



Introduction to Version 5.2

Version 5.0 introduced a large new feature set which was further expanded in subsequent releases. Regardless of model, appliances running Version 4.10.x of the system **cannot** be updated directly to Version 5.x. To update, you must reimage your physical appliances and re-create your virtual appliances, which results in a loss of all stored events and most configuration data.

For your convenience, Cisco provides the following export, import, and sensor migration scripts:

- Four scripts allow you to export configurations and events from a Version 4.10.3.x (patch 4.10.3.5 or later) Defense Center® or standalone sensor and import them onto a Version 5.2.0.x Defense Center:
 - configuration export script
 - configuration import script
 - event export script
 - event import script
- A sensor migration script allows you to remotely reimage up to twenty (ten maximum recommended) Version 4.10.3 (or a later patch) Series 2 and Series 3 sensors in parallel to Version 5.2 using a Version 5.2.0.x Defense Center. Note that it is not necessary to update sensors from Version 4.10.3 to 4.10.3.5 to use the sensor migration script.

Before you begin the migration process for your deployment you **must** make sure you have a detailed plan and that you have fully prepared your appliances, including obtaining and installing the new licenses, resolving issues that could prevent a clean migration, setting up replacement appliances, installing the migration scripts, and so on. Although Cisco recommends you perform the migration in a maintenance window or at a time when the interruption will have the least impact on your deployment, the migration process can take a significant amount of time. You can minimize disruption by thoroughly preparing, but it is unlikely you will be able to avoid it completely.



Caution

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

The topics that follow introduce you to Version 5.2, including its differences from earlier versions. For differences in a release subsequent to Version 5.2, see the release notes for that version.

- [Cisco® Security Migration Services, page 1-2](#)
- [New and Changed Terminology, page 1-2](#)
- [New, Changed, and Updated Features and Functionality, page 1-3](#)
- [Deprecated Functionality, page 1-24](#)

- [Appliance Series, Models, and Capabilities](#), page 1-25
- [Where Do I Begin?](#), page 1-28

Cisco® Security Migration Services

Cisco® Security Migration Services help customers move from Version 4.x software to Version 5.x. Cisco will perform an analysis of the current environment, develop a migration plan, test the plan in a lab, and perform the migration in the production environment. With detailed planning and careful change management, we help ensure that your security solution protects the infrastructure while meeting your business needs. Contact your Cisco account representative to order Cisco Security Migration Services.

New and Changed Terminology

Due to the many new and changed features introduced in Version 5.0 through Version 5.2, the terminology in both the software and its documentation has changed accordingly. To ensure maximum ease of use and familiarity with Version 5.2, review these changes carefully.

The table below contains a brief overview of the most important changed terms. For more information on new and changed features, see the next sections in this chapter. For detailed definitions of both new and changed terms, see the glossary in the [Version 5.2 Sourcefire 3D System User Guide](#).

Table 1-1 Terminology Changes

This term in Version 4.10.3	Is now this term in Version 5.2
IPS, RNA, RUA, PEP	These technologies have been fully integrated into the system and are no longer referred to separately.
3D Sensor, sensor	device, managed device
SEU (Security Enhancement Update)	rule update, intrusion rule update, SRU (rarely)
client application	client, client application (rarely)
service	application protocol, server (when there is an associated vendor and version)
payload (discovery)	web application
flow (as a general term and before data, event, graph, summary, tracker)	connection
compliance (before event, policy, rule), Policy and Response	correlation Note that the term compliance, when referring to compliance white lists, remains in use.
Default Dashboard	Summary Dashboard
RNA detection policy	network discovery policy
RNA detector	application detector
RNA event	discovery event
RNA Recommended Rules	FireSIGHT recommendations
RUA Agent	User Agent
RUA event	user activity

Table 1-1 Terminology Changes (continued)

This term in Version 4.10.3	Is now this term in Version 5.2
RUA user	user, user identity
report profile	report template
system settings	local configuration
fail-open (interface protection mode)	bypass (interface set bypass mode)

New, Changed, and Updated Features and Functionality

The Version 5.2 web interface is streamlined and improved; it is significantly different from Version 4.10.3 releases. The look and feel is updated, many terms have changed, and new menus and options support new functionality.

New predefined dashboards, new workflows, and a reorganized host profile present your network assets in a manner consistent with the new features and terminology changes. Predefined user roles have changed to reflect the overall organization of the system and the web interface.

For Series 3 and virtual devices, Version 5.2 includes CLI commands that correspond with the new features and functionality and removes commands that are no longer needed. If you enable Simple Network Management Protocol (SNMP) polling, there are new counters in the management information base (MIB) files for managed devices that include traffic statistics associated with the new features.

The following sections summarize the new, changed, and updated functionality that you will encounter when you migrate a deployment to Version 5.2:

- [Device Management, page 1-4](#)
- [Licensing, page 1-4](#)
- [Redundancy and Resource Sharing, page 1-15](#)
- [Network Traffic Management, page 1-16](#)
- [Access Control, page 1-16](#)
- [Intrusion Detection and Prevention, page 1-19](#)
- [File Tracking, File Control, and Malware Protection, page 1-19](#)
- [Network Discovery, page 1-21](#)
- [Geolocation Information, page 1-21](#)
- [Dashboards, page 1-22](#)
- [Context Explorer, page 1-22](#)
- [Reusable Objects, page 1-22](#)
- [Reporting, page 1-23](#)
- [Health Monitoring, page 1-23](#)
- [Client Vulnerabilities and VDB Updates, page 1-23](#)
- [User Certificates, page 1-23](#)
- [IPv6 Support, page 1-23](#)
- [Application Programming Interfaces, page 1-24](#)

Device Management

In Version 5.2, only essential management and monitoring functions are available on managed devices. Almost all configuration and analysis functions are restricted to the Defense Center, including the configuration of the new features available in Version 5.2.

Standalone 3D Sensors used as an intrusion detection and prevention system (IPS) are no longer supported. Use the migration feature to transfer intrusion policies and events from your standalone 3D Sensor with IPS to a Version 5.2 Defense Center.

Licensing

Your organization can license a variety of features to create an optimal deployment. Version 5.2 uses a different licensing scheme than Version 4.10.3. Most licenses from previous releases are not supported. You must use the Defense Center to control licenses for itself and the devices it manages.



Tip

Add licenses during the initial setup of your Version 5.2 Defense Centers. Otherwise, any devices you register during initial setup are added to the Defense Center as unlicensed. You must then enable licenses on each device individually after the initial setup process is over. For more information, see the [Sourcefire 3D System Installation Guide, Version 5.2](#).

For more information, see:

- [Host and User Licenses, page 1-4](#)
- [Feature Licenses, page 1-5](#)
- [Using the Product Upgrade Tool, page 1-7](#)
- [Selecting PIDs for Upgrade Licenses, page 1-13](#)
- [Selecting PIDs for Additional Feature Licenses, page 1-14](#)
- [Additional Information, page 1-15](#)
- [Configuring and Verifying Sensing Interfaces and Inline Sets, page 4-33](#)

Host and User Licenses

In Version 5.2, a FireSIGHT license is required to perform host, application, and user discovery. The FireSIGHT license on your Defense Center also determines how many individual hosts and users you can monitor with the Defense Center and its managed devices, as well as how many users you can use to perform user control. FireSIGHT host and user license limits are model-specific, as listed in the following table.

Table 1-2 FireSIGHT Limits by Defense Center Model

Defense Center Model	FireSIGHT Host and User Limit
DC500	1000 (no user control)
DC750	2000
DC1000	20,000
DC1500	50,000

Table 1-2 *FireSIGHT Limits by Defense Center Model (continued)*

Defense Center Model	FireSIGHT Host and User Limit
DC3000	100,000
DC3500	300,000

When you migrate your deployment to Version 5.2, you can use your legacy RNA Host and RUA User licenses instead of a FireSIGHT license. Version 5.2 Defense Centers with legacy licenses use the RNA Host limit as the FireSIGHT host limit and the RUA User limit as both the FireSIGHT user and access-controlled user limit.

**Tip**

During the Version 4.10.3 to Version 5.2 manual reimage process of a physical appliance, you are prompted to delete license and management interface network settings. Keep these settings, although you can re-add them later if you accidentally delete them. For more information, see the [Version 5.2 Sourcefire 3D System Installation Guide](#).

RNA Host and RUA User limits are cumulative. That is, you can add multiple licenses of each type to the Defense Center to monitor the total number of hosts or users allowed by the licenses.

If you later add a FireSIGHT license, the Defense Center uses the higher of the limits. For example, the FireSIGHT license on the DC1500 supports up to 50,000 hosts and users. If the RNA Host limit on your Version 4.10.3 DC1500 was higher than 50,000, using that legacy host license on the same Defense Center running Version 5.2 gives you the higher limit. For your convenience, the web interface displays only the licenses that represent the higher limits.

**Note**

Because FireSIGHT license limits are matched to the hardware capabilities of Defense Centers, Cisco does **not** recommend exceeding them when using legacy licensing. For guidance, contact Support.

Feature Licenses

Model-specific licenses allow your managed devices to perform a variety of functions, as follows:

Protection

A Protection license allows managed devices to perform intrusion detection and prevention, file control, and Security Intelligence filtering. Note you do not enable a Protection license on Series 2 devices. Registering a Series 2 device to a Version 5.2 Defense Center automatically enables intrusion detection and prevention and file control, without a license. Security Intelligence is not supported on Series 2 devices.

Control

A Control license allows Series 3 managed devices to perform user and application control. It also allows devices to perform switching and routing (including DHCP relay), NAT, and to cluster devices and stacks. A Control license requires a Protection license.

URL Filtering

A URL Filtering license allows Series 3 managed devices to use regularly updated cloud-based category and reputation data to determine which traffic can traverse your network, based on the URLs requested by monitored hosts. A Version 5.2 URL Filtering license also requires Protection and Control licenses.

Malware

A Malware license allows Series 3 managed devices to perform network-based advanced malware protection (AMP), that is, to detect and block malware in files transmitted over your network. It also allows you to view trajectories, which track files transmitted over your network. A Malware license requires a Protection license.

VPN

A VPN license allows you to build secure VPN tunnels among the virtual routers on Series 3 managed devices, or from managed devices to remote devices. A VPN license requires Protection and Control licenses.

Because of architecture and resource limitations, not all licenses can be applied to all managed devices. In general, you cannot license a capability that a device does not support; see [Table 1-4 on page 1-27](#).

The following table summarizes which licenses you can add to your Defense Center and apply to each device model. The Defense Center rows (for all licenses except FireSIGHT) indicate whether that Defense Center can manage devices using those licenses. For example, you can use a Series 2 DC1000 to create a VPN deployment using Series 3 devices, but you cannot use a DC500 to perform category and reputation-based URL filtering, regardless of the devices it manages. Note that n/a marks Defense Center-based licenses that are not relevant to managed devices.

Table 1-3 Supported Licenses by Model

Models	FireSIGHT or RNA/RUA	Protection	Control	URL Filtering	Malware	VPN
Series 2 devices: <ul style="list-style-type: none"> 3D500/1000/2000 3D2100/2500/3500/4500 3D6500 	n/a	no license required; all Protection capabilities automatically granted except Security Intelligence, which is not supported	no	no	no	no
Series 3 devices: <ul style="list-style-type: none"> 7000 Series 8000 Series 	n/a	yes	yes	yes	yes	yes
virtual devices	n/a	yes	no support for hardware features	yes	yes	no
DC500 Series 2 Defense Center	yes	no Security Intelligence	no user control	no	no	yes
DC1000/3000 Series 2 Defense Centers	yes	yes	yes	yes	yes	yes
DC750/1500/3500 Series 3 Defense Centers	yes	yes	yes	yes	yes	yes
virtual Defense Centers	yes	yes	yes	yes	yes	yes

Using the Product Upgrade Tool

This section explains how to use the self-service Cisco Product Upgrade Tool to acquire FireSIGHT and Control perpetual licenses for \$0 when migrating from 4.10 to 5.x. These licenses are necessary to enable all the base functionality of the FireSIGHT Management Center (previously referred to as the *Defense Center*) and any FirePOWER Appliances it manages (previously referred to as *managed devices*).

Note the following:

- The Control upgrade license that you get using the Product Upgrade Tool also provides the capabilities of the Protection license.
- FirePOWER 5.x does not support standalone devices, so all sensor appliances running Version 5.x must be managed via a FireSIGHT Management Center.

To use the PUT tool to order upgrade licenses:

- Step 1** Login to the Product Upgrade Tool (<http://tools.cisco.com/gct/Upgrade/jsp/index.jsp>) using your CCO ID.

Product Upgrade Tool

HOME

HOW TO BUY

Product Upgrade Tool

News and Enhancements

User Guides

Questions and Answers

Glossary

New Product Search

Start Product Upgrade

Enter Contract number and select method to upgrade.

Contract Number

94713860

Guided

This method provides with step-by-step process to upgrade.

Advanced

Use this method if you know exactly which upgrade product to order.

Continue

408171

- Step 2** Enter the service contract number 94713860 **EXACTLY AS SHOWN** and select the **Continue** button. **YOU MUST USE THIS SERVICE CONTRACT NUMBER. YOU CANNOT SUBSTITUTE ANY OTHER NUMBER.**

Guided Method

Contract Number → **Upgrade Selection** → Upgrade SKU

Select Product Group *Required Field

Product Group* Current Version* Upgrade Version*

SOURCEFIRE Version 4.X Version5.X

Back Continue

403172

- Step 3** Under Product Group, click on **SOURCEFIRE**. Under Current Version, click on **Version 4.X**. Under Upgrade Version click on **Version 5.X**. Select **Continue** in the lower right corner.

Guided Method

Upgrade SKU

Add another upgrade or continue to complete your order.

L-3D2500-5UPG-K9=
Cisco Software Upgrade from 4.x to 5.x for 3D2500

SF-FSVMW-5UPG-K9
Cisco FireSIGHT 4.x to 5.x Upgrade PID

L-3D1000-5UPG-K9=
Cisco Software Upgrade from 4.x to 5.x for 3D1000

Add Another Upgrade Continue

403173

- Step 4** On the Upgrade SKU page, select **Continue** in the lower right corner.

Guided Method

Upgrade Summary

Select Delivery Option and enter quantity of product upgrades.
Some products are not available for eDelivery.

Product Number	Special Ordering Note	License Key Requested	Delivery Option	Quantity
L-3D1000-5UPG-K9=		<input type="radio"/> Single <input checked="" type="radio"/> Multiple	<input type="radio"/> Physical <input checked="" type="radio"/> eDelivery	<input type="text"/>
Cisco Software Upgrade from 4.x to 5.x for 3D1000 ⓘ				
L-3D2000-5UPG-K9=		<input type="radio"/> Single <input checked="" type="radio"/> Multiple	<input type="radio"/> Physical <input checked="" type="radio"/> eDelivery	<input type="text"/>
Cisco Software Upgrade from 4.x to 5.x for 3D2000 ⓘ				
L-3D2100-5UPG-K9=		<input type="radio"/> Single <input checked="" type="radio"/> Multiple	<input type="radio"/> Physical <input checked="" type="radio"/> eDelivery	<input type="text"/>
Cisco Software Upgrade from 4.x to 5.x for 3D2100 ⓘ				

403174


- Step 5** Specify the delivery option and quantity you need for each upgrade license shown, then select **Continue** in the lower right corner. See [Selecting PIDs for Upgrade Licenses, page 1-13](#) for more information regarding which PID(s) to select.

Guided Method

Shipping Details

Shipping Contact *Required Field

Shipping Address



Add a Shipping Address...*

Enter your *Technical Assistance Center (TAC)* or *Customer Service (SR)* case number, if applicable.

TAC/SR Case Number:

eDelivery Email:*

Optionally you can fill notes to provide any additional information.

Carton Notes:

[Copy to Ordering Notes](#)

[Copy to Shipping Notes](#)

Order Processing Notes:

[Copy to Shipping Notes](#)

Shipping & Packaging Notes:

Additional E-mail

Enter additional email addresses that you wish to receive for confirmation of your order.

Additional E-mail

Note: Multiple email addresses can be entered using comma, e.g. xxx@yyy.zzz, aaa@bbb.ccc.

Back

Continue

403175

- Step 6** Enter your shipping address & shipping contact. Click on **Add a Shipping Address** and scroll down to the bottom to select your address or add an address. .
- Step 7** Enter your **TAC/SR Case Number** (if applicable), **eDelivery Email**, **Additional Email** addresses (if applicable), **Carton Notes**, **Order Processing Notes**, and **Shipping & Packaging Notes**. Select **Continue** in the lower right corner.
- Step 8** Please read and agree to the Product Upgrade Tool – Software Ordering Rules.
- Step 9** Review your order detail for correctness and select **Submit Order**.
- Step 10** You will receive an email confirmation of your order and an order acknowledgment with an estimated shipping date once the order is scheduled.



New Request

Thank you for placing your order.
Your Online Order ID is **UG442994**

An e-mail confirmation of your order has been automatically sent to **ES@ES.COM**.

403176

- Step 11** Once the order has been fulfilled, you will receive either an email or a physical paper Claim Certificate, depending on the delivery preference you selected while ordering.
- Step 12** If you received a Claim Certificate, skip to *To register and fulfill a license through Cisco.*

To download your Claim Certificate when you receive an eDelivery Email:

- Step 1** Open the email confirming your order.

Product Upgrade Tool

[HOME](#)

[Start Product Upgrade](#)

[HOW TO BUY](#)

Enter Contact number and select method to upgrade

- Step 2** Scroll down the email until you see the box titled *eDelivery Access Order*. Select the **eDelivery Access Order** link at the bottom.

eDelivery

Order Based Access

[Send Order Based Access Email](#)

Cisco SO	100278161	Bill-To PO
Carton/Cust Ref Notes	Test Not Real	

Products Ordered

<input type="checkbox"/> L-3D2100-5UPG-K9= (QTY - 1)	Cisco Software Upgrade from 4.x to 5.x for 3D2100
Description	Test Not Real
Carton/Cust Ref Line Notes	Test Not Real

[Download Selected](#) [Download All Licenses](#) [Download Entire Order](#)

403178

- Step 3** Click the plus sign under Products Ordered.

L-3D2100-5UPG-K9= (QTY - 1)						Status	Downloaded
Description						Available	03/11/15
Carton/Cust Ref Line Notes							
Cisco Software Upgrade from 4.x to 5.x for 3D2100							
Test Not Real							
Select All Deselect All							
	Line ID	File Type	Product ID	Description	Status	QT	
<input type="checkbox"/>	926033752	License	L-3D2100-5UPG-K9=	Cisco Software Upgrade from 4.x to 5.x for 3D2100	Downloaded	1	
<input type="checkbox"/>		License (Claim)		LIC,Generic Software Claim Certificate, 7x8.5"	Downloaded	1	↓

Step 4 Click the green arrow.

License Agreement Confirmation

You must accept the [End User License Agreement](#) to download this software.

Accept License Agreement
 Decline License Agreement

License Download Cart Download All Licenses

<input type="checkbox"/>	Order #	Line ID	Product ID	File Type	Description	QT	
<input checked="" type="checkbox"/>	100278161	926033752	L-3D2100-5UPG-K9=	License (Claim)	LIC,Generic Software Claim Certificate, 7x8.5"	1	Remove

[Delete Selected Licenses from Cart](#)

Step 5 Select **Accept License Agreement**. In the License Download Cart, select the check box of the claim certificate to download. Click **Download All Licenses**.

Step 6 Save the zip file to your desktop, which includes an End User License Agreement and your Claim Certificate, which includes your PAK number.

To register and fulfill a license through Cisco:

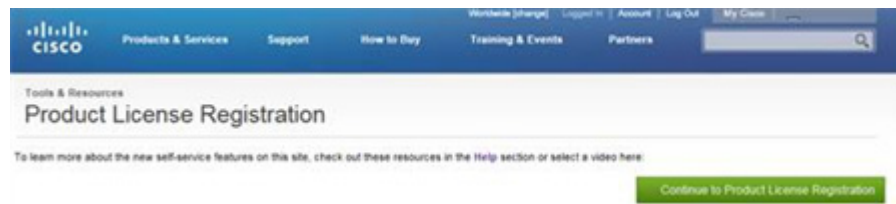
To register your Product Authorization Key and obtain a license, please follow the steps below:

Step 1 Go to www.cisco.com/go/license.

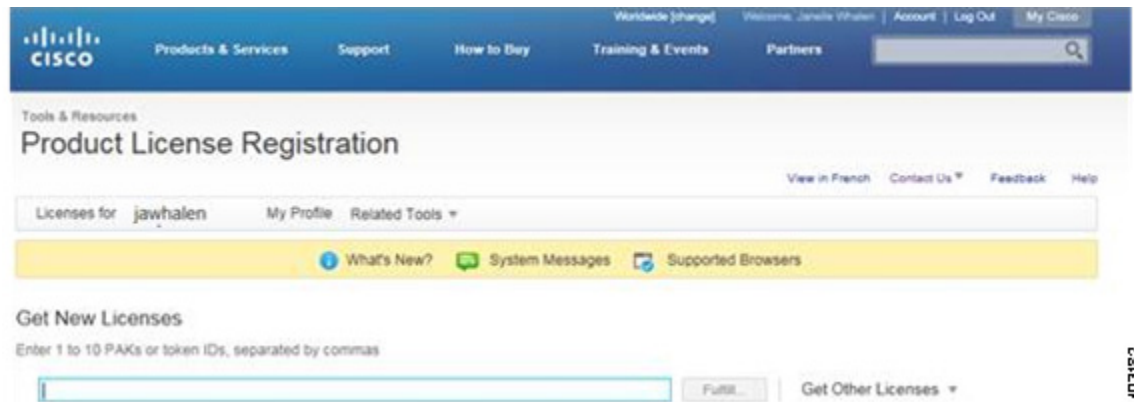


Note

You will need a CCO ID to access the License Registration Portal.



Step 2 Click the green **Continue to Product License Registration** button on the right-hand side of the screen.



- Step 3** Enter the Cisco PAK into the **Get New Licenses** text box and click the **Fulfill** box.
- Step 4** Your license is generated on the screen as well as emailed to you directly.

Selecting PIDs for Upgrade Licenses

Use this table to select PIDs to use with the Product Upgrade Tool.

Need a Protection and Control OR FireSIGHT License for:	Select Below:	For Reference by Partners and Account teams only		
Model	Upgrade Licenses	Source Fire PID	Cisco Equivalent PIDs	Description
3D500	L-3D500-5UPG-K9=	3D500-IPS-C04-000	FP500-PROT-LIC	
3D1000	L-3D1000-5UPG-K9=	3D1000-IPS-C04-000	FP1000-PROT-LIC	
3D2000	L-3D2000-5UPG-K9=	3D2000-IPS-C04-000	FP2000-PROT-LIC	
3D2100	L-3D2100-5UPG-K9=	3D2100-IPS-C04-000	FP2100-PROT-LIC	
3D2500	L-3D2500-5UPG-K9=	3D2500-IPS-C04-F04	FP2500-PROT-LIC	
3D3500	L-3D3500-5UPG-K9=	3D3500-IPS-C04-F04	FP3500-PROT-LIC	
3D4500	L-3D4500-5UPG-K9=	3D4500-IPS-C04-F04	FP4500-PROT-LIC	
3D6500	L-3D6500-5UPG-K9=	3D6500-IPS-C06-F02-LR	FP6500-PROT-LIC	
FP7010	L-FP7010-5UPG-K9=	LIC-CTRL-3D7010	FP7010-CTRL-LIC	Cisco FirePOWER 7010 Control License
FP7020	L-FP7020-5UPG-K9=	LIC-CTRL-3D7020	FP7020-CTRL-LIC	Cisco FirePOWER 7010 Control License
FP7030	L-FP7030-5UPG-K9=	LIC-CTRL-3D7030	FP7030-CTRL-LIC	Cisco FirePOWER 7010 Control License
FP7110	L-FP7110-5UPG-K9=	LIC-CTRL-3D7110	FP7110-CTRL-LIC	Cisco FirePOWER 7010 Control License
FP7120	L-FP7120-5UPG-K9=	LIC-CTRL-3D7120	FP7120-CTRL-LIC	Cisco FirePOWER 7010 Control License

Need a Protection and Control OR FireSIGHT License for:	Select Below:	For Reference by Partners and Account teams only		
Model	Upgrade Licenses	Source Fire PID	Cisco Equivalent PIDs	Description
FP8120	L-FP8120-5UPG-K9=	LIC-CTRL-3D8120	FP8120-CTRL-LIC	Cisco FirePOWER 7010 Control License
FP8130	L-FP8130-5UPG-K9=	LIC-CTRL-3D8130	FP8130-CTRL-LIC	Cisco FirePOWER 7010 Control License
FP8140	L-FP8140-5UPG-K9=	LIC-CTRL-3D8140	FP8140-CTRL-LIC	Cisco FirePOWER 7010 Control License
FP8250	L-FP8250-5UPG-K9=	LIC-CTRL-3D8250	FP8250-CTRL-LIC	Cisco FirePOWER 7010 Control License
FP8260	L-FP8260-5UPG-K9=	LIC-CTRL-3D8260	FP8260-CTRL-LIC	Cisco FirePOWER 7010 Control License
FP8270	L-FP8270-5UPG-K9=	LIC-CTRL-3D8270	FP8270-CTRL-LIC	Cisco FirePOWER 7010 Control License
FP8290	L-FP8290-5UPG-K9=	LIC-CTRL-3D8290	FP8290-CTRL-LIC	Cisco FirePOWER 7010 Control License
Virtual FirePOWER	L-FPVMW-5UPG-K9=	V3D-RedHat-IPS-1	FP-VM-RH-IPS-LIC=	
		V3D-VMWARE-IPS-1	FP-VMW4-IPS-LIC=	
		V3D-XEN-IPS-1	FP-VM-XEN-IPS-LIC=	
		LIC-CTRL-VMWARE	FP-VMW-IPS-LIC	
		V3D-NGFW-VMWARE		
FireSIGHT License for management center on v5.x	SF-FSVMW-5UPG-K9	VDC-RedHat	FS-VM-REDHAT-SW-K9	
		VDC-VMWARE	FS-VMW-SW-K9	
		VDC-XEN	FS-VMW-XEN-SW-K9	
		VDC-64bit-VMWARE-BNDL-0	FS-VMW-SW-K9	
		VDC-VMWARE-FS410-0	FS410X-VMW-SW-K9	
		VDC-XEN-FS410-0	FS-VM-XEN-MAX-K9	

Selecting PIDs for Additional Feature Licenses

Use this table to select PIDs for ordering subscription licenses for additional features. See [Cisco Security Ordering Guide for Legacy Sourcefire and Related Cisco Offerings](#) for more information.

Model	IPS+Apps+SI	IPS+Apps+SI & Advanced Malware Protection	IPS+Apps+SI & URL Filtering	IPS+Apps+SI & URL Filtering & Advanced Malware Protection
3D500	FP500-TA-LIC=	n/a	n/a	n/a
3D1000	FP1000-TA-LIC=	n/a	n/a	n/a
3D2000	FP2000-TA-LIC=	n/a	n/a	n/a

Model	IPS+Apps+SI	IPS+Apps+SI & Advanced Malware Protection	IPS+Apps+SI & URL Filtering	IPS+Apps+SI & URL Filtering & Advanced Malware Protection
3D2100	FP2100-TA-LIC=	n/a	n/a	n/a
3D2500	FP2500-TA-LIC=	n/a	n/a	n/a
3D3500	FP3500-TA-LIC=	n/a	n/a	n/a
3D4500	FP4500-TA-LIC=	n/a	n/a	n/a
3D6500	FP6500-TA-LIC=	n/a	n/a	n/a
FP7010	FP7010-TA-LIC=	FP7010-TAM-LIC=	FP7010-TAC-LIC=	FP7010-TAMC-LIC=
FP7020	FP7020-TA-LIC=	FP7020-TAM-LIC=	FP7020-TAC-LIC=	FP7020-TAMC-LIC=
FP7030	FP7030-TA-LIC=	FP7030-TAM-LIC=	FP7030-TAC-LIC=	FP7030-TAMC-LIC=
FP7110	FP7110-TA-LIC=	FP7110-TAM-LIC=	FP7110-TAC-LIC=	FP7110-TAMC-LIC=
FP7120	FP7120-TA-LIC=	FP7120-TAM-LIC=	FP7120-TAC-LIC=	FP7120-TAMC-LIC=
FP8120	FP8120-TA-LIC=	FP8120-TAM-LIC=	FP8120-TAC-LIC=	FP8120-TAMC-LIC=
FP8130	FP8130-TA-LIC=	FP8130-TAM-LIC=	FP8130-TAC-LIC=	FP8130-TAMC-LIC=
FP8140	FP8140-TA-LIC=	FP8140-TAM-LIC=	FP8140-TAC-LIC=	FP8140-TAMC-LIC=
FP8250	FP8250-TA-LIC=	FP8250-TAM-LIC=	FP8250-TAC-LIC=	FP8250-TAMC-LIC=
FP8260	FP8260-TA-LIC=	FP8260-TAM-LIC=	FP8260-TAC-LIC=	FP8260-TAMC-LIC=
FP8270	FP8270-TA-LIC=	FP8270-TAM-LIC=	FP8270-TAC-LIC=	FP8270-TAMC-LIC=
FP8290	FP8290-TA-LIC=	FP8290-TAM-LIC=	FP8290-TAC-LIC=	FP8290-TAMC-LIC=
Virtual FirePOWER	FPVMW-TA-LIC=	FPVMW-TAM-LIC=	FPVMW-TAC-LIC=	FPVMW-TAMC-LIC=

Additional Information

Watch the [License Activation Video](#) for a demonstration.

You can find additional information on licensing in the [Sourcefire Licensing Support Forum](#).

Redundancy and Resource Sharing

The redundancy and resource-sharing features allow you to ensure continuity of operations and to combine the processing resources of multiple physical devices. Device stacking and Defense Center high availability are still supported on many models. Version 5.2 adds clustering, clustered stacks, and other methods of achieving Layer 3 redundancy.

Defense Center High Availability

To ensure continuity of operations, a Defense Center *high availability* feature allows you to designate redundant DC1000, DC1500, DC3000, or DC3500 Defense Centers to manage devices. The new configurations available in Version 5.2 are maintained on peer Defense Centers. Additionally, the Vulnerability Database (VDB) is now synchronized.

Device Stacking

Device stacking allows you to increase the amount of traffic inspected on a network segment by connecting two to four physical devices in a stacked configuration. When you establish a stacked configuration, you combine the resources of each stacked device into a single, shared configuration. The same devices that supported stacking in Version 4.10.3 support it in Version 5.2.

Device Clustering

Device clustering (sometimes called device high availability) allows you to establish redundancy of networking functionality and configuration data between two or more Series 3 devices or stacks. Clustering two or more peer devices or stacks results in a single logical system for policy applies, system updates, and registration. With device clustering, the system can fail over either manually or automatically.

SFRP

In most cases, you can achieve Layer 3 redundancy without clustering devices by using the Sourcefire Redundancy Protocol (SFRP). SFRP allows Series 3 devices to act as redundant gateways for specified IP addresses. With network redundancy, you can configure two or more devices or stacks to provide identical network connections, ensuring connectivity for other hosts on the network.

Network Traffic Management

Version 5.2 has multiple network traffic management features that allow licensed Series 3 devices to act as part of your organization's network infrastructure. You can:

- configure a Layer 2 deployment to perform packet switching between two or more network segments
- configure a Layer 3 deployment to route traffic between two or more interfaces
- enable strict enforcement for an inline set, virtual router, or virtual switch on a physical managed device, which blocks connections where the three-way handshake is incomplete
- perform network address translation (NAT)
- build secure VPN tunnels from virtual routers on managed devices to remote devices

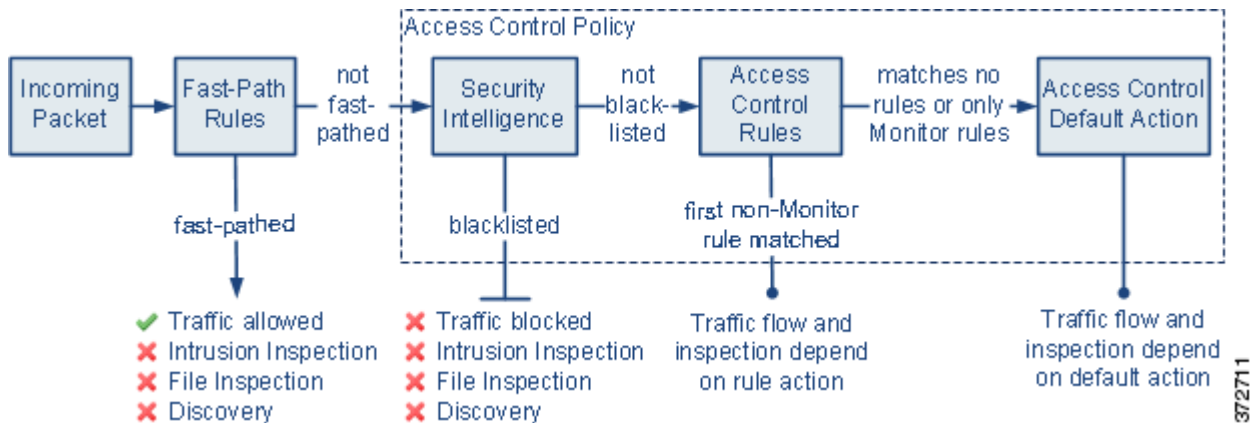
Access Control

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.

Access control rules inside a policy define how traffic is handled by managed devices. These rules can allow, monitor, inspect, or block traffic based on multiple criteria. They can perform simple IP matching, or create complex scenarios involving different networks, users, applications, ports, and URLs.

Using rules within access control policies, you can also invoke intrusion detection and prevention, file control, and advanced malware protection on specific traffic. Finally, access control policies define the traffic that you permit and, therefore, the traffic you can monitor with the discovery feature (previously called *RNA*).

The diagram below illustrates traffic flow through the system, and provides some details on the types of inspection performed on that traffic.



For more information, see:

- [Security Intelligence Filtering](#), page 1-17
- [Application Control](#), page 1-17
- [User Control](#), page 1-18
- [URL Filtering](#), page 1-18
- [Connection Logging](#), page 1-18
- [Intrusion Detection and Prevention](#), page 1-19
- [File Tracking, File Control, and Malware Protection](#), page 1-19
- [Network Discovery](#), page 1-21

Security Intelligence Filtering

As part of access control, *Security Intelligence* allows you to blacklist—deny traffic to and from—specific IP addresses before the traffic is subjected to analysis by access control rules.

Series 2 devices cannot perform Security Intelligence filtering, nor can the DC500 manage a Security Intelligence deployment.

Application Control

Application control allows you to use the application detection capabilities to determine the traffic that you want to block, allow, or inspect further. The system detects the following types of application:

- *application protocols* (formerly *services*) such as HTTP and SSH, which represent communications between hosts
- *clients* (formerly *client applications*) such as web browsers and email clients, which represent software running on the host
- *web applications* (formerly *payloads*) such as MPEG video and Facebook, which represent the content or requested URL for HTTP traffic

The system also associates each application that it detects with a predetermined risk and business relevance, as well as a category and optional tags that describe the application's functions and effects.

You can use access control to handle traffic based on the detection of individual applications, or for groups of applications called application filters (see [Reusable Objects](#), page 1-22).

Series 2 devices cannot perform application control.

User Control

User control allows you to use the user detection capabilities, in conjunction with a Microsoft Active Directory deployment, to determine the traffic that you want to block, allow, or inspect. User control replaces and augments the Version 4.10.3 Real-Time User Awareness (RUA) component.

The Defense Center retrieves groups and user names from an Active Directory server you specify. *Sourcefire User Agents* (formerly *RUA Agents*) monitor those users as they log into the network or when they authenticate against Active Directory credentials for any other reason. You can handle network traffic for these *access-controlled users* on an individual or group basis.

You can also track (but not control) activity for *non-access-controlled users*, including users detected in specific types of network traffic (for example, IMAP or SIP/VoIP) by managed devices. User Agents can also report LDAP logins for *non-access-controlled users*, and the Defense Center can retrieve user metadata from Active Directory servers.



Note

Use at least Version 2.1 of the User Agent with your Version 5.2 deployment. Version 2.1 has flexible deployment options and includes IPv6 support. It also can detect logoffs and provide information on various types of logins, including interactive user logins to a host, remote desktop logins, file-share authentication, and computer account logins. Support for legacy agents will be phased out in future releases. For more information, see the [Sourcefire 3D System User Agent Configuration Guide](#).

Series 2 devices cannot perform user control, nor can the DC500 manage a user control deployment, although each of these appliances can gather user identity data.

URL Filtering

URL filtering is a licensed feature that allows you to determine the traffic that you want to block, allow, or inspect, based on URLs requested by monitored hosts.

When you enable URL filtering, the Defense Center contacts a cloud service, retrieves data on many commonly visited URLs, and saves that data on licensed appliances. Each of these URLs has an associated category and reputation. These attributes allow you to quickly create URL conditions for access control rules, which can group and combine URL categories and reputations.

Because the cloud service is continually updated with new URLs, as well as new categories and risks for existing URLs, using the cloud service ensures that the system uses up-to-date information to filter requested URLs. Malicious sites that represent security threats such as malware, spam, botnets, and phishing may appear and disappear faster than you can update and apply new policies.

You can also achieve more granular, custom control over URL conditions in access control rules by specifying individual URLs or groups of URLs.

Series 2 devices cannot perform URL filtering of any kind. The DC500 cannot manage a deployment where you filter traffic by URL category and reputation. However, the DC500 can manage devices that filter web traffic using individual URLs or groups of URLs.

Connection Logging

In Version 5.2, you now use the access control feature (instead of the RNA detection policy) to configure the logging of *connection events* (formerly *flow data*) detected by managed devices.

For each access control rule, you must decide whether you want to log connections that match the rule. Tying connection logging to individual rules gives you granular control over the connections you want to log.

You should log connections according to the security and compliance needs of your organization. If your goal is to limit the number of events you generate, only enable logging for the traffic critical to your analysis. However, if you want a broader view of your network traffic, you can enable logging for additional rules.

Depending on the rule, you can log a connection event at the beginning or end of a matched connection, or both. In Version 4.10.3, RNA logged connection events only at the end of connections.

In general, if you want to perform analysis on connection data, log end-of-connection events. This is because beginning-of-connection events do not have information that must be determined by examining traffic over the duration of the session. If, however, you simply want to log an event each time the system detects a new connection, beginning-of-connection events are sufficient.

**Note**

As in previous releases, you configure NetFlow connection logging in the network discovery policy.

Intrusion Detection and Prevention

In Version 5.2, intrusion detection and prevention is integrated with access control. Instead of applying intrusion policies independently, you can now associate an intrusion policy with specific access control rules. When traffic matches an access control rule, the system uses the associated intrusion policy to inspect it. The system can also use an intrusion policy associated with the default action of an access control policy to inspect traffic that does not match rules in the policy.

Intrusion Rule Updates

Intrusion *rule updates*, sometimes called SRUs, replace Security Enhancement Updates (SEUs).

Rule updates provide new and updated intrusion rules and preprocessor rules, modified states for existing rules, and modified default intrusion policy settings. Rule updates may also delete rules and provide new rule categories and system variables. However, they no longer provide new or updated intrusion prevention features such as preprocessors.

FireSIGHT Rule Recommendations

If you use FireSIGHT rule recommendations, the system no longer makes intrusion rule state recommendations for rules with a very high overhead rating. Now, you must manually set the rule state for any rule with a very high overhead rating. If you have intrusion policies where the threshold is set to very high, the migration process changes it to high.

Adaptive Profiles

In Version 5.2, the system applies an intrusion rule to traffic if the rule's service metadata matches application traffic. This occurs regardless of whether you enable adaptive profiles. Enabling adaptive profiles still applies host information gathered from the network to traffic for processing.

File Tracking, File Control, and Malware Protection

To help you identify and mitigate the effects of malware, Version 5.2 of the system includes file control, network file trajectory, and advanced malware protection (AMP) components. You can detect, track, and optionally block the transmission of files (including malware files) in network traffic.

File Control

File control allows managed devices to detect and block your users from uploading (sending) or downloading (receiving) files of specific types over specific application protocols. You configure file control as part of your overall access control configuration; file policies associated with access control rules inspect network traffic that meets rule conditions.

Network-Based Advanced Malware Protection (AMP)

Network-based *advanced malware protection* (AMP) allows the system to inspect network traffic for malware in several types of files, including PDFs, many Microsoft Office documents, and other types. When a managed device detects one of these file types, the Defense Center obtains the file's disposition and the managed device uses this information to block or allow the file.

You configure malware protection as part of your overall access control configuration; file policies associated with access control rules inspect network traffic that meets rule conditions.

Series 2 devices cannot perform network-based AMP, nor can the DC500 manage a network-based AMP deployment.

FireAMP Integration

FireAMP is an enterprise-class, advanced malware analysis and protection solution that discovers, understands, and blocks advanced malware outbreaks, advanced persistent threats, and targeted attacks.

If your organization has a FireAMP subscription, individual users install *FireAMP Connectors* on their computers and mobile devices (also called *endpoints*). These lightweight agents communicate with the Cisco cloud, which in turn communicates with the Defense Center. After you configure the Defense Center to connect to the cloud, you can use the Defense Center web interface to view endpoint-based malware events generated as a result of scans, detections, and quarantines on the endpoints in your organization.

Use the *FireAMP portal* (<http://amp.sourcefire.com/>) to configure your FireAMP deployment. The portal helps you quickly identify and quarantine malware. You can identify outbreaks when they occur, track their trajectories, understand their effects, and learn how to successfully recover. You can also use FireAMP to create custom protections, block execution of certain applications based on group policy, and create custom whitelists.

Network File Trajectory

The network file trajectory feature allows you to track a file's transmission path across a network. The system uses SHA-256 hash values to track files; so, to track a file, the system must either:

- calculate the file's SHA-256 value and perform a cloud lookup using that value
- receive endpoint-based threat and quarantine data about that file, using the Defense Center's integration with your organization's FireAMP subscription

Each file has an associated trajectory map, which contains a visual display of the file's transfers over time as well as additional information about the file.

You cannot view file trajectories for files detected by Series 2 devices, nor can you view network-based trajectories on a DC500 Defense Center.

Network Discovery

Version 5.2 integrates RNA and RUA into a feature called *discovery*, and also adds additional capabilities. Discovery can analyze IPv4 and IPv6 network traffic that is not fast-pathed at the device level, or blocked or trusted by the access control policy. In other words, only allowed traffic can be analyzed.

In the *network discovery policy*, which replaces the RNA detection policy, you can create *discovery rules* that specify exactly which network segments the system should monitor. For each segment, you can discover applications, hosts, and user activity.

Host Detection

Version 5.2 uses details unique to mobile device traffic to identify a wide variety of mobile operating systems, mobile applications, and associated mobile device hardware. The system can also detect “jailbroken” devices, that is, devices where the user has removed manufacturer limitations on the operating system.

Application Detection

Version 5.2 adds a significant number of detected applications, and introduces application control based on this detection; see [Application Control, page 1-17](#). The application management page is also redesigned and improved. For a complete list of the applications detected, see the Support Site.

User Detection

With Version 5.2, you retain the ability to perform network-based user identification using managed devices to monitor logins over IMAP, POP3, SIP/VoIP, and so on.

In conjunction with a Microsoft Active Directory deployment, you can also deploy User Agents to monitor and retrieve metadata for users as they log into the network or when they authenticate against Active Directory credentials for any other reason. Version 5.2 of the system adds the ability to perform user control for what are called *access-controlled users*; see [User Control, page 1-18](#).

Version 2.1 of the agent has flexible deployment options and includes IPv6 support. It also can detect logoffs and provide information on various types of logins, including interactive user logins to a host, remote desktop logins, file-share authentication, and computer account logins.



Note

If you want to perform user control, you **must** install and use Sourcefire User Agents. Use at least Version 2.1 of the User Agent with your Version 5.2 deployment. Support for legacy agents will be phased out in future releases. For more information, see the [Sourcefire 3D System User Agent Configuration Guide](#).

NetFlow

In Version 5.2, you continue to configure NetFlow connection logging (formerly flow data logging) in the network discovery policy. Because NetFlow data collection is not linked to access control rules, you do not have granular control over which connections you want to log. The system automatically saves all NetFlow-based connection events to the Defense Center database; NetFlow events are unidirectional and end-of-connection only.

Geolocation Information

Version 5.2's *geolocation* feature provides you with additional data about the geographical sources of routable, detected IP addresses (country, continent, and so on).

By regularly updating the geolocation database (GeoDB), you can use the Defense Center to view up-to-date granular information available for an IP address, such as postal code, coordinates, time zone, Autonomous System Number (ASN), Internet service provider (ISP), use type (home or business), organization, domain name, connection type, and proxy information. You can also pinpoint the detected location with any of four third-party map tools.

Dashboards

Version 5.2 adds predefined dashboards, as well as presets for Custom Analysis widgets and configuration options in other widgets. The changes are consistent with the added features and functionality, including: AMP, geolocation, user activity, URL tracking, and so on.

Context Explorer

Version 5.2 features the Context Explorer, which displays detailed, interactive graphical information about your monitored network, using intrusion, connection, file, geolocation, malware, and discovery data.

Distinct sections present information in the form of vivid line, bar, pie, and donut graphs, accompanied by detailed lists. You can easily create and apply custom filters to fine-tune your analysis, and you can examine data sections in more detail by clicking or hovering your cursor over graph areas.

Compared with a dashboard, which is highly customizable, compartmentalized, and updates in real time, the Context Explorer is manually updated, designed to provide broader context for its data, and has a single, consistent layout designed for active user exploration.

Reusable Objects

The system's new object manager helps you manage objects and other reusable configurations. Objects associate a name with some value or values. When you want to use that value, you can use the named object instead.

Objects can represent IP addresses or ranges of IP addresses, port-protocol combinations, VLAN tags, or URLs. You can use objects in various policies, searches, rules, and so on.

You can also use the object manager to administer:

- *application filters*, which group applications according to criteria associated with the application risk, business relevance, type, categories, and tags. You can use these filters to constrain access control rules, searches, dashboard widgets, and reports.
- the *global malware whitelist* of files (based on SHA-256 hash values) that you do not want to inspect or block using AMP; see [File Tracking, File Control, and Malware Protection, page 1-19](#).
- Security Intelligence *lists* and *feeds* of IP addresses; see [Security Intelligence Filtering, page 1-17](#).
- *security zones*, which group one or more inline, passive, switched, or routed interfaces. The interfaces in a single zone can span multiple devices; you can also configure multiple security zones on a single device. Zones allow you to manage and classify traffic flow in various policies and configurations.

Reporting

The reporting interface has been significantly redesigned to give you increased flexibility when designing *report templates* (previously *report profiles*), as well as to improve the ease of use. You can now email reports upon generation, as well as import and export report templates. You can no longer modify system-provided report templates.

The new interface also introduces the concept of report *input parameters*, which allow you to configure a report template to require the user to provide values at generation time that customize the generated report. In this way, you can dynamically tailor a report at generation time to show a particular subset of data, without changing the template.

Health Monitoring

The Defense Center now has only one default health policy, which is used as the basis for the initial health policy applied to the Defense Center, and which you can use to create your own custom health policies.

New health modules provide additional monitoring capabilities. Also, the process of blacklisting individual health modules (instead of entire appliances) is now more straightforward.

Client Vulnerabilities and VDB Updates

The system now correlates vulnerabilities with clients (previously *client applications*) running on monitored hosts, and can use those vulnerabilities to perform impact assessment. Note, however, that you cannot import third-party client vulnerabilities using the host input feature, nor can you map vendorless or versionless clients to vulnerabilities.

Also, updating the VDB on a Defense Center automatically performs the update on all its managed devices. You no longer have to explicitly update all the appliances in your deployment. Similarly, the VDB is synchronized in high-availability pairs.

User Certificates

You can now add an additional layer of authentication for client connections to the web interface. If you require user certificates, the server checks that any client browser connecting to the web server has a valid user PKI certificate, issued by the same certificate authority that issued the server certificate.

If a client's browser does not have a valid certificate, it cannot connect to the server when user certificates are enabled. You can also configure the system to check certificate revocation lists (CRLs) to identify certificates that have been revoked by the certificate authority, then ignore the invalid certificates.

IPv6 Support

You can configure the Version 5.2 management interface for IPv4-only, IPv6-only, or dual-stacked IPv4/IPv6 networks. The system can integrate with other infrastructure components and detect and process both IPv4 and IPv6 traffic. Except in a few cases, the system supports IPv6 component integration and traffic detection and processing.

For information on the unsupported and partially supported features in an IPv6 environment, please contact Support.

Application Programming Interfaces

Version 5.2 changes the way you interact with the system using a couple of the supported application programming interfaces (APIs).

Database Access

For increased security, an access list now controls which hosts can query the Defense Center's database using a third-party database access client. You can specify individual IP addresses or IP address ranges.

eStreamer

eStreamer for Version 5.2 includes many new and replaced data blocks associated with new features. Additionally, the names of some of the record and block structures and their fields have been changed to align with new terminology. There is also a new "extended" method of requesting event streams that uses a new message streaming protocol.

Although the eStreamer server continues full support of the event stream request mode used in earlier versions, to request many of the new versions of event types, you must use the extended request mode.

Depending on the type of data you stream from the system, you may need to update your eStreamer client. For detailed information, see the [Version 5.2 Sourcefire 3D System eStreamer Integration Guide](#).

Also, you can now modify your Defense Center's eStreamer configuration to stream data from an alternate management port.

Deprecated Functionality

The following sections describe the deprecated features and functionality from Version 4.10.3 to Version 5.2.

Standalone IPS Devices

Standalone devices deployed as an Intrusion detection or prevention system are no longer supported. In Version 5.2, you must manage all devices with a Defense Center.

32-Bit Virtual Appliances and Xen Hypervisor Hosting

64-bit virtual appliances running Version 5.2 are supported on the VMWare vSphere version 4.1 or 5.0 hosting environment by VMWare. Neither the Xen Hypervisor hosting environment nor 32-bit appliances are supported.

You can migrate legacy configurations and events to a new 64-bit Defense Center that you create. For information on creating a new virtual appliance, see the [Version 5.2 Sourcefire 3D System Virtual Installation Guide](#).

OPSEC

Version 5.2 does not support OPSEC integration with the intrusion policy.

Master Defense Centers

The Master Defense Center is not available with Version 5.2.

PEP

Version 5.2 integrates PEP functionality with device management (fast-path rules) and access control (PEP rules). PEP is no longer separately configurable.

Detection Engines

The system now automatically allocates its computing and detection resources. You no longer have to explicitly assign detection engines to interface sets. Most configurations and statistics that were available on a per-detection engine basis are now available on a per-device or per-interface basis, as appropriate.

Appliance Series, Models, and Capabilities

The system combines the security of an industry-leading network intrusion detection and prevention system (IPS) with the power to control access to your network based on detected applications, users, and URLs.

You can also use appliances in a switched, routed, or hybrid (switched and routed) environment; to perform network address translation (NAT); and to build secure virtual private network (VPN) tunnels among the virtual routers on managed devices, or from managed devices to remote devices.

The Defense Center provides a centralized management console and database repository. Managed devices, installed either passively or inline, on network segments monitor traffic for analysis. In addition to physical appliances, Cisco packages 64-bit virtual Defense Centers and virtual devices for the VMWare vSphere version 4.1 or 5.0 hosting environment by VMWare.

Version 5.2 is available on two series of physical appliances, as well as virtual appliances. Many capabilities are appliance dependent.

For more information, see:

- [Series 2 Appliances, page 1-25](#)
- [Series 3 Appliances, page 1-26](#)
- [Virtual Appliances, page 1-26](#)
- [Supported Capabilities by Appliance Model, page 1-26](#)

Series 2 Appliances

Version 5.2 is the first 5.x release where Series 2 appliances are supported. Series 2 is the second series of physical appliances and includes:

- 3D500, 3D1000, and 3D2000 devices
- 3D2100, 3D2500, 3D3500, and 3D4500 devices
- 3D6500 devices
- DC500, DC1000, and DC3000 Defense Centers

Series 2 devices running Version 5.2 have the same capabilities they had when running Version 4.10.3: intrusion detection and prevention (IDS/IPS), network and user discovery (RNA and RUA), and so on. They also support some new 5.x features, such as file control and basic access control.

Because of resource and architecture limitations, Series 2 devices do not support features such as Security Intelligence filtering, advanced access control, and advanced malware protection. Series 2 devices do not support any of the hardware-based features associated with Series 3 devices: switching, routing, NAT, and so on.

The DC1000 and DC3000 Defense Centers support all features; the DC500 has more limited capabilities.

Series 3 Appliances

Series 3 is the third series of physical appliances, and includes:

- 7000 Series devices
- 8000 Series devices
- DC750, DC1500, and DC3500 Defense Centers

Note that 8000 Series devices are more powerful and support a few features that 7000 Series devices do not.

Virtual Appliances

You can host 64-bit virtual Defense Centers and devices on the VMWare vSphere version 4.1 or 5.0 hosting environment by VMWare. Virtual Defense Centers can manage physical and virtual devices; physical Defense Centers can manage physical and virtual devices.

Regardless of the licenses installed and applied, virtual appliances do not support any of the system's hardware-based features: redundancy (high availability, stacking, clustering), switching, routing, and so on. Also, virtual devices do not have web interfaces.

32-bit virtual appliances and Xen Hypervisor hosting environments are not supported with Version 5.2. You can, however, migrate configurations from your existing 32-bit Version 4.10.3 virtual appliances to a newly created 64-bit Version 5.2 Defense Center.

Supported Capabilities by Appliance Model

Many capabilities are appliance and license dependent. The following table matches the major capabilities of the system with the appliances that support those capabilities, assuming you have the correct licenses installed and applied.



Tip

For information on the terms used in the table, see: [New and Changed Terminology, page 1-2](#) and [New, Changed, and Updated Features and Functionality, page 1-3](#). You can also find detailed information in the [Version 5.2 Sourcefire 3D System User Guide](#).

Keep in mind that in Version 5.x, analysis functions are restricted to the Defense Center. Only essential management and monitoring functions are available on managed devices; standalone device deployments are not supported. In the table, the Defense Center column for device-based capabilities (such as stacking, switching, and routing) indicates whether that Defense Center can manage and configure devices to perform their functions. For example, you can use a Series 2 DC1000 to manage NAT on Series 3 devices. Also note that certain Defense Center-based features, such as high availability and FireAMP integration, are not relevant to managed devices.

Table 1-4 Supported Capabilities by Appliance Model

Feature	Series 2 Device	Series 2 Defense Center	Series 3 Device	Series 3 Defense Center	Virtual Device	Virtual Defense Center
network discovery: host, application, and user	yes	yes	yes	yes	yes	yes
geolocation data	yes	DC1000, DC3000 only	yes	yes	yes	yes
intrusion detection and prevention (IPS)	yes	yes	yes	yes	yes	yes
Security Intelligence filtering	no	DC1000, DC3000 only	yes	yes	yes	yes
access control: basic network control	yes	yes	yes	yes	yes	yes
access control: applications	no	yes	yes	yes	yes	yes
access control: users	no	DC1000, DC3000 only	yes	yes	yes	yes
access control: literal URLs	no	yes	yes	yes	yes	yes
access control: URL filtering by category and reputation	no	DC1000, DC3000 only	yes	yes	yes	yes
file control: by file type	yes	yes	yes	yes	yes	yes
network-based advanced malware protection (AMP)	no	DC1000, DC3000 only	yes	yes	yes	yes
FireAMP integration	no	yes	no	yes	no	yes
fast-path rules	no	yes	8000 Series only	yes	no	yes
strict TCP enforcement	no	yes	yes	yes	no	yes
configurable bypass interfaces	yes	yes	except where hardware limited	yes	no	yes
tap mode	no	yes	yes	yes	no	yes
switching and routing	no	yes	yes	yes	no	yes
NAT policies	no	yes	yes	yes	no	yes
VPN	no	yes	yes	yes	no	yes
high availability	no	DC1000, DC3000 only	no	DC1500, DC3500 only	no	no
device stacking	no	yes	3D8140, 82xx Family only	yes	no	yes

Table 1-4 Supported Capabilities by Appliance Model (continued)

Feature	Series 2 Device	Series 2 Defense Center	Series 3 Device	Series 3 Defense Center	Virtual Device	Virtual Defense Center
device clustering	no	yes	yes	yes	no	yes
clustered stacks	no	yes	3D8140, 82xx Family only	yes	no	yes
interactive CLI	no	no	yes	no	yes	no

Where Do I Begin?

The chapters in this guide step you through the process of migrating vital configurations and events from either a Version 4.10.3 Defense Center or standalone 3D Sensor to a Version 5.2 Defense Center. To migrate your deployment, read and follow the directions in these chapters.

Understanding the Migration Process

[Understanding the Migration Process, page 2-1](#) provides an overview of the migration process. This chapter explains the importance of planning your migration and the advantages and limitations of reimaging your existing Version 4.10.3 appliances or deploying new Version 5.2 appliances.

Example scenarios are designed to help you develop a plan for migrating your unique deployment:

- migrating a multi-sensor deployment with either a replacement or a reimaged Defense Center, or a re-created virtual Defense Center
- performing a “rolling” migration where you replace sensors in turn to minimize inspection downtime
- migrating stacked 3D Sensors
- migrating a deployment with a high availability Defense Center pair
- migrating standalone 3D Sensors with IPS

Preparing for Migration

[Preparing for Migration, page 3-1](#) helps you prepare to migrate your deployment from Version 4.10.3 to Version 5.2 smoothly and without error. Read this chapter to make sure you understand:

- the appliance models that you can migrate, including licensing requirements, and the capabilities of your deployment after you install Version 5.2
- system software and intrusion rule update requirements
- for virtual appliances, host environment and memory requirements
- how the migration affects your organization’s network traffic
- when and how to perform the migration so as to least disrupt your deployment
- the consequences of and how to avoid configurations that translate poorly to the Version 5.2 architecture
- how to obtain, identify, and install the migration scripts

Performing the Migration

[Performing the Migration, page 4-1](#) steps you through the actual migration process, which is done by running system-provided scripts using an appliance's shell according to your migration plan. For your convenience, the chapter also describes steps you must take after you run the scripts, using the Version 5.2 Defense Center web interface.

Understanding Migrated Configurations and Events

[Understanding Migrated Configurations and Events, page 5-1](#) helps you understand exactly:

- which configurations and events will be migrated
- which configurations have changed location or names due to terminology changes and the redesigned web interface
- what new configurations will be created on the Version 5.2 Defense Center

The chapter also helps you understand what will not be migrated, and therefore which configurations you must re-create.

For More Information

For more information on how you can upgrade to newer versions of the Sourcefire 3D System, now known as the FireSIGHT System, refer to the documentation resources listed in the [FireSIGHT System Documentation Roadmap](#).

