Configuration...                                6 Passed
Gathering Sensor Information...                               6 Passed
Uploading New Data...                                         5 Passed
Updating OS Components...                                     4 Passed, 1 Failed
Removing Legacy 4.x Code...                                   4 Passed
```

```
Installing New 5.x Code...                                    4 Passed
Convert/Restore Legacy Configuration...                       4 Passed
Reboot/Update Sensors (may take 30 mins)...                   4 Passed
Cleaning Up...                                                4 Passed
Establishing Registration...                                  2 Passed, 2 Failed

42:33 until timeout
```

The screen flickers with each update, adding stages as a sensor reaches each stage and incrementing the number of sensors that have passed and failed each stage. The script also displays the minutes and seconds until the timer expires. The timer starts when you respond to the final prompt and counts down from either the default time of 120 minutes or the time you configure. See Table 4-6 on page 4-24 for more information.

**Caution** You cannot use the sensor migration script to migrate sensors that were included in a previous script run where the timer expired. In most cases, you can reimage the sensors manually using the restore procedure. See the Version 5.2 *Sourcefire 3D System Installation Guide* for information on restoring your sensors. Contact Support if the timer expires and you cannot restore your sensors.

The following table explains each stage of the migration:

***Table 4-7 Sensor Migration Stages***

| Migration Stage | Description |
|---|---|
| Backup Legacy Configuration | Collects the Version 4.10.3 sensor interface configurations |
| Gathering Sensor Information | Collects the sensor model number, model series, and so on so the correct migration package can be assembled |
| Uploading New Data | Uploads sensor-specific data and packages, including RPMs, from the Defense Center to the sensor |
| Updating OS Components | Installs the Version 5.2 operating system on the sensor |
| Removing Legacy 4.x Code | Uninstalls Version 4.10 RPMs on the sensor |
| Installing New 5.x Code | Installs Version 5.2 RPMs on the sensor |
| Convert/Restore Legacy Configuration | Recreates interface configurations on the newly updated Version 5.2 sensor |
| Reboot/Update Sensors | Reboots the sensor and completes the update (this can take up to 30 minutes) |
| Cleaning Up | Removes unneeded data specific to the current migration process |
| Establishing Registration | Registers the migrated Version 5.2 devices to the Version 5.2 Defense Center |

Sensors are migrated in parallel in a forked arrangement; that is, they begin the migration simultaneously and proceed individually, each at its own pace. Counters update to identify the number of sensors that have passed or failed each stage.

## Understanding End-of-Run Error Messages

When the migration process completes, the script identifies each sensor that successfully completed the migration and displays the same completion message for each, as shown in the following example:

```
Migration script complete.

MySensor1.example.com (192.168.13.11)
     Success: Migration and registration completed successfully.
MySensor2.example.com (192.168.13.12)
     Success: Migration and registration completed successfully.
```

When a sensor fails, the script identifies the failed sensor in a single error message that indicates the reason for the failure and suggests a course of action. For example:

```
MySensor1.example.com (192.168.13.13)
     Failure: Unable to determine sensor model.
Please confirm that the sensor specified is online and then rerun migration.
```

When a failure occurs early in the process, you can often include the failed sensor in a script rerun after addressing the reason for the failure. When a failure occurs later in the process, the script suggests (with one exception) that you contact Support. In most cases, you can manually reimage late-stage failures using the restore procedure. The exception is when the migration succeeds and registration fails, in which case the script suggests that you register the sensor manually.

If a sensor loses connectivity for any reason during the migration, the sensor does not complete the migration and the script displays at least one end-of-run error message. These messages indicate the stage that was in progress when connectivity was lost, and the suggested actions indicate whether you can include the sensor in a script rerun.

The following table describes error messages that might display after the migration process completes.

***Table 4-8 Sensor Migration Script End-of-Run Error Messages***

| Error Message | Description |
|---|---|
| ERROR: Attempt to contact <name> failed.<br>Skipping this device and attempting to continue. | The specified sensor could not be reached. |
| ERROR: Sensor appears to be running an unsupported version of the STIG Hotfix.<br>Please uninstall this hotfix and retry migration or contact support. | The STIG hotfix version on the specified sensor was unavailable when the migration script was developed and is untested and unsupported. |
| ERROR: SSH Host Identification key problem for Sensor <name><br>Please resolve this SSH key difference and restart migration for this sensor. | The migration script could not automatically resolve an invalid SSH key. See Resolving SSH Key Conflicts, page 4-31. |
| ERROR: Unable to connect to <sensor_data>{entry}{id}.<br>Please contact support. | The migration script proceeded beyond a point of no return and lost communication with the specified sensor. |
| ERROR: Unable to resolve system name <name>.<br>Please check name and rerun migration for that system. | The specified host name could not be resolved. |
| ERROR: Unsupported model type (Defense Center) found for system <name> (<ip>).<br>Only Sensors can be migrated using this script. | The host name or IP address identified a Defense Center. |

*Table 4-8 Sensor Migration Script End-of-Run Error Messages*

| Error Message | Description |
|---|---|
| ERROR: Unsupported model type (Virtual System) found for system <name> (<ip>).<br>Migration of Virtual Systems is not supported. | The host name or IP address identified a virtual Defense Center. |
| ERROR: Unsupported software version found for Sensor <name>.<br>All Sensors must be running version 4.10.3 or later (but less than 5.x). | The version of the specified sensor was earlier than Version 4.10.3, or Version 5.0 or later. |
| Failure: md5sum of uploaded package does not match expected value.<br>Please verify communication between sensor and DC and then rerun migration. | The md5sum of the uploaded package did not match the expected value. |
| Failure: Unable to copy legacy configuration data.<br>Please contact support. | The migration script could not copy legacy configuration files. |
| Failure: Unable to correctly determine system architecture.<br>Please contact support. | The migration script could not determine if the sensor is 32-bit or 64-bit. |
| Failure: Unable to delete legacy detection engine data.<br>Please contact support. | The migration script could not delete Version 4.10.3 detection engine data. |
| Failure: Unable to determine sensor model.<br>Please confirm that the sensor specified is online and then rerun migration. | The migration script could not determine the sensor model. |
| Failure: Unable to establish registration with Defense Center.<br>Migration successful. Please attempt to establish registration with Defense Center manually. | The migration script could not establish management between the migrating Defense Center and migrated sensor. |
| Failure: Unable to install 5.2.0 RPM packages.<br>Please contact support | The migration script could not install the Version 5.2 RPM. |
| Failure: Unable to process legacy LILO configuration<br>Please contact support. | The migration script could not process the LILO boot configuration. |
| Failure: Unable to remove migration files<br>Please contact support. | The migration script could not delete unneeded migration files during the cleanup step. |
| Failure: Unable to scp import/export tools from DC to localhost sensor.<br>Please verify communication between sensor and DC and then rerun migration. | The migration script could not transfer migration tools to the sensor. |
| Failure: Unable to scp legacy configuration data from sensor to localhost DC.<br>Please verify communication between sensor and DC and then rerun migration. | The migration script could not transfer legacy data from the sensor being migrated to the Defense Center. |

*Table 4-8 Sensor Migration Script End-of-Run Error Messages*

| Error Message | Description |
|---|---|
| Failure: Unable to uninstall 4.10.x RPM files.<br>Please contact support. | The migration script could not uninstall the Version 4.10.x code. |
| Failure: Unable to upgrade OS packages properly.<br>Please contact support. | The migration script could not update the operating system package. |
| Failure: Unable to upload new data to sensor.<br>Please verify communication between sensor and DC and then rerun migration. | The migration script could not upload migration RPMs and related files. |
| killing forked processes due to timeout | The timeout value expired before the migration completed. |

## Resolving SSH Key Conflicts

During the migration, the sensor migration script uses SSH on port 22 to establish connections between the Defense Center and the sensors you identify. Before beginning the migration, the script verifies that it can establish these connections. When the script encounters an invalid SSH key for the targeted sensor, the script resolves the conflict by automatically backing up the `known_hosts` file to `/home/<user>/.ssh/known_hosts_<date>_<time>` and removing the line in the file that includes the invalid key.

A message at the end of the migration process notifies you when the migration script is not able to automatically resolve an SSH key conflict. See Understanding End-of-Run Error Messages, page 4-29 for more information. In this case, you can resolve the conflict and include the affected sensor in a subsequent migration.

You can resolve the conflict using either or both forms of the following command from the Version 5.2 Defense Center command line:

```
ssh keygen -R IP_address
ssh keygen -R hostname
```

If you enter the command only once, you must identify the sensor in the command using the same form (IP address or host name) that you used to identify the sensor while running the sensor migration script. If you enter both forms of the command, you can use the IP address or host name to identify the sensor while running the sensor migration script.

# Manually Adding Version 5.2 Devices to the Defense Center

When you replace physical sensors, recreate virtual sensors, or manually reimage physical sensors instead of using the sensor migration script, you must manually register the Version 5.2 devices to the Version 5.2 Defense Center. In these cases, you should register your devices after importing configurations and events so your policies and security zones are in place.

For detailed instructions on adding devices to a Defense Center, including adding devices in a NAT environment, see the *Managing Devices* chapter in the Version 5.2 *Sourcefire 3D System User Guide*.

**To add a device to a Defense Center:**

**Access:** Admin/Network Admin

**Step 1** Configure the device to be managed by the Defense Center.

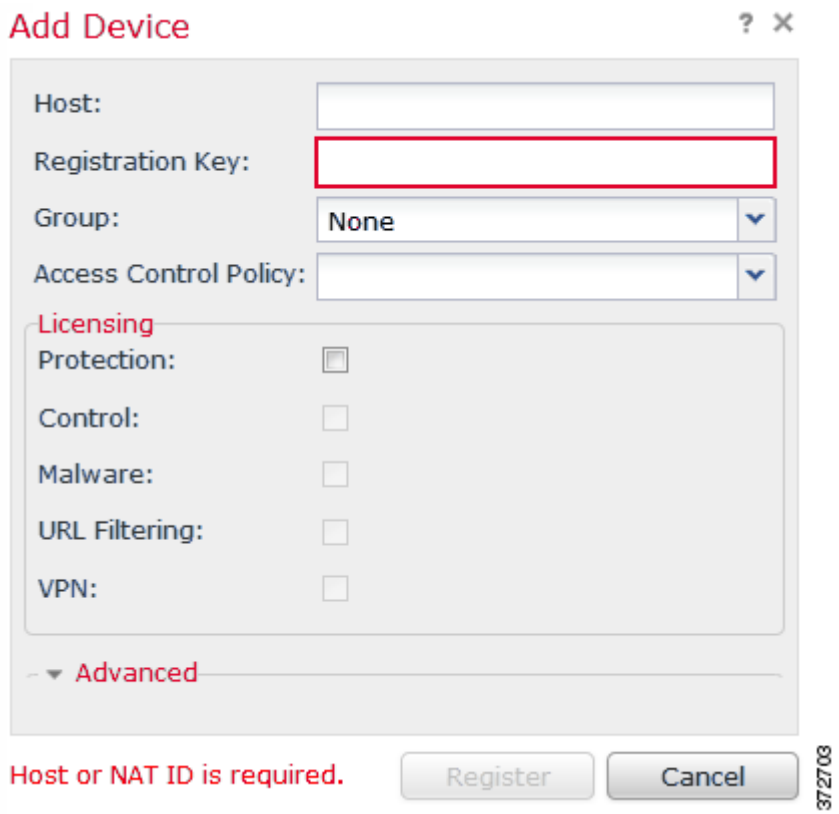
You should have designated the Defense Center as the remote manager during the device's initial setup. If you did not, use a physical device's web interface (**System > Local > Registration**) or a virtual device's CLI to add the Defense Center.

**Step 2** Log into the Defense Center's web interface, then select **Devices > Device Management**.

The Device Management page appears.

**Step 3** From the **Add** drop-down menu, select **Add Device**.

The Add Device pop-up window appears.




**Step 4** In the **Host** field, type the IP address or the hostname of the device you want to add.

The hostname of the device is the fully qualified domain name or the name that resolves through the local DNS to a valid IP address.

**Caution** Use a hostname rather than an IP address if your network uses DHCP to assign IP addresses.

**Step 5** In the **Registration Key** field, type the same registration key that you used when you configured the device to be managed by the Defense Center.

**Step 6** From the **Access Control Policy** drop-down list, select an initial policy to apply to the device.

Select the new access control policy created by the configuration import; see Providing Basic Access Control Settings, page 4-15. If you imported multiple configuration packages and therefore the migration process created several access control policies, make sure you select the policy that contains configuration data specific to that device.

**Step 7** If necessary, select the **Protection** check box to apply a model-specific Protection license to the device.

So that this migrated deployment can behave equivalently with your Version 4.10.3 deployment, you **must** apply a Protection license to any former Series 3 or virtual 3D Sensor with IPS. You do **not** have to apply Protection licenses to devices in discovery-only deployments, nor do Series 2 devices require a Protection license. For more information, see Version 5.2 License Requirements, page 3-4.

**Step 8** To allow the device to transfer packets to the Defense Center, select the **Transfer Packets** check box in the **Advanced** page area.

This option is enabled by default. If you disable it, you completely prohibit packet transfer to the Defense Center.

**Step 9** Click **Register**.

The device is added to the Defense Center. Note that it may take up to two minutes for the Defense Center to verify the device's heartbeat and establish communication.

**Tip** The initial access control policy apply may fail, depending on the interface configuration on the device you just added. You can reapply the access control policy later.

**Step 10** After communications are successfully established, continue with Completing Your Version 5.2 Deployment, page 4-33.

# Completing Your Version 5.2 Deployment

After you replace, re-create, reimage, or add devices to the Version 5.2 Defense Center, you should configure all managed devices so they can begin to handle network traffic and report events. In most cases, this is the final step in your migration before placing any out of band devices inline and, optionally, importing legacy events.

For more information, see:

- Configuring and Verifying Sensing Interfaces and Inline Sets, page 4-33
- Applying Network Discovery and Access Control Policies, page 4-38

## Configuring and Verifying Sensing Interfaces and Inline Sets

The configuration process for interfaces and inline sets depends on whether you used the sensor migration script or reimaged your sensors manually.

### Completing the Configuration After Reimaging Sensors Using the Sensor Migration Script

When you use the sensor migration script to reimage Version 4.10.3 (or a later patch) sensors, the script also registers your Version 5.2 devices to the Version 5.2.0.x Defense Center and configures your interfaces to match their Version 4.10.3 configurations.

In addition to configuring your interfaces, the sensor migration script also:

- creates a security zone for each Version 4.10.3 passive interface, giving the security zone the same name as the detection engine used by the passive interface
- assigns Version 4.10.3 inline interfaces to a Version 5.2 inline set with **Bypass Mode** enabled for Version 4.10.3 inline with failopen interfaces and disabled for Version 4.10.3 inline only interfaces
- applies your interface configurations to enable detection capability

To complete your sensor migration, Cisco recommends that you view your interface configurations to ensure that they are still appropriate for your Version 5.2 deployment. After verifying your interface configurations, you can continue with the next section, Applying Network Discovery and Access Control Policies, page 4-38.

#### Completing the Configuration After Reimaging Sensors Manually

When you reimage devices manually, for your migrated deployment to function properly you must manually configure the interfaces and inline sets on your devices after you add them to the Defense Center.

For your convenience, Cisco provides a script that, when you run it after a configuration import, displays the correct interface configurations for the devices associated with that configuration package.

**Note** Running the configuration import script cleans up information from any previous invocations. Therefore, if you have multiple unique configuration packages to import, run the display interfaces script **immediately** after each import, and save that script's output to a file that will not be overwritten. Alternately, add and configure all devices referenced in the imported package before you perform the next import.

Run the display interfaces script as the root user from the migration directory (`/var/sf/migration`) using `sudo`, providing your password when prompted. After you log in to the appliance's shell as an Administrator (see Logging Into an Appliance to Run Migration Scripts, page 4-2), the syntax for running the script is as follows:

```
sudo ./display_interfaces.pl
```

Optionally, redirect the output to save it:

```
sudo ./display_interfaces.pl >> my_interface_configs.txt
```

The script provides the name, IP address, and model of each device associated with the most recently imported configuration package, and also provides the following information:

- the link mode and MDI/MDIX settings for the sensing and management interfaces on the device
- for each interface set, the security zone you associated with the set when you imported configurations; see Creating Security Zones Based on Interface Sets, page 4-13
- for each inline interface set, the bypass (failopen) mode and whether tap mode, link state propagation, or transparent inline mode is enabled

As an example:

```
Sensor_A (10.10.123.123)                      3D Sensor 8140
============================================================
eth0 (Management)  Mode: 1Gb/Full (Auto)         MDI/MDIX: Auto
------------------------------------------------------------
s1p1 <-> s1p2      Security Zone: failopen interfaces
                   Type: failopen                Tap mode: off
                   Link Propagation: off
                   Transparent Inline: on
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
    s1p1           Mode: 1Gb/Full (Auto)         MDI/MDIX: Auto
    s1p2           Mode: 1Gb/Full (Auto)         MDI/MDIX: Auto
```

```
-------------------------------------------------------
s1p3 <-> s1p4      Security Zone: failopen interfaces
                   Type: failopen                Tap mode: off
                   Link Propagation: off
                   Transparent Inline: on
- - - - - - - - - - - - - - - - - - - - - - - - - - - - -
    s1p3           Mode: N/A (Auto)              MDI/MDIX: Auto
    s1p4           Mode: N/A (Auto)              MDI/MDIX: Auto
```

Using the output of the display interfaces script as a guide, you can use the Defense Center's web interface to configure the interfaces and inline sets on your managed devices.

You can configure either inline sets or interfaces first depending on your preference. However, keep in mind that if you configure interfaces first, you cannot add them to inline sets until you create the inline sets. On the other hand, if you create inline sets first, you may not be able to add interfaces until you configure the interfaces themselves.

**Note** After you configure the interfaces and inline sets on a device, you **must** apply the device configuration (**Devices > Device Management**) for your changes to take effect and therefore for your deployment to function properly. After you apply the device configuration, you can continue with Applying Network Discovery and Access Control Policies, page 4-38.

For detailed instructions on configuring interfaces and inline sets, see the *Managing Devices* and *Setting Up an IPS Device* chapters in the *Sourcefire 3D System User Guide*.

**To configure a managed device's interfaces:**

**Access:** Admin/Network Admin

**Step 1** Log into the Defense Center's web interface, then select **Devices > Device Management**.

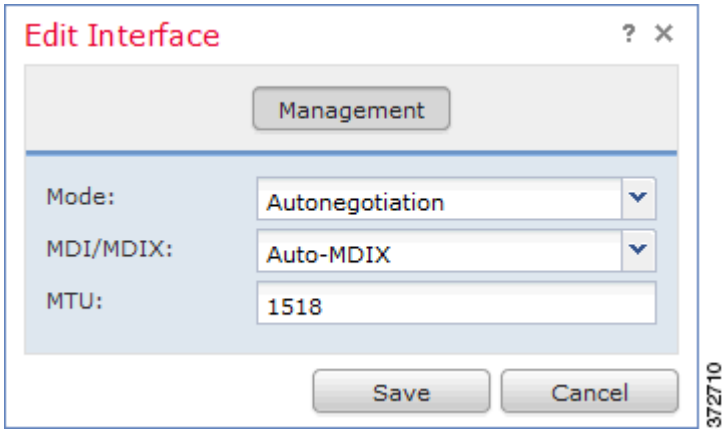
The Device Management page appears.

**Step 2** Next to the device whose interfaces you want to configure, click the edit icon ( ).

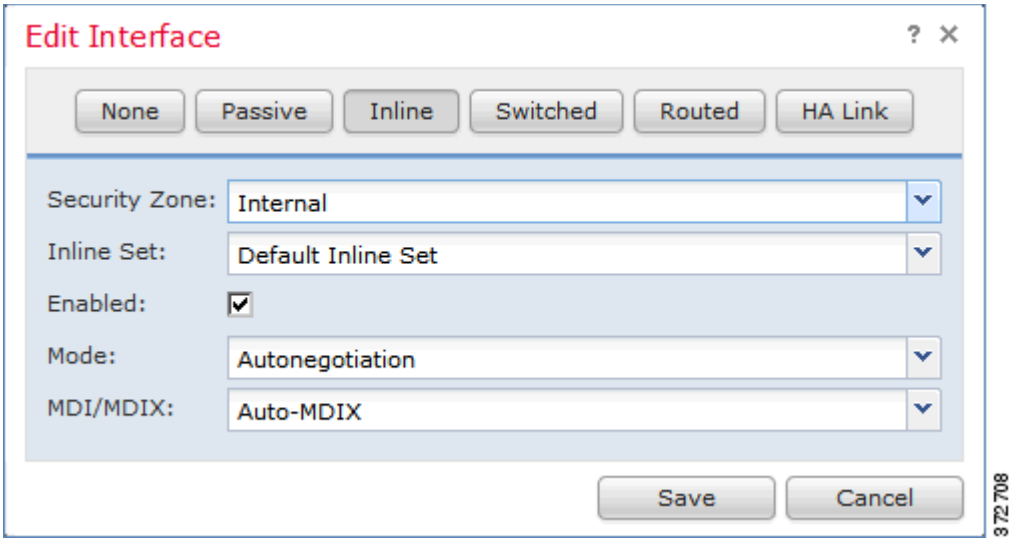
The Interfaces tab for that device appears.

**Step 3** Next to the interface you want to edit, click the edit icon ( )).

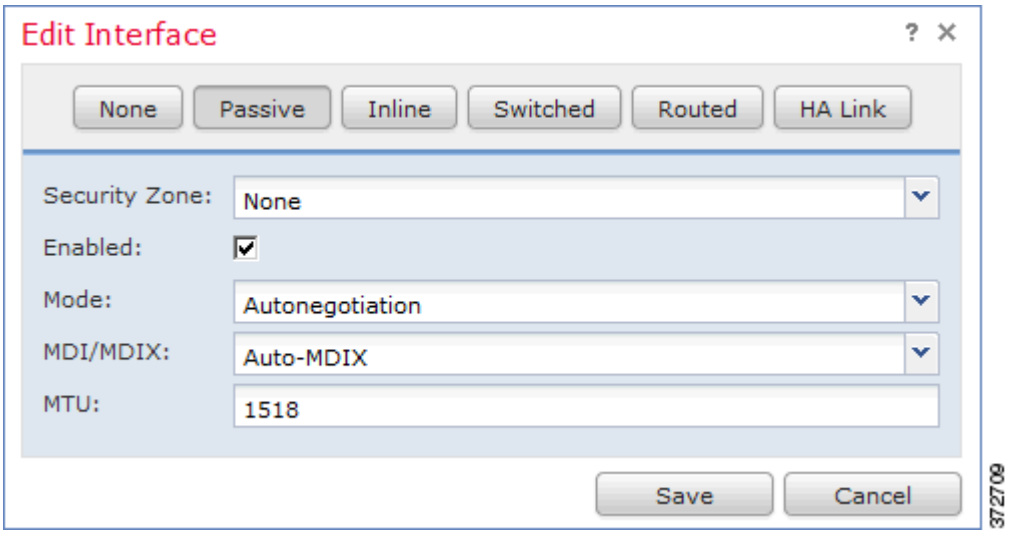
The Edit Interface pop-up window appears. The following graphic shows the options for the management interface.



For a sensing device, you can change the type of interface from inline to passive and back. The following graphic shows the options for an inline interface.




The following graphic shows the options for a passive interface.




**Step 4** Using the output of the display interfaces script as a guide, configure the interface according to the needs of your organization.

If you are able, you can add the interface to an inline set now, or you can do it later when you configure inline sets.

Note that you assign interfaces to security zones individually. You are **not** required to assign all the interfaces in an inline set to the same security zone. Security zones are meant to group multiple interfaces for security purposes; in practice you might, for example, group all ingress interfaces in the same zone regardless of their inline set. For more information on how interfaces, inline sets, and zones interact in Version 5.2, see the *Sourcefire 3D System User Guide*.

**Step 5** Click **Save**.

**To add an inline set:**

**Access:** Admin/Network Admin

**Step 1** Select **Devices > Device Management**.

The Device Management page appears.

**Step 2** Next to the device where you want to add the inline set, click the edit icon ( ).

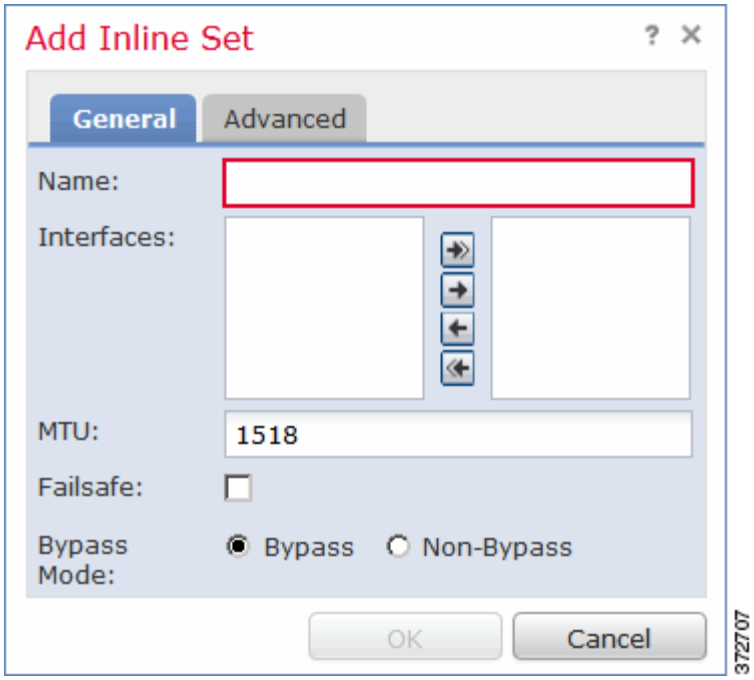
The Interfaces tab appears.

**Step 3** Click **Inline Sets**.

The Inline Sets tab appears.

**Step 4** Click **Add Inline Set**.

The Add Inline Set pop-up window appears.




**Step 5** Using the output of the display interfaces script as a guide, configure the inline set according to the needs of your organization.

If you are able, you can add inline interface pairs now, or you can do it later when you configure the individual interfaces.

**Tip** To configure advanced settings for the inline set, such as tap mode, link state propagation, and transparent inline mode, use the **Advanced** tab.

**Step 6** Click **OK**.

# Applying Network Discovery and Access Control Policies

As a final step, to make sure traffic is flowing and being handled correctly, you must apply access control and network discovery policies to the migrated devices in your deployment. First apply access control policies, then the network discovery policy.

**Tip** After you apply these policies, the migration process is over and you can begin to fine tune your deployment, including recreating any configurations that were not migrated. See Next Steps, page 4-39.

### Applying Access Control Policies

You must apply a **complete** access control policy (which includes intrusion policies) to each migrated device in your deployment.

If performed correctly, the migration process created at least one new access control policy on the Version 5.2 Defense Center, and each of these policies targets one or more of your migrated devices. Apply each of these new policies to its target devices.

**To quick-apply a complete access control policy:**

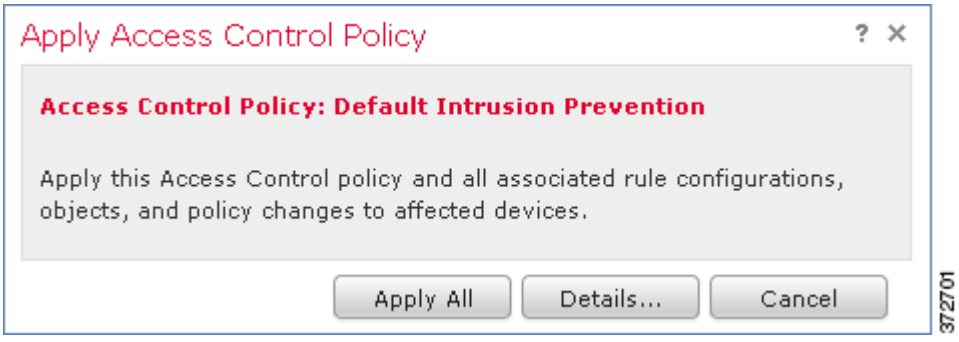
**Access:** Admin/Security Approver

**Step 1** Log into the Defense Center's web interface, then select **Policies > Access Control**.

The Access Control page appears.

**Step 2** Click the apply icon ( ) next to the policy you want to apply.

The Apply Access Control Rules pop-up window appears.




**Step 3** Click **Apply All**.

Your policy apply task is queued. Click **OK** to return to the Access Control page.

### Applying the Network Discovery Policy

If you want to perform network and user discovery using your imported configurations, apply the network discovery policy to all the devices in your deployment.

**To apply the network discovery policy:**

**Access:** Admin/Security Approver

**Step 1** Log into the Defense Center's web interface, then select **Policies > Network Discovery**.

The Network Discovery Policy page appears.

**Step 2** Click **Apply**.

A message appears, confirming that you want to apply the policy to all zones targeted by access control policies on the Defense Center.

**Step 3** Click **Yes** to apply the policy.

# Next Steps

After you complete the migration process, Cisco recommends that you complete any administrative tasks you skipped during the initial setup. You may also want to:

- re-create essential configurations that were not migrated; see Understanding Migrated Configurations and Events, page 5-1
- specify configurations you skipped migrating, for example, local intrusion rules without service metadata
- modify any configurations created by the migration according to the needs of your organization, for example, security zones and inline sets

For detailed information on any the above tasks, the tasks described in the following sections, as well as information on how you can begin to configure your deployment, see the *Sourcefire 3D System User Guide*.

### Individual User Accounts

After you complete the initial setup, the only user on the system is the `admin` user, which has the Administrator role and access. Users with that role have full menu and configuration access to the system, including via the shell or CLI. Cisco recommends that you limit the use of the `admin` account (and the Administrator role) for security and auditing reasons.

Creating a separate account for each person who will use the system allows your organization not only to audit actions and changes made by each user, but also to limit each person's associated user access role or roles. This is especially important on the Defense Center, where you perform most of your configuration and analysis tasks. For example, an analyst needs access to event data to analyze the security of your network, but may not require access to administrative functions for the deployment.

The system includes ten predefined user roles designed for a variety of administrators and analysts. You can also create custom user roles with specialized access privileges.

### Health and System Policies

By default, all appliances have an initial system policy applied. The system policy governs settings that are likely to be similar for multiple appliances in a deployment, such as mail relay host preferences and time synchronization settings. Cisco recommends that you use the Defense Center to apply the same system policy to itself and all the devices it manages.

By default, the Defense Center also has a health policy applied. A health policy, as part of the health monitoring feature, provides the criteria for the system continuously monitoring the performance of the appliances in your deployment. Cisco recommends that you use the Defense Center to apply a health policy to all the devices it manages.

#### Software and Database Updates

Cisco recommends that all the appliances in your deployment run the most recent version of the system software. If you plan to use them in your deployment, you should also install the latest intrusion rule updates, vulnerability database (VDB), and geolocation database (GeoDB).

**Caution** Before you update any part of the system software, you **must** read the release notes or advisory text that accompanies the update. The release notes provide important information, including supported platforms, compatibility, prerequisites, warnings, and specific installation and uninstallation instructions.