



Product Guide
Revision A

Intel® Security Controller 2.0

COPYRIGHT

Copyright © 2015 McAfee, Inc., 2821 Mission College Boulevard, Santa Clara, CA 95054, 1.888.847.8766, www.intelsecurity.com

TRADEMARK ATTRIBUTIONS

Intel and the Intel logo are registered trademarks of the Intel Corporation in the US and/or other countries. McAfee and the McAfee logo, McAfee Active Protection, McAfee DeepSAFE, ePolicy Orchestrator, McAfee ePO, McAfee EMM, McAfee Evader, Foundscore, Foundstone, Global Threat Intelligence, McAfee LiveSafe, Policy Lab, McAfee QuickClean, Safe Eyes, McAfee SECURE, McAfee Shredder, SiteAdvisor, McAfee Stinger, McAfee TechMaster, McAfee Total Protection, TrustedSource, VirusScan are registered trademarks or trademarks of McAfee, Inc. or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others.

LICENSE INFORMATION

License Agreement

NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANY YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEBSITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.

Contents

	Preface	5
	About this guide	5
	Conventions	5
	Find product documentation	6
1	Overview	7
	Security challenges in an SDDC	8
	How Intel Security Controller secures virtual networks	9
	Advantages of Intel Security Controller	12
2	Installing the Intel Security Controller virtual appliance	13
	Requirements for Intel Security Controller	13
	Assumptions before setting up Intel Security Controller	14
	Install the Intel Security Controller virtual appliance	14
3	Setting up Intel Security Controller	21
	Accessing the Intel Security Controller web application	21
	Managing Intel Security Controller users	23
	Configuring the Intel Security Controller appliance	24
	View the summary details for Intel Security Controller	24
	Manage the network settings for Intel Security Controller	25
	Maintaining the Intel Security Controller virtual appliance	29
4	Working with the Intel Security Controller web application	37
	Terminology	39
	Define virtualization connectors	40
	Define Security Groups	44
	Define manager connectors	48
	Manage software images for virtual security appliances	51
	Define the service function catalog	52
	Change the software version of security appliances	54
	Define distributed appliances	57
	Define Deployment Specifications	64
	Define Traffic Policy Mappings	67
	Maintaining virtual appliance instances	68
	Delete a distributed appliance	71
	Jobs and tasks	74
	Viewing jobs and tasks	74
	Alarms, alerts, and archives	79
	Alarms	79
	Alerts	83
	Archiving	85
5	Intel Security Controller CLI commands - normal mode	89
	clear	90

debug	90
exit	90
help	90
history	91
list	91
ping	91
ping6	92
reset	92
server restart	92
server start	92
server status	92
server stop	93
set network dns	93
set network domain	93
set network gateway	93
set network hostname	94
set network ip	94
set network ntp	95
set passwd	95
set time	95
set timezone	96
show arp	96
show clock	96
show filesystems	96
show log	97
show log follow	97
show log last	97
show log reverse	97
show network dns	97
show network domain	98
show network hostname	98
show network ip	98
show network ntp	98
show network route	98
show process	99
show process monitor	99
show system memory	99
show system uptime	99
show version	99
shutdown	99
traceroute	100
traceroute6	100
6 Deploying a security service function to virtual networks	101
High-level steps to implement a security service	102
Define an IP address pool for virtual security appliances	104
Deploy virtual systems	108
Create a security group in VMware NSX	113
Create a security policy in VMware NSX	116
Apply a security policy to a security group in VMware NSX	120
Configure Virtual Security System to fail-close or fail-open	123
Assign policy groups to virtual security systems	126
Quarantine endpoints using NSX features	128
Index	135

Preface

This guide provides the information you need to work with your McAfee product.

Contents

- *About this guide*
- *Find product documentation*

About this guide

This information describes the guide's target audience, the typographical conventions and icons used in this guide, and how the guide is organized.

Conventions

This guide uses these typographical conventions and icons.

Book title, term, emphasis

Title of a book, chapter, or topic; a new term; emphasis.

Bold

Text that is strongly emphasized.

User input, code, message

Commands and other text that the user types; a code sample; a displayed message.

Interface text

Words from the product interface like options, menus, buttons, and dialog boxes.

Hypertext blue

A link to a topic or to an external website.



Note: Additional information, like an alternate method of accessing an option.



Tip: Suggestions and recommendations.



Important/Caution: Valuable advice to protect your computer system, software installation, network, business, or data.



Warning: Critical advice to prevent bodily harm when using a hardware product.

Find product documentation

After a product is released, information about the product is entered into the McAfee online Knowledge Center.

Task

- 1 Go to the **Knowledge Center** tab of the McAfee ServicePortal at <http://support.mcafee.com>.
- 2 In the **Knowledge Base** pane, click a content source:
 - **Product Documentation** to find user documentation
 - **Technical Articles** to find KnowledgeBase articles
- 3 Select **Do not clear my filters**.
- 4 Enter a product, select a version, then click **Search** to display a list of documents.

1

Overview

Intel Security Controller is a centralized platform to enable software-defined security for software-defined datacenters (SDDC). Intel Security Controller provides a common set of management services, acting as a broker between the security solutions and the virtual infrastructure. You can use Intel Security Controller to provide services such as next-generation IPS and firewall to virtual infrastructures.

Intel Security Controller integrates with a hypervisor and an networking provider to provide security solutions as a service to your virtual networks. Using Intel Security Controller as a liaison between the security service and its associated components, and the virtualization providers, you are able to provide security services for virtual networks. Currently, you are able to integrate with:

- McAfee® Network Security Platform (Network Security Platform)
- McAfee® Next Generation Firewall (McAfee NGFW)

To illustrate this, consider a virtual environment that uses VMware vCenter as its hypervisor and VMware NSX as its SDN controller to deploy security services on virtual infrastructure.

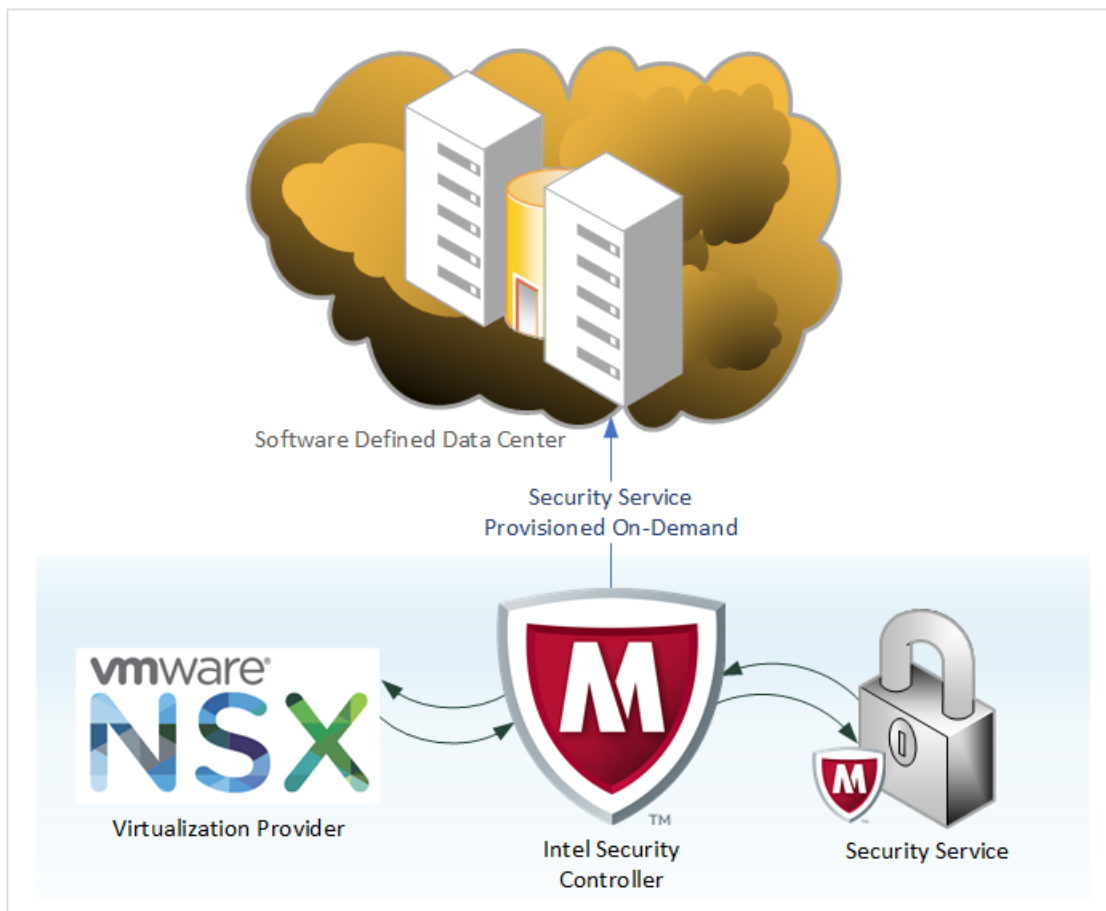


Figure 1-1 Intel Security Controller solution overview

Intel Security Controller is a virtual appliance that you install on an ESXi host. It provides a Java-based web application for configuration and management. You can deploy Intel Security Controller on existing virtual infrastructure without any configuration changes to those virtual networks.

Contents

- *Security challenges in an SDDC*
- *How Intel Security Controller secures virtual networks*
- *Advantages of Intel Security Controller*

Security challenges in an SDDC

Consider a large-scale SDDC consisting of hundreds of hosts aggregated under multiple clusters. Virtualization provides flexibility and agility to its users, wherein they can spin up virtual machines (VMs). Users can spin up isolated logical networks as easily as one can spin up VMs. All these possibilities require no changes in the physical networking configuration. When multiple users spin up new networks and move working VMs across physical boxes in such a large-scale data center, security is threatened.

To match with the capabilities of virtualization solutions, Intel Security Controller can seamlessly, non-intrusively, and non-disruptively integrate security services with existing virtualized environments. This enables network security services to keep pace with the speed, agility, and scalability of virtualization features and solutions.

How Intel Security Controller secures virtual networks

To understand how Intel Security Controller can orchestrate security for virtual networks, consider a VMware-based SDDC as illustrated here. For the sake of explanation, this SDDC is shown to contain only a few ESXi hosts.

Two ESXi hosts are clustered together. A few Windows VMs are connected to a distributed vSwitch that spans across these two ESXi hosts. VMware vCenter and NSX are installed on a third ESXi host in the same data center but outside the cluster. With vMotion, you can move the VMs between host-1 and host-2.

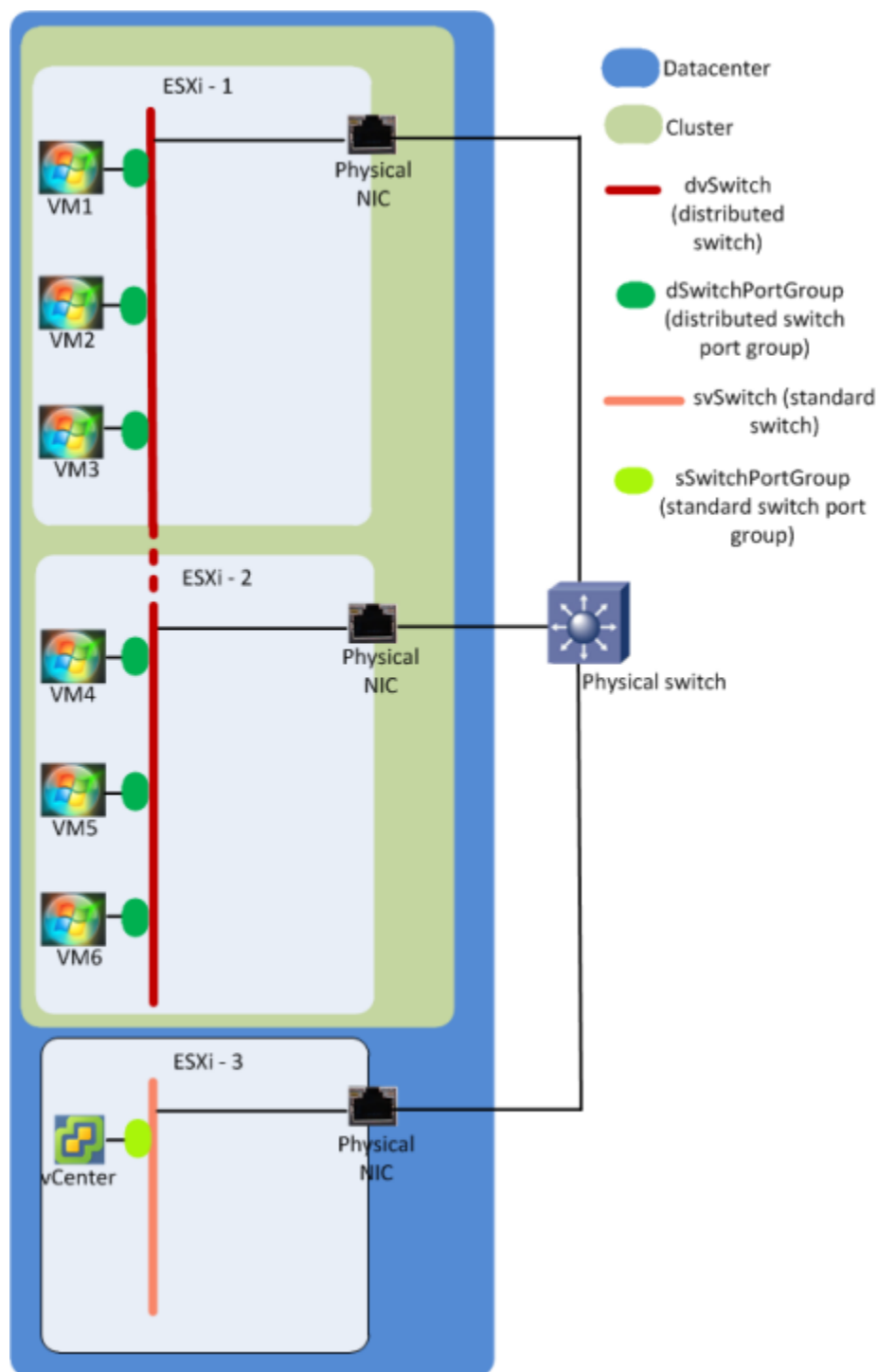


Figure 1-2 An example SDDC

Consider a datacenter in which you want to implement a security service function (security service) using Intel Security Controller. This illustration shows next-generation IPS.

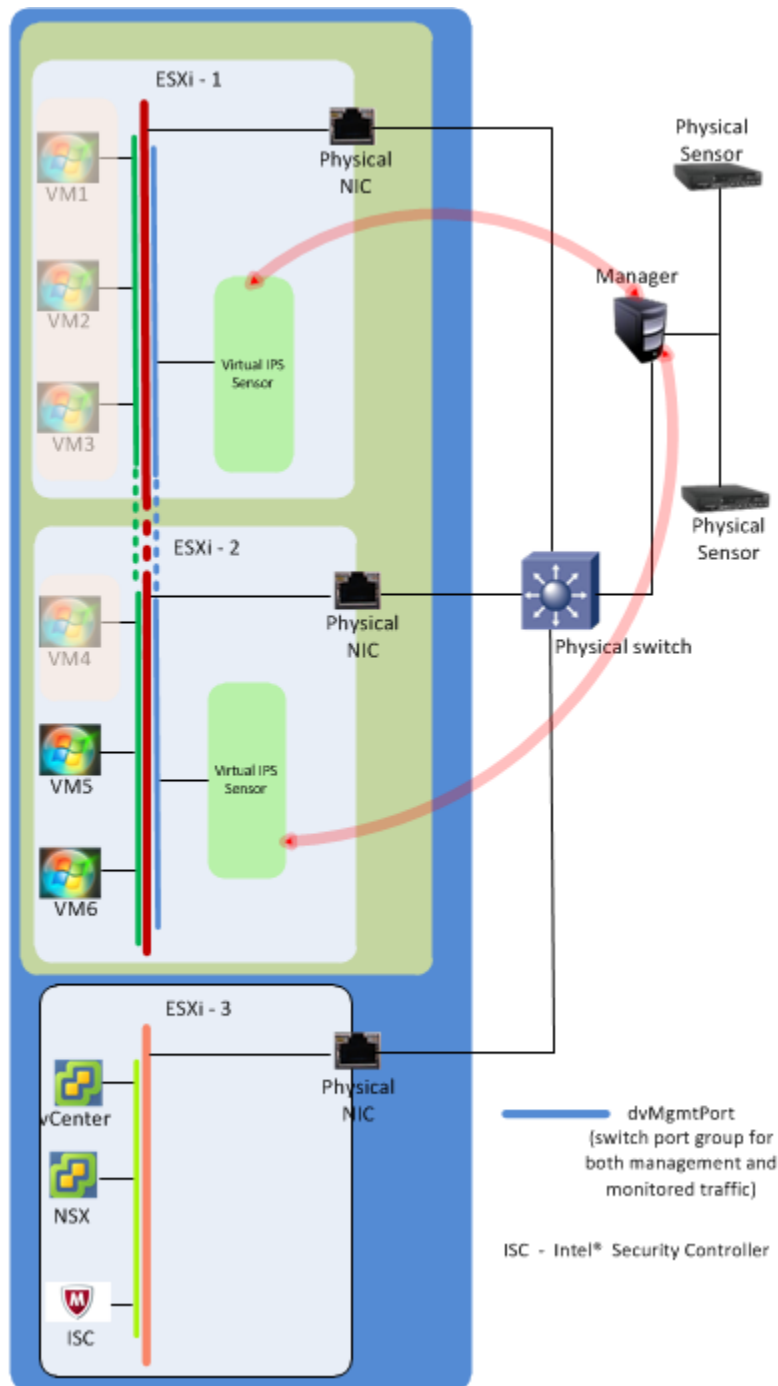


Figure 1-3 SDDC with IPS service through Intel Security Controller

To deploy a security service, some of the generic tasks you need to complete are.

- 1 Install the Intel Security Controller virtual appliance in an ESXi host outside the cluster in which you want to deploy the security service.
- 2 You deploy the security service to an ESXi cluster such that when you select an ESXi cluster, the security service is available to all VMs on the corresponding ESXi hosts. In this example, there is only one cluster. Intel Security Controller collaborates with vCenter and NSX such that virtual security is automatically deployed in every host in the selected cluster.
- 3 You select a security manager for managing these security appliances. Consider that you are using an existing security manager, which is managing other security appliances in your network. Only minimal user intervention is required to install these security appliances. Discovery and establishment of trust with the corresponding security manager is automatic.
- 4 In NSX, you create security groups containing the objects you want to protect in the cluster. For example, you can select the cluster itself or the distributed switch port group. Then the security service is available for all VMs corresponding to the selected object. In this example, VMs 1 through 4 are selected for IPS service. So traffic related to these VMs is subjected to next-generation IPS analysis. In effect, if VM1 communicates with VM2, traffic does not exit the host. However, the security service inspects such traffic.

Notes:

- Even if you migrate one of the protected VMs to a different host, the same security service is automatically provided to that VM.
- If you add a host to the cluster, you must make sure that network virtualization components are installed on the host as part of host preparation through NSX. Then, an instance of the security service is automatically installed on that host. Trust is also automatically established, by way of exchange or a password or a certificate key, between this instance of the security service and the corresponding security manager.
- Consider that you select the distributed switch port group (dSwitchPortGroup) as the object to be protected. Then any new VM added to this switch port group is automatically subjected to IPS (or other security service).

Advantages of Intel Security Controller

- Intel Security Controller facilitates simple, seamless, non-intrusive, and non-disruptive security service integration with an existing virtualized environment.
- The best-in-class security solutions available to your physical networks are available to your virtual networks as a software-based service.
- Regarding securing virtual networks, Intel Security Controller can cope with the flexibility, scalability, and agility of virtualization solutions. After you deploy a security service, your virtual networks are protected with minimal user-intervention as they scale up.
- When you deploy IPS or firewall service, you can use your current security manager and those security policies for the SDDC.
- You do not need to change your physical or virtual network architecture to provide a security service to your virtual networks.
- Provides visibility of intra-VM traffic (east-to-west) for security.
- Under test conditions, Intel Security Controller did not impact functionality or performance of virtualization solutions.

2

Installing the Intel Security Controller virtual appliance

Intel Security Controller is a virtual appliance, which you install on a hypervisor. Use the corresponding virtualization manager to install Intel Security Controller. In the case of VMware, for example, you would use VMware vSphere Web Client to install Intel Security Controller.

Contents

- *Requirements for Intel Security Controller*
- *Assumptions before setting up Intel Security Controller*
- *Install the Intel Security Controller virtual appliance*

Requirements for Intel Security Controller

You require these components to successfully install, deploy, and run Intel Security Controller.

- McAfee recommends the following options to install Intel Security Controller:
 - VMware vCenter Server (vCenter Server) version 5.5 or later
 - OpenStack Juno, OpenStack Kilo, OpenStack Liberty

If you are using OpenStack, the distributions that are supported include:

- RedHat
 - Mirantus
 - HP
 - Cononico (Ubuntu)
 - Rackspace
- VMware vSphere Web Client 5.5 or later.
- The host on which you install Intel Security Controller must be running ESXi 5.1 or later.
- The hosts for which you want to provide a security service must be on ESXi 5.5 or later.
- IP addresses for Intel Security Controller, Security Manager, vCenter Server, and NSX Manager.



You must install the Intel Security Controller virtual appliance on a hypervisor (host), which is different than the one hosting the protected VMs (workload VMs).



Currently, you can assign only an IPv4 address to Intel Security Controller. Therefore, all the related servers must have an IPv4 address.

After you successfully install Intel Security Controller, you can configure a network name for Intel Security Controller using the `set network hostname` command. See, [set network hostname](#) on page 94.

Assumptions before setting up Intel Security Controller

This product guide assumes that you have set up the requisite virtual infrastructure to install and deploy Intel Security Controller. The assumptions that we make before we explain the steps to setup Intel Security Controller are that you have:

- Installed VMware vSphere
- Installed VMware vCenter Server Appliance.
- Defined data center and clusters.
- Installed and configured VMware NSX.
 - Deployed VMware NSX Manager.
 - Configured VMware NSX Manager.
 - Created a distributed virtual switch port group.
 - Prepared an ESXi host for NSX.

For more information about each of these steps, please refer VMware Product Documentation.

Install the Intel Security Controller virtual appliance

Before you begin

- McAfee recommends that you use root administrator user privileges to install Intel Security Controller.
- You have necessary network settings for the Intel Security Controller virtual appliance.



Remember only IPv4 addresses are supported.

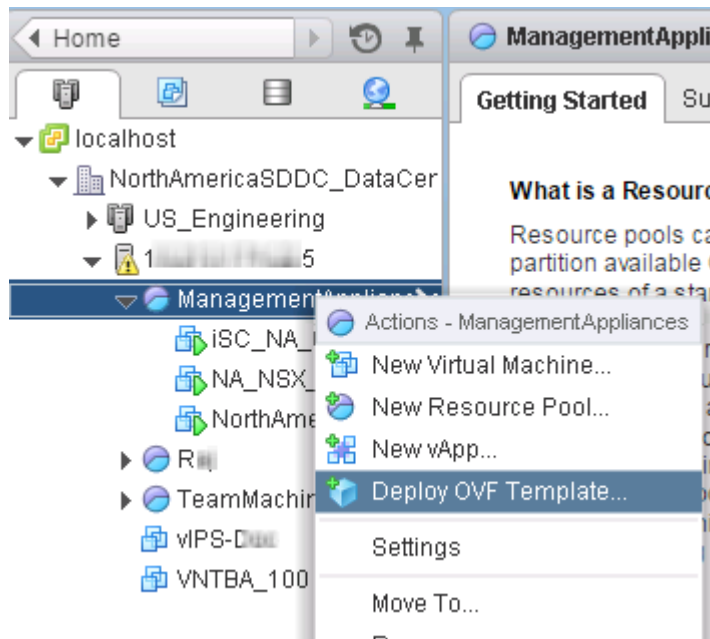
- The Intel Security Controller installation file (.ovf) is accessible from your client machine.

You can install Intel Security Controller in a VMware environment using vSphere Web Client. This section uses vSphere Web Client version 5.5.0 build 1879799 as an example.

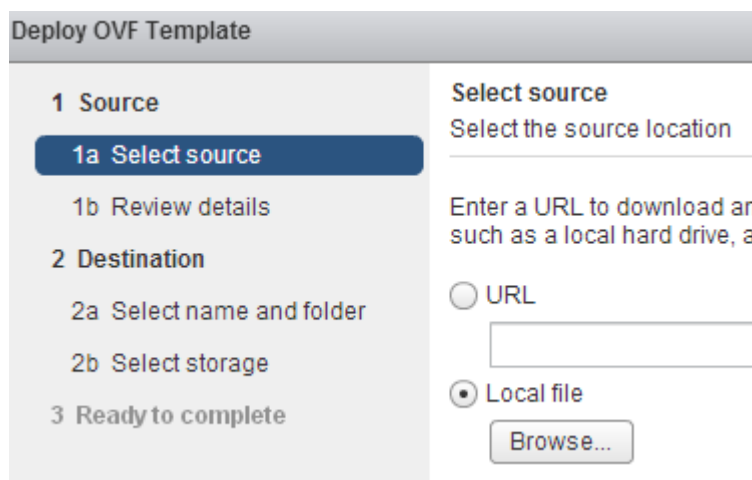
Task

- 1 Log on to vCenter Server using the vSphere Web Client as the root user.
- 2 In the vSphere **Home** tab, select **Hosts and Clusters**.

- 3 Select the required node such as a resource pool, right-click, and select **Deploy OVF Template**.



- 4 Click **Browse** and locate the .ova file.



If not done already, you might be prompted to install and allow access to the VMware Client Integration Plug-In.

- 5 Review the details and click **Next**.
- 6 In the **Accept EULAs** window, click **Accept** and then **Next**.
- 7 Enter a relevant name for the Intel Security Controller virtual appliance.



The name must be unique within a data center.

- 8 Select a folder or data center where to deploy Intel Security Controller and click **Next**.

- 9 Select the required value from the **Select virtual disk format** drop-down list based on your requirement.

- 10 Select the required datastore and click **Next**.

Name	Capacity	Provisioned	Free	Type
datastore1	1.80 TB	5.02 TB	795.80 GB	VMFS

- 11 In the **Setup networks** section, select the required switch port group.

The switch port group must enable Intel Security Controller to communicate to the related applications such as the Security Manager, vCenter, NSX, and virtual security appliances. You must also be able to access the Intel Security Controller web application as well as the Intel Security Controller CLI from your client machine.

The screenshot shows the 'Deploy OVF Template' wizard with the 'Setup networks' step selected. The left sidebar shows the progress: 1 Source (1a Select source, 1b Review details, 1c Accept EULAs), 2 Destination (2a Select name and folder, 2b Select storage, 2c Setup networks, 2d Customize template), and 3 Ready to complete. The main area is titled 'Setup networks' and 'Configure the networks the deployed template should use'. It contains a table with two columns: 'Source' and 'Destination'. The first row has 'VM Network' in both columns. Below the table, it shows 'IP protocol: IPv4' and 'IP allocation: Static - Manual'. At the bottom, there are two sections: 'Source: VM Network - Description' with the text 'The VM Network network', and 'Destination: VM Network - Protocol settings' with the text 'No configuration needed for this network'.

Source	Destination
VM Network	VM Network

IP protocol: IPv4 IP allocation: Static - Manual ⓘ

Source: VM Network - Description
The VM Network network

Destination: VM Network - Protocol settings
No configuration needed for this network

- 12 In the **Customize template** section, enter the network settings for the Intel Security Controller appliance and click **Next**.
- Enter an IPv4 address for the Intel Security Controller virtual appliance. IPv6 is not supported currently.
 - Enter the subnet mask for the IP address.
 - Enter the default gateway IP address.
 - Enter the IPv4 addresses of DNS servers separated by a space. You can specify up to 2 DNS servers; that is, one primary and the other secondary DNS server.

Customize template

Customize the deployment properties of this software solution

i All properties have valid values

▼ Network properties	3 settings
Network 1 IPv4 Address	The IPv4 Address for this interface. 10.255.255.0
Network 1 Netmask	The netmask for this interface. 255.255.255.0
Default IPv4 Gateway	The default gateway for this VM. 10.255.255.0
▼ DNS	1 setting
DNS Server list	The DNS server list(space separated) for this VM. 10.255.255.0

- 13 Review the information displayed in the **Ready to Complete** section, select **Power on after deployment**, then click **Finish**.

Deploy OVF Template

1 Source

- 1a Select source
- 1b Review details
- 1c Accept EULAs

2 Destination

- 2a Select name and folder
- 2b Select storage
- 2c Setup networks
- 2d Customize template

3 Ready to complete

Ready to complete
Review your settings selections before finishing the wizard.

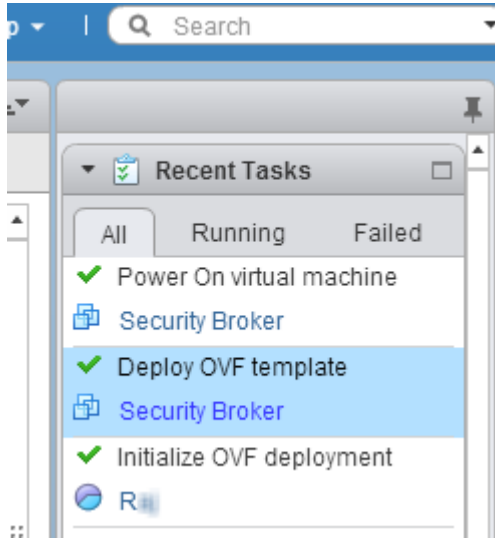
OVF file	C:\01_Work\midc\InstallationFiles\Buku1218_atohwmidcServer-Customer.ovf
Download size	1.0 GB
Size on disk	1.5 GB
Name	Security Broker
Datastore	datastore1
Target	RAI
Folder	Datacenter
Disk storage	Thin Provision
Network mapping	VM Network to VM Network
IP allocation	Static - Manual, IPv4
Properties	Network 1 IPv4 Address = 10.255.255.0 Network 1 Netmask = 255.255.255.0 Default IPv4 Gateway = 10.255.255.0 DNS Server list = 10.255.255.0

☒ Power on after deployment

Back Next Finish Cancel

To make any changes, click **Back**.

- 14 In the **Recent Tasks** section, monitor the installation.



Confirm successful installation by logging on to Intel Security Controller; make sure you are able to access the CLI as well as the web application.

- Open an SSH client session or click **Launch Console** in the vSphere Web Client. Use *admin* and *admin123* as the user name and password, respectively.
- From a client browser, log on to the Intel Security Controller web application. See [Accessing the Intel Security Controller web application](#) on page 21.

3

Setting up Intel Security Controller

After you install the Intel Security Controller virtual appliance, you can set it up and manage it using the Intel Security Controller web application.

Contents

- *Accessing the Intel Security Controller web application*
- *Managing Intel Security Controller users*
- *Configuring the Intel Security Controller appliance*

Accessing the Intel Security Controller web application

Before you begin

- Make sure the Intel Security Controller virtual appliance is configured with IP settings and is reachable from your client machine.
- Make sure the corresponding firewalls are configured to allow HTTPS over ports 443 and 8090.
 - The web application communicates over port 443.
 - Intel Security Controller communicates with other servers over port 8090.
- The following are the recommended browsers to access the Intel Security Controller web application.
 - Internet Explorer version 11 or later
 - Google Chrome 39.0.2171.71 or later
 - Mozilla Firefox 33.1 or later
 - Safari 8.0 or later

You use the Intel Security Controller web application to set up and manage the Intel Security Controller virtual appliance. You also use the Intel Security Controller web application to configure it for orchestrating a security service.

Task

- 1 Open a supported browser and enter `https://<IP address of Intel Security Controller>` as the URL.
- 2 In the **Login ID** field, enter the user name and the corresponding password provided by your Intel Security Controller administrator.

If you are setting up Intel Security Controller for the first time, use the default user name and password, which are `admin` and `admin123` respectively.

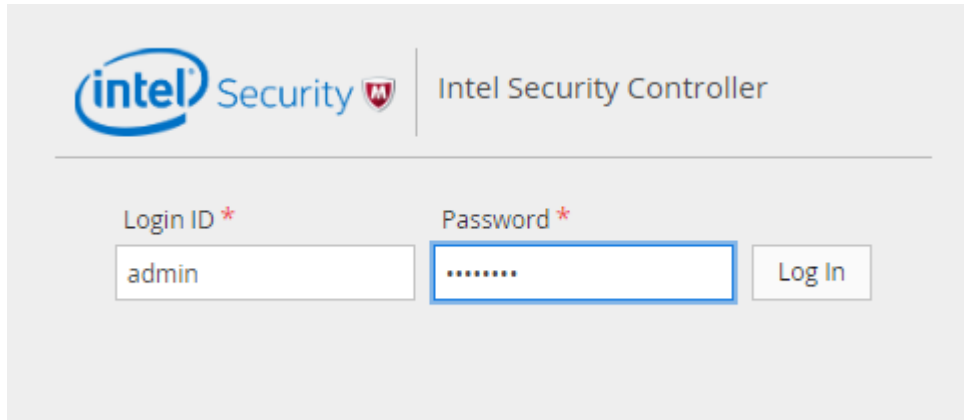
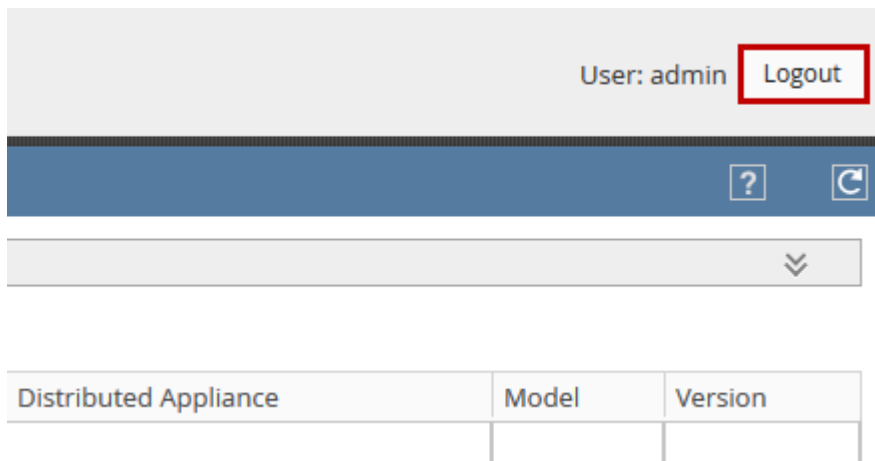


Figure 3-1 Logon screen

- 3 Click **Log In**.
- 4 To log out from the Intel Security Controller web application, click **Logout** in the top-left corner of the screen.



Distributed Appliance	Model	Version

Figure 3-2 Position of the logout button



If your Intel Security Controller web application session is idle for 30 minutes or more, you are automatically logged out. This setting is not configurable.

Managing Intel Security Controller users

Before you begin

- Make sure that you have administrator user credentials to manage Intel Security Controller users.
- Before you edit or delete a user record, as a best-practice make sure that the corresponding user is not logged on.

You can manage login credentials for other Intel Security Controller web application users.

Task

- 1 Log on to Intel Security Controller web application and select **Manage | Users**.

The **Users** page displays with the three default Intel Security Controller users.

- **admin** — Used to provide initial access to Intel Security Controller web application and to authenticate REST callbacks from Network Security Manager.
- **agent** — Used to authenticate REST registration requests from the Intel Security Controller control path agent on each security appliance instance.
- **nsx** — Used to authenticate REST callbacks from the NSX Manager into Intel Security Controller.



The default users are for the internal functions as described above. McAfee recommends that you create user records to enable access to the Intel Security Controller web application. Default user records are visible so that you can change their default passwords. As a security precaution, make sure you change the passwords of the three default users.

- 2 Take the appropriate action:

To add a user click **Add** and provide the user details.




The users you create in the **Users** page can access only the Intel Security Controller web application and not the Intel Security Controller appliance CLI.

Users				
<div>? ↺</div>				
<div>+ Add ✎ Edit ✕ Delete</div>				
User Name	First	Last	Role	Email
admin			ADMIN	
admin1			ADMIN	
agent			SYSTEM_AGENT	
nsx			SYSTEM_NSX	

Figure 3-3 Users

Table 3-1 Option definitions

Option	Definition
User Name	Enter the Intel Security Controller logon name for the user. After you save the user record, you cannot change the User Name for a user. The user name can contain between 1 and 31 characters, which must start with an uppercase or lower case alphabet, followed by alphanumeric characters and an underscore symbol.
First Name	Enter the first name of the user.
Last Name	Enter the last name of the user.
Password	Enter the corresponding password. The password must meet the following pre-requisites: <ul style="list-style-type: none"> • A number from 0-9 must occur at least once. • A lower-case alphabet from a-z must occur at least once. • An upper-case alphabet from A-Z must occur at least once. • A special character which includes (@#\$%^&+=!_) must occur at least once. • No spaces must occur in the entire string. • Must contain between 8 and 155 characters. <div>  Other special characters such as <space>, *, (,), <, and > are also supported provided the password criteria mentioned above are met. </div>
Email	Enter a valid email address of the user.
Role	Select the role for the user.
Cancel	Click to cancel the operation.
OK	Click to save the user record.

- To edit a user record, select the record and click **Edit**.
You cannot edit the **User Name**. After you have edited the fields you want to change, select **OK**.
- To delete a user record, select it and click **Delete**.
Confirm if you want to delete the record.

Configuring the Intel Security Controller appliance

If you have admin privileges in the Intel Security Controller web application, you can reconfigure the IP settings for the Intel Security Controller virtual appliance as well as execute maintenance activities such as Intel Security Controller version upgrade and Intel Security Controller database backup.

View the summary details for Intel Security Controller

You can view current details of your Intel Security Controller deployment through its web application.

Task

- In the Intel Security Controller web application, select **Manage | Server | Summary**.

The **Summary** page appears, displaying current details of your Intel Security Controller deployment.

Summary	
DNS Name:	localhost
IP Address:	10.
Version:	2.00 (Build:)
Uptime:	0 Days 21 Hours 21 Minutes 42 Seconds
Current Server Time:	Thu Oct 15 05:38:22 UTC 2015

☐ Include Database Backup with Log Bundle

Download Logs Restart

Figure 3-4 Intel Security Controller Summary page

Table 3-2 Field descriptions

Option	Definition
DNS Name	The DNS name you configured for Intel Security Controller. If you have not configured a DNS name, <i>localhost</i> is displayed. To configure a DNS name, use the <code>set network hostname</code> command. See set network hostname on page 94.
IP Address	The IP address you configured for the Intel Security Controller appliance. For information about changing the IP address, see Manage the network settings for Intel Security Controller on page 25.
Version	The current version and build number of Intel Security Controller.
Uptime	The number of minutes lapsed since the last restart.
Current Server Time	The current system time on the Intel Security Controller appliance.
Download Logs	Click to download the Intel Security Controller log files for troubleshooting. Include database backup with log bundle — Select to include the database backup when you download the Intel Security Controller logs. Intel Security Controller automatically triggers a database backup and includes the backup files to the log bundle.
Restart	Restarts the Intel Security Controller virtual appliance.

Manage the network settings for Intel Security Controller

Before you begin

You have admin rights in the Intel Security Controller web application.

You can reconfigure the network settings for the Intel Security Controller virtual appliance from the Intel Security Controller web application.

Summary Network Email Maintenance Archive Support

Network Settings ?

IP Details

Edit ☐ DHCP ☒ Static

IPv4 Address: 10. [masked]

Netmask: [masked]

Default Gateway: 10. [masked]

Primary DNS Server: 10. [masked]

Secondary DNS Server: [masked]

NAT Details

Edit

Public IPv4 Address: 10. [masked]

Figure 3-5 Network Settings page

Task

- 1 In the Intel Security Controller web application, select **Manage | Server | Network**.

The **Network Settings** page appears, displaying the current IP details of your Intel Security Controller appliance.

- You can configure either static network settings or use DHCP for Intel Security Controller. However, McAfee highly recommends that you assign static network settings for Intel Security Controller.

The DHCP option is provided so that even if you have not identified the IP address for Intel Security Controller at the time of installation, you can still complete the installation by selecting the DHCP option. Before you deploy any security service, you can select the static option and assign the required network settings to Intel Security Controller.

You cannot switch from static to DHCP.

- It is important that you do not change the static IP address of Intel Security Controller after you deploy a security service. For example, you must not change the IP address after you deploy the virtual security system for next-generation IPS.

When you change the IP address after you deploy a security service, the URL pointing to the OVF file for that security service is affected. NSX assumes that you swapped the image for the corresponding virtual appliances providing the security service. As a result, the installation status fails and you must resolve it in the **Network & Security Service Deployments** page in NSX. Until you resolve the installation, the corresponding security service might not function fully. For the same reason, the DHCP option is not an option after you deploy a security service.

Consider that the IP address of Intel Security Controller is 1.1.1.1 and that you deployed virtual security system for IPS service. Under deployment specification in NSX, the OVF URL is `https://1.1.1.1:8090/ovf/<Sensor image name>.ovf`. If you change the IP address to 2.2.2.2, the URL is also changed accordingly. Though you have only changed the IP address of Intel Security Controller, NSX assumes that you changed the image for the deployed Virtual Sensors since the URL of the OVF is now changed. For all functions of the IPS service to resume, you must resolve the installation status for IPS.

When you resolve the IPS installation, NSX removes the existing virtual security system instances (ESX agents) and installs them again.

- If you must change the IP address, make sure you first remove the service deployments in NSX and then reinstall the services after you change the IP address.



- 2 To edit the static network settings, click **Edit** and specify the details.
- Make sure Intel Security Controller can communicate with virtualization provider, the security manager, and the virtual security service with the new network settings.

Set Network Settings

IPv4 Address *

10.

Netmask *

Default Gateway *

10.

Primary DNS Server

10.

Secondary DNS Server

Cancel

OK

Figure 3-6 IP details for the network

Table 3-3 IP details

Option	Definition
IPv4 Address	Enter a valid IPv4 address for the Intel Security Controller virtual appliance. Currently, IPv6 address is not supported.
Netmask	Enter the subnet mask for the IPv4 address you entered.
Default Gateway	Enter the default gateway IP address for the IPv4 address you entered.
Primary DNS Server	Optionally, enter the preferred DNS server IP address for Intel Security Controller to resolve host names.
Secondary DNS Server	Optionally, enter the alternative or the secondary DNS server IP address.
Cancel	Click to cancel the changes.
OK	Click to save the changes.

Set Network Settings

IPv4 Address *

10.

Cancel

OK

Figure 3-7 NAT details

Table 3-4 NAT details

Option	Definition
IPv4 Address	Enter a valid IPv4 address for NAT. Currently, IPv6 address is not supported.
Cancel	Click to cancel the changes.
OK	Click to save the changes.

Maintaining the Intel Security Controller virtual appliance

If you have admin rights in the Intel Security Controller web application, you can perform maintenance tasks such as upgrading the Intel Security Controller virtual application to a later version, backing up the Intel Security Controller database, and restoring a backed-up database.

Back up the Intel Security Controller database

Before you begin

You have admin rights in the Intel Security Controller web application.

As a precaution, you can back up the Intel Security Controller database at regular intervals. Currently, you cannot schedule automatic backups.

Task

- 1 In the Intel Security Controller web application, select **Manage** | **Server** | **Maintenance**.

The **Maintenance** page appears.

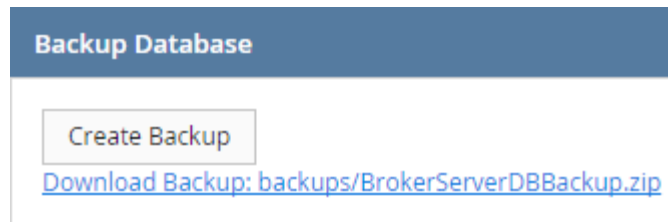


Figure 3-8 Backup Database section

- 2 In the **Backup Database** section, click **Create Backup**

The database is backed up as a .zip file and the link to the backup file is displayed under **Create Backup**.

- 3 Click the hyperlink pointing to the backup file and save the file to a network location for future use.



The path mentioned in the hyperlink is that of the folder in the folder structure of Intel Security Controller that is currently being backed up. The file that you receive after the download is placed in the default download location configured in your computer.

Upgrade the Intel Security Controller virtual appliance

Before you begin

- Confirm you have admin rights in the Intel Security Controller web application.
- As a precaution, back up the Intel Security Controller database.
- You have the image bundle (.zip) of the version you want to upgrade to.

You can upgrade the version of Intel Security Controller appliance from the Intel Security Controller web application.

Task

- 1 In the Intel Security Controller web application, select **Manage | Server | Maintenance**.

The **Maintenance** page displays.

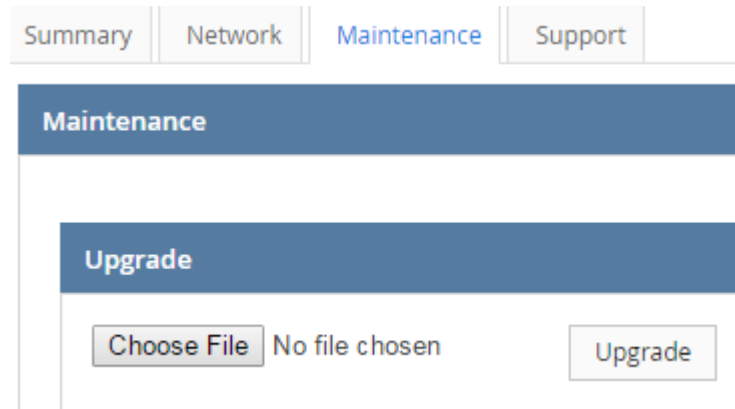


Figure 3-9 Upgrade section

- 2 In the **Upgrade** section, click **Choose file** and select the .zip file of the version you want to upgrade to.
- 3 Click **Upgrade**.
Wait for a few minutes until the upgrade process completes.
- 4 If you are upgrading from Intel Security Controller version 1.0, follow these steps to resume using the virtual appliance through the web application.
- 5 Close the previous session of Intel Security Controller web application.
- 6 Open a new tab and enter the Intel Security Controller IP address in the format, `https://<Intel Security Controller IPv4 address>`.

The logon screen appears.

Restore an Intel Security Controller database backup

Before you begin

- Confirm you have admin rights in the Intel Security Controller web application.
- The backed-up file is accessible through your client.
- The Intel Security Controller version when you backed up the database and the current Intel Security Controller version are same.

You can revert the Intel Security Controller database to an earlier state by uploading the corresponding database file from your client. The Intel Security Controller version at the time of backup and at the time of restoration must be the same.



McAfee recommends you do not restore the database of a different Intel Security Controller virtual appliance on your current Intel Security Controller virtual appliance. For example, if the IP address in the backup is different, Intel Security Controller might not function as configured.

Task

- 1 In the Intel Security Controller web application, select **Manage | Server | Maintenance**.

The **Maintenance** page appears.

- 2 In the **Restore Database** section, click **Choose File** and select the database backup file.
 - 3 Click **Restore**.
- The **Upload Status** pop-up appears.

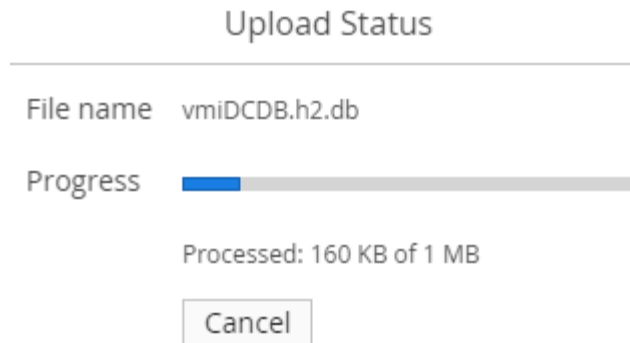


Figure 3-10 Database restore status

After the upload is complete you receive a message stating the success of the database restore.

Troubleshoot an upgrade or restore

At times, after an upgrade from version 1.0 to version 1.2 or after a database restore, you might encounter the following situations:

- The server does not come back up after upgrade in a few minutes, or
- When you refresh the page, nothing appears, or
- When you refresh the page, the server notifies you that it is in maintenance mode.

Task

- 1 Using root administrator credentials, log on to the vSphere Web Client.
- 2 Go to **vCenter | Inventory Trees | Hosts and Clusters**.
- 3 Locate the Intel Security Controller virtual machine and right-click on it.
- 4 Click **Restart Guest OS**.
- 5 After the virtual machine restarts, try logging on to the Intel Security Controller web application.

Setup email configuration

Whenever there is a failure, if an alarm is configured, an email notification is sent to the email ID configured. You can setup email notification to be sent for failures that require immediate attention. For the email notifications to be sent, you have to first define an SMTP server.

Summary

Network

Email

Maintenance

Archive

Support

Email Settings

?

Edit

Outgoing Mail Server (SMTP):	10.
Port:	25
Email Id:	

Figure 3-11 SMTP server configuration

To setup an SMTP server, perform the following tasks:

Task

1 Navigate to **Manage | Server | Email**.

2 Click **Edit**.

The **Set Email Settings** pop-up opens.

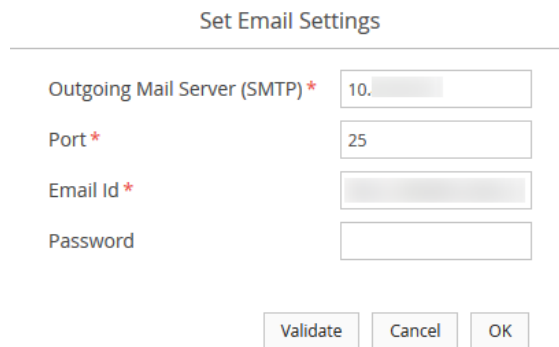
The image shows a 'Set Email Settings' dialog box. It has a title bar with the text 'Set Email Settings'. Below the title bar, there are four input fields: 'Outgoing Mail Server (SMTP) *' with the value '10.', 'Port *' with the value '25', 'Email Id *' which is empty, and 'Password' which is empty. At the bottom of the dialog, there are three buttons: 'Validate', 'Cancel', and 'OK'.

Figure 3-12 Add an email server

3 Enter the following details:

Option	Definition
Outgoing Mail Server (SMTP)	Enter the IPv4 address of the SMTP mail server
Port	Enter the port number
Email ID	Enter the email ID of the system administrator to whom the email notification has to be sent
Password	Enter the password for the email ID
Validate	Validates if Intel Security Controller is able to communicate with the SMTP server
OK	Click to save the settings
Cancel	Click to cancel the changes

Sending information to Intel Security threat base

Attacks are ever evolving. By choosing to send information to Intel Security threat base, which is McAfee Global Threat Intelligence (GTI), any new type of attack is immediately updated in the database. Information about system health, general setup, feature usage are sent to GTI. To enable sending data to GTI, select the **Send anonymous statistics to Intel Security** option. Data sending is a background process that will not interrupt other Intel Security functions.

Sending of data is considered as a system event. When Intel Security Controller fails to send data to GTI, a system failure event is triggered if an alarm is enabled for system failures. This alarm then generates a talkback failure alert.

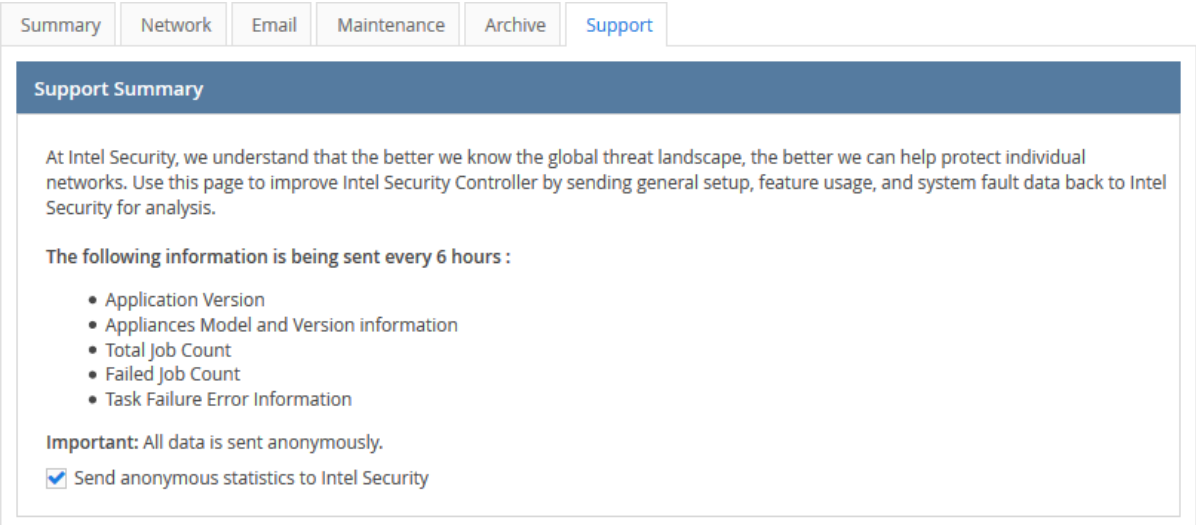


Figure 3-13 Support summary

Download Intel Security Controller logs

You can download the Intel Security Controller log files to troubleshoot an issue or provide the logs to Support. You can also include the database backup in the support bundle.

Task

- 1 In the Intel Security Controller web application, select **Manage | Server | Summary**.

The **Summary** page appears.

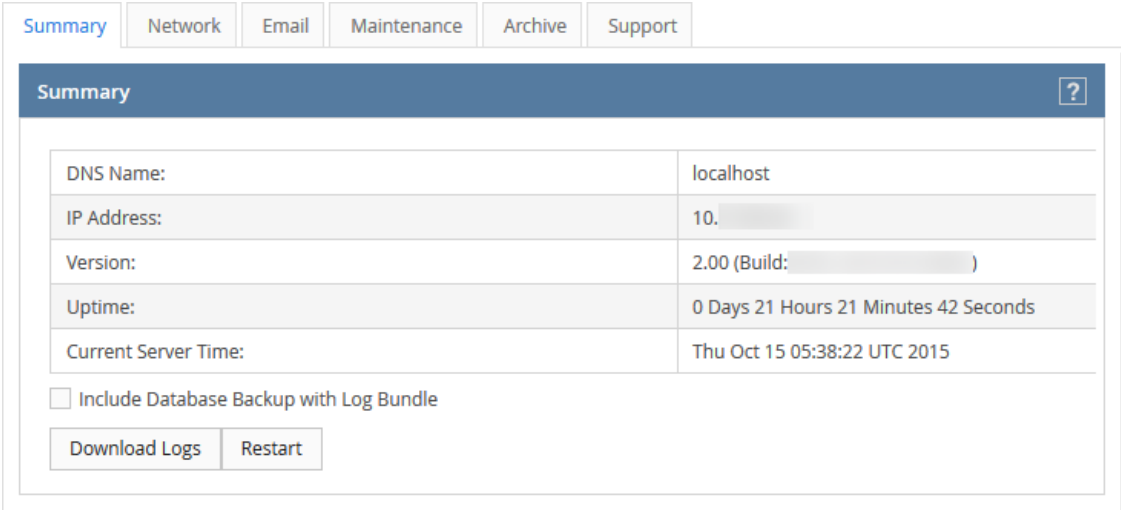


Figure 3-14 Intel Security Controller Summary page

- 2 To include the database back-up along with logs, select **Include Database Backup with Log Bundle**.

If you include the database backup, Intel Security Controller takes a backup of the database and includes the back-up file with the logs.

Uptime:		
Current Server Time:		
<input checked="" type="checkbox"/> Include Database Backup with Log Bundle		
Download Support Bundle	Shutdown	Restart

Figure 3-15 Downloading logs bundle



The default button label changes to **Download Support Bundle**.

- 3 Click **Download Support Bundle** and save the file on your local computer or a network location.
- 4 To download the logs without the database backup, uncheck **Include Database Backup with Log Bundle** and click **Download Logs**.
- 5 Save the zipped log files to your local computer or a network location.

4

Working with the Intel Security Controller web application

To use the Intel Security Controller web application effectively, familiarize yourself with the user interfaces and terminologies.

- To refresh a page or a section of a page, click .
- To select the columns to display in the Intel Security Controller web application, hover over the column headers to reveal and click , and select the column name you want to show or hide.

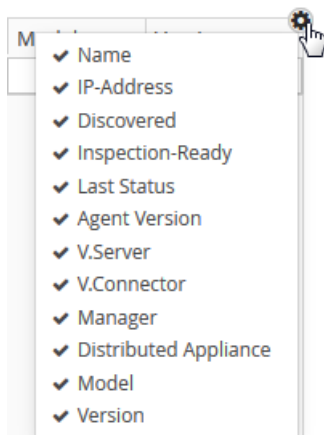


Figure 4-1 Column options to display

- To filter displayed records, enter a string or select an option in the header field and press *Enter* on your keyboard. The filters are case insensitive.

Tasks				
Order	Name	Objects	State	Status
	Prod			
1	Checking Appliance Manager Connector 'ProductDoc'	ProductDoc	COMPLETED	PASSED
2	Register Domain Notifications for Manager Connector 'ProductDoc'	ProductDoc	COMPLETED	PASSED
3	Register Policy Notifications for Manager Connector 'ProductDoc'	ProductDoc	COMPLETED	PASSED
4	Syncing Domains for Manager Connector 'ProductDoc'	ProductDoc	COMPLETED	PASSED
5	Create Domain '/My Company'	ProductDoc	COMPLETED	PASSED
6	Syncing Policies for Manager Connector 'ProductDoc'	ProductDoc	COMPLETED	PASSED
7	Create Policy 'Default Client and Server Protection' in Domain '/My Company'	ProductDoc	COMPLETED	PASSED
8	Create Policy 'Default Client Protection' in Domain '/My Company'	ProductDoc	COMPLETED	PASSED
9	Create Policy 'Default Server Protection' in Domain '/My Company'	ProductDoc	COMPLETED	PASSED
10	Syncing public key Manager Connector 'ProductDoc'	ProductDoc	COMPLETED	PASSED
11	Downgrade To 'Read Lock' for Lock Object 'ProductDoc' (Manager Connector)		COMPLETED	PASSED
12	Unlock object 'ProductDoc' (Manager Connector)		COMPLETED	PASSED

Figure 4-2 Filtering data for specific column headers can be done using a string

For example, if you enter *prod* in the **Name** column and press *Enter*, only those records containing *prod* are displayed.

Tasks	
Order	Name
	Prod
1	Checking Appliance Manager Connector 'ProductDoc'
2	Register Domain Notifications for Manager Connector 'ProductDoc'
3	Register Policy Notifications for Manager Connector 'ProductDoc'
4	Syncing Domains for Manager Connector 'ProductDoc'
6	Syncing Policies for Manager Connector 'ProductDoc'
10	Syncing public key Manager Connector 'ProductDoc'
11	Downgrade To 'Read Lock' for Lock Object 'ProductDoc' (Manager Connector)
12	Unlock object 'ProductDoc' (Manager Connector)

Figure 4-3 Filtered data is picked up from each row for display

To remove the filtering, delete the string in the header and press *Enter*.

- To sort the records, click the upward or downward arrow key at the end of each column to sort the records in either ascending or descending order.

Contents

- Terminology
- Define virtualization connectors
- Define manager connectors
- Manage software images for virtual security appliances
- Define distributed appliances
- Jobs and tasks
- Alarms, alerts, and archives

Terminology

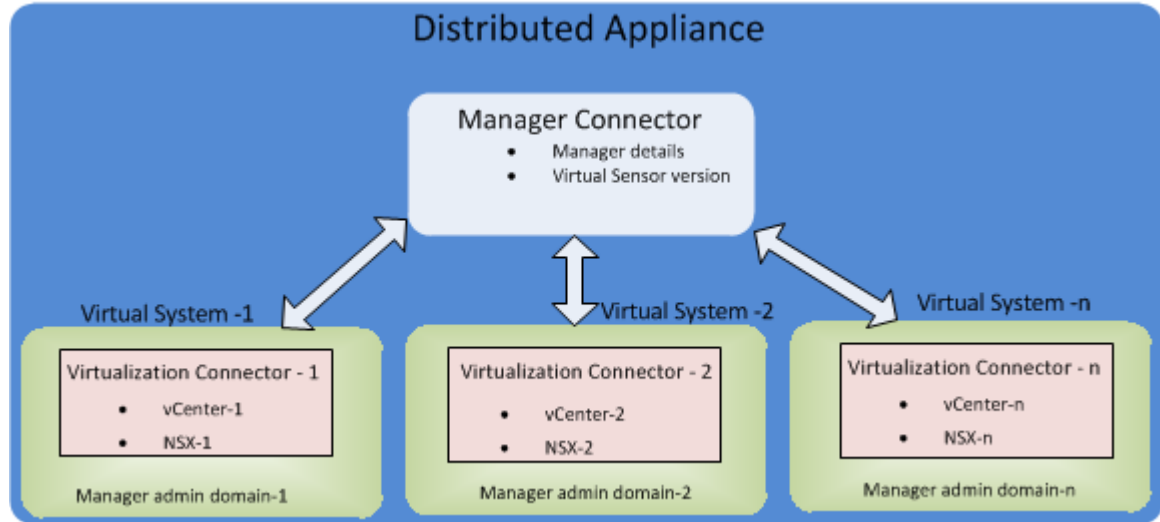
To configure Intel Security Controller to act as a broker, you first define the building blocks. You then use these building blocks to configure Intel Security Controller so that it can act as a broker between the virtualization provider and security solutions.

- **Virtualization connector** — In this building block, you define the virtualization provider entities. You must confirm that the virtualization provider is accessible to Intel Security Controller.
 - For VMware, you define the IP address and administrator logon credentials for NSX and vCenter.
 - For OpenStack, you must make sure to define administrator credentials to Horizon, which is the OpenStack user-interface.
- **Appliance instances** — The virtual security appliances, which intercept the traffic from the VMs. For IPS, Virtual Sensors are the security appliance instances, which are referred to as *Virtual Security System instances*. For firewall, Virtual Layer 2 Firewalls are the security appliance instances, which are referred to as VSS Container Firewalls.
- **Security service manager connector (Manager connector)** — In this building block, you define the management console for managing the security appliances. For IPS, you define the Manager IP address and the root admin logon credentials, which will manage the Virtual Sensors installed in the hosts. For firewall, you define the Security Management Console (SMC) IP address and the API authentication key.
- **Security service function (security service)** — This component refers to the security service you intend to deploy such as next-generation IPS or next-generation firewall. You can use the **Service Function Catalog** page to upload corresponding software images for further deployment through Intel Security Controller.
- **Distributed appliances** — A distributed appliance, associates the security solution and the virtualization solution. That is, you define a distributed appliance using the virtualization connectors and security manager connector as building blocks.

In a distributed appliance, you specify the following:

- One security manager connector.
- The model and version of the security appliance.

For IPS, this is the version and model of the virtual Sensors, which are later deployed in the ESXi hosts. For firewall, this is the version of the VMware vCenter compatible image of
- One or more virtualization connectors.
- For each virtualization connector, you must select a Manager admin domain. The security appliances are managed under the specified admin domain. In the case of IPS, if you select *My Company* (root admin domain), all virtual Sensors are managed under *My Company* in the Manager. In case of firewall, select *shared domain* in SMC to view the managed devices.



- Virtual system: A virtualization connector associated with a manager domain is a virtual system. The most common example of a virtual system is the Virtual Security System for IPS and Virtual Security System container for firewall. A Virtual Security System is the logical container object for all deployed virtual security service functions or Virtual Security System instances.
- Intel Security Controller agents: Security services deployed through Intel Security Controller have the following agents.
 - Control Path Agent: This agent is responsible for communication between the security services and the security manager.
 - Data Path Agent: This agent makes sure the traffic from the VMs are routed through the security service for inspection in case of VMware. The data path agent does not manage traffic for Openstack.
- Job and tasks: Some of the actions that you perform in Intel Security Controller are treated as jobs and tasks. The high-level action is treated as a job. For example, synchronizing a distributed appliance is a job. A job might consist of a number of tasks. That is, a job can be broken down into tasks. For example, if synchronizing a distributed appliance is the job, checking the manager connector and validating existing NSX components are some of the tasks. When all tasks are completed successfully, the corresponding job is complete.
Jobs and tasks enable you to easily track and troubleshoot your actions in Intel Security Controller. When you trigger a job, the state, status, start time, completed time, and so on are displayed for the job as well as its component tasks.

Define virtualization connectors

You are able to define virtualization connectors from the Intel Security Controller web application.

Task


- 1 In the Intel Security Controller web application, select **Setup | Virtualization Connectors**.

The **Virtualization Connector** page displays the currently available virtualization connectors.

Virtualization Connector			
<div> + Add Edit Delete </div>			
Name	Type	Controller IP	Provider IP
Doc-VC	VMWARE	10.10.10.10	10.10.10.10
HQ Openstack (.13)	OPENSTACK	10.10.10.10	10.10.10.10

Figure 4-4 Virtualization Connector page

Table 4-1 Option definitions

Option	Definition
Name	Name of the virtualization connector record.
Type	Virtualization provider which you mention when you create the virtualization connector. An example is VMware or Openstack.
Controller IP	IP address of the virtual security controller such as VMware NSX or Openstack Horizon.
Provider IP	IP address of the virtualization provider server. Clicking the hyperlink provided for the IP address opens the login screen of the virtualization provider.
<div>  Certain virtualization providers are configured on specific ports of the server. You are required to enter the port at the end of the URL. </div>	

- 2 Take one of the following actions:

To create a new virtualization connector, click **Add** and enter the options in the **Add Virtualization Connector** dialog.

Add Virtualization Connector

Name * Doc_1

Type * VMWARE

NSX

IP *

User Name * Demo

Password *

vCenter

IP *

User Name * Test

Password *

Cancel OK

Figure 4-5 VMware virtualization connector

Add Virtualization Connector

Name * Doc_2

Type * OPENSTACK

SDN Controller

Type NSC

IP *

User Name * Demo

Password *

Keystone

IP *

Admin Tenant Name *

User Name * Test

Password *

Show Advanced Settings


Cancel OK

Figure 4-6 Openstack virtualization connector

Table 4-2 Option definitions

Option	Definition
Name	Name that enables you easily identify a virtualization connector record.
Type	Virtualization provider from the list of currently supported providers. You are provided with two options: <ul style="list-style-type: none"> • VMware • OpenStack
Cancel	Closes the dialog without saving the changes.
OK	Closes the dialog box with the changes saved to the Intel Security Controller database. A warning displays if Intel Security Controller is unable to connect to virtualization provider using the IP address and credentials. You can still create the virtualization connector. However, if you use this virtualization connector in a distributed appliance, you cannot delete the distributed appliance or virtualization connector record. If you are using NSX and delete a virtualization connector, Intel Security Controller deletes the related data from NSX. So, if Intel Security Controller is unable to log on to the NSX defined in the virtualization connector, the task of deleting the virtualization connector fails.
VMWare	
NSX	
IP	IPv4 address of VMware NSX Manager Virtual Appliance.
User Name	Logon name of an admin user.
Password	Corresponding password.
vCenter	
IP	IPv4 address of VMware vCenter with which the NSX management service is connected.
User Name	Root admin user name of the vCenter.
Password	Corresponding password.
OpenStack	
SDN Controller	[Optional] SDN controllers allow network programming capability in which the control plane and data plane are separated. You are able to steer or redirect traffic from the virtual machines to the inspection device, depending on the SDN controller you are using.

Table 4-2 Option definitions *(continued)*

Option	Definition
Type	<p>SDN controller that is used by your virtual network.</p> <p>An SDN controller replaces the control plane of underlying hardware and replaces it with software thereby removing the dependency on hardware type.</p> <p>Select from the list of currently supported providers. You are provided with the following options:</p> <ul style="list-style-type: none"> • NSC (Network Security Controller) – A simple SDN controller used by used primarily to redirect traffic. It does not offer service function chaining, failure policy support, and off-box redirection. • MIDO_NET – An full-service SDN controller developed by Midokura. • NONE – Intel Security Controller can operate in a deployment-only mode in which it will not redirect traffic. Instead, your virtual network has its own infrastructure to redirect traffic. The only requirement is for the switching device to add an identifier which notifies the security service about which policy is to be used during traffic inspection.
IP	IPv4 address of the SDN controller.
Username	Username of the SDN controller.
Password	Password of the SDN controller.
Keystone	
IP	Enter the IPv4 address of the tenant environment in OpenStack.
Admin Tenant Name	<p>Name of the admin tenant that is used in OpenStack.</p> <p>This tenant must have sufficient privileges to query and perform all operations and must have to access other tenants in the environment.</p>
User Name	Username of the administrator.
Password	Password of the administrator.
Show Advanced Settings	<p>(Optional) Clicking this button opens the Advanced Settings pop-up, which provides you the ability to configure RabbitMQ settings.</p> <div>  It is not mandatory to configure these settings if you do not require the dynamic capabilities of Intel Security Controller. </div> <p>A message broker is used to translate messages from the formal messaging protocol of a sender into the formal messaging protocol of the receiver.</p> <p>RabbitMQ is an integral component of OpenStack. It is an open-source message broker software that implements Advanced Message Queuing Protocol.</p> <p>In this context, it is used to translate messages between Intel Security Controller and OpenStack since each uses a unique messaging protocol.</p>
Advanced Settings	
HTTPS	Communication OpenStack and Intel Security Controller is over secure HTTP channels.
RabbitMQ User Name	Username of the RabbitMQ application. The default username is <code>guest</code> .
RabbitMQ Password	Password of the RabbitMQ application. The default password is <code>guest</code> .
RabbitMQ Port	Dedicated port for communication with the RabbitMQ application. The default port used is 5672.

- 3 To edit a virtualization connector record, select the record and click **Edit**.

You cannot change the **Type**. After you complete making the changes, click **OK** to save the changes.



McAfee highly recommends that you do not change the IP addresses of the virtualization connector servers (the SDN and the virtualization provider) after deployment of virtual security system instances.

- 4 To delete a virtualization connector record, select the record and click **Delete**.

If the virtualization connector you want to delete is used in a distributed appliance, you must first delete the distributed appliance record. To delete a distributed appliances record, see [Delete a distributed appliance](#) on page 71.

Tasks

- [Define Security Groups](#) on page 44

Define Security Groups

Before you begin

- To create a security group, you must have already set up a virtualization connector on one of the supported virtualization environments. While you create a security group, you may follow any order to create security groups, deployment specifications, and binding.
- It is also advisable to define the manager connector, the service function catalog, and the distributed appliance and deployment specification before you come to this step.



Only if you have set up a distributed appliance with a successfully validated deployment specification can you bind a policy to a security group.

Several virtual environments do not allow you to define a security group to which you can deploy security services. Instead, when your assets and instances (which can be entire tenant networks or individual virtual machines) exist in a virtualization environment, Intel Security Controller provides you the option to define a security group and deploy security services and policies to that group. An example of a virtual environment that allows you create security groups within its own environment is VMware NSX. An example of one that does not provide this option is OpenStack.

To define or modify a security group in Intel Security Controller, follow these steps.

Task

- 1 Go to **Setup | Virtualization Connectors**.

The **Virtualization Connectors** page appears with a list of existing virtualization connectors.

- 2 To create a security group for a virtualization connector, select one from the list.

The **Security Groups** section in the lower half of the page displays a list of security groups already defined. For a new deployment of Intel Security Controller, this list will be empty.

- 3 (OpenStack) In the **Security Group** section, click **Add** to create a new security group.

The **Add Security Group** window appears.

4 Define all the parameters necessary for a security group.

Add Security Group

Name *

Test

Select Tenant *

Coke

▼

Select Region

regionOne

▼

Selection Type:

☒ All Servers belonging to Tenant

☐ By Type

VM

▼

Select Items To Include

Name

>

<

Count: 0

[Select All](#)

[Select None](#)

[Invert Selection](#)

Name	Region	Type
		▼

Count: 0

[Select All](#)

[Select None](#)

[Invert Selection](#)

Cancel

OK

Figure 4-7 Add security group

Table 4-3 Option definitions

Option	Definition
Name	Unique name of the security group.
Select Tenant	Tenant from which you want to select objects to be included in the security group. Once you create a security group, the tenant cannot be changed.
Select Region	A region in OpenStack is a logical construct which groups several OpenStack services which are geographically co-located. For instance, you might select a region from which to select objects to protect. It is possible for a security group to contain objects from different regions.
Selection Type	
All Servers belonging to Tenant	When you select this option, you are including every virtual machine instance present currently and virtual machines launched in the future. This is selected on behalf of that tenant for inclusion within the security group.
By Type	When you select this option, you have the following choices: <ul style="list-style-type: none"> VM – choice of selecting individual virtual machines within the tenant. Any new network interface cards added to these servers will automatically be protected. NETWORK – choice of selecting individual networks within the tenant. Any port connected to the network or added in the future is available to be included in the security group.

Table 4-3 Option definitions *(continued)*

Option	Definition
Select Items To Include	<p>In this section, you are provided with a list of available instances which, depending on your choice above, can be networks, virtual machines or tenant networks.</p> <p>From the options provided to you, you are able to select a method of filtering and you are given the option to create a subset of this list.</p> <p>At any time, you can modify your choice by using the > and < buttons. For ease of selection, you can select all options at once, select no options, or invert the selection.</p>
Cancel	Cancels your configuration.
OK	Saves your configuration and closes the window.

- 5 After you have configured all settings for the security group, click **OK**.



A VM port can exist in only one security group. There can be no overlap, that is, a single VM cannot belong to more than one security group.

The window closes and the security group that you just created appears in the list in the **Security Groups** section. The next step is to bind the security group to a security policy.


- 6 To assign a policy (as defined in the security manager) to a security group, click **Bind**.

The **Bind Policy to Security Group** window appears. If you have already defined any distributed appliances – which effectively implies that you have defined a manager connector and uploaded a software image – they appear in this window.

Table 4-4 Option definitions

Option	Definition
Enabled	<p>Checkbox to indicate your choice of policy. Selecting this checkbox indicates your choice of security service with inspection policy and failure chaining policy.</p> <p>This checkbox is disabled by default.</p>
Order	Specifies the service function chaining and the order shows the chain order in which traffic is inspected.
Distributed Appliance	Distributed appliance that you are binding with the inspection policy.
Inspection Policy	Security policy that is defined in the security manager domain.

Table 4-4 Option definitions *(continued)*

Option	Definition
Chaining Failure Policy	<p>Since devices such as IPS are configured as L2-bump-in-the-wire devices, they have the potential to disrupt traffic flow in case of a device failure or reboot. The failure policy to be implemented by the security service governs whether traffic flow must continue uninterrupted or must stop in case of a service failure. However, configuring a service as fail-open means traffic is not inspected in case of device failure or reboot.</p> <p>So to prevent security breaches during a service outage, default behavior is fail-closed.</p> <ul style="list-style-type: none"> • Fail_Open – When you activate fail-open, there is no disruption of traffic but there is no inspection either. • Fail_Closed – When you activate fail-closed, all traffic flow is disrupted in case of a service outage since there is no traffic inspection.
Configure Dynamic Deployments	<p>A dynamic deployment specification is one that is created on demand to accommodate unique inspection requirements. Sometimes you might not want to create a deployment specification in advance. An example of such an instance is if you are a cloud service provider and are sharing your resources across several customers, you might have different service level objectives agreed on with different customers. In such circumstances, a customer to whom you have committed exclusive inspection to will not necessitate you to opt for sharing. Clicking the hyper-link directs you to a window in which you may select dynamic deployment specifications that have been created.</p> <div>  You can only create a new dynamic deployment specification with a certain combination of Tenant, Region, and Virtual System if it is not already present in the system. </div>

- 7 To create a deployment specification in on demand, click the **Manage Dynamic Deployments** hyper-link.



You must have selected the **Enabled** checkbox to activate this hyper-link.


The **Dynamic Deployment Configurator** window appears.

Table 4-5 Option definitions

Option	Definition
Enabled	<p>Checkbox to indicate your choice of deployment specification. When you select this checkbox, you are selecting a combination of the virtualization connector, region, and dynamic deployment specification if applicable. If you do not have dynamic deployment specification created, the security group uses the deployment specification created for that distributed appliance. This checkbox is disabled by default.</p>
Virtualization Connector	The connector for which you are defining the dynamic deployment specification.
Region	Region within which you want to define the dynamic deployment specification.
Dynamic Deployment Specification	Provides you with a window to create a dynamic deployment specification.

- 8 Enter all the necessary information in the **Dynamic Deployment Configurator** window.

Table 4-6 Option definitions

Option	Definition
Name	Unique identifier of the deployment specification you are about to create.
Select Tenant	<p>Tenant on which you want to deploy the security service. Since the distributed appliance is a logical grouping of all elements – virtualization connector, security manager, and security service appliances – you are able to view all tenants within a specific virtual environment.</p> <p>When you select the tenant, you are effectively instructing Intel Security Controller which tenant to deploy the security service appliance defined in the selected distributed appliance.</p>
Select Region	Region within a tenant on which you want to deploy the security service.
Select Management Network	Network to which all the security service appliances will be connected for management purposes.
Select Inspection Network	<p>Network where the traffic is inspected by security service appliances.</p> <div>  <p>It must be different from the network specified for the management network. If not, it will show an error.</p> </div>
Select Floating IP Pool	An optional choice if virtual machines that need to be accessed are located behind a private IP address. If that is the case they must have a different public IP address to be accessed and for a security service to be deployed.

Define manager connectors

You are able to configure manager connectors from the Intel Security Controller web application.

Task

- 1 In the Intel Security Controller web application, select **Setup | Manager Connectors**.

The **Manager Connector** page appears, displaying currently available manager connectors.


The screenshot shows two sections of the web application. The top section is titled "Manager Connector" and contains a table with columns: Name, Type, Host, and Last Job Status. Below the table are buttons for Add, Edit, Delete, and Sync. The bottom section is titled "Policies" and contains a table with columns: Name and Domain.

Name	Type	Host	Last Job Status
NSM_35	NSM	10.10.10.10	FAILED (Job Id: 14,237)
SNORT_MGR	ISM	10.10.10.10	PASSED (Job Id: 12,481)

Name	Domain
Default Client and Server Protection	/My Company
Default Client Protection	/My Company
Default Server Protection	/My Company

Figure 4-8 Manager Connector page

Table 4-7 Option definitions

Option	Definition
Manager Connector	
Name	Name of the manager connector record.
Type	Security service manager type which you select when you create the virtualization connector, such as Network Security Manager or SMC.
Host	<p>IP address of the security service manager server.</p> <p>Clicking the hyperlink provided for the IP address opens the login screen of the security service manager.</p> <div>  <p>Certain security service managers are configured on specific ports of the server. You are required to enter the port at the end of the URL.</p> </div>
Last Job Status	<p>Status of the most recent job.</p> <p>Clicking the hyperlink provided for the job ID, routes you directly to the Jobs page with tasks for the specific job displayed in the Tasks pane.</p>
Policies	
Name	<p>Name of the policy in the security service manager.</p> <p>Initially all default policies from the security service manager are linked with Intel Security Controller. Different default policies are linked depending on the security service manager it is deployed in.</p>
Domain	Name of the domain from which the policies are linked in the security service manager

2 Take the appropriate action:

To create a new manager connector, click **Add** and enter the options in the **Add Manager Connector** dialog.

Figure 4-9 Add manager connector

Table 4-8 Option definitions

Option	Definition
Name	Enter a name, which enables you easily identify a manager connector record.
Type	Based on the type of security service, select the manager connector type. For IPS service, select NSM which refers to the Network Security Manager. For firewall service, select SMC which refers to the Security Management Center.
Cancel	Click to close the dialog without saving the changes.
OK	Click to close the dialog box with the changes saved to the Intel Security Controller database. When you click OK , all the admin domains and policy groups available in the Manager are sent to Intel Security Controller.
NSM	
IP	Enter the IPv4 address of the Manager server.
User Name	Enter the logon name for the Manager. This logon name must have Super User role assigned to it. The default logon name with Super User role is <i>admin</i> .
Password	Enter the corresponding password.
SMC	
IP	Enter the IPv4 address of the Management Server. There might be multiple IPv4 addresses configured to reach the Management Server. However, you must enter the one that is configured for listening. For more details, refer the section <i>Define Management Server or Log Server contact addresses</i> in the <i>McAfee Next Generation Firewall Product Guide</i>
API Key	A 24-character alphanumeric authentication key that is randomly generated when you configure the API Client in the Management Client. Intel Security Controller uses this key to communicate with the SMC API. For more details, refer the section <i>Configure the SMC API</i> in the <i>McAfee Next Generation Firewall SMC API Reference Guide</i>

- 3 To edit a manager connector record, select the record and click **Edit**.

You cannot change the **Type**. After you complete making the changes, click **OK** to save the changes. A job is started and the job number is displayed at the right-side bottom of the **Manager Connector** page. You can monitor the progress of this job in the **Jobs** page.



McAfee highly recommends that you do not change the IP address of the security manager after deployment of the virtual security system instances.

- 4 To delete a manager connector record, select the record and click **Delete**.

If the manager connector you want to delete is used in a distributed appliance, you must disassociate the manager connector from the distributed appliances before you delete the manager connector. Alternatively, you can delete the distributed appliance record. To delete a distributed appliances record, see [Delete a distributed appliance](#) on page 71.

- 5 To synchronize any changes with the manager connectors, click **Sync**.

When there are any policy updates made in the security appliance manager, you can trigger manual synchronization to update the changes in the manager connector. A new information pop-up appears notifying you that the job has begun along with the job number. After the synchronization is complete, the **Last Job Status** for that instance changes from **RUNNING** to **PASSED** or **FAILED** depending on the result.

Manage software images for virtual security appliances

To provide a security service, Intel Security Controller orchestrates the installation of the corresponding virtual security appliance on designated hosts. Or in the case of virtualization connectors such as OpenStack, go a step further and provides you the ability to create security groups with such tenants or virtual machines. For this, it is essential to follow this sequence of steps for the reasons explained beside the step:

- 1 Import relevant software images into Intel Security Controller – Software images imported to Intel Security Controller will be used to deploy security service on designated assets which can be located on any of the supported virtual environments.
- 2 Create a distributed appliance, in Intel Security Controller – This is where you specify the model and software version combination for that security service.
 - For security service function such as IPS, you select the virtual security system (Virtual Sensor) model and software version, manager connector, and virtualization connector.
 - For security service function such as firewall, you select the McAfee NGFW image, manager connector and virtualization connector.

When you later deploy either of the security services, the SDN controller installs the corresponding model and software version of the security appliance in each designated instance.

You use the **Service Function Catalog** page in Intel Security Controller to import software images for security appliances. When you import a particular software image, the model and version information are automatically populated. You can import multiple software image versions for each virtual security appliance model. You can then upgrade or downgrade the software image for deployed appliances.

Define the service function catalog

Before you begin

- You have admin rights in the Intel Security Controller web application.
- The .zip file containing the virtual security appliance software image is available from your endpoint.

You use the **Service Function Catalog** page to manage the software for security service deployments. For example, you can manage the Virtual Sensor software images for IPS or the McAfee NGFW images for the firewall.

Managing the security function catalog consists of just one step.

- Import the required software images corresponding to that model. Using the example of IPS, IPS-VM100-VSS model and version of that model is added by default. You can several software versions of the same appliance model. For example, you can add 8.1 and 8.2 software versions of IPS-VM100-VSS in the security function catalog.

After you add software images to the security function catalog, you are able to select a specific image for each virtualization system at the time when you create distributed appliances. For existing distributed appliances, you are able to modify the choice of software image for that security service. You are also able to also downgrade the software image in the same manner.

The **Service Function Catalog** page provides information about the existing security service deployments. You can view information or delete the security service deployments.

Model			?	↺
✖ Delete ↗ Auto Import				
Model	Manager Type	Manager Software Version		
IPS-VM100-VSS	NSM	8.2		
NGFW-CLOUD	SMC	5.10		
SNORT-0.2	ISM	1.0		
Software Version			↺	
✖ Delete				
Software	Virtualization Type	Image Name		
8.1.7.22	OPENSTACK	sensorsw_vm100-vss_81722-disk1.qcow		

Figure 4-10 Security service function catalog

Option	Definition
Model	
Model	Displays the name of the security service Manager
Manager Type	Displays the type of Manager
Manager Software Version	Displays the Manager software version installed
Software Version	
Software	Displays the software version of the security service installed

Option	Definition
Virtualization Type	Displays the name of the type of virtualization deployed
Image Name	Name of the security service image installed

Task

- 1 In the Intel Security Controller web application, select **Setup | Service Function Catalog**.
- 2 Click **Auto Import** in the **Model** section.

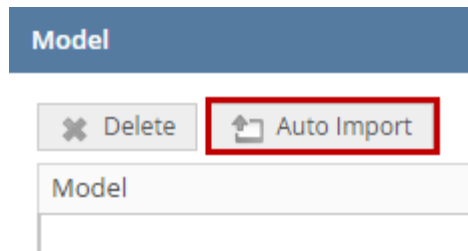


Figure 4-11 Auto Import option to upload software image files

The Auto Import Appliance Software Version pop-up appears.

- 3 In this pop-up, click **Choose File** and select the zipped virtual security system image file.
- 4 Click **OK** to begin uploading this file.



You cannot edit any records for a model.

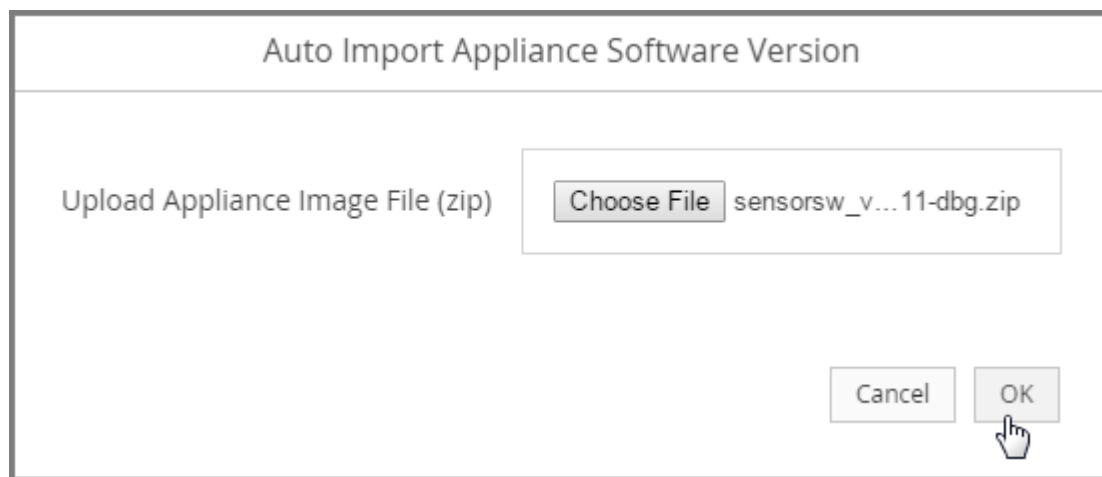


Figure 4-12 Auto Import File Select Pop-up

A progress bar appears providing the status of the file upload. At the end of the upload, it validates the image file before applying it.

Change the software version of security appliances

Before you begin

- Using the security function catalog, you have successfully imported the required software image in Intel Security Controller web application. Importantly, make sure that you specified the software version of the image correctly. See [Define the service function catalog](#) on page 52
- You have the required access to deploy security services in NSX.

Before or after deploying a security service, you might want to change the software version of the corresponding security appliances. For example, after you deploy IPS or firewall service, you might want to upgrade the software image of the virtual security system instance. Alternatively, you can downgrade to an earlier version as well.

After you import the required software images in the security function catalog of Intel Security Controller, you can change the image to the required version.



- After you change the version of security appliances, you must resolve installation status of the service deployment in NSX. NSX then deletes the current security appliances from the datastore and installs the version that you selected. It is evident that security appliances are not actually upgraded or downgraded but replaced with new instances installed with a selected software version. For Openstack, all these functions are automatically replaced during upgrade or downgrade. You have to check the **Jobs/Tasks** status to make sure that the process is complete without failures.
- In case of some security service functions such as IPS, the security service manager is unaware that the existing instances of the virtual security system are deleted and new ones are installed. The security service manager considers that the version of the virtual security systems has changed and trust is re-established. The name of virtual security system and the instances remain unchanged in the security service manager. The IP addresses assigned to the deployed security appliances also remain unaffected.
- After you change the software version, you must resolve the installation status of the corresponding service deployment in NSX.
- Until the new instances of the security appliances are fully up and running, the security service is suspended.
- Because security appliances are installed and not upgraded or downgraded, you can switch to a different version regardless of the current functional state of the appliances.

Task

- 1 In the Intel Security Controller web application, select **Setup | Distributed Appliances**.
- 2 Select the required distributed appliance record and click **Edit**.

- 3 In the **Edit Distributed Appliance** dialog box, select the required security model-version combination from the **Service Function Definition** drop-down list and click **OK**.

Edit Distributed Appliance

Name *

Manager Connector *

Service Function Definition * IPS-VM100-VSS-8.1.7.22

Virtualization System: IPS-VM100-VSS-8.1.7.27

Enabled	Virtualization Connector	Type	Manager Domain	Encapsulation Type
<input checked="" type="checkbox"/>	Doc-Openstack	OPENSTACK	/My Company	VLAN

Cancel OK

Figure 4-13 Select the required version for the security appliance

- 4 Review the warning message and click **OK** to proceed with the version change.



Warning messages disappear from the screen automatically if you move your mouse or click a key on your keyboard. However, they remain on the screen if you do not perform either of these actions.

NSX stops the corresponding virtual security appliances to install the selected version of the security appliances. So the installation status of the virtual security appliances is now *Failed*.

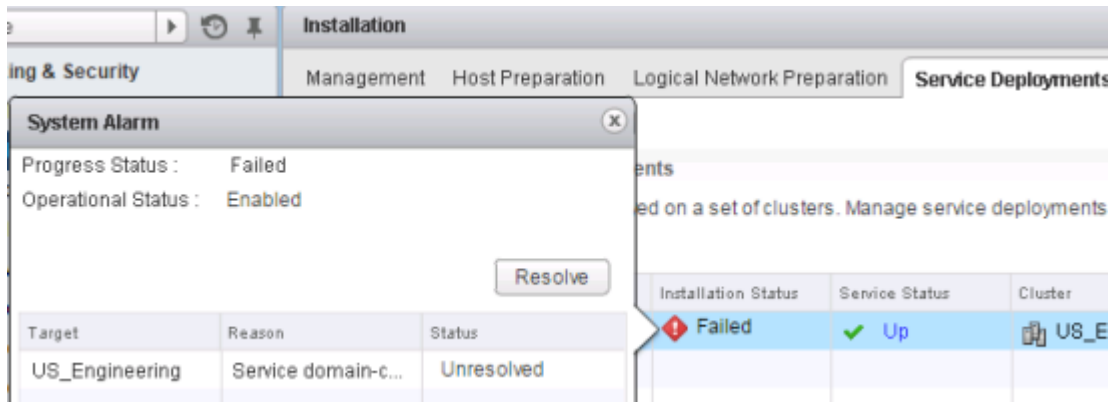


Figure 4-15 Installation status of service deployment

- 5 Log on to vCenter and resolve the installation status for the corresponding service.

The status on this will be one of four possibilities:

- *Unknown* – No information is available.
- *Down* – Includes an error message about the health of the security service. The most relevant indicators in this context are *Discovery* and *Inspection-Ready*. When the status is *Down*, it implies that both indicators are *False* and that you must investigate your deployment.

- *Warning* – Implies that the security service discovery was complete, but is not inspection-ready.
 - *Up* – Implies that both indicators are positive.
- 6 After the **Installation Status** turns to *Succeeded* and the **Service Status** displays *Up*, deploy the configuration changes to the virtual security system from the Manager.

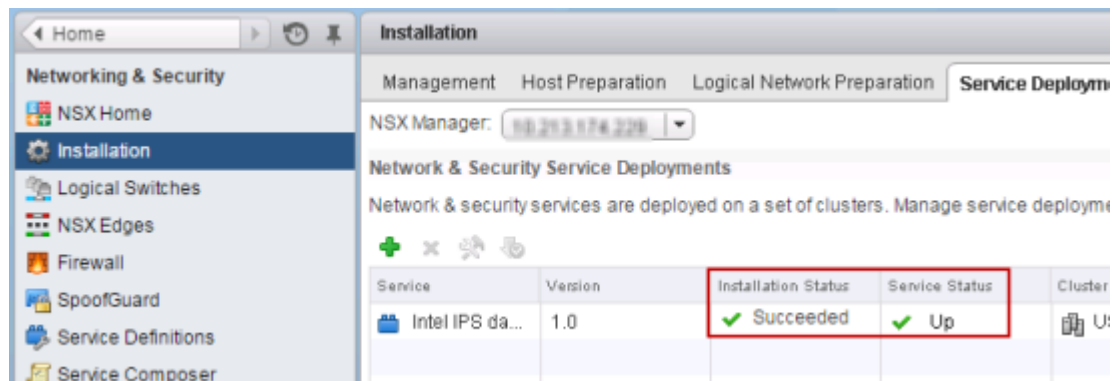


Figure 4-16 Installation status of service deployment

When you deploy the configuration changes, the Manager pushes the signature set to the virtual security system instances.

- 7 When you deploy configuration changes, the *Propagating Manager File...* job is triggered in Intel Security Controller. Select **Status | Jobs** and make sure that *Propagating Manager File...* job is passed.

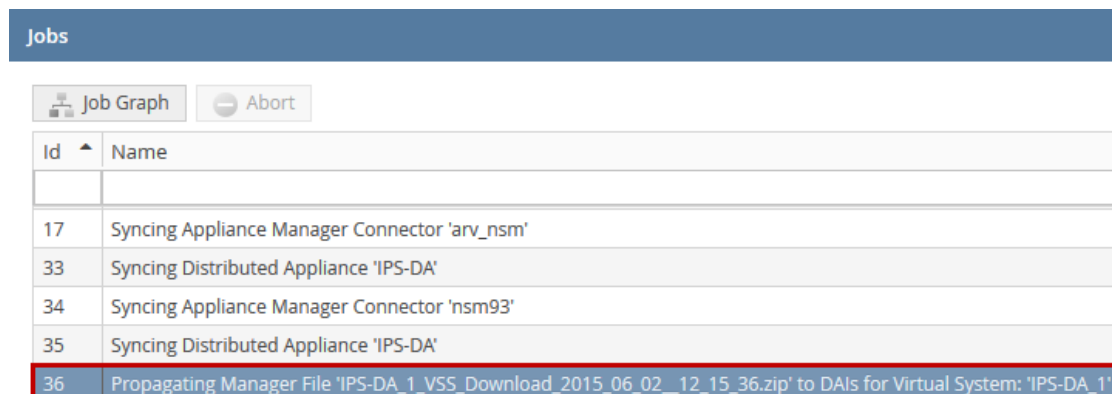


Figure 4-17 Propagating Manager File....

If the *Propagating Manager File....* job fails, deploy the configuration changes again from the Manager.

- 8 In the security manager, make sure the virtual security system and its member instances are connected and up-to-date.
- 9 Select **Status | Appliance Instances** and make sure the **Discovered** and **Inspection-Ready** for the corresponding appliances are *true*. If not, the security service function is suspended.

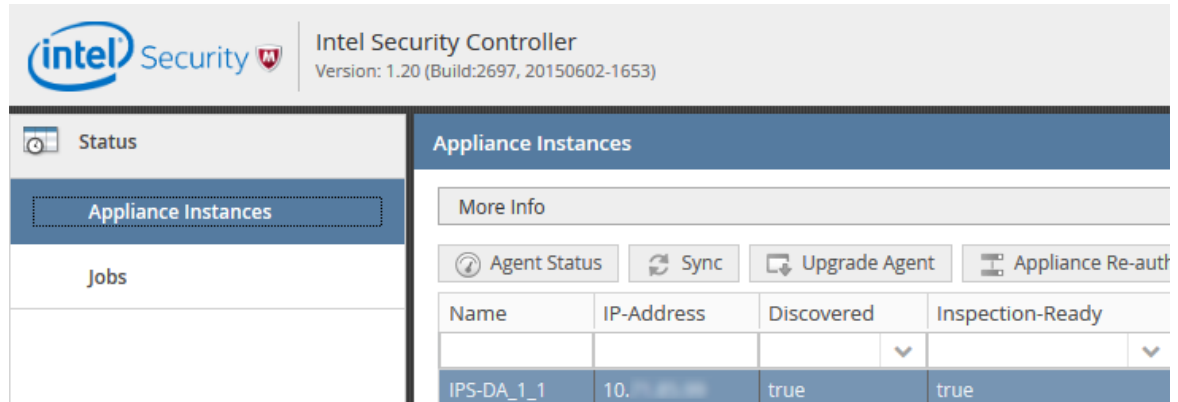


Figure 4-18 Appliance instances status

Define distributed appliances

Before you begin

- The virtualization connector and the manager connector are configured on the appropriate virtual environments.
- Necessary security-appliance image files – appropriate model and version – are uploaded to Intel Security Controller.
- The virtualization connectors and the security managers necessary for creating the distributed appliance are reachable to Intel Security Controller.

To define distributed appliances from the Intel Security Controller web application, perform these steps in the order provided.

Task

- 1 In the Intel Security Controller web application, select **Setup | Distributed Appliances**.

The **Distributed Appliances** page appears, displaying available distributed appliances if any.

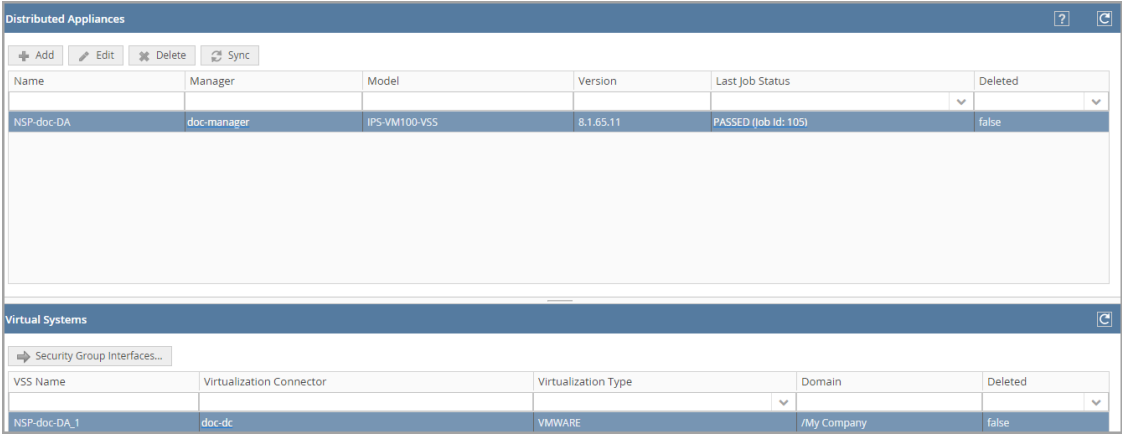


Figure 4-19 Distributed Appliances page

Table 4-9 Option definitions

Option	Definition
Distributed Appliances	
Name	Relevant name for the distributed appliance record.
Manager	Unique name of the manager connector for the distributed appliance. <ul style="list-style-type: none">• For IPS, it refers to a Network Security Manager.• For firewall, it refers to the SMC. Clicking the hyperlink provided, routes you to the list of manager connectors in the Manager Connectors page.
Model	Model of the virtual security appliance uploaded to Intel Security Controller.
Version	Version of the virtual security appliance in use.
Last Job Status	Result of the last job that was run for this distributed appliance. Clicking the hyperlink provided routes you directly to the Jobs page with selected job displaying all its tasks in the Tasks section.
Deleted	Indicates whether any component of that distributed appliance has been removed.

- 2 To create a new distributed appliance, click **Add** and enter the options in the **Add Distributed Appliance** dialog.

Add Distributed Appliance

Name *

Manager Connector *

Service Function Definition *

Virtualization System:

Enabled	Virtualization Connector	Type	Manager Domain	Encapsulation Type
<input type="checkbox"/>	Doc-Openstack	OPENSTAC	/My Company	VLAN

Figure 4-20 Add Distributed Appliance dialog box

Table 4-10 Option definitions

Option	Definition
Name	Enter a relevant name for the distributed appliance record.
Manager Connector	<p>Select the manager connector for the distributed appliance.</p> <p>For IPS, select the manager connector that refers to a Network Security Manager.</p> <p>For firewall, select the manager connector that refers to the SMC.</p>
Service Function Definition	Select a corresponding security appliance. This list of security appliances is from the security function catalog. So if you are unable to find a specific appliance definition, add it in the appliance catalog. Depending on the type of service function selected, the corresponding virtualization connectors are displayed in the Virtualization System section.
Virtualization System	
Enabled	Click to select a particular virtualization connector.
Virtualization Connector	This is the list of all added virtualization connectors. You can select multiple virtualization connectors. However, there is only one manager connector per distributed appliance. That is, you can map multiple virtualization connectors with one manager connector.
Type	This is the virtualization provider corresponding to a virtualization connector.
Manager Domain	<p>This is the list of admin domains from the security manager which you specified in the corresponding manager connector.</p> <ul style="list-style-type: none"> When you select the manager connector, Intel Security Controller displays the current admin domains from the corresponding security manager. When you select an admin domain, Intel Security Controller creates the Virtualization System under this admin domain in the security manager. <p>This is called as VSS in the Manager and is the logical container of the Virtual Sensors installed in each ESXi host. A VSS is similar to a failover Sensor object in the Manager.</p>

Table 4-10 Option definitions *(continued)*

Option	Definition
[OpenStack] Encapsulation Type	<p>Traffic between the switch and the virtual security service is encapsulated depending on the what the security service supports.</p> <p>In this case VLAN is the only encapsulation type supported by virtual IPS, virtual NGFW, and virtual SNORT. The type of encapsulation is used to encapsulate and de-encapsulate each packet with a tag that represents the policy mapping that should be used for inspection by the relevant service. The tag can simply be header information which is specific to the security service.</p>
Cancel	Closes the dialog without saving the changes.
OK	<p>Closes the dialog with the changes saved to the Intel Security Controller database.</p> <p>When you create a manager connector, all the admin domains and policy groups available in the Manager are sent to Intel Security Controller. So when you click OK, while creating the distributed appliance, Intel Security Controller gathers the current policy groups from the Manager and provides this list to the NSX Manager. This is how the Network Security Platform policy groups are available in the vCenter as profiles. You select these profiles when you create a security policy in vCenter.</p> <p>In OpenStack, policy groups created in the security manager are available to be selected within Intel Security Controller. When you create a security group, you must bind the security group to a security policy.</p> <p>For virtual environments which do not require you to create security policies and security groups in that virtualization manager, you able to view all policies available in the security manager within Intel Security Controller. For more information, refer the Define virtualization connectors on page 40.</p>



You cannot edit if the distributed appliance record is deleted. This is indicated by the status mentioned in the **Deleted** column for a record.

The distributed appliance appears in the list.

- 3 Click on the distributed appliance that you just created.

Information in the **Virtual Systems** section changes to display all the details about that distributed appliance.

Table 4-11 Option definitions

Option	Definition
[OpenStack] Deployments	Clicking this option displays a section in which details about the deployment specification is displayed. A deployment specification is a deployment strategy that a security administrator wants to employ. Detailed descriptions of all options are provided further below.
Traffic Policy Mappings	Clicking this option displays a section in which the inspection policy used for that virtual system is mentioned. Detailed descriptions of all options are provided further below.
VSS Name	Unique name assigned to the virtual security system.
Virtualization Connector	Unique name of the virtualization connector that you selected when you created the distributed appliance. This name is also the same name you provided at the time of creating the virtualization connector. Clicking the hyperlink provided routes you directly to the list of virtualization connectors in the Virtualization Connectors page.
Virtualization Type	Virtualization provider that you selected when you created the virtualization connector.
Domain	Admin domain in the security manager that you selected when you created the distributed appliance.
Deleted	Displays <i>true</i> or <i>false</i> which corresponds to whether any component of the distributed appliance has been removed.

- 4 [OpenStack] Click the **Deployments** button to define a deployment specification.

To create or modify a Deployment Specification, refer [Define Deployment Specifications](#) on page 64.

A sub-section known as **Deployment Specifications for Virtual Systems** appears.

Table 4-12 Option definitions

Option	Definition
Deployments	<p>Clicking this option displays a section in which details about the deployment specification is displayed. A deployment specification is a deployment strategy that a security administrator wants to employ.</p> <p>This section displays the following columns:</p> <ul style="list-style-type: none"> • Name — Name to identify the deployment specification. • Tenant — Tenant on which the deployment specification has been created. Once selected, you cannot modify the tenant for which this deployment specification is created and will have to create it afresh for another tenant. • Network — Management network that you must select at the time of creating a deployment specification. Each tenant has a tenant network which is the management network that connects all virtual machines within it to one another. To review which management network suits your deployment specification, you must review the network topology in the Horizon dashboard. • Auto Created — A deployment specification shows <i>false</i> in this column if you have created it using the add option in this section. However, there are instances in which this column will show <i>true</i>, which means you have used the Dynamic Deployment Specification window to create a deployment specification. To learn more about dynamic deployment specification, refer Define Security Groups on page 44. • Deleted — If the column shows <i>false</i>, it means the deployment specification still exists in the system. However, if you select the deployment specification and click Delete, this column initially shows <i>true</i> before it disappears from the list. In effect, it changes to <i>true</i> while the job is running. • Last Job Status — The status of the last task that you attempted on this deployment specification. It might have been a modification or even a re-synchronization using the Sync button.

- 5 Click the **Traffic Policy Mappings** button to assign a specific policy (as defined in the security manager) to particular traffic.

To create or modify a Traffic Policy Mapping, refer [Define Traffic Policy Mappings](#) on page 67.

A sub-section known as **Policy Mapping for Virtual Systems** appears.

Table 4-13 Option definitions

Option	Definition
Traffic Policy Mappings	<p>Clicking this option displays a section in which the inspection policy used for that virtual system is mentioned.</p> <p>This page displays the following columns:</p> <ul style="list-style-type: none">• Name — Name to identify the traffic inspection policy.• Inspection Policy — Name of the inspection policy used. This is the same name that will be seen in the security manager.• Tag — ID of the inspection interface. In the instance that two or policies existing in different admin domains of the security manager can have the same name, interfaces are automatically tagged with a unique ID in Intel Security Controller to distinguish them.• User-Defined — Policy mappings are not user-defined when a security group is bound to a service and therefore modification is not enabled for such bindings.• Security Group — The Security Group that the policy mapping belongs to. This field is automatically populated after you bind the Security Group to a policy.• Failure Policy — The failure policy that is selected in the Security Group.• Back — Clicking on this button takes you back to the default view of the Distributed Appliances page.

- 6 To edit a distributed appliance record, select the record and click **Edit**.



You cannot change the **Name**, the **Manager Connector**, and the **Manager Domain** options.

After you complete making the changes, click **OK** to save the changes. A notification indicating that a new job is started appears and the job number is displayed at the right-side bottom of the **Distributed Appliances** page. You can monitor the progress of this job by clicking the hyperlink to the job, which routes you to the **Jobs** page.

- 7 [VMware] To delete a distributed appliances record for a VMware deployment, see [Delete a distributed appliance](#) on page 71.

- 8 [OpenStack] To delete a distributed appliance for an OpenStack deployment:

- a Select the record and click **Delete**.

You are prompted to confirm if you are sure you want to delete this record.

- b Click **OK** to confirm.

- 9 If you have reconfigured an existing deployment specification or a distributed appliance and want these settings to take effect, click **Sync**.

A new information pop-up appears notifying you that the job has begun along with the job number. After the synchronization is complete, the **Last Job Status** for that instance changes from **RUNNING** to **PASSED** or **FAILED** depending on the result.

- 10 If the job fails, click the hyperlink to the job.

You are routed to the **Jobs** page where you are able to view the tasks for each job. Drilling down enables you to affirm which task failed in the job.

Tasks

- [Define Deployment Specifications](#) on page 64
- [Define Traffic Policy Mappings](#) on page 67
- [Maintaining virtual appliance instances](#) on page 68
- [Delete a distributed appliance](#) on page 71

Define Deployment Specifications

Before you begin

You will be able to create a deployment specification instance only for a distributed appliance. So before you set out to create a deployment specification, make sure you have created a distributed appliance.

A deployment specification empowers you to mobilize the objective of your service deployment strategy. Since every implementation varies from another, you can employ a strategy that best suits your requirements. In the meanwhile, Intel Security Controller continually monitors the infrastructure to make sure that your objectives are implemented.

Examples of what you can achieve through a deployment specification are:

- deploy security services only on particular hosts or tenants
- provision more than one instance of a security service on a single host to load balance traffic
- designate a set of hypervisor to have many security instances so as to handle all traffic flowing to and from VMs to pass through that host.

To create or modify a deployment specification for a specific distributed appliance, follow these steps.

Task

- 1 Go to **Setup | Distributed Appliance**.

A list of distributed appliances appears.

- 2 Click on one of the distributed appliances for which you want to create a deployment specification.

If you have any deployment specification already created, they appear in the **Deployments** section in the lower half of the screen. If there are none, this section is empty

- 3 Click the **Deployments** button to define a deployment specification.

You are directed to another section known as the **Deployment Specifications for Virtual System** section. You are able to create a deployment specification here, which is tied to a particular distributed appliance. Selecting different distributed appliances in the upper half of the page alters the deployment specifications that are displayed.

- 4 In this section, click **Add** to create a new deployment specification.

Add Deployment Specification

Name *

Select Tenant * ▼

Select Region * ▼

Selection Criterion:

☐ All (Hosts in selected Region)

☐ By Availability Zone

☐ By Host Aggregates

☒ By Host

Enabled	Name
<input checked="" type="checkbox"/>	compute-05
<input checked="" type="checkbox"/>	compute-03
<input type="checkbox"/>	compute-04

Select Management Network * ▼

Select Inspection Network * ▼

Select Floating IP Pool ▼

Deployment Count ▼

☒ Shared

Figure 4-21 Add deployment specification

Table 4-14 Option definitions

Option	Definition
Name	Unique identifier of the deployment specification you are about to create.
Select Tenant	<p>Tenant on which you want to deploy the security service. Since the distributed appliance is a logical grouping of all elements – virtualization connector, security manager, and security service appliances – you are able to view all tenants within a specific virtual environment.</p> <p>When you select the tenant you are effectively instructing Intel Security Controller to deploy the security service appliance defined in the selected distributed appliance.</p>
Select Region	Region within a tenant on which you want to deploy the security service.

Table 4-14 Option definitions *(continued)*


Option	Definition
Selection Criterion	<p>You are required to select one of the following choices:</p> <ul style="list-style-type: none"> • All (Hosts in the selected region) – Deploy on one or more hosts that exist in and are added to the selected region. Intel Security Controller continually monitors infrastructure changes to implement your most recent requirements. • By Availability Zone – Deploy on one or more availability zones which appear in the list as defined in your OpenStack environment. In OpenStack, you have the ability logically organize compute hosts in groups. You can also consider creating a physical isolation from other availability zones by using a separate power source or network equipment. • By Host Aggregates – Deploy on one or more host aggregates which appear in the list as defined in your OpenStack environment. In addition to regions and availability zones, you can also create host aggregates in OpenStack. Host aggregates enable you to partition compute zones into logical groups for load balancing and instance distribution. You can use host aggregates to partition an availability zone into several groups of hosts that either share common resources, such as storage and network, or have a special property, such as trusted computing hardware. • By Host – Deploy on one or more hosts, across all regions within the tenant, which appear in the list. When you select this option, you have the option to deploy more than one instance of a security service. <p>For more details about all of the above segregation constructs offered by OpenStack, refer to OpenStack Product Documentation.</p>
Select Management Network	Network to which all the security service appliances will be connected to for management purposes.
Select Inspection Network	<p>Port which you have created in OpenStack simply for the purpose of identifying a neutron port to which traffic will be sent. Since service functions are inserted as an L2-bump-in-the-wire, this port only requires a MAC address.</p> <div>  <p>This network does not actually pass traffic through it and therefore does not require an IP address. It must be different from the network specified for the management network, or else you will receive an error.</p> </div>
Select Floating IP Pool	An optional choice if virtual machines that need to be accessed are located behind a private IP address. If that is the case they must have a different public IP address to be accessed and for a security service to be deployed.
Deployment Count	<p>If your selection criterion above was By Hosts, you have the option to provision more than one instance of the distributed appliance per host.</p> <p>An example of such a deployment is to route all traffic that needs to be monitored by the security service to pass through one virtual machine. This virtual machine has many security instances of the same distributed appliance which provides you the ability to load balance using generic hardware.</p>
Shared	<p>This measure is related to QoS and refers to tenant sharing. If a deployment specification is marked for sharing, any appliance that is deployed through it can provide inspection services to any tenant VMs. If the deployment specification is not marked for sharing, a deployed appliance provides inspection services only to VMs belonging to that tenant.</p> <p>As a cloud administrator, you sometimes have service level agreements with your customers to provide exclusive inspection services through appliances which are not shared. In such instances, you must not mark a deployment specification for sharing.</p>

Table 4-14 Option definitions (*continued*)

Option	Definition
Cancel	Discards all changes and closes this window.
OK	Saves all changes and begins to deploy the distributed appliances using the configuration that you have set up.

- 5 To edit an existing deployment specification, select a deployment specification for a distributed appliance and click **Edit**.
- 6 To delete an existing deployment specification, select a deployment specification for a distributed appliance and click **Delete**.
- 7 If a previous job failed as a result of an issue with your virtual environment and you have resolved the issue, click **Sync** retry the job.

A new information pop-up appears notifying you that the job has begun along with the job number. After the synchronization is complete, the **Last Job Status** for that instance changes from **RUNNING** to **PASSED** or **FAILED** depending on the result.

- 8 If the job fails, click the hyperlink to the job.

You are routed to the **Jobs** page where you are able to view the tasks for each job. Drilling down enables you to affirm which task failed in the job.

After the deployment specification is created, clicking **OK** instructs Intel Security Controller to begin creating security service instances in the security manager. To view these security service instances, log on to your security manager and navigate to the appropriate page. This page will depend on the security service you are attempting to deploy.



The deployment of security services to designated hosts might not yet be complete since creating a deployment specification does not deploy security services to hosts. To complete deploying security services to designated hosts, you must create a security group and bind it to a policy. If you have not done this so far, you must complete those tasks now. However, although all these tasks are mandatory, there is no set order in which you must perform them. For more details about security groups and binding such a group to a policy, refer [Define Security Groups](#) on page 44.

Define Traffic Policy Mappings

Traffic Policy Mappings exist to provide you a means of enabling you to map a security policy to a **Virtual System**. When you bind a Security Group to a policy in the Security Groups window, this mapping is created automatically. However, you have the option to manually select which policy maps to which **Virtual System**.

Task

- 1 Click the **Add** button.

The **Add Policy Mapping** pop-up window appears.

- 2 Enter the details as mentioned in the table.

Table 4-15 Option definitions

Option	Definition
Name	Name of the policy mapping within Intel Security Controller.
Select Policy	Inspection policies available in the domain that is selected in the Distributed Appliance .
Tag	Tag — ID of the inspection interface. In the instance that two or policies existing in different admin domains of the security manager can have the same name, interfaces are automatically tagged with a unique ID in Intel Security Controller to distinguish them.
Cancel	Cancels your configuration and closes the window.
OK	Saves your configuration. The policy mapping appears in the Policy Mappings for Virtual System section indicating that the mapping is complete.

Maintaining virtual appliance instances

When you create a distributed appliance, you enable the required virtualization connectors in the distributed appliance. For every enabled virtualization connector, Intel Security Controller creates a virtual security system (virtual system) by default. In case of IPS, this virtual security system in the distributed appliance corresponds to the virtual security system in the Network Security Manager.

A virtual security system is assigned a name by assigning a sequentially increasing number to the name of the distributed appliance. When you deploy this virtual security system on the required cluster, NSX automatically installs a virtual security appliance in each ESXi host of the cluster. In the case of IPS and firewall services, a virtual security appliance corresponds to the virtual security system instance, that is the virtual IPS Sensor installed in each ESXi host.

After you deploy the virtual security system, you can view and maintain deployed virtual appliances from the **Appliance Instances** page of Intel Security Controller.

Task

- 1 In Intel Security Controller, select **Status | Appliance Instances**.

Name	IP-Address	Discovered	Inspection-Ready	Last Status	Agent Version	V.Server	V.Connector	Manager	Distributed Appliance	Model
	10.1.1.1	true	true	May 25, 2015 11:17:15 AM	1.00 (Build:2295, 2015/02/13-13:27)	10.71.118.131		NSM		IPS-VM100-VSS
	10.1.1.2	true	true	May 25, 2015 11:14:57 AM	1.20 (Build:2582, 2015/05/02-00:01)	10.71.118.131		NSM		IPS-VM100-VSS

The **Appliance Instances** page lists all the virtual appliances that are currently deployed.

- 2 Select an appliance instance and click **Agent Status** to view the details of the Intel Security Controller agents running on the appliance. Most of these details are also visible in the security manager.
 - **Refresh** — Refreshes the **Intel Security Controller Agent(s) Status Window**.
 - **Close** — Closes the **Intel Security Controller Agent(s) Status Window**.
 - **Name** — Name assigned to the virtual security system.

- **IP:**
 - For VMware — The IP address assigned to the management port of the virtual appliance. This IP address is randomly assigned from the IP pool, which you specified when you deployed the security service.
 - For Openstack:
 - **Local IP** — The IP address that is assigned to the virtual appliance within OpenStack.
 - **Public IP** — IP address assigned to a virtual appliance that is accessible from an external network.
 - **V. Server**— IP address of the virtualization provider or hypervisor server.
 - **ISC IP** — The IP address of Intel Security Controller.
 - **Manager IP** — The IP address of the corresponding Manager, which manages the appliance. In the case of IPS service for example, it is the IP address of the Network Security Manager.
 - **Version** — The version of the Control Path Agent (CPA) on the appliance.
 - **Agent time** — The time as per CPA's clock.
 - **Uptime** — Indicates how long the CPA is up and running.
 - **CPA PID** — Unique ID for the CPA.
 - **DPA PID** — Unique ID for the Data Path Agent (DPA) running on the appliance.
 - **DPA Info** — The version details of the DPA.
 - **DPA Stats** — Displays the number of packets received, transmitted, dropped, and so on by the appliance.
 - **Discovered** — Displays *true* or *false* which are corresponding values that suggest whether the instance of the security service is discovered or not.
 - **Inspection Ready** — Displays *true* or *false* which are corresponding values that suggest whether the instance of the security service is available for deployment and configuration or not.
- 3 Click **Sync** to manually synchronize changes by selecting the required appliance instance.
- The most common scenario in which you will use this is if an automatic update fails. Such an update is initiated if you change network settings of Intel Security Controller or change the password of the default *agent* user name. Intel Security Controller agents in the virtual security system instances (appliances) are updated automatically. If the default update fails, use the manual sync option.
- When you click **Sync**, a *Syncing Intel Security Controller Agent(s)* job is triggered.
- 4 To upgrade Intel Security Controller agents in the virtual security system instances (appliances), select an appliance instance and click **Upgrade Agent**.
- An *Upgrade Intel Security Controller Agent(s)* job is triggered.

- 5 If the **Discovered** state of an appliance is *false*, select the appliance and click **Appliance Re-authentication** to re-authenticate the appliance with the corresponding manager.

In the case of IPS service or firewall service, the virtual security system instance re-establishes trust with the security service Manager when you click **Appliance Re-authentication**.

For firewall, perform re-authentication only when the status of the virtual security system container node is white in SMC.



In some situations, there might be a slight delay before the **Discovered** state turns to *true*. One such example is when you just deploy a security service in NSX. In such cases, please wait for the state to change instead of clicking **Appliance Re-authentication** again.

- 6 Select an appliance instance and click **Download Agent Log** to save log files related to the appliance. You can forward log files to McAfee Support for troubleshooting if necessary.
- 7 To filter the displayed records, enter or select a value in the required column headers and press the Enter key.

Table 4-16 Option definitions

Option	Definition
Name	Unique name assigned to each virtual appliance by default. The name consists of numeric ID appended to the virtual security system name. For example, if <i>DA_N_America_6_7</i> is the name, <i>DA_N_America_6</i> is the name of the virtual security system and 7 is the numeric ID appended to give the virtual appliance a unique name.
IP-Address	IP address assigned to the management port of the virtual appliance. This IP address is randomly assigned from the IP pool, which you specified when you deployed the security service.
Discovered	Indicates if an appliance is discovered by the manager managing that appliance. If this is false for an appliance, click Appliance Re-authentication to trigger re-authentication with the corresponding manager. In case of IPS, the discovered state is true if the output of the <code>status</code> command for the appliance indicates the following: <ul style="list-style-type: none"> • Trust is established with the security manager. • Alert and log channels are up.
Inspection-Ready	Indicates that the appliance is ready for traffic. As an example, the inspection-ready state in IPS is <i>True</i> if the output of the <code>status</code> command indicates the following: <ul style="list-style-type: none"> • Signature file is present in the virtual security system instance. • System is initialized. • System health is good.
Last Status	Timestamp of when Intel Security Controller last checked on the virtual appliance. This time is as per the Intel Security Controller system clock .
Agent Version	Intel Security Controller agent on the virtual security system instance. This agent handles the management traffic between the appliance and the corresponding manager.
V.Server	IP address of the virtualization (ESXi) server on which the virtual appliance is installed.

Table 4-16 Option definitions *(continued)*

Option	Definition
V.Connector	Unique name of the corresponding virtualization connector that you mentioned when you configured that connector. Clicking the hyperlink provided for the virtualization connector of any of the agents, routes you directly to the list of virtualization connectors in the Virtualization Connectors page.
Manager	Unique name of the corresponding manager connector that you mentioned when you configured that connector. Clicking the hyperlink provided for the manager of any of the agents, routes you directly to the list of manager connectors in the Manager Connectors page.
Distributed Appliance	Unique name of the corresponding distributed appliance that you mentioned when you configured that appliance. Clicking the hyperlink provided for the distributed appliance of any of the agents, routes you directly to the list of distributed appliances in the Distributed Appliances page.
Model	Model number of the security appliance as mentioned in the Service Function Catalog page.
Version	Software version of the security appliance as mentioned in the Service Function Catalog page.

Delete a distributed appliance

Before you begin

- 1 You have access rights to uninstall service deployments in NSX.
- 2 The details you provided in the virtualization connectors and manager connector used in the corresponding distributed appliance are valid.




Since distributed appliance information is not stored in Openstack, you can directly delete a distributed appliance in the Intel Security Controller web application.

When you successfully delete a distributed appliance, the corresponding virtual security system instances (ESX agents) are deleted. Therefore, it results in the termination of the security service provided by these virtual security system instances.

To delete a distributed appliance, you must first sequentially delete the related objects in NSX as explained in this section.

Task

- 1 In the vSphere Home tab, select **Networking & Security | Installation | Service Deployments**.
- 2 Select the corresponding service deployment and click .





Installation

















ManagementHost PreparationLogical Network PreparationService Deployments


NSX Manager: 10.10.10.10

Network & Security Service Deployments

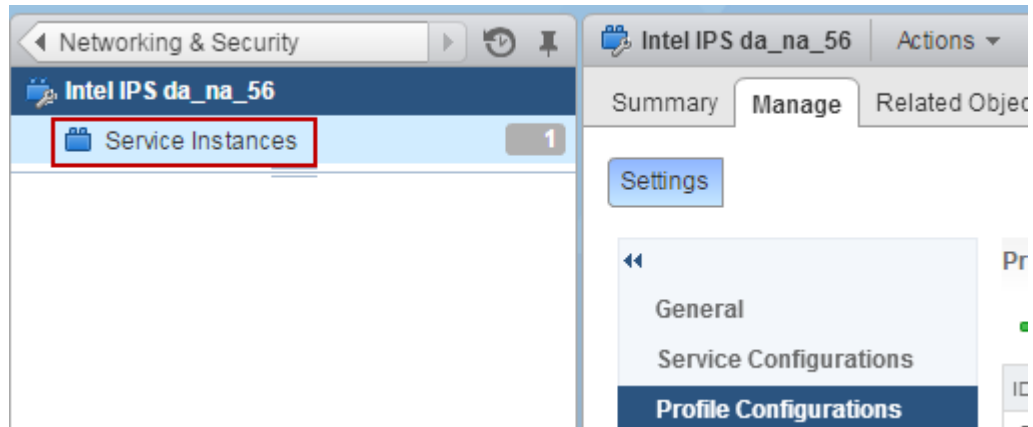
Network & security services are deployed on a set of clusters. Manage service deployments here by adding new services or deleting existing ones.



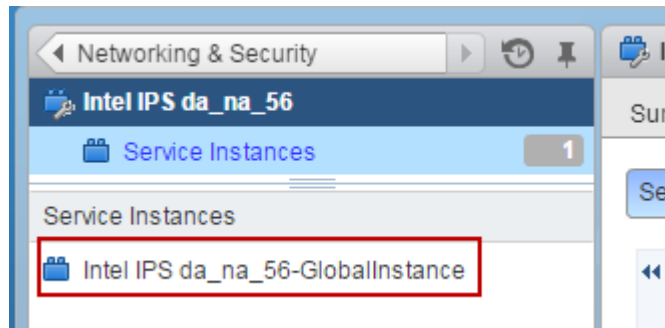
Service	Version	Installation Status	Service Status	Cluster
 Intel NG-IPS DA-10.10.10.10	1.20	✓ Succeeded	✓ Up	 Logical cluster
 Intel NG-IPS DA-10.10.10.10	1.20	✓ Succeeded	✗ Down	 Logical cluster
 Intel NG-IPS DA-10.10.10.10	1.20	✓ Succeeded	✓ Up	 Logical cluster
 Intel NG-IPS DA-10.10.10.10	1.20	✗ Failed	Unknown	 Logical cluster
 Intel IPS old	1.00	✗ Failed	✓ Up	 Logical cluster
 Intel NG-IPS DA-10.10.10.10	1.20	✗ Failed	✓ Up	 Logical cluster
 Intel IPS DA	1.00	✓ Succeeded	✓ Up	 Logical cluster
 Intel NG-IPS DA-10.10.10.10	1.20	✓ Succeeded	✓ Up	 Logical cluster

- 3 Select **Delete now** or schedule the deletion and click **OK**.
Depending on your configuration, it might take several minutes to uninstall the service deployment. This process deletes the virtual security system instances (ESX agents), implying the security service is terminated.
- 4 Select **Service Composer | Security Policies** and then select the NSX Manager.
- 5 Select the security policy used in the deleted IPS or NGFW service deployment and click .
The security groups to which you assigned the security policy are displayed in pop-up window.
- 6 Deselect all the security groups to which you assigned the security policy and click **OK**.
- 7 In the **Networking & Security** pane, select **Service Definitions**.
- 8 Select the corresponding service definition and click the edit icon.
You can identify the service definition by the name of the distributed appliance you want to delete.

9 Select **Service Instances**.



10 Select the instance, which is displayed.



The corresponding service profiles are listed on the right side.

Service Profiles

<div> + 📄 ✖ ⚙️ Actions ▾ </div>	
Name	Description
Intel IPS da_na_56_Default ...	AutoCreated Default Ser
Intel IPS da_na_56_Default ...	AutoCreated Default Ser
Intel IPS da_na_56_Default ...	AutoCreated Default Ser

- 11 Select and delete all the service profiles one by one.
- 12 Select the service instance and delete the service instance.
The corresponding security policy in NSX is automatically deleted.
- 13 In the **Networking & Security** pane, select **Service Definitions**.

- 14 Delete the corresponding service definition.

Locate the service definition based on the name of the distributed appliance you want to delete. This completes the deletion of the related objects in NSX.

- 15 In Intel Security Controller web application, select **Setup | Distributed Appliances**.

- 16 Select the distributed appliance and click **Delete**.

- Deleting the distributed appliance, deletes the service definition in NSX.
- After the distributed appliance deletes successfully, you can delete the corresponding manager connector and virtualization connector, if required.

Jobs and tasks

Certain actions you perform in Intel Security Controller are tracked as jobs. When you start a job, it triggers one or more background activities in Intel Security Controller. These background activities are tracked as tasks of that job. Therefore, a job is completed only when all its tasks are successfully completed.

Jobs and tasks enable easy tracking and troubleshooting. For example, if a job failed, you just have to look at the failed task to locate the stage at which the job failed. If a job is running for a long time, you can troubleshoot by looking at the task at which the processing is stuck.

Intel Security Controller triggers a job, when you take any of the following actions:

- Create, edit, synchronize, or delete a manager connector.
- Create, edit, synchronize, or delete a distributed appliance.
- Synchronize appliance instances.
- Appliance instance re-authentication.
- Upgrade the software for an appliance instance.
- Modify the password of the default users.

Viewing jobs and tasks

You can view the jobs and the corresponding tasks in the **Jobs** page.

Task

- 1 In the Intel Security Controller web application, select **Status | Jobs**.

The jobs are listed in the top pane of the page. When you click on a job, the corresponding tasks are listed in the bottom pane.



All time stamps displayed in the **Jobs** page are according to Intel Security Controller system time. You can use `show clock` command or the **Manage | Server | Summary** page to check the current date and time on Intel Security Controller. To change the system time, use the `set time` and `set timezone` commands.

Jobs									
<div> Job Graph Abort </div>									
ID	Name	Objects	State	Status	Started	Completed	Failure Reason	Queued	Submitted By
14,265	Syncing Security Group 'Coke-SG'	Coke-SG	COMPLETED	PASSED	Oct 13, 2015 11:58:43 AM	Oct 13, 2015 11:58:49 AM		Oct 13, 2015 11:58:43 AM	admin
14,264	Syncing Distributed Appliance 'Doc2'	Doc2	COMPLETED	PASSED	Oct 13, 2015 11:58:43 AM	Oct 13, 2015 11:58:44 AM		Oct 13, 2015 11:58:43 AM	admin
14,263	Syncing Security Group 'Pepsi-SG'	Pepsi-SG	COMPLETED	PASSED	Oct 13, 2015 11:58:43 AM	Oct 13, 2015 11:58:45 AM		Oct 13, 2015 11:58:43 AM	admin
14,262	Syncing Distributed Appliance 'IPS-SVC'	IPS-SVC	COMPLETED	PASSED	Oct 13, 2015 11:58:43 AM	Oct 13, 2015 11:58:48 AM		Oct 13, 2015 11:58:43 AM	admin
14,261	Syncing Security Group 'Coke-SG'	Coke-SG	COMPLETED	PASSED	Oct 13, 2015 10:58:43 AM	Oct 13, 2015 10:58:49 AM		Oct 13, 2015 10:58:43 AM	admin
14,260	Syncing Distributed Appliance 'Doc2'	Doc2	COMPLETED	PASSED	Oct 13, 2015 10:58:43 AM	Oct 13, 2015 10:58:44 AM		Oct 13, 2015 10:58:43 AM	admin
14,259	Syncing Distributed Appliance 'IPS-SVC'	IPS-SVC	COMPLETED	PASSED	Oct 13, 2015 10:58:43 AM	Oct 13, 2015 10:58:48 AM		Oct 13, 2015 10:58:43 AM	admin
14,258	Syncing Security Group 'Pepsi-SG'	Pepsi-SG	COMPLETED	PASSED	Oct 13, 2015 10:58:43 AM	Oct 13, 2015 10:58:44 AM		Oct 13, 2015 10:58:43 AM	admin
14,257	Syncing Security Group 'Coke-SG'	Coke-SG	COMPLETED	FAILED	Oct 13, 2015 9:58:43 AM	Oct 13, 2015 9:58:45 AM	One of the tasks in the job failed	Oct 13, 2015 9:58:43 AM	admin

Tasks									
Order	Name	Objects	State	Status	Started	Completed	Error	Predecessors	ID
1	Sync Security Group 'Coke-SG' members mapping to DAIs	Coke-SG	COMPLETED	PASSED	Oct 13, 2015 11:58:43 AM	Oct 13, 2015 11:58:43 AM		[1]	385,487
2	Validating Security Group 'Coke-SG' for tenant 'Coke'	Coke-SG	COMPLETED	PASSED	Oct 13, 2015 11:58:43 AM	Oct 13, 2015 11:58:43 AM		[1]	385,489
3	Checking Security Group 'Coke-SG' members	Coke-SG	COMPLETED	PASSED	Oct 13, 2015 11:58:43 AM	Oct 13, 2015 11:58:43 AM		[2]	385,490
4	Checking Security Group Member of type 'VM' with Name 'victim'		COMPLETED	PASSED	Oct 13, 2015 11:58:43 AM	Oct 13, 2015 11:58:44 AM		[3]	385,495
5	Updating Security Group Member 'VM' 'victim'		COMPLETED	PASSED	Oct 13, 2015 11:58:44 AM	Oct 13, 2015 11:58:44 AM		[4]	385,503
6	Checking Inspection hooks for VM Security Group Member 'victim'		COMPLETED	PASSED	Oct 13, 2015 11:58:44 AM	Oct 13, 2015 11:58:44 AM		[5]	385,504
7	Checking 'IPS-SVC' Service Inspection hooks for VM 'victim' port with MAC 'fa:16:3ed3:06:ca' belonging to Security Group 'Coke-SG'	Coke-SG	COMPLETED	PASSED	Oct 13, 2015 11:58:44 AM	Oct 13, 2015 11:58:44 AM		[6]	385,505
8	Updating Traffic Policy Mappings for Security Group 'Coke-SG'	Coke-SG	COMPLETED	PASSED	Oct 13, 2015 11:58:44 AM	Oct 13, 2015 11:58:44 AM		[7]	385,496
9	Checking Traffic Policy Mappings of VS 'IPS-SVC-39' with Appliance Manager 'NSM_35'	NSM_35	COMPLETED	PASSED	Oct 13, 2015 11:58:44 AM	Oct 13, 2015 11:58:48 AM		[8]	385,491
10	Update Manager Security Group Interface 'my-tag' (48) of Virtualization System 'HQ Opendstack (.13)'	my-tag	COMPLETED	PASSED	Oct 13, 2015 11:58:48 AM	Oct 13, 2015 11:58:48 AM		[9]	385,558

Figure 4-22 Jobs page

Table 4-17 Option definitions in the Jobs pane

Option	Definition
Job Graph	Click to see a graphical representation of the order of tasks for the selected job.
Abort	Click if you do not need a job to be processed any further or remove it from the processing queue. <div> Even when you abort a job, the entries for all tasks of that job are created; task IDs are assigned for all tasks; job ID is assigned for the job. </div>
ID	This is a system-assigned unique ID to each job. This ID is assigned in a sequential order.
Name	This is a system-defined name to a job. The name of the connector is appended at the end of the name. For example, if you delete a distributed appliance named <i>example_DA</i> , the name assigned for this job is <i>Delete Distributed Appliance 'example_DA'</i> .
Objects	Unique name of the distributed appliance executing that job. Clicking the hyperlink provided routes you directly to the list of distributed appliances in the Distributed Appliances page.

Table 4-17 Option definitions in the Jobs pane *(continued)*

Option	Definition
State	Indicates the current state of the job. The following are the possible values: <ul style="list-style-type: none"> • NOT_RUNNING — indicates that Intel Security Controller started the job but is unable to complete the process. • QUEUED — indicates that the job is in the queue to be processed. For example, there might be too many concurrent jobs being processed and the jobs in the queue are processed as soon as system resources are available. • RUNNING — indicates that the job is now being processed. • COMPLETED — indicates that Intel Security Controller completed processing the job. However, check the status of the job to see if the job was completed successfully.
Status	Indicates the result for a job. The following are the possible values: <ul style="list-style-type: none"> • FAILED — indicates that one or more the tasks of that job failed. So, Intel Security Controller is unable to complete the job successfully. • PASSED — indicates that all tasks of the job are completed successfully. Hence, the jobs are also completed successfully. • ABORTED — A user clicked Abort to stop processing the job further.
Started	The time stamp of when the job is started. This is empty for jobs which processing never started. For example, if you aborted jobs, which are queued for processing, this time stamp is empty.
Completed	The time stamp of when the job is completed regardless of the job Status . The Completed time stamp is available only for those jobs, which are in completed State . Regarding Status , the completed time stamp is displayed for all failed, passed, and aborted jobs. In case of failed and passed jobs, this time stamp indicates when the last task was completed. In case of aborted jobs, this time stamp indicates when a user aborted the job.
Failure Reason	Displays the reason for the failure of the job
Queued	The time stamp of when a user started the action. If Intel Security Controller processes the job as soon as it is triggered, this time stamp is the same as that of the Started time stamp.
Submitted By	Name of the user who initiated the job.

When you click **Job Graph**, a graphical representation of the order and dependency of tasks displays. The tasks are color-coded to indicate their status.

- Green indicates the task succeeded.
- (Not shown) Yellow indicates the task is in progress.
- Red indicates the task failed.

- Gray indicates that the task is skipped.
- White indicates that the task is aborted.

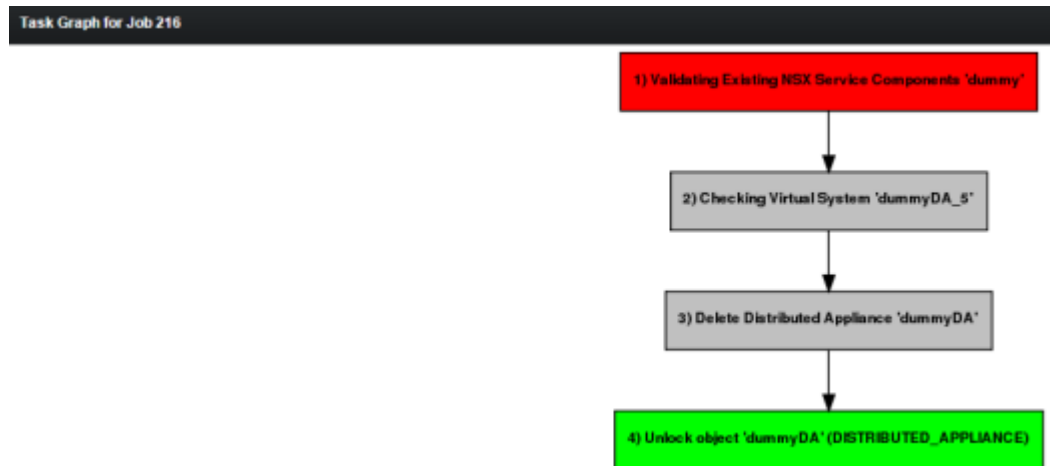


Figure 4-23 Job graph

- 2 Click a job to view its tasks.


Table 4-18 Option definitions in the Tasks pane

Option	Definition
Order	Indicates the sequence in which the tasks are executed.
Name	This is a system-defined name to a task. The name of the relevant connector is appended at the end for some of the tasks.
Objects	Unique name of the distributed appliance executing that task. Clicking the hyperlink provided routes you directly to the list of distributed appliances in the Distributed Appliances page.
State	Indicates the current state of the job. The following are the possible values: <ul style="list-style-type: none">• NOT_RUNNING — indicates that Intel Security Controller started the task but is now aborted.• QUEUED — indicates that the task is in the queue to be processed. For example, there might be too many concurrent tasks being processed and the tasks in the queue are processed as soon as system resources are available.• PENDING — indicates that there are predecessor tasks and only some of them are currently completed.• RUNNING — indicates that the task is now being processed.• COMPLETED — indicates that Intel Security Controller completed processing the task. However, check the status of the task to see if it was completed successfully.

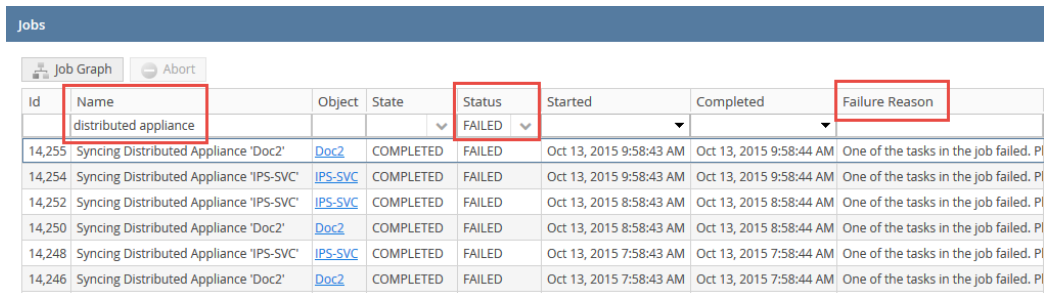
Table 4-18 Option definitions in the Tasks pane *(continued)*

Option	Definition
Status	Indicates the result for a task. The following are the possible values: <ul style="list-style-type: none"> • FAILED — indicates that the task failed. So, Intel Security Controller is unable to complete the job successfully. • SKIPPED — indicates that Intel Security Controller skipped this task and proceeded to the next task. When a prerequisite task fails, the current task is skipped. • PASSED — indicates that the task is completed successfully. • ABORTED — indicates that the task was started but a user clicked Abort to stop processing the job further.
Started	The time stamp of when the task is started. This is empty for tasks which never started.
Completed	The time stamp of when the task is completed regardless of the job Status . The Completed time stamp is available only for those tasks, which are in completed State . Regarding Status , the completed time stamp is displayed for all failed, passed, skipped, and aborted tasks. In case of failed and passed tasks, this time stamp indicates when the task was completed. In case of aborted jobs, this time stamp indicates when a user aborted the job. In case of skipped tasks, this time stamp indicates when a task was skipped.
Error	Displays the reason for failed tasks.
Predecessors	Indicates the Order number of one or more tasks, which must be completed to complete this task. Click Job Graph to see the graphical representation of the order in which tasks are executed.
ID	This is a system-assigned unique ID to each task. This ID is assigned in a sequential order and is unique across jobs.

3 Use the following options to change the display in the jobs and tasks pane.

- The page automatically shows the updated content. If necessary, you can click  in the jobs or the tasks pane.
- To change the order of the columns in the jobs or tasks pane, click on a column header and drag it to where you want in the pane.
- Click on a column header to sort the records in the ascending or descending order. For example, click on the **Order** column in the tasks pane to display the records in descending order, that is, the last task is displayed first and the first task is displayed last.

- To filter the records, enter or select the values in the required columns and press the Enter key. All records containing the specified values are listed. For example, enter *distributed appliance* **Name** column and select **Failed** in the **Status** column to view the failed jobs with the **Failure Reason** related to distributed appliances. Follow a similar procedure to filter records in the tasks pane.



Id	Name	Object	State	Status	Started	Completed	Failure Reason
14,255	Syncing Distributed Appliance 'Doc2'	Doc2	COMPLETED	FAILED	Oct 13, 2015 9:58:43 AM	Oct 13, 2015 9:58:44 AM	One of the tasks in the job failed. PI
14,254	Syncing Distributed Appliance 'IPS-SVC'	IPS-SVC	COMPLETED	FAILED	Oct 13, 2015 9:58:43 AM	Oct 13, 2015 9:58:44 AM	One of the tasks in the job failed. PI
14,252	Syncing Distributed Appliance 'IPS-SVC'	IPS-SVC	COMPLETED	FAILED	Oct 13, 2015 8:58:43 AM	Oct 13, 2015 8:58:44 AM	One of the tasks in the job failed. PI
14,250	Syncing Distributed Appliance 'Doc2'	Doc2	COMPLETED	FAILED	Oct 13, 2015 8:58:43 AM	Oct 13, 2015 8:58:44 AM	One of the tasks in the job failed. PI
14,248	Syncing Distributed Appliance 'IPS-SVC'	IPS-SVC	COMPLETED	FAILED	Oct 13, 2015 7:58:43 AM	Oct 13, 2015 7:58:44 AM	One of the tasks in the job failed. PI
14,246	Syncing Distributed Appliance 'Doc2'	Doc2	COMPLETED	FAILED	Oct 13, 2015 7:58:43 AM	Oct 13, 2015 7:58:44 AM	One of the tasks in the job failed. PI

Figure 4-24 Filter records in the Jobs page

- To remove the filters, delete the search strings and selections from the columns and press *Enter* on your keyboard.


Alarms, alerts, and archives

You can now setup alarms that trigger alerts. The alarms can be set for different types of failures like job failures, system failure, or appliance instance failures. Different severity levels can be defined for each type of failure, and also add an email notification to be sent out in case of a failure. An alert is generated for every failure event that occurs. The description for the failure provides an easy way to troubleshoot the failure thereby reducing downtime. Alerts are generated with different severity level which depends on the severity level defined in the alarm. You can also acknowledge alerts that have been viewed so that you can filter alerts that require attention. You can archive older jobs and alerts. Tasks related to the jobs are also archived. You can either set an auto schedule to archive the jobs and alerts, or manually trigger archiving whenever required. There are different options by which you can set a schedule for archiving. You can also download the previous archived files for analysis.

Alarms

You can setup alarms in the **Alarms** tab and thereby generate an alert when there is a failure. Alerts are generated only for the alarms that are enabled. You can also set the severity level for alarms which helps identify critical failures. Email notifications can be configured as a part of the action to take when a failure occurs. An email is sent to the security administrator whose email address can be configured for a particular type of failure.

There are three types of failures you encounter in Intel Security Controller:

Failure type	Description
System Failure	<p>Classified as failures due to which a critical process cannot be performed. Some of the system failures are as follows:</p> <ul style="list-style-type: none"> • Email Failure – Failure to send an email as a part of alert action • Archive Failure – Failure while archiving • Talkback Failure – Failure while sending talkback data to McAfee Global Threat Intelligence regarding system health • Manager Web Socket Notification Failure – Failure to connect with Manager Web Socket notifications service • Openstack Notification Failure – Failure to connect with openstack notification service • Scheduler Failure – Failure in periodic synchronization with the distributed appliances
Appliance Instance Failure	<p>Classified as failures that occur when Appliance Instances Discovered or Inspection-ready status changes from true to false. This failure is also triggered when the heartbeat from an Appliance Instance is not received within three minutes. This time interval cannot be configured.</p> <div>  No alert is generated when an Appliance Instance is initially deployed, as the initial status is false. </div>
Job Failure	Classified as failures that are generated when a job is not completed successfully.

By default the **Default System Failure** and **Default Appliance Instance Failure** alarms are enabled. The **Default Job Failure** is disabled.

When there are multiple alarms configured, you can filter specific alarms depending on relevance. To resize a column, hover the mouse between the columns till the cursor changes to parallel lines and then resize the columns.


Alarms ? ↺				
+ Add ✎ Edit ✕ Delete				
Name	Enabled	Event Type	Severity	Action 
	<input type="checkbox"/>			
Default Appliance Instance Failure Alarm	false	DAI Failure	Medium	None
Default Job Failure Alarm	false	Job Failure	Low	None
Default System Failure Alarm	true	System Failure	High	None

Figure 4-25 Alarms page

Table 4-19 Option definition

Option	Definition
Name	Displays the name of the alarm
Enabled	Displays if the alarm is enabled or disabled. true specifies enabled, false specifies disabled.

Table 4-19 Option definition (*continued*)

Option	Definition
Event Type	Displays the type of failure. There are three types of failure: <ul style="list-style-type: none">• System Failure• DAI Failure• Job Failure
Severity	Customize the severity of the alarm. The default values are: <ul style="list-style-type: none">• High – System Failure• Medium – DAI Failure• Low – Job Failure
Action	Displays if the notification for failure is enabled or not.

Create alarms

You can create alarms and customize them as per your requirement. After you create an alarm, you can enable email notifications for the failure and also customize the severity as per your requirement.

To create a new alarm, perform the following tasks:

Task

- 1 Navigate to **Manage | Alarms**.
- 2 Click **Add**.
The **Add Alarm** pop-up opens.
- 3 Type/select the following details:

Table 4-20 Option definition



Option	Definition
Enabled	Select the checkbox if you want to enable the alarm.  You can create an alarm and enable it at a later time.
Alarm Name	Name of the alarm
Event Type	Displays the type of failure. There are three types of failure: <ul style="list-style-type: none">• System Failure• DAI Failure• Job Failure
Regex Match	Provides match for the alert message that allows you to customize which alerts are generated or suppressed
Severity	Customize the severity of the alarm. The default values are: <ul style="list-style-type: none">• High – System Failure• Medium – DAI Failure• Low – Job Failure

Table 4-20 Option definition *(continued)*

Option	Definition
Alarm Action	Select which action to trigger along with the alert. Currently, only email notification is supported.
	 If you select Email , you have to provide the email ID in the Send email to field to which the notification will be sent. You must configure the SMTP server settings for the email when you setup the alert action.
OK	Click to create the alarm
Cancel	Click to cancel creating an alarm

Add Alarm

☒ Enabled

Alarm Name *

Event Type *

Regex Match

Severity *

Alarm Action *

Send email to *

Figure 4-26 Create an alarm

An example for the alert generated through an email notification is as follows:

An alert has been generated in your ISC environment.

Type: Job Failure

Severity: Low

Object: Syncing Appliance Manager Connector 'NSM_DEV.1'

Message: One of the tasks in the job failed. Please look at the tasks to figure out the root cause.

Please click on the following URL or login to your ISC for more details: <https://10.x.x.x/#!/Alerts/alertId=4765>

Modify alarms

You can modify an existing alarm as per your requirement. For example, when you create an alarm but do not enable it, you can enable it by editing the alarm. When an alarm is no more necessary, you can delete it.



You can edit/delete the default alarms.

To create a new alarm, perform the following tasks:

Task

- 1 Navigate to **Manage | Alarms**.
- 2 Select the alarm and click **Edit**.
The **Edit Alarm** pop-up opens.
- 3 Make the necessary changes and click then **OK**.

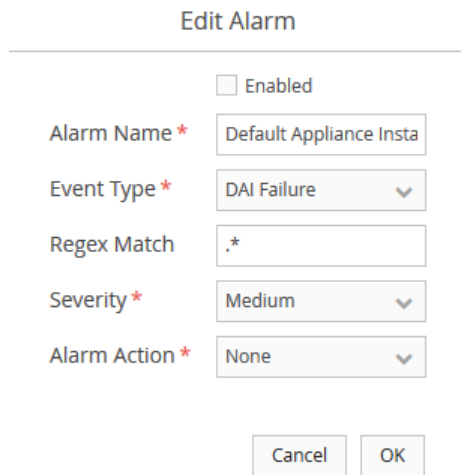


Figure 4-27 shows the 'Edit Alarm' pop-up form. The form is titled 'Edit Alarm' and contains the following fields and controls:

- ☐ Enabled
- Alarm Name *: Default Appliance Insta
- Event Type *: DAI Failure
- Regex Match: .*
- Severity *: Medium
- Alarm Action *: None
- Buttons: Cancel, OK

Figure 4-27 Edit an alarm

To delete an alarm, select the alarm and click **Delete**. However, you cannot delete multiple alarms at the same time.

Alerts

The **Alerts** tab in Intel Security Controller displays alerts generated for system, job and appliance instance (DAI) failures. Critical failures can lead to outage in attack detection, in which case the network becomes vulnerable to threats. Alerts are continuously generated for any failure till the problem is resolved. The failure description provided for alerts, eases the process of troubleshooting. Alerts are triggered depending on the alarms configured in the **Alarms** tab.



The **Alerts** page is the landing page when you first login to Intel Security Controller. This will help you troubleshoot any critical failure that may have occurred.

Alert filters provide help drill down specific alerts which otherwise becomes difficult when there are many alerts. To resize a column, by hover the mouse between the columns till the cursor changes to parallel lines and then resize the columns.

Id	Name	Objects	Severity	Message	Created	Status	Acknowledged	Acknowledged By
52,873	Default System Failure Alarm	RHEL-NSC1	High	Fail to connect to Openstack Notification Server for Vir	Oct 8, 2015 11:26:37 AM	Pending Acknowledgment		
52,872	Default System Failure Alarm	RHEL-NSC1	High	Fail to connect to Openstack Notification Server for Vir	Oct 8, 2015 11:25:37 AM	Pending Acknowledgment		
52,871	Default System Failure Alarm	RHEL-NSC1	High	Fail to connect to Openstack Notification Server for Vir	Oct 8, 2015 11:24:37 AM	Pending Acknowledgment		
52,870	Default System Failure Alarm	RHEL-NSC1	High	Fail to connect to Openstack Notification Server for Vir	Oct 8, 2015 11:23:37 AM	Pending Acknowledgment		
52,869	Default System Failure Alarm	RHEL-NSC1	High	Fail to connect to Openstack Notification Server for Vir	Oct 8, 2015 11:22:37 AM	Pending Acknowledgment		
52,868	Default System Failure Alarm	RHEL-NSC1	High	Fail to connect to Openstack Notification Server for Vir	Oct 8, 2015 11:21:37 AM	Pending Acknowledgment		
52,867	Default System Failure Alarm	RHEL-NSC1	High	Fail to connect to Openstack Notification Server for Vir	Oct 8, 2015 11:20:37 AM	Pending Acknowledgment		
52,866	Default System Failure Alarm	RHEL-NSC1	High	Fail to connect to Openstack Notification Server for Vir	Oct 8, 2015 11:19:37 AM	Pending Acknowledgment		
52,865	Default System Failure Alarm	RHEL-NSC1	High	Fail to connect to Openstack Notification Server for Vir	Oct 8, 2015 11:18:37 AM	Pending Acknowledgment		
52,864	Default System Failure Alarm	RHEL-NSC1	High	Fail to connect to Openstack Notification Server for Vir	Oct 8, 2015 11:17:37 AM	Pending Acknowledgment		
52,863	Default System Failure Alarm	RHEL-NSC1	High	Fail to connect to Openstack Notification Server for Vir	Oct 8, 2015 11:16:37 AM	Pending Acknowledgment		
52,862	Default System Failure Alarm	RHEL-NSC1	High	Fail to connect to Openstack Notification Server for Vir	Oct 8, 2015 11:15:37 AM	Pending Acknowledgment		
52,861	Default System Failure Alarm	RHEL-NSC1	High	Fail to connect to Openstack Notification Server for Vir	Oct 8, 2015 11:14:37 AM	Pending Acknowledgment		
52,860	Default System Failure Alarm	RHEL-NSC1	High	Fail to connect to Openstack Notification Server for Vir	Oct 8, 2015 11:13:37 AM	Pending Acknowledgment		
52,859	Default System Failure Alarm	RHEL-NSC1	High	Fail to connect to Openstack Notification Server for Vir	Oct 8, 2015 11:12:37 AM	Pending Acknowledgment		
52,858	Default System Failure Alarm	RHEL-NSC1	High	Fail to connect to Openstack Notification Server for Vir	Oct 8, 2015 11:11:37 AM	Pending Acknowledgment		
52,857	Default System Failure Alarm	RHEL-NSC1	High	Fail to connect to Openstack Notification Server for Vir	Oct 8, 2015 11:10:37 AM	Pending Acknowledgment		
52,856	Default System Failure Alarm	RHEL-NSC1	High	Fail to connect to Openstack Notification Server for Vir	Oct 8, 2015 11:09:37 AM	Pending Acknowledgment		
52,855	Default System Failure Alarm	RHEL-NSC1	High	Fail to connect to Openstack Notification Server for Vir	Oct 8, 2015 11:08:37 AM	Pending Acknowledgment		
52,854	Default System Failure Alarm	RHEL-NSC1	High	Fail to connect to Openstack Notification Server for Vir	Oct 8, 2015 11:07:37 AM	Pending Acknowledgment		
52,853	Default System Failure Alarm	RHEL-NSC1	High	Fail to connect to Openstack Notification Server for Vir	Oct 8, 2015 11:06:37 AM	Pending Acknowledgment		
52,852	Default System Failure Alarm	RHEL-NSC1	High	Fail to connect to Openstack Notification Server for Vir	Oct 8, 2015 11:05:37 AM	Pending Acknowledgment		
52,851	Default System Failure Alarm	RHEL-NSC1	High	Fail to connect to Openstack Notification Server for Vir	Oct 8, 2015 11:04:37 AM	Pending Acknowledgment		

Figure 4-28 Alerts page

Table 4-21 Option definition

Option	Definition
Name	Displays the name of the failure alarm that generated the alert
Objects	Provides link to the relevant object for the failure in the alert. For example, in case of job failure, it will contain the job ID link. In case of DAI failure, it contains the DAI link, System failure points to the relevant VC, MC, or relevant component.
Severity	Customize the severity of the alarm. The default values are: <ul style="list-style-type: none"> • High – System Failure • Medium – DAI Failure • Low – Job Failure
Message	Displays the description for the failure
Created	Time when the alert was generated/ failure occurred
Status	Status of the alert, Acknowledged or Pending Acknowledgment
Acknowledged	Time when the alert was acknowledged
Acknowledged By	Name of the user who acknowledged the alert

Alert summary

Alerts exist in either of the two states:

- **Pending Acknowledgment** – Alerts that need action by a user and not acknowledged
- **Acknowledged** – Alerts that are reviewed and acknowledged by a user

When an alert is generated, it initially appears in the **Pending Acknowledgment** state. You can also mark an acknowledged alert as unacknowledged for further review at a later time. When you mark an alert as unacknowledged, the status of the alert reverts to **Pending Acknowledgment**.

Manage alerts

You can manage alerts by performing various tasks listed here:

- To acknowledge an alert, select the alert and click **Acknowledge**.



All users have access to acknowledge the alerts.

- To unacknowledge an alert, select the alert and click **Unacknowledge**.
- The **Show Pending** button also lists all the alerts that are in **Pending Acknowledgment** state.
- The **Show All** button clears all the filters and displays alerts in both acknowledged and pending acknowledgment states.
- You can delete a single alert or multiple alerts. To delete an alert, select the alert and click **Delete**.



Once an alert is deleted, it cannot be retrieved unless it was archived.

You can select multiple alerts by holding down the *Ctrl* key and selecting the alerts.

Archiving

Many jobs and tasks are executed for each process carried out by an Intel Security Controller. This sometimes leads to a large number of jobs. In such cases, you can archive obsolete jobs which will still be available for later use. This also clears space in the database for more recent jobs that are executed, thus improving the performance. Archiving can be auto scheduled or executed on demand. The tasks and alerts related to the jobs are also archived.

Archive jobs

To access the archived files, click the archive file link in the **Download** column. Archived folders are downloaded as .zip files and archived files are in .csv format. It zip file contains CSV formatted files holding raw data for all archived jobs/tasks/alerts. You can this data for auditing and reporting purpose.

Table 4-22 Option definition

Option	Definition
Name	Name of the archive file
Date	Date and time when the archiving is triggered
Size	Size of the archive file
Download	Download link for the archive file. The download link file format is <code>Download archive/isc-archive-<Date>_<Time>.zip</code> . The date/time represent the threshold date for which the records that are older than that date/time are archived.
Delete	Click to delete the archive file

The columns can be resized for easy viewing purpose. To resize a column, by hover the mouse between the columns till the cursor changes to parallel lines and then resize the columns. You can also sort the archive files in ascending or descending order based on the date by clicking the arrow in the **Date** column.

Create archives

Auto Schedule

You can auto schedule archiving where archives are automatically created periodically. You are able to define auto archiving using two parameters:

- Define the frequency of archiving – you can trigger an archive operation either every week or every month.
- Define the age of the jobs to be archived – regardless of the frequency, you can choose which jobs must be archived at each point by defining the age of jobs in the **Archive Jobs older than the last** field. This defines the threshold date which archives records older than that date. The date is always relative to current server system time.

For example, assuming that you want to create an auto schedule weekly archives for job, tasks, and alerts older than 1 month, perform the following tasks:

- 1 Navigate to **Manage | Server | Archive**.
- 2 Select the **Auto Schedule** option.
- 3 Select the **Weekly** option.
- 4 Type 1 in the **Archive Jobs older than the last** field and select **Months** option.

This triggers and creates an archive file on a weekly basis. It also take into account jobs older than one month while archiving due to the **Archive Jobs older than the last** configuration. This means that each week, jobs that are older than one month are archived.

When you modify any settings for auto schedule, click **Update Schedule** for the changes to be updated.

Name	Date	Size	Download	Delete
isc-archive-2015-09-05_05-47-38.zip	Oct 5, 2015 5:47:43 AM	414,483	Download archive/isc-archive-2015-09-05_05-47-38.zip	Delete
isc-archive-2015-08-28_02-16-05.zip	Sep 28, 2015 2:16:11 AM	513,527	Download archive/isc-archive-2015-08-28_02-16-05.zip	Delete
isc-archive-2015-08-20_06-36-02.zip	Sep 20, 2015 6:36:02 AM	58,896	Download archive/isc-archive-2015-08-20_06-36-02.zip	Delete
isc-archive-2015-08-19_16-33-30.zip	Sep 19, 2015 4:33:40 PM	820,350	Download archive/isc-archive-2015-08-19_16-33-30.zip	Delete
2015-08-18_02-46-30	Sep 18, 2015 2:46:32 AM	4,096	Download archive/2015-08-18_02-46-30	Delete

Figure 4-29 Auto schedule archives

On Demand

Due to space constraints sometimes the database will have to be cleared to make way for new jobs. In such cases you can archive data on demand. There are two ways by which you can perform an archive on demand:

- 1 Use the auto schedule options and perform on demand archiving
- 2 Change the configurations and perform on demand archiving

In the second type of archiving, the auto schedule configuration will not be affected when you change the configuration. The auto schedule configuration will change only when you click **Update Schedule**.

When you create an archive on demand, the message **On demand archiving started in the background** is displayed at the bottom of the window. The message **On demand request successful** is displayed once the archiving is completed.

5

Intel Security Controller CLI commands - normal mode

This section explains the Intel Security Controller CLI commands, which you can run in the normal mode.

For CLI commands related to Virtual Security System instances for IPS, see *Network Security Platform 8.2 CLI Guide*.

For CLI commands related to Virtual Security System instances for firewall, see *McAfee Next Generation Firewall 5.9.0 Product Guide*.

Contents

- *clear*
- *debug*
- *exit*
- *help*
- *history*
- *list*
- *ping*
- *ping6*
- *reset*
- *server restart*
- *server start*
- *server status*
- *server stop*
- *set network dns*
- *set network domain*
- *set network gateway*
- *set network hostname*
- *set network ip*
- *set network ntp*
- *set passwd*
- *set time*
- *set timezone*
- *show arp*
- *show clock*
- *show filesystems*
- *show log*
- *show log follow*
- *show log last*
- *show log reverse*
- *show network dns*
- *show network domain*

- *show network hostname*
- *show network ip*
- *show network ntp*
- *show network route*
- *show process*
- *show process monitor*
- *show system memory*
- *show system uptime*
- *show version*
- *shutdown*
- *traceroute*
- *traceroute6*

clear

This command clears only your CLI screen. This command has no impact on the database of Intel Security Controller.

Syntax: `clear`

debug

Helps you to debug the connection between the Intel Security Controller appliance and your client computer.

Syntax: `debug`

exit

Logs off the current SSH connection with the Intel Security Controller appliance and closes the PuTTY window.

This command has no parameters.

Syntax: `exit`

help

Provides a description of all commands.

This command has no parameters.

Syntax: `help`

history

Lists all the commands attempted so far on your Intel Security Controller appliance. This command lists even the unsuccessful commands as well as commands attempted in the earlier sessions.

This command has no parameters.

Syntax: `history`

list

Lists all the commands available in the normal mode along with the description for each.

This command has no parameters.

Syntax: `list`

ping

Pings an IPv4 network host.

Syntax:

`ping <A.B.C.D>`

Parameter	Description
<A.B.C.D>	denotes the 32-bit IPv4 address written as four eight-bit numbers separated by periods. Each number (A,B,C and D) is an eight-bit number between 0-255.

Sample Output:

```
localhost> ping 10.10.10.10

PING 10.10.10.10 (10.10.10.10) 56(84) bytes of data.

64 bytes from 10.10.10.10: icmp_seq=1 ttl=56 time=246 ms
64 bytes from 10.10.10.10: icmp_seq=2 ttl=56 time=246 ms
64 bytes from 10.10.10.10: icmp_seq=3 ttl=56 time=246 ms
64 bytes from 10.10.10.10: icmp_seq=4 ttl=56 time=246 ms
64 bytes from 10.10.10.10: icmp_seq=5 ttl=56 time=264 ms

--- 10.10.10.10 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4270ms
rtt min/avg/max/mdev = 246.284/250.107/264.960/7.446 ms
```

In this example, you are able to ping host 10.10.10.10 successfully from your Intel Security Controller appliance. For this test, Intel Security Controller appliance sends 5 ICMP packets of 64 bytes each. The sequence of the packets, time to live (ttl), and the time taken for the reply are displayed for each reply packet from 10.10.10.10.

The statistics section displays the minimum, average, and maximum round-trip time (RTT) in milliseconds. The mean deviation (mdev) is also displayed, which is the average of each ping's RTT deviation from the average RTT.

ping6

Pings an IPv6 network host.

Syntax:

```
ping6 <A:B:C:D:E:F:G:H>
```

Parameter	Description
<A:B:C:D:E:F:G:H>	denotes the 128-bit address written as octet (eight groups) of four hexadecimal numbers, separated by colons. Each group (A,B,C,D and so on) represents a group of hexadecimal numbers between 0000-FFFF. You can also use the shorter notations of an IPv6 address.

Example:

The following command pings a 128-bit address written as an octet of four hexadecimal numbers.

```
ping 1058:0cd8:8d2f:0000:0000:0000:0000:0050
```

reset

Resets the Intel Security Controller appliance.

Syntax: `reset`



This command immediately restarts the Intel Security Controller appliance without asking for confirmation.

server restart

This command stops and then again starts the Intel Security Controller server.

Syntax: `server restart`

server start

This command starts the Intel Security Controller server.

Syntax: `server start`

server status

This command displays the current status of the Intel Security Controller server.

Syntax: `server status`

server stop

This command stops the Intel Security Controller server.

Syntax: `server stop`

set network dns

Use this command to configure primary and secondary name servers (IPv4 addresses) for the Intel Security Controller appliance.

Syntax: `set network dns <A.B.C.D> <E.F.G.H>`

Parameter	Description
<A.B.C.D> <E.F.G.H>	<A.B.C.D> is the IPv4 address of the primary name server and <E.F.G.H> the IPv4 address of an optional secondary name server. If you specify a secondary name server IP address, use a space as the separator.

Example: `set network dns 10.10.10.10 10.10.10.11`

Notes:

- To remove the name server configuration, enter `set network dns`. That is, use the command without any IP address.
- To remove just the secondary name server IP address, enter `set network dns <A.B.C.D>`. That is, use the command and only the IP address of the primary name server.
- You can also configure the name server IP addresses in the **Network Settings** page of Intel Security Controller web application. The name servers you configure using the `set network dns` command reflect in the **Network Settings** page.

set network domain

Use this command to add Intel Security Controller to a network domain.

Syntax: `set network domain <domain name>`

Example: `set network domain SecurityDevices`

set network gateway

Use this command to configure the IPv4 address of the default gateway for the Intel Security Controller appliance.

Syntax:

`set network gateway <A.B.C.D>`

Parameter	Description
<A.B.C.D>	a 32-bit address written as four eight-bit numbers separated by periods. A,B,C or D represents an eight-bit number between 0-255.

Example: `set network gateway 10.10.10.8`

Notes:

- To remove the network gateway configuration just enter `set network gateway`. That is, use the command without any IP address.



If you do not configure a default gateway, Intel Security Controller appliance can communicate only with hosts on the same subnet. Even your current SSH session will be closed, unless your client machine is on the same subnet as that of Intel Security Controller.

- You can also configure the gateway IP addresses in the **Network Settings** page of Intel Security Controller web application. The default gateway you configure using the `set network gateway` command reflects in the **Network Settings** page.

set network hostname

Use this command to configure a network name for the Intel Security Controller appliance. If this name is resolvable to the IP address of Intel Security Controller appliance, you can use this host name to use the Intel Security Controller web application instead of the IP address.

Syntax: `set network hostname <WORD>`

Parameter	Description
<WORD>	indicates a case-sensitive character string up to 25 characters. The string can include hyphens, underscores, and periods, and must begin with a letter.

Example: `set network hostname SanJose_ISC`

The host name of Intel Security Controller is displayed in the **Summary** page of Intel Security Controller web application.

set network ip

Use this to reconfigure a static or dynamic IPv4 address for the Intel Security Controller appliance. If it is a static IP address, you must specify the CIDR notation as well.

Syntax: `set network ip <A.B.C.D/CIDR> | dhcp`

Parameter	Description
<A.B.C.D/CIDR>	Indicates an IPv4 address followed by the CIDR notation to specify the network part and the host part. For example, the CIDR notation for a Class C address is 24.
dhcp	Indicates that the network settings must be configured through a DHCP server.

Example: `set network ip 10.10.10.10/24`

Notes:

- The configured IP address is displayed in the **Summary** page of Intel Security Controller web application.
- You can also configure the IP address from the **Network Settings** page of Intel Security Controller web application.

set network ntp

Use this to configure Network Time Protocol (NTP) servers as the time source for the Intel Security Controller appliance. You can specify the IPv4 addresses or host names of the NTP servers separated by a space. Intel Security Controller appliance considers the first available NTP server from your list.



If you specify the host name of NTP servers, you must configure a name server for Intel Security Controller appliance to resolve the host name.

Syntax: `set network ntp <A.B.C.D or host name> <E.F.G.H or host name>
<W.X.Y.Z or host name>`

Parameter	Description
<A.B.C.D or host name>	The IPv4 address or name of the first priority NTP server.
<E.F.G.H or host name>	The IPv4 address or name of the second priority NTP server.
<W.X.Y.Z or host name>	The IPv4 address or name of the nth priority NTP server.

Example: `set network ntp 50.97.210.169 50.97.210.169 50.97.210.169`

To view the currently configured NTP server details, use `show network ntp` command.

set passwd

Changes the log-on password for the Intel Security Controller appliance. It prompts for the old password and then prompts for a new password. A password must contain at least eight characters and can consist of any alphanumeric character or symbol.

This command has no parameters.

Syntax: `set passwd`

set time

Use this command to set the date and time on Intel Security Controller appliance.

Syntax: `set time MMDDmmhhCCCC`



All parameters are mandatory.

Parameter	Description
MM	The month in numbers.
DD	The date.
mm	Minutes
hh	Hour
CCCC	Year

Example: `set time 013006302014`

This sets the time to Thursday, January 30, 06:30:00 2014

You can use the `show clock` command or the **Summary** page to check the current date and time on Intel Security Controller.

set timezone

Use this command to set the time zone on the Intel Security Controller appliance.

To set the time zone, complete the following:

- 1 Enter `set timezone`. The continents and oceans are listed.
- 2 Enter the number corresponding to the continent or ocean. For example, to set the time zone to Pacific time, enter 10. The countries corresponding to the continent or ocean are listed.
- 3 Enter the number corresponding to the country you want to select. For example, to set the time zone to Pacific time, enter 25. The time zones applicable to the selected country are listed.
- 4 Enter the number corresponding to the time zone you want to select. For example, select 21 to set to Pacific time.
- 5 Press 1 to confirm or 2 to cancel the operation.

You can use `show clock` command or the **Summary** page to check the current time zone on Intel Security Controller.

show arp

Displays the current Address Resolution Protocol (ARP) entries on the Intel Security Controller appliance.

This command has no parameters.

Syntax: `show arp`

show clock

Displays the current date, time, and time zone configured on Intel Security Controller appliance.

This command has no parameters.

Syntax: `show clock`

show filesystems

Displays the filesystems in Intel Security Controller appliance.

This command has no parameters.

Syntax: `show filesystems`

This command displays the following information:

- File system name
- Space allocated
- Space used currently
- Available space
- Space used in percentage
- Where the file system is mounted

show log

Displays the Intel Security Controller log files.

This command has no parameters.

Syntax: `show log`

show log follow

Follow Intel Security Controller logs.

This command has no parameters.

Syntax: `show log follow`

show log last

Use this to view the last n log entries

Syntax: `show log last <number>`

Example: `show log last 5`

Displays the last 5 log entries.

show log reverse

Use this to view the log entries in the reverse chronological order. That is, the latest log entry is displayed first.

Syntax: `show log reverse`

This command has no parameters.

show network dns

Displays the IP addresses of the currently configured name servers

Syntax: `show network dns`

Notes:

- The **Network Settings** page also displays the name servers.
- To configure the name servers, use the `set network dns` command or the **Network Settings** page.

show network domain

Displays the network domain to which you have added Intel Security Controller.

Syntax: `show network domain`

If no result is displayed, it means Intel Security Controller is not part of any domain.

show network hostname

Displays the network name for the Intel Security Controller appliance.

Syntax: `show network hostname`

The host name of Intel Security Controller is also displayed in the **Summary** page of Intel Security Controller web application.

show network ip

Displays the IP address of the Intel Security Controller appliance.

Syntax: `show network ip`

You can also view the IP address in the **Summary** and **Network Settings** pages of Intel Security Controller web application.

show network ntp

Displays the IP addresses or the host names of the Network Time Protocol (NTP) servers configured for the Intel Security Controller appliance.

Syntax: `show network ntp`

To configure NTP server details, use `set network ntp` command.

show network route

Displays the routes configured on the Intel Security Controller appliance.

Syntax: `show network route`

show process

Displays the current system processes running on the Intel Security Controller appliance.

Syntax: `show process`

show process monitor

Use this command to monitor the system running on Intel Security Controller.

Syntax: `show process monitor`

show system memory

Displays the current memory usage on Intel Security Controller.

Syntax: `show system memory`

show system uptime

Displays how long the Intel Security Controller has been up since the last restart, the number of users logged on, and the average load.

Syntax: `show system uptime`

show version

Displays the software version of Intel Security Controller virtual appliance.

Syntax: `show version`

shutdown

Halts the Intel Security Controller appliance and powers it off.

This command has no parameters.

Syntax: `shutdown`



This command immediately shuts down the Intel Security Controller appliance upon execution; you are not required to confirm before it is shut down. You can restart Intel Security Controller appliance from the vSphere Web Client.

traceroute

Displays the traceroute to host.

Syntax: traceroute

traceroute6

Displays the traceroute to host.

Syntax: traceroute6

6

Deploying a security service function to virtual networks

Intel Security Controller currently supports next-generation IPS and next-generation firewall services to be deployed on virtual networks. When you deploy any of these security services, traffic from and to the protected VMs is subject to inspection that corresponds to each service. If a VM is the source of malicious traffic, these services are equipped to take configured response actions.

You have the option to deploy security services to virtual environments deployed on VMware and OpenStack. For a list of versions of each environment supported, refer [Requirements for Intel Security Controller](#) on page 13.

One security service function is installed per host or can be shared across hosts depending on your configuration and your virtual environment. The security manager that you specified in the **Manager Connector** page manages each of these virtual security service appliances. Although these virtual security service appliances are configured similarly, they function independently. For example, Virtual IPS Sensors provide IPS to their respective ESXi hosts but implement the same IPS policies, advanced firewall policies, and other IPS configuration.

To deploy security service functions, Intel Security Controller integrates with NSX. Integration even ensures that relevant traffic is routed through the virtual security service appliance for inspection.

The IPS service, for instance, makes all relevant next-generation IPS features available to your dynamic virtual networks. Deploying the security service is non-intrusive and non-disruptive even though corresponding virtual security service appliances are deployed inline. Scaling up or modifying your virtual networks does not warrant any user-intervention. Also, any change to the security service function configuration is automatically applied to all individual appliances. Intel Security Controller does not take any action directly but orchestrates the actions through its integration with ESX, vCenter, the security service manager, and the virtual security service appliances.

Contents

- *High-level steps to implement a security service*
- *Define an IP address pool for virtual security appliances*
- *Deploy virtual systems*
- *Create a security group in VMware NSX*
- *Create a security policy in VMware NSX*
- *Apply a security policy to a security group in VMware NSX*
- *Configure Virtual Security System to fail-close or fail-open*
- *Assign policy groups to virtual security systems*
- *Quarantine endpoints using NSX features*

High-level steps to implement a security service

Any security service through Intel Security Controller is a collaboration between vCenter, NSX, the security service manager, and the virtual security service appliances that orchestrated by Intel Security Controller. To illustrate what this means, consider an SDDC as shown here. Assume that you want to provide a security service such as IPS or firewall to VMs 1 through 4. vCenter and NSX are up and running on ESXi-3.

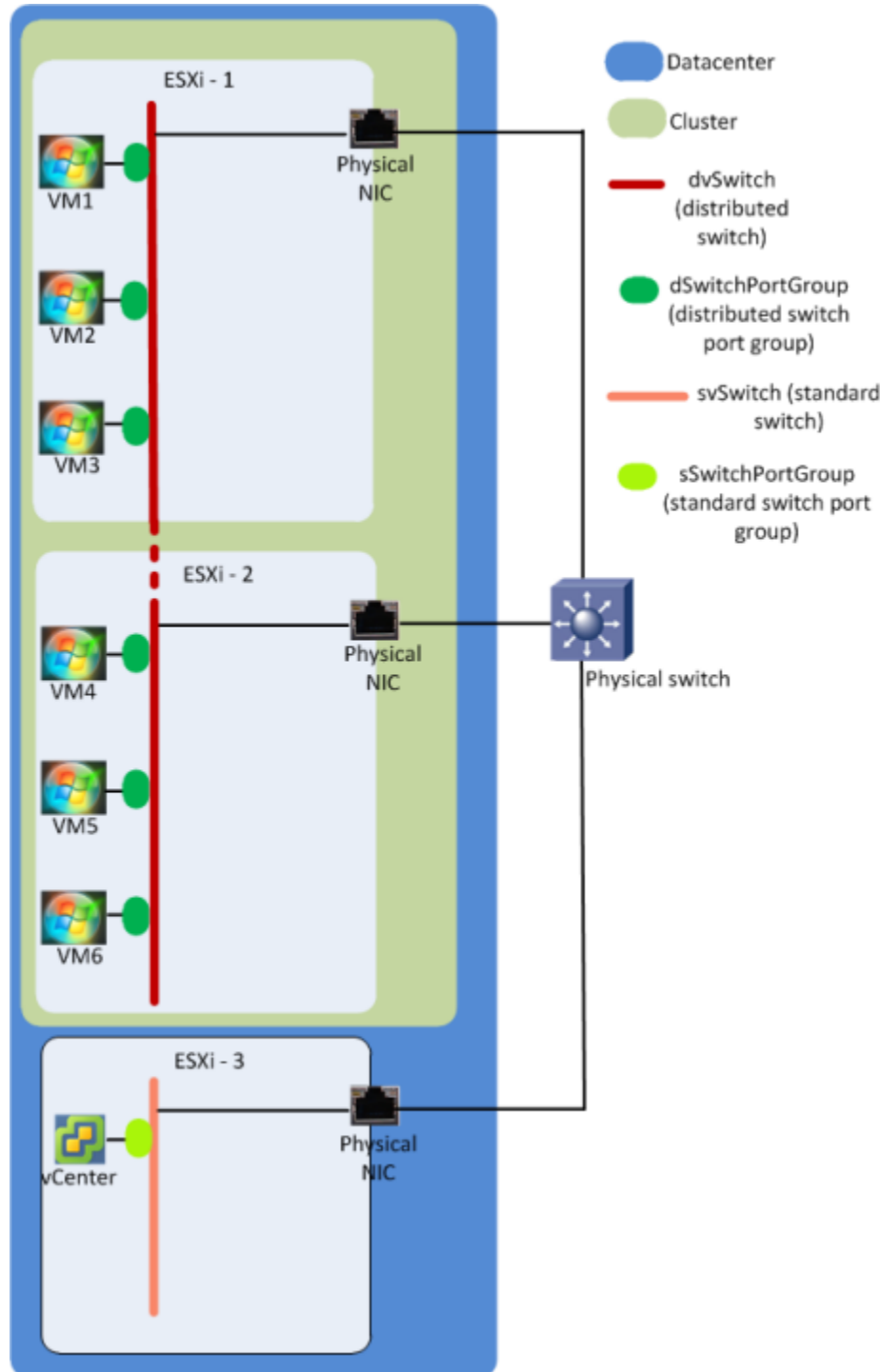


Figure 6-1 An example SDDC

The following are the high-level steps for configuring the security service using Intel Security Controller. There are multiple orders by which you can complete this configuration. The steps provided here are in the recommended order.

- 1 When you deploy the security service to a cluster, Intel Security Controller collaborates with NSX to install a virtual security service appliance in each host of that cluster. Each of these virtual security service appliances needs a management port IP address. In this example, there are two hosts in the cluster which means that you need two IP addresses for the management ports of these appliances.

You define a pool of IP addresses in the NSX Manager. For each IP address pool, you also define the required network details such as the default gateway and DNS server IP addresses.

The number of IP addresses in an IP address pool depends on the number of ESXi hosts that you plan to include in the corresponding cluster. You must also factor in the ESXi hosts that you might add to the cluster in future. When you add ESXi hosts to the cluster after deploying a security service, NSX automatically installs an instance of the virtual security service appliance in those ESXi hosts. NSX needs an IP address to assign to these virtual appliances. Consider that the cluster for which you plan to provide the security service currently has two ESXi hosts. However, you plan to include 5 more ESXi hosts later on. Though two IP addresses are currently sufficient, you need 5 more for the ESXi hosts that you plan to add.

- 2 Complete the following configuration in Intel Security Controller.
 - a Create a virtualization connector by providing the IP address and logon credentials for NSX and vCenter. You can create as many virtualization connectors as you require. For example, you want to provide the same security service to multiple clusters managed by different vCenters. Then create virtualization connector for each vCenter. The same security policies are applied to all hosts in all these clusters when you implement the security service.

In this example, one virtualization connector is sufficient since there is only one cluster managed by one vCenter. See [Define virtualization connectors](#) on page 40.
 - b Create a manager connector by providing its IP address and admin logon credentials. See [Define manager connectors](#) on page 48.
 - c Define the virtual security service appliance in Intel Security Controller and import the required security service function images into Intel Security Controller. See [Change the software version of security appliances](#) on page 54.
 - d Create a distributed appliance using the virtualization connectors, manager connector, and the required virtual security service image from the previous 3 steps. When you associate a virtualization connector with a security manager domain, a Virtualization System is created in Intel Security Controller. See [Manage distributed appliances](#).
 - e Deploy the Virtualization Systems that you created in the previous step in the relevant clusters. If there are multiple clusters that you want to protect, you must deploy the Virtualization System separately for each cluster. Then, Intel Security Controller collaborates with the corresponding vCenter and NSX to deploy Virtual Sensors in each ESXi host in the specified cluster. See [Deploy virtual systems](#) on page 108.

- 3 Complete the following configuration in NSX using vCenter web client.
 - a NSX needs to know the IP addresses of the VMs to be protected for it to route the traffic for the network introspection service (that is, to the Virtual Security System instances). For NSX to know the IP addresses, VMware tools must be running on the VMs. If VMware tools is not running, you must include the IP addresses of such VMs in a security group. Before you create the security group, create an IP set object containing the IP addresses of VMs on which VMware tools is not running. See [GroupObjectsBasedOnIPsets](#).
 - b In the **Networking & Security** tab of vCenter, create a security group and add the VMs that you want to protect. In our example, you include VMs 1 through 4 in the security group. See [Create a security group in VMware NSX](#) on page 113.
 - c Create a security policy and in the **Network Introspection Services** step, select the corresponding distributed appliance and the security service policy for both inbound and outbound traffic. The distributed appliances are listed as **Service Name** and the security service policies are listed as **Profiles** in vCenter. See [Create a security policy in VMware NSX](#) on page 116.

Apply the security policy that you created in the previous to the policy group created in step 1. See [Apply a security policy to a security group in VMware NSX](#) on page 120.
- 4 Complete the following in the security service manager.
 - a Log on to the security service manager and verify whether the Virtual Security System is listed in the appropriate device list.
 - b Check the status of the Virtual Security System in the security service manager. Also, in case of IPS, verify whether a signature set is present. If not, take appropriate measures to provide one. For example, in Network Security Platform, you must deploy pending changes to the Virtual Security System from the Devices tab. The pending changes are automatically updated to all individual Virtual IPS Sensors of that Virtual Security System.
 - c If necessary, log on to the CLI of the virtual security service appliance and view the configuration.
- 5 To verify successful deployment, send sample attack traffic from one of the protected VMs and check if an alert is displayed in the security service manager.
- 6 By default, Virtual Security System instances are deployed in fail-open mode. You can configure a Virtual Security System to fail-close if necessary. See [Configure Virtual Security System to fail-close or fail-open](#) on page 123.

Define an IP address pool for virtual security appliances

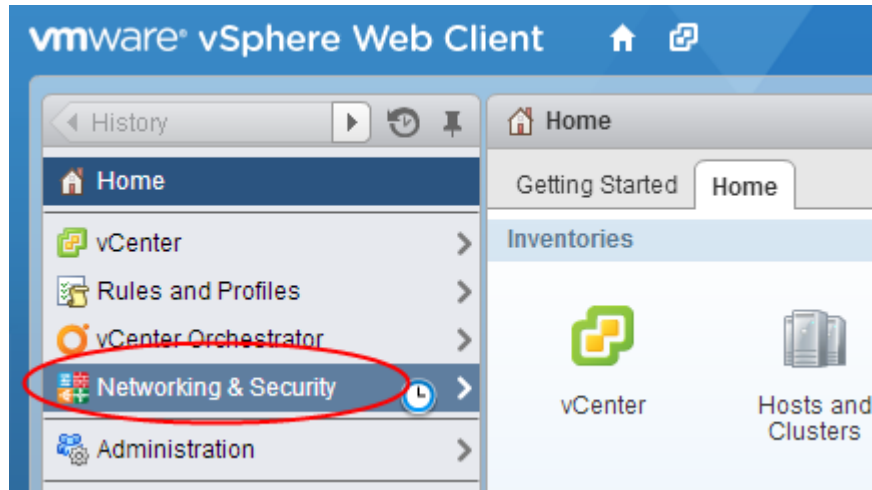
If you have installed NSX, you can define the IP pool for the virtual security appliances. Along with the IP addresses, you also define other network settings such as the default gateway IP address and the subnet mask.



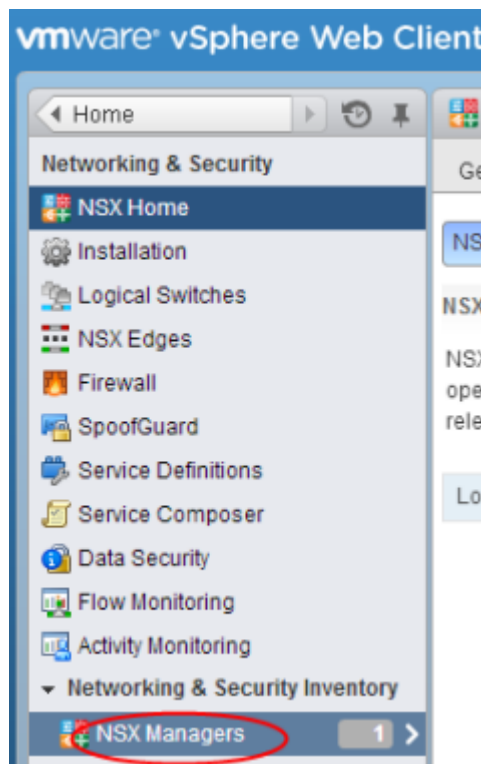
Currently, Intel Security Controller supports only IPv4 addresses. So, the IP pool must contain IPv4 addresses only.

Task

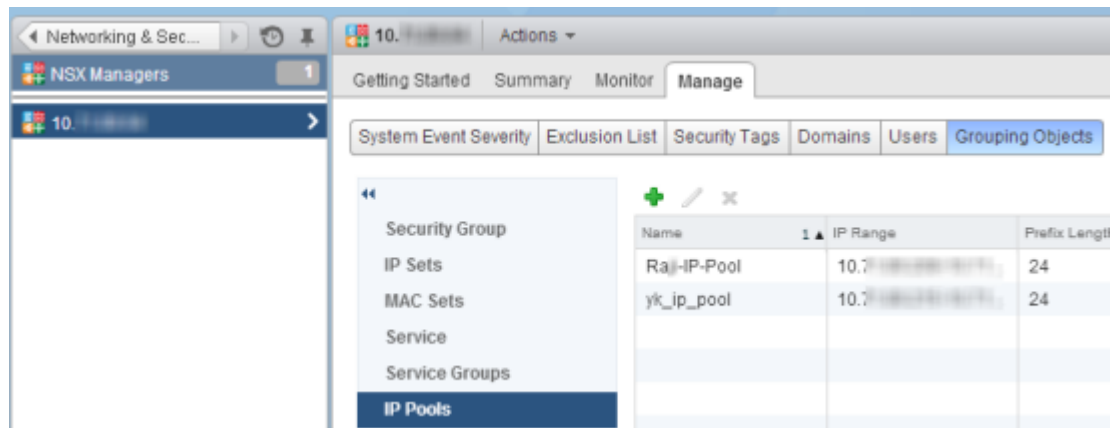
- 1 Log on to vSphere Web Client as the root user.
- 2 In the vSphere **Home** tab, select **Networking & Security**.



- 3 Select **Networking & Security Inventory | NSX Managers**.



- 4 Select the NSX Manager in which you want to define the IP pool and then select **Manage | Grouping Objects | IP Pools..**






- 5 Click  to add an IP pool.
- 6 In the Add IP Pool window, enter the details and click **OK**.

Table 6-1 Option definitions

Option	Definition
Name	Enter a relevant name for the IP pool.
Gateway	Enter the IP address of the default gateway for the IP addresses.  After you create the IP pool, you cannot modify the default gateway IP address.
Prefix Length	Enter the network prefix length of the IP addresses.
Primary DNS	Enter the IP address of the primary or the preferred DNS server for the IP addresses.
Secondary DNS	Optionally, enter the IP address of the secondary DNS server.
Static IP Pool	Enter the range of valid IPv4 addresses. Make sure there is no IP address clash. That is, the IP addresses in the IP pool must not have been assigned to a network object or already included in a different IP pool.
OK	Click to save the settings and create the IP pool.
Cancel	Click to close the dialog box without saving the changes.

 Add IP Pool

Name: * VSensors_Engineering

Gateway: * 10.71.88.212
A gateway can be any IPv4 or IPv6 address.

Prefix Length: * 24

Primary DNS: 10.44.85.134

Secondary DNS:

DNS Suffix:

Static IP Pool: * 10.71.88.215-10.71.88.219
A static IP pool can be specified as a list of comma-separated IP address ranges, for example 192.168.1.2-192.168.1.100 or abcd:87:87::10-abcd:87:87::20.

OK

Cancel



The summary view displays the count of IP addresses in an IP pool and the count of addresses in use.

Grouping Objects					
Name	IP Range	Prefix Length	Gateway	Used / Total	
Raj-IP-Pool	10.1.1.1/24	24	10.1.1.1	1/5	
yk_ip_pool	10.1.1.1/24	24	10.1.1.1	1/5	

Deploy virtual systems

Before you begin

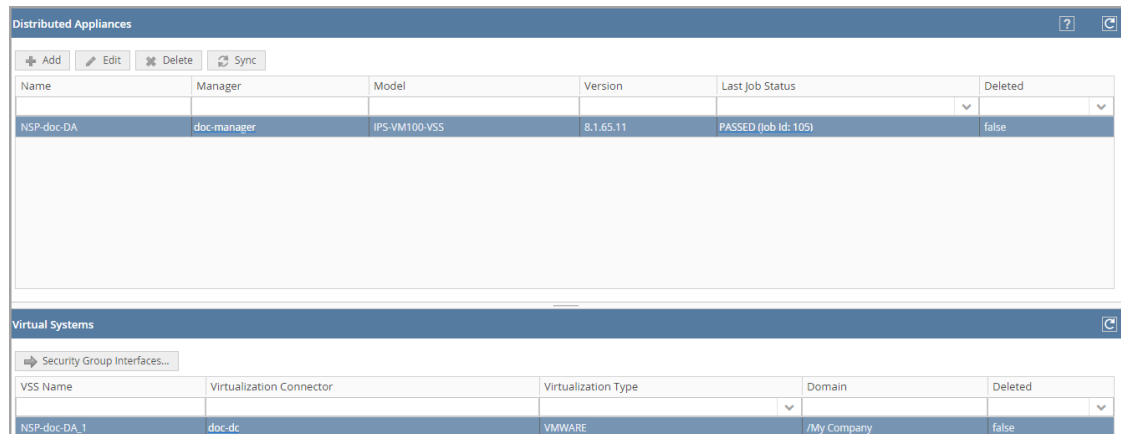
- You have created the distributed appliance successfully.
- VMware vCenter, NSX Manager, and the security manager are all up and can be reached by Intel Security Controller.
- If the cluster contains more than one ESXi host, you must set up an NFS datastore to deploy the virtual systems. In case of clusters with more than one ESXi host, virtual security service appliances are installed only in NFS datastores. If a cluster contains only one ESXi host, a VMFS datastore will suffice.
- You have prepared the ESXi hosts in the cluster for NSX. See [Prepare an ESXi host for NSX](#).
- You have created a distributed switch port group for the virtual security service appliance management ports. Through this switch port group, the virtual security service appliance must be able to communicate with the security manager, Intel Security Controller, NSX, and vCenter Server. See [Create a distributed switch port group](#).
- You have created the IP address pool to assign IP addresses for the virtual security service appliance management ports. See [Define an IP address pool for virtual security appliances](#) on page 104.

When you create a distributed appliance, a virtual system (virtual security system) record is automatically created. The virtual security system is visible in the security service manager, in Intel Security Controller, and in NSX as a security service. You can then deploy the virtual system as a security service from NSX.

When you deploy a virtual system, Intel Security Controller collaborates with vCenter, NSX, and the security manager to deploy the virtual security appliance in all hosts (hypervisors). In the case of IPS service, for example, NSX installs a virtual security system instance (a virtual IPS Sensor) in each ESXi host of the cluster. These virtual security system instances are automatically assigned network details and have established trust with the security manager.

Task

- 1 In the Intel Security Controller web application, select **Setup | Distributed Appliances**.
The **Distributed Appliances** page displays the currently available distributed appliances.

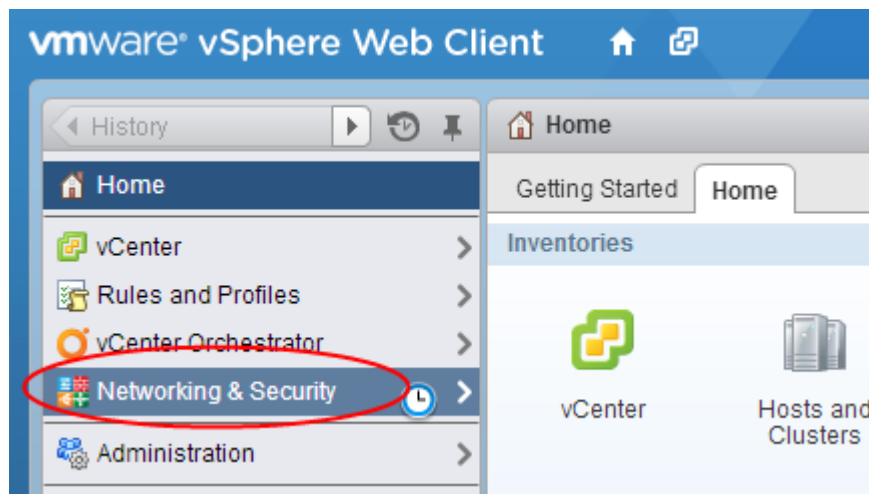


Name	Manager	Model	Version	Last Job Status	Deleted
NSP-doc-DA	doc-manager	IPS-VM100-VSS	8.1.65.11	PASSED (Job Id: 105)	false

VSS Name	Virtualization Connector	Virtualization Type	Domain	Deleted
NSP-doc-DA_1	doc-dc	VMWARE	/My Company	false

Figure 6-3 Distributed Appliances page

- 2 Select the required distributed appliance you created and ensure the following.
 - The **Last Job Status** shows *Passed*.
 - The virtual system is created and listed in the **Virtual Systems** section of the page.
- 3 In the security manager, make sure that the virtual system is automatically added.
- 4 Log on to vSphere Web Client as the root user.
- 5 In the vSphere **Home** tab, select **Networking & Security | Installation | Service Deployments**.



- 6 From the **NSX Manager** list, select the required NSX Manager.
- 7 Click **+** to create a service deployment.
The **Deploy Network & Security Services** wizard opens.

- 8 In the **Select services & schedule** step, select the service named after the distributed appliance you created.

For example, if the distributed appliance you created is *DA_N_America*, the corresponding service is *Intel IPS DA_N_America*.

Deploy Network & Security Services

1 Select services & schedule

2 Select clusters
3 Select storage
4 Configure management network
5 Ready to complete

Select services & schedule
Select one or more Network & Security services to deploy. You can also specify a schedule for deployment.

Select services:

	Name	Description
<input type="checkbox"/>	VMware Data Security	Discovery of sensitive data
<input checked="" type="checkbox"/>	Intel IPS DA_N_America	Intel Security Controller
<input type="checkbox"/>	VMware Endpoint	Base service for all solutions
<input type="checkbox"/>	Intel IPS DANAmerica	Intel Security Controller

- 9 If you want to deploy the virtual system now, select **Deploy now** and then click **Next**. Else, select the date and time for deployment and then click **Next**.
- 10 In the **Select clusters** step, select the required data center and the cluster, for which you want to provide IPS service.

Deploy Network & Security Services

✓ **1 Select services & schedule**
2 Select clusters
3 Select storage
4 Configure management network
5 Ready to complete

Select clusters
Select one or more clusters on which to deploy the service will be upgraded.

Datacenter: * NorthAmericaSDDC_Da... ▼

	Name
<input checked="" type="checkbox"/>	US_Engineering

- 11 In the **Select storage** step, select the required datastore.



If the corresponding cluster contains more than one ESXi host, you must select an NFS datastore.

Name	Datastore
US_Engineering	DatastoreNFS

- 12 In the **Configure management network** page, the record containing the selected service and cluster is displayed. Complete the following in **Configure management network** step.

Name	Cluster	Network	IP assignment
Intel IPS DA_N_America	US_Engineering	dMgmtPort	vSensors_NAmeri...

- From the **Network** drop-down list, select the distributed switch port group which the virtual security service appliances must use for management data. That is, the virtual security service appliance management port uses the switch port group you select here.
 - From the **IP assignment** drop-down list, select the IP address pool which you configured and then click **Next**.
- 13 In the **Ready to complete** step, review the configuration and click **Finish**.
- Depending on the number of ESXi hosts and your network infrastructure, it takes some minutes for the virtual security service appliances to be deployed.

- 14 Make sure that the **Installation Status** shows up as *Succeeded* and **Service Status** shows up as *Up* in the **Installation** page.

Installation

Management

Host Preparation





Logical Network Preparation

Service Deployments

NSX Manager: 10.10.10.10

Network & Security Service Deployments

Network & security services are deployed on a set of clusters. Manage service deployments here by adding new service

Service	Version	Installation Status	Service Status
Intel NG-IPS DA-10.10.10.10	1.20	✓ Succeeded	✓ Up
Intel NG-IPS DA-10.10.10.11	1.20	✓ Succeeded	✗ Down
Intel NG-IPS DA-10.10.10.12	1.20	✓ Succeeded	✓ Up
Intel NG-IPS DA-10.10.10.13	1.20	✗ Failed	Unknown
Intel IPS old	1.00	✗ Failed	✓ Up
Intel NG-IPS DA-10.10.10.14	1.20	✗ Failed	✓ Up
Intel IPS DA	1.00	✓ Succeeded	✓ Up
Intel NG-IPS DA-10.10.10.15	1.20	✓ Succeeded	✓ Up





- 15 In the security manager, deploy all changes to make sure the individual virtual security service appliances are updated.

- 16 Select the virtual system name based on the distributed appliance name and then select the appropriate option to view summary information about it.

Recall that one virtual security service appliance is automatically deployed per ESXi host in the cluster.

- 17 In Intel Security Controller, select **Status | Appliance Instances**.

The deployed virtual security system instances (security appliances) are listed. Make sure the state of **Discovered** and **Inspection-Ready** are *True*.

More Info				
 Agent Status  Sync  Upgrade Agent  Appliance Re-authentication				
NAME	IP-ADDRESS	DISCOVERED	INSPECTION-READY	LAS
da_na_04_1_1	10.213.174.231	true	true	Dec
da_na_04_1_2	10.213.174.232	true	true	Dec

Create a security group in VMware NSX

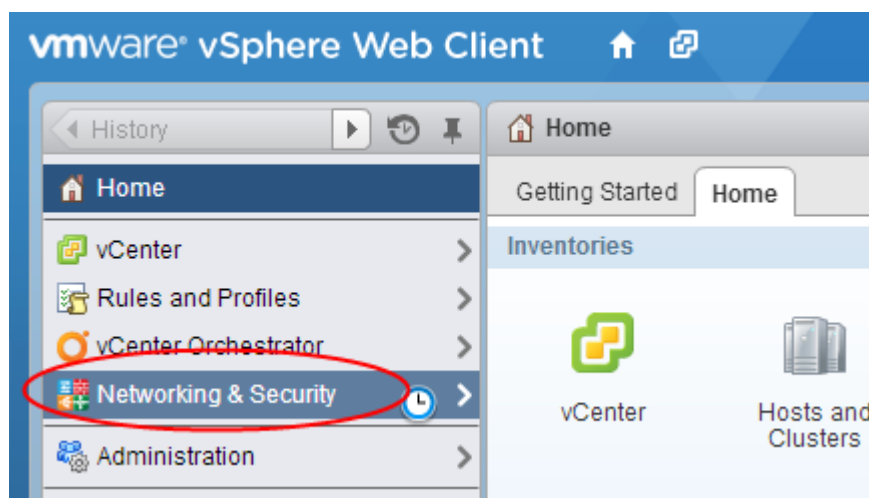
In an NSX Manager, you create a security group and then include the required VMs in that group. Then you can apply an NSX security policy to this security group, the corresponding security service is provided to those VMs included in the security group.



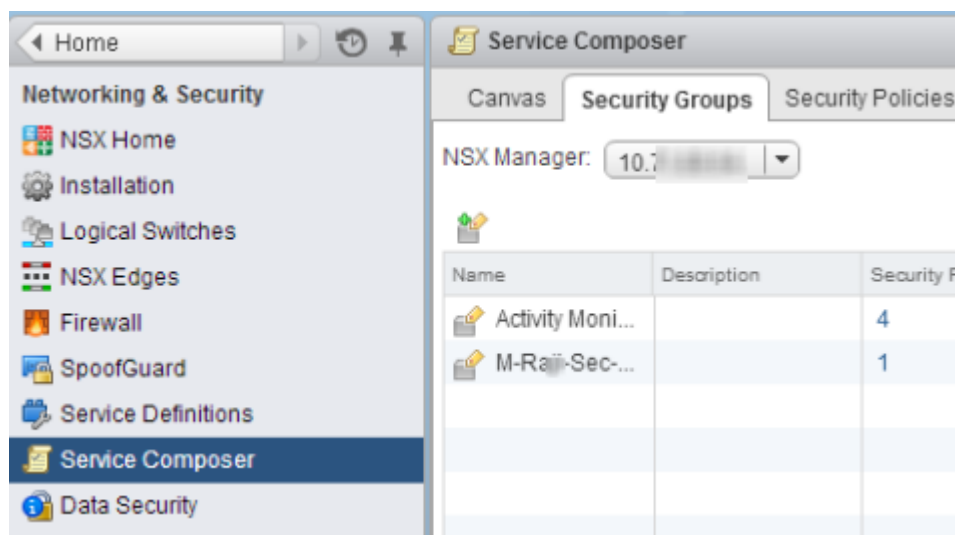
If VMware tools is not running on the VMs, you must include those VMs in the security group and also create an IP set containing the IP addresses of those VMs and include that IP set in the security group. The steps for creating an IP set object is under "[Group objects based on IP sets.](#)"

Task


- 1 Log on to vSphere Web Client as the root user.
- 2 In the vSphere **Home** tab, select **Networking & Security**.

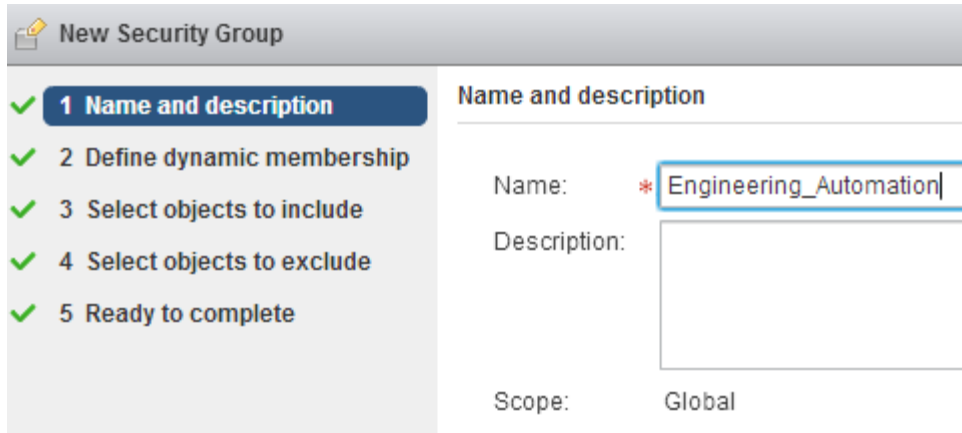


- 3 Select **Service Composer | Security Groups**.



- 4 From the **NSX Manager** list, select the NSX Manager in which you want to define the security group.

- 5 Click  to create a security group.
- 6 In the **New Security Group** wizard, enter a meaningful name and, if required, a description, then click **Next**.



New Security Group

- ✓ 1 **Name and description**
- ✓ 2 Define dynamic membership
- ✓ 3 Select objects to include
- ✓ 4 Select objects to exclude
- ✓ 5 Ready to complete

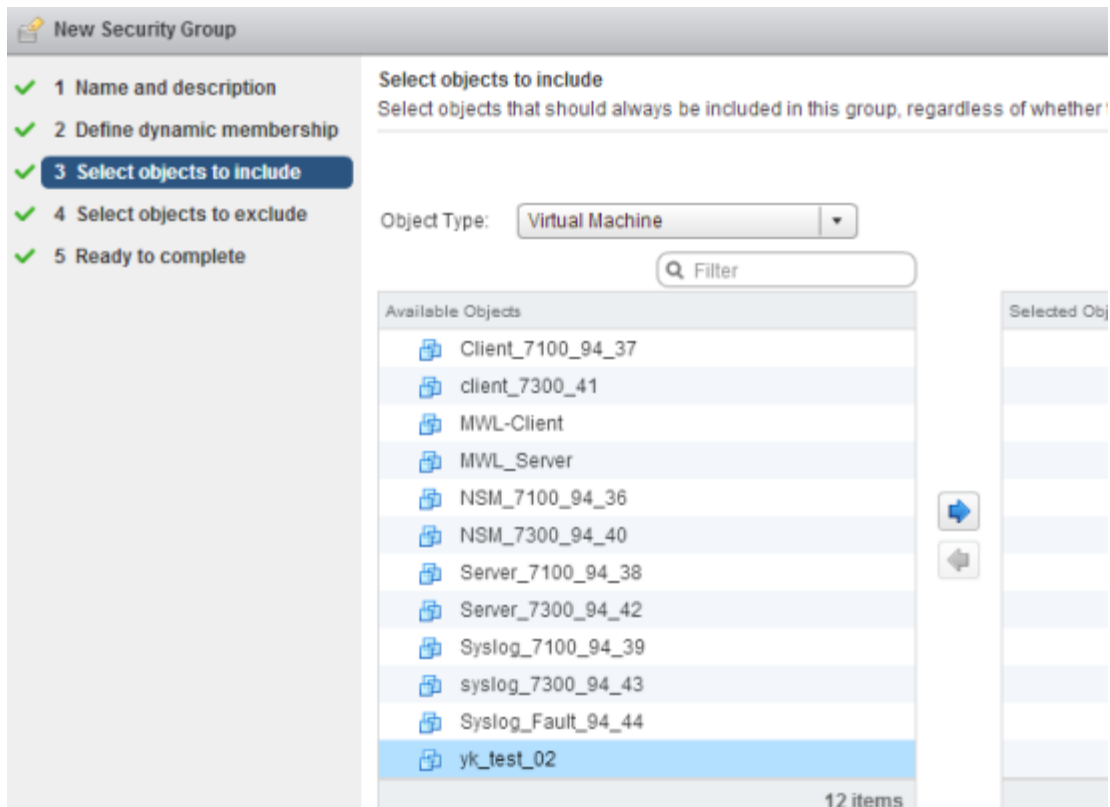
Name and description

Name: *

Description:

Scope: Global

- 7 Select **Select objects to include**.















New Security Group

- ✓ 1 Name and description
- ✓ 2 Define dynamic membership
- ✓ 3 **Select objects to include**
- ✓ 4 Select objects to exclude
- ✓ 5 Ready to complete

Select objects to include
Select objects that should always be included in this group, regardless of whether

Object Type:

Filter

Available Objects	Selected Objects
 Client_7100_94_37	
 client_7300_41	
 MWL-Client	
 MWL_Server	
 NSM_7100_94_36	
 NSM_7300_94_40	
 Server_7100_94_38	
 Server_7300_94_42	
 Syslog_7100_94_39	
 syslog_7300_94_43	
 Syslog_Fault_94_44	
 yk_test_02	


12 items

- 8 From the **Object Type** drop-down list, select the object based on which you want to include VMs.

For example, if you select distributed port group in this list, the distributed port groups currently defined in the data center are listed. When you select a distributed port group, all the VMs connected to this port group are included in the security group.

- You can also base the inclusion on multiple object types. For example, you can select a few distributed switch port groups and some VMs.
- For VMs on which VMware tools is not running, you must include them in the security group. Also, you must create an IP set object and include that IP set in the security group. To include the IP set, select **IP Sets** from the **Object Type** list.

Consider that you selected **Virtual Machine** from the **Object Type** drop-down list.

- 9 Select the required objects (in our example, VMs) and click  to move them under **Selected Objects**. Then click **Next**.
- 10 If you want to exclude any VMs, click **Select objects to exclude** in the **New Security Group** wizard.
This is similar to how you included VMs based on objects. For example, you want to include all the VMs connected to a distributed switch port group except for 5 server VMs. Then, you can include the distributed switch port group in step 3 of **New Security Group** wizard and exclude only those 5 VMs in step 4.
- 11 Click **Ready to complete**, review the objects included and those excluded. Then click **Finish** to create the security group.

The security group you created is listed in the **Security Groups** tab for the corresponding NSX Manager.

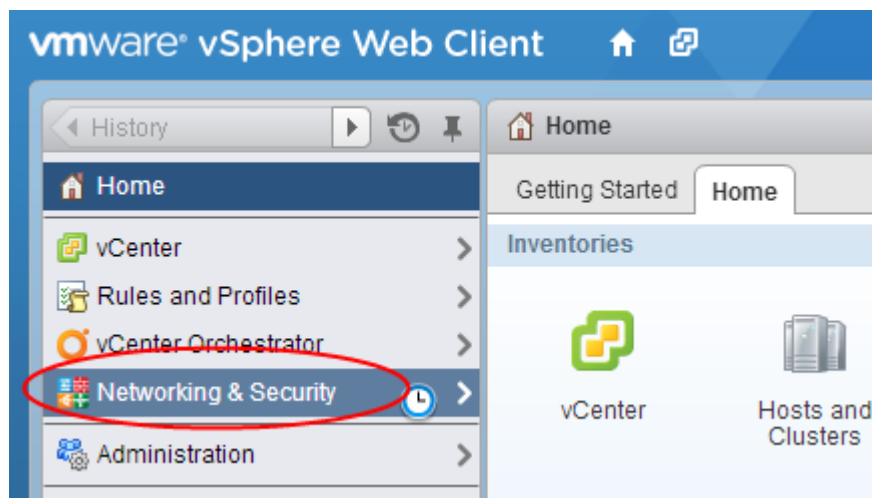
Create a security policy in VMware NSX

In an NSX Manager, you create a security policy, which you can apply to a security group in NSX. This security policy contains the security profile to be applied on the VMs included in that security group.

For example, in the case of IPS service, you select the Network Security Platform policy group as a security profile in a security policy of NSX. Then, when you apply this security policy to a security group, a Virtual Sensor uses this Network Security Platform policy group to inspect traffic related to the protected VMs.

Task


- 1 Log on to vSphere Web Client as the root user.
- 2 In the vSphere **Home** tab, select **Networking & Security**.

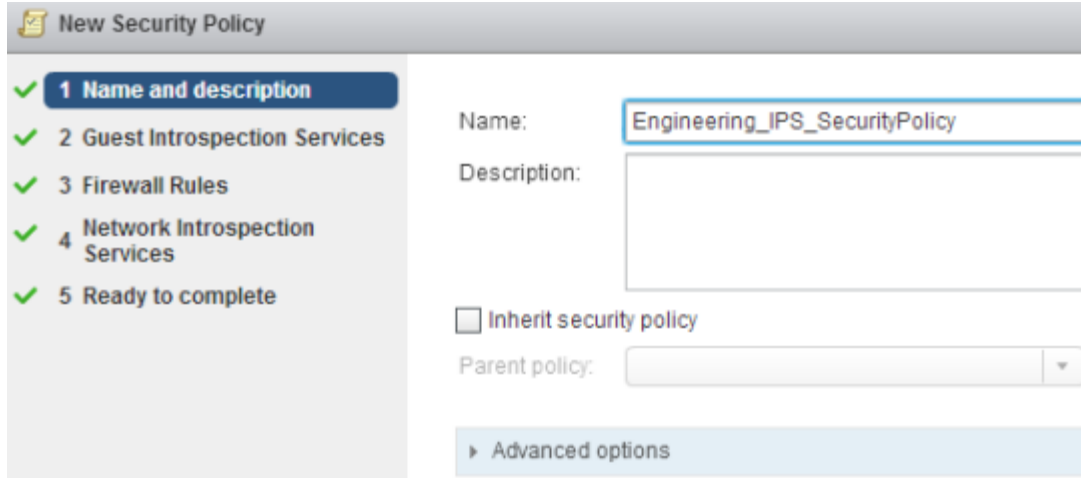



- 3 Select **Service Composer | Security Policies**.



- 4 From the **NSX Manager** list, select the NSX Manager in which you want to define the security policy.

- 5 Click  to create a security policy.
- 6 In the **New Security Policy** wizard, enter a meaningful name and, if required, a description and click **Next**.

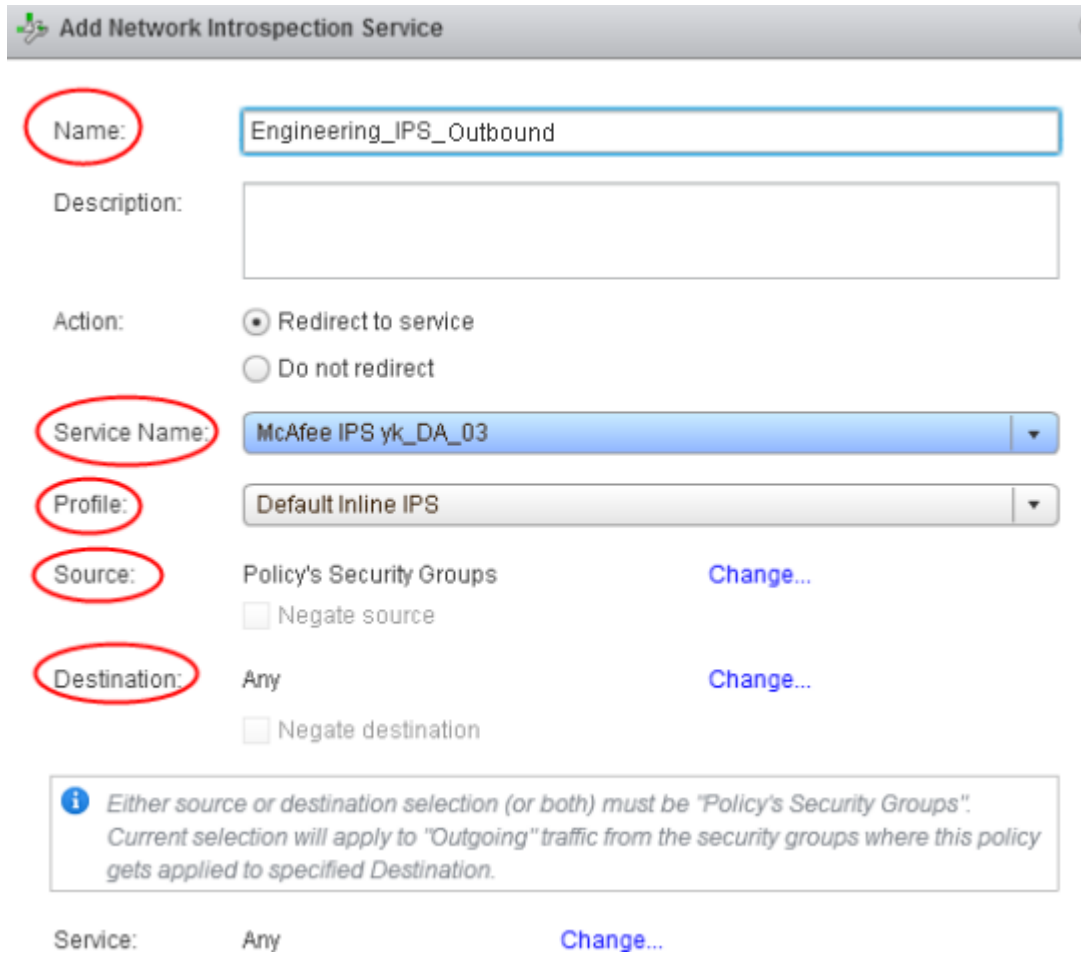


- 7 Select **Network Introspection Services** and click  to add a network introspection service.
All products that currently integrate with Intel Security Controller are network introspection services.



For the security services to work as expected, you must add two network introspection services. One introspection service is for inbound traffic to the security group. The second one is for the outbound traffic from the security group.

- 8 In the **Add Network Introspection Service** dialog, enter the required options and click **OK**.



Add Network Introspection Service

Name: Engineering_IPS_Outbound

Description:

Action: ☒ Redirect to service
☐ Do not redirect

Service Name: McAfee IPS yk_DA_03

Profile: Default Inline IPS

Source: Policy's Security Groups [Change...](#)
☐ Negate source

Destination: Any [Change...](#)
☐ Negate destination

Service: Any [Change...](#)

Information: Either source or destination selection (or both) must be "Policy's Security Groups". Current selection will apply to "Outgoing" traffic from the security groups where this policy gets applied to specified Destination.

Table 6-2 Option definitions

Option	Definition
Name	Enter a relevant name for the inbound or outbound security service. Consider you are adding the outbound first.
Service Name	This is the list of relevant distributed appliances defined in Intel Security Controller. In a distributed appliance, specify the virtualization connector which, in turn, contains the NSX Manager IP address. The Service Name list contains the distributed appliances in which the current NSX Manager is referenced.
Profile	This is the list of security policies defined in the security service manager. In a distributed appliance, specify the security manager. Based on the Service Name (distributed appliance) you selected, the security policies are displayed here.
Source	Click Change... and select Policy's Security Groups because this security service is for outbound traffic from the security group. Click OK .
Destination	Click Change... and select Any because this security service is meant for outbound traffic from the security group. Click OK .
OK	Click OK to create the outbound security service.
Cancel	Click to close the dialog box without saving the changes.

- 9 Follow a similar procedure to create the inbound security service.
 - You can opt for the same **Profile** or choose another.
 - You must select **Any** for **Source** and **Policy's Security Groups** for **Destination**.

Add Network Introspection Service

Name:

Description:

Action: ☒ Redirect to service
☐ Do not redirect

Service Name:

Profile:

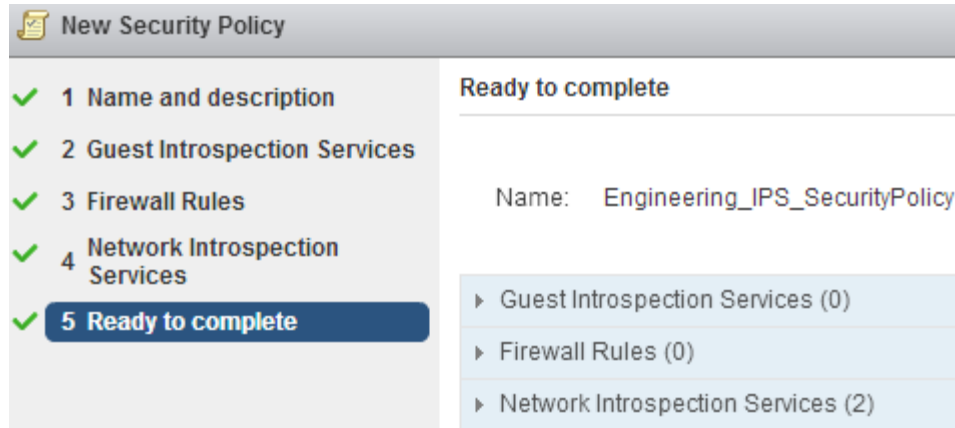
Source: Any [Change...](#)
☐ Negate source

Destination: Policy's Security Groups [Change...](#)
☐ Negate destination

i Either source or destination selection (or both) must be "Policy's Security Groups". Current selection will apply to "Incoming" traffic from specified Source to the security groups where this policy gets applied.

Service: Any [Change...](#)

- 10 Select **Ready to complete**, review the configuration, and click **Finish** to create the security policy.



New Security Policy

- ✓ 1 Name and description
- ✓ 2 Guest Introspection Services
- ✓ 3 Firewall Rules
- ✓ 4 Network Introspection Services
- ✓ 5 Ready to complete

Ready to complete

Name: Engineering_IPS_SecurityPolicy

- ▶ Guest Introspection Services (0)
- ▶ Firewall Rules (0)
- ▶ Network Introspection Services (2)

The security policy you created is listed in the **Security Policies** tab for the corresponding NSX Manager.

Apply a security policy to a security group in VMware NSX

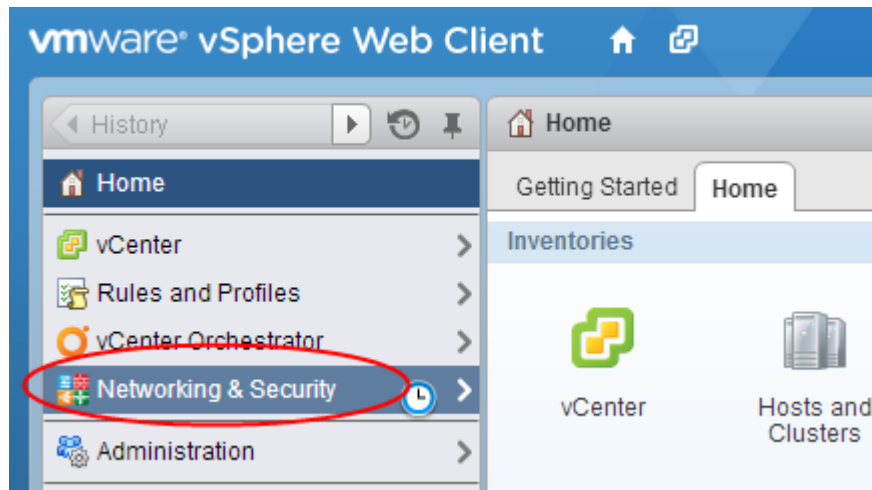
Before you begin

Make sure you have created the required security groups and the security policies in the NSX Manager.

In an NSX Manager, you create a security policy, which you can apply to a security group. This creates the association between security groups and security policies.

Task


- 1 Log on to vSphere Web Client as the root user.
- 2 In the vSphere **Home** tab, select **Networking & Security**.



- 3 Select **Service Composer | Security Policies**.

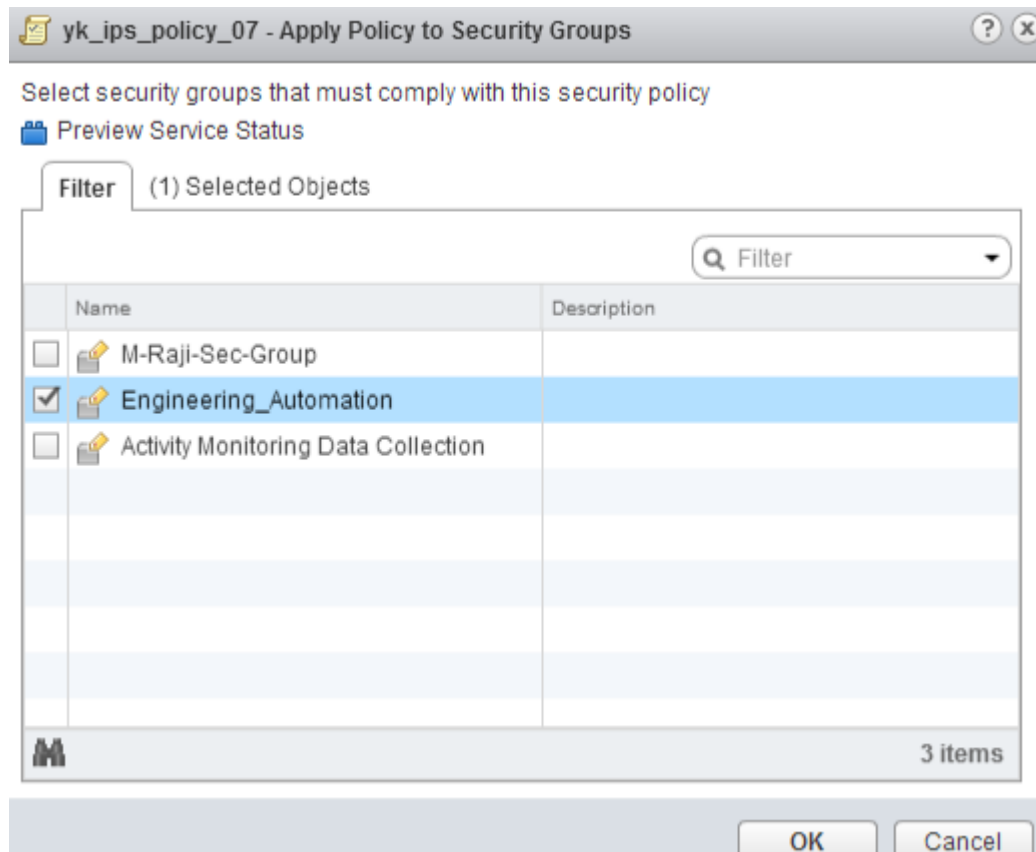


- 4 From the **NSX Manager** list, select the corresponding NSX Manager.

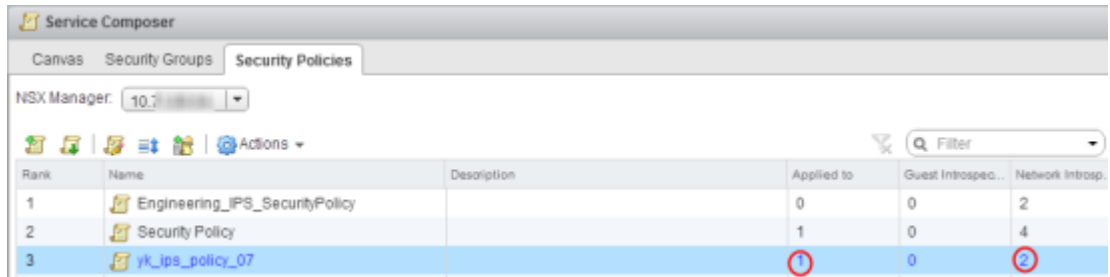
- 5 Select the security policy you want to apply and click 



- 6 Select the security groups on which you want to apply the security policy and click **OK**.



You can view the details in the **Security Policies** tab.



Rank	Name	Description	Applied to	Guest Introspec...	Network Introspec...
1	Engineering_IPS_SecurityPolicy		0	0	2
2	Security Policy		1	0	4
3	yk_ips_policy_07		1	0	2

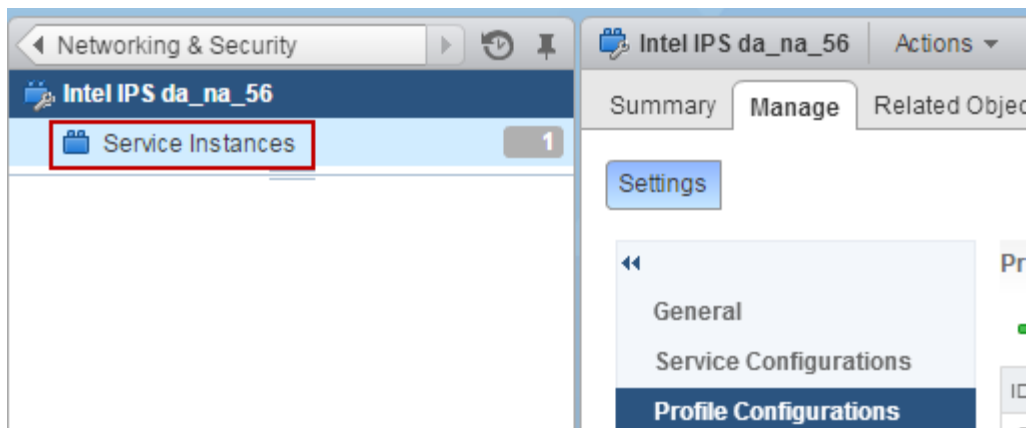
Configure Virtual Security System to fail-close or fail-open

When you successfully install the security service, the Virtual Security System instances are deployed in fail-open mode by default. You can configure the Virtual Security System instances to run in fail-close or fail-open mode. Similar to any other configuration, the fail-close or fail-open setting of a Virtual Security System applies to all its instances.

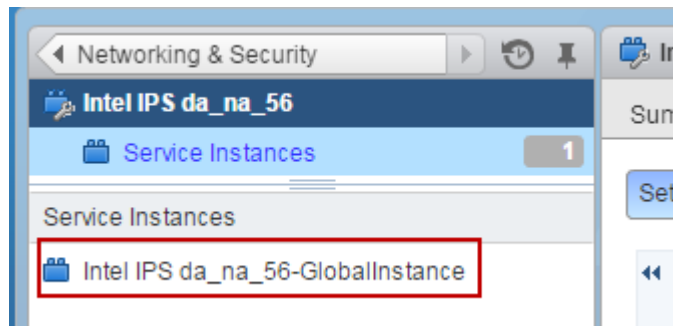
The fail-open or fail-close configuration is implemented through an NSX mechanism. The solution uses an attribute in the service definitions of NSX to implement fail-open or fail-close configuration.

Task

- 1 In the vSphere Home tab, select **Networking & Security | Service Definitions**.
- 2 Select the corresponding service definition and click the edit icon.
You can identify the service definition by the name of the distributed appliance.
- 3 Select **Service Instances**.



- 4 Select the instance, which is displayed.



The corresponding service profiles are listed on the right side.

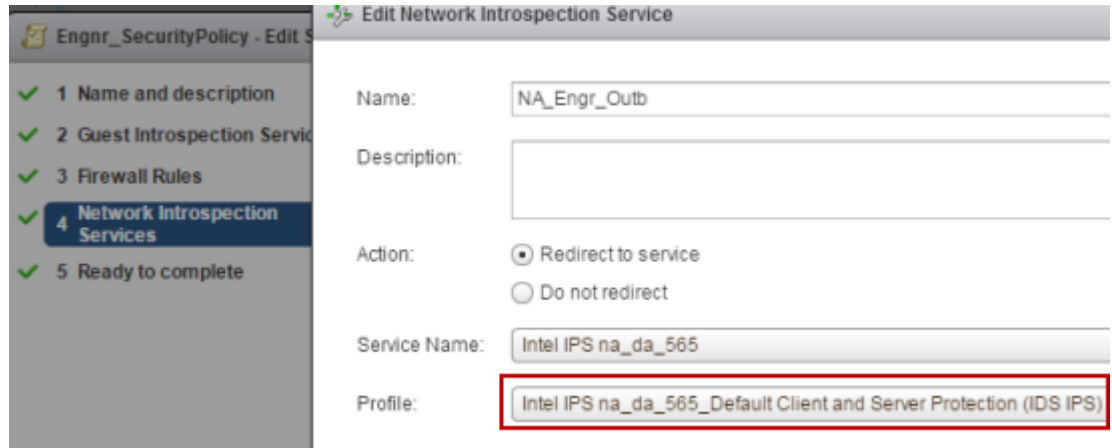
Service Profiles

+ | 📄 ✖ | ⚙ Actions ▼

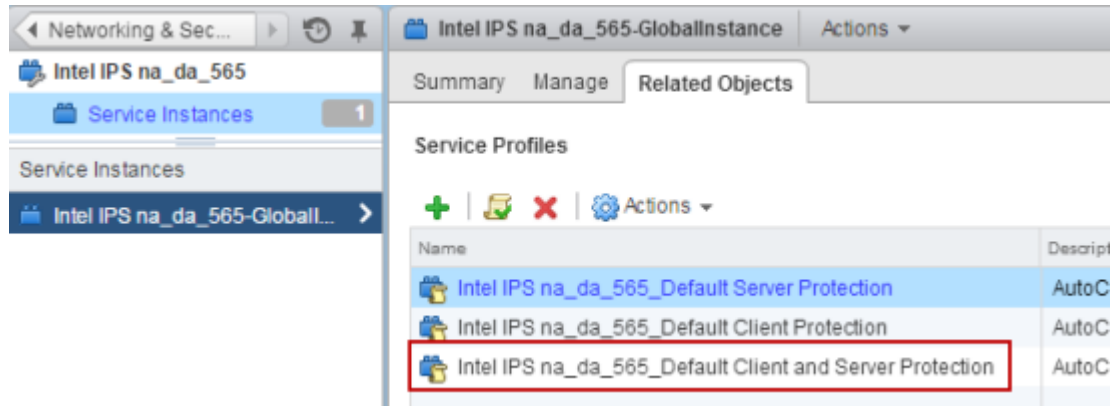
Name	Description
Intel IPS da_na_56_Default ...	AutoCreated Default Ser
Intel IPS da_na_56_Default ...	AutoCreated Default Ser
Intel IPS da_na_56_Default ...	AutoCreated Default Ser

- 5 Double-click on the service profile, which you have used in the network introspection service of the applied security policy.

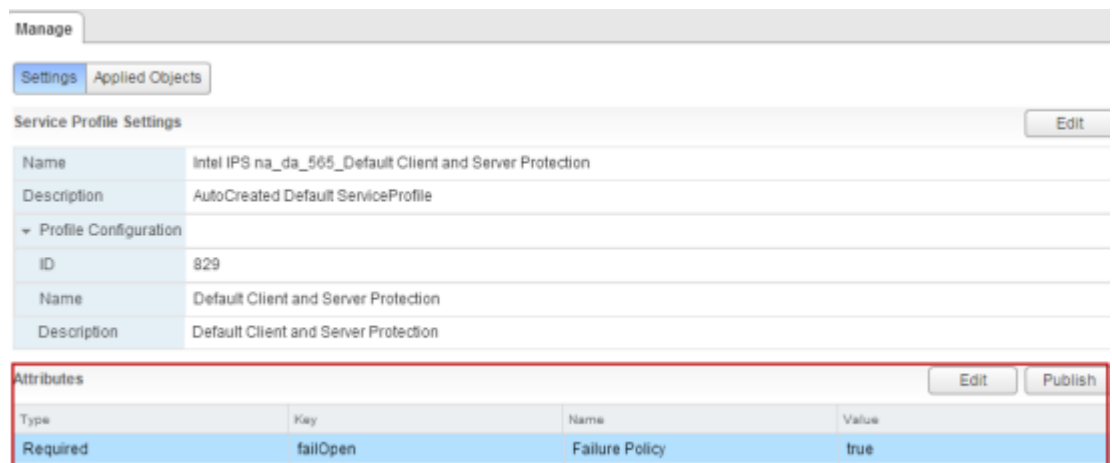
Consider that you selected the *Default Client and Server Protection (IDS IPS)* profile in the inbound and outbound network introspection service (as shown below).



Double-click on *Default Client and Server Protection* service profile.



- 6 Select the **Failure Policy** attribute and click **Edit**.



- 7 By default, the **Failure Policy** attribute's fail-open key is set to true. This means the Virtual Security System instance fail-opens in case of a failure. Set the value to false, if you want the Virtual Security System instance to fail-close.

Type	Key	Name	Value
Required	failOpen	Failure Policy	true

☐ Publish changes to underlying service profile

OK Cancel

- 8 In the **Edit attributes** dialog box, select **Publish changes to underlying service profile** and click **OK**.
- 9 Select the attribute and click **Publish**.

Intel IPS na_da_565_Default Client and Server Protection

Manage Settings Applied Objects

Service Profile Settings

Name: Intel IPS na_da_565_Default Client and Server Protection

Description: AutoCreated Default ServiceProfile

Profile Configuration

ID: 829

Name: Default Client and Server Protection

Description: Default Client and Server Protection

Attributes

Type	Key	Name	Value
Required	failOpen	Failure Policy	true

Edit Publish

Repeat the process if you used different profiles for inbound and outbound network introspection services.


Assign policy groups to virtual security systems

Before you begin

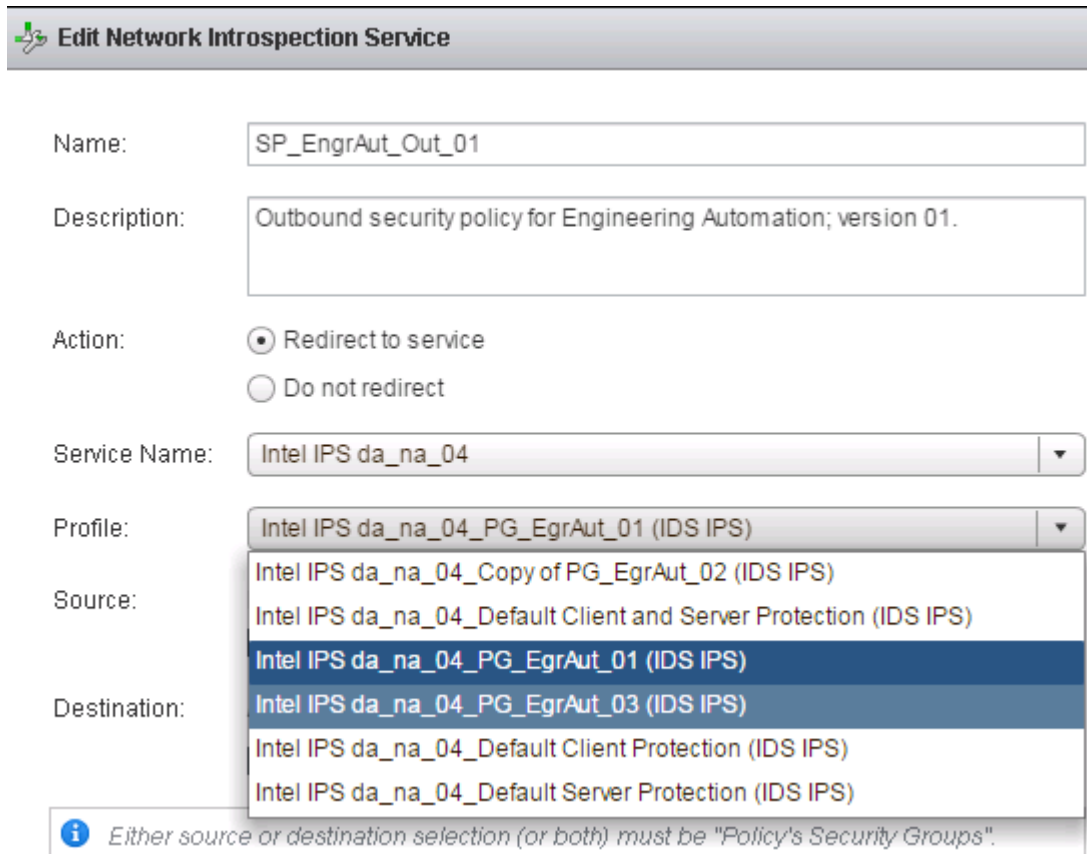
You have created the required policy group in the Manager.

You might want to apply a different policy group to the deployed instances of a virtual security system.

Task

- 1 Log on to vSphere Web Client as the root user.
- 2 In the vSphere **Home** tab, select **Networking & Security**.
- 3 Select **Service Composer | Security Policies**.
- 4 From the **NSX Manager** list, select the corresponding NSX Manager.
- 5 Select the required security policy and click .
- 6 Select **Network Introspection Services**.
- 7 Select the required network introspection service and click the edit icon.

- 8 From the **Profile** drop-down list, select the required policy group and then click **OK**.



Edit Network Introspection Service

Name: SP_EngrAut_Out_01

Description: Outbound security policy for Engineering Automation; version 01.

Action: ☒ Redirect to service
☐ Do not redirect

Service Name: Intel IPS da_na_04

Profile: Intel IPS da_na_04_PG_EgrAut_01 (IDS IPS)

Source: Intel IPS da_na_04_Copy of PG_EgrAut_02 (IDS IPS)
Intel IPS da_na_04_Default Client and Server Protection (IDS IPS)
Intel IPS da_na_04_PG_EgrAut_01 (IDS IPS)

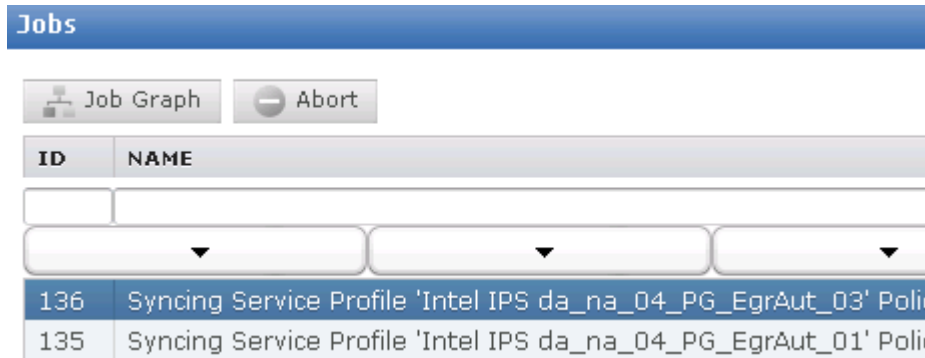
Destination: Intel IPS da_na_04_PG_EgrAut_03 (IDS IPS)
Intel IPS da_na_04_Default Client Protection (IDS IPS)
Intel IPS da_na_04_Default Server Protection (IDS IPS)

Either source or destination selection (or both) must be "Policy's Security Groups".

Figure 6-4 Select the policy group in NSX

- 9 Click **Finish**.

In Intel Security Controller, the *Syncing Service Profile* job is triggered for every network introspection service that you change. Make sure this job passes successfully.



Jobs

Job Graph Abort

ID	NAME
136	Syncing Service Profile 'Intel IPS da_na_04_PG_EgrAut_03' Pol...
135	Syncing Service Profile 'Intel IPS da_na_04_PG_EgrAut_01' Pol...

Figure 6-5 Job for synchronizing change in policy group

You do not require to deploy configuration changes from the Manager.

Quarantine endpoints using NSX features

Before you begin

You have the required access to create security groups and security policies in NSX.

In case of alerts detected by Virtual Security System instances, you can use the native Quarantine feature to quarantine the source endpoint of an attack. You can also use the security tags and security policies in NSX to quarantine the source or the target endpoint of an attack.


To quarantine endpoints using NSX features, you tag the source or destination VM in alert from the Threat Analyzer. In NSX, create a security group, which dynamically includes VMs tagged in the Threat Analyzer. To this group, you assign a security policy, which effectively quarantines the tagged VM.

Notes:

- The Quarantine feature of Network Security Platform and the security tags of NSX are exclusive to each other.
- In case of security tags, currently you can only quarantine endpoints from the **Real-time** or **Historical Threat Analyzer**. You cannot enable quarantine through security tags in the attack definitions.
- Currently, there is no indication in the Threat Analyzer that an endpoint is tagged.
- Currently, to release an endpoint from quarantine, you must manually remove the tag in NSX.

This section uses an example to explain how to quarantine endpoints using security tags and security policies in NSX.

Task

- 1 In NSX, create a security group to dynamically include tagged VMs.
 - a In vCenter web client, select **Home | Networking & Security | Service Composer | Security Groups**.
 - b In the **Service Composer** page, select the NSX Manager from the drop-down list.
 - c Click  to create a security group.
 - d Enter a relevant name and description.
 - e In the **Define dynamic membership** step, select **any** for **Match**.
 - f In **Criteria Details**, select **Security Tag** and **Equals to** in the first two drop-down.
 - g In the text box, exactly enter `ISC-Quarantine`.

The Manager assigns `ISC-Quarantine` as the tag. So, you must also exactly enter this string for a tagged VM to be included in this security group.

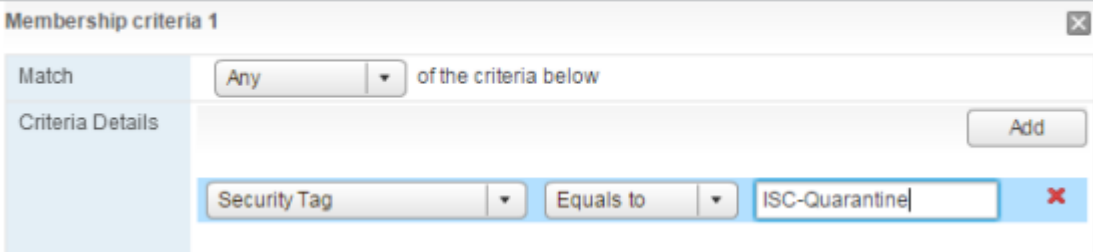




Figure 6-6 Adding criteria to include tagged VMs

- h Click **Finish**.

- 2 In NSX, create a security policy to quarantine VMs tagged as *ISC-Quarantine*.
 - a In the **Securities Policies** tab of **Service Composer** page, click  to create a security policy.
 - b Enter a relevant name and description and proceed to step 3, **Firewall Rules**.
 - c Add a firewall rule to allow traffic to the VM hosting the remediation portal.
 For **Source**, select **Policy's Security Groups**. For **Destination** select the security group, which contains the VM hosting the remediation portal.

 **New Firewall Rule**


Name:	AllowTrafficToRemediationPortal	
Description/Comments:	Rule to allow traffic to remediation portal	
Action:	<input checked="" type="radio"/> Allow <input type="radio"/> Block <input type="radio"/> Reject	
Source:	Policy's Security Groups Change... <input type="checkbox"/> Negate source	
Destination:	SG_70 Change... <input type="checkbox"/> Negate destination	
<div style="display: flex; align-items: flex-start;"> <div style="margin-right: 10px;"></div> <div> <p><i>Either source or destination selection (or both) must be "Policy's Security Groups".</i></p> <p><i>Current selection will apply to "Outgoing" traffic from the security groups when it gets applied to specified Destination.</i></p> </div> </div>		
Service:	HTTP Change...	
State:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	
Log:	<input type="radio"/> Log	

Figure 6-7 Rule to allow traffic to remediation portal

- d Add the last rule, which blocks all traffic.

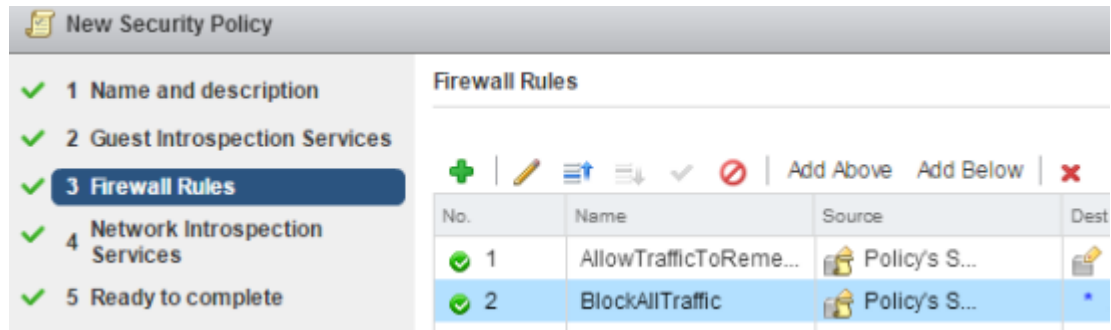



Figure 6-8 Rule to block all traffic

- e Click Finish.
- 3 Apply the security policy from the previous step to the security group created in step 1.
- a In the **Securities Policies** tab of **Service Composer** page, select the relevant security policy and click 
- 4 Select the relevant security group and click **OK**.
- 5 Tag a VM from the Real-time or Historical Threat Analyzer.
- a Right-click on an alert and select **Tag (via ISC)**.
- b Select either **Source** or **Destination**.
- c Click **OK** to confirm tagging the VM.
- d If tagging is successful, the details are displayed in the **Tag successfully assigned** dialog box. Review the details and click **OK**.

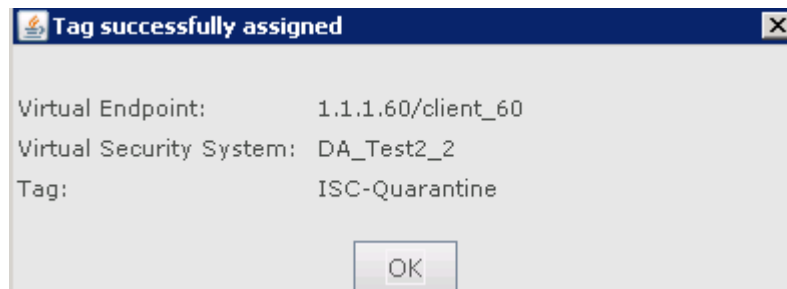


Figure 6-9 Tagging details

6 Confirm tagging in NSX.

- a In vCenter web client, select **Home | Networking & Security | Networking & Security Inventory | NSX Managers**.
- b Select the relevant NSX Manager and then select **Manage | Security Tags**.
- c Click on the **VM Count** for **ISC-Quarantine**.

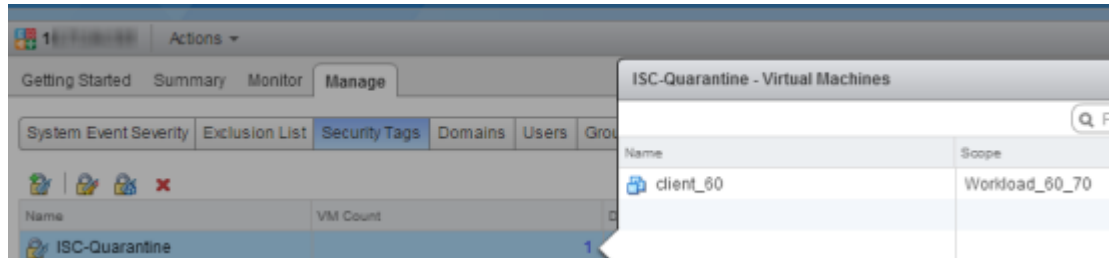


Figure 6-10 VM Count for ISC-Quarantine

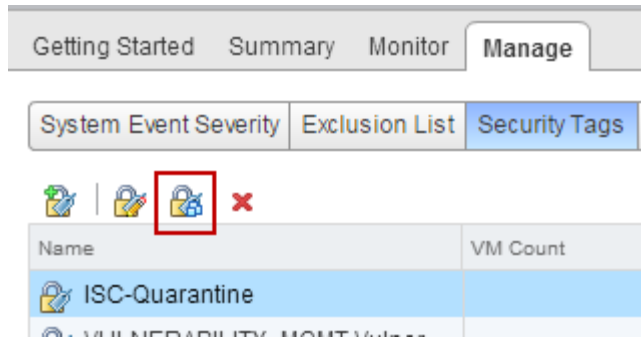
You can also check the current virtual machines included in the corresponding security group.

7 If required, release a VM from quarantine.

To release a VM from quarantine, you must remove the *ISC-Quarantine* tag for the VM.

- a In vCenter web client, select **Home | Networking & Security | Networking & Security Inventory | NSX Managers**.
- b Select the relevant NSX Manager and then select **Manage | Security Tags**.

- c Select *ISC-Quarantine* and click 



- d Deselect the check box for the VMs you want to release from quarantine.

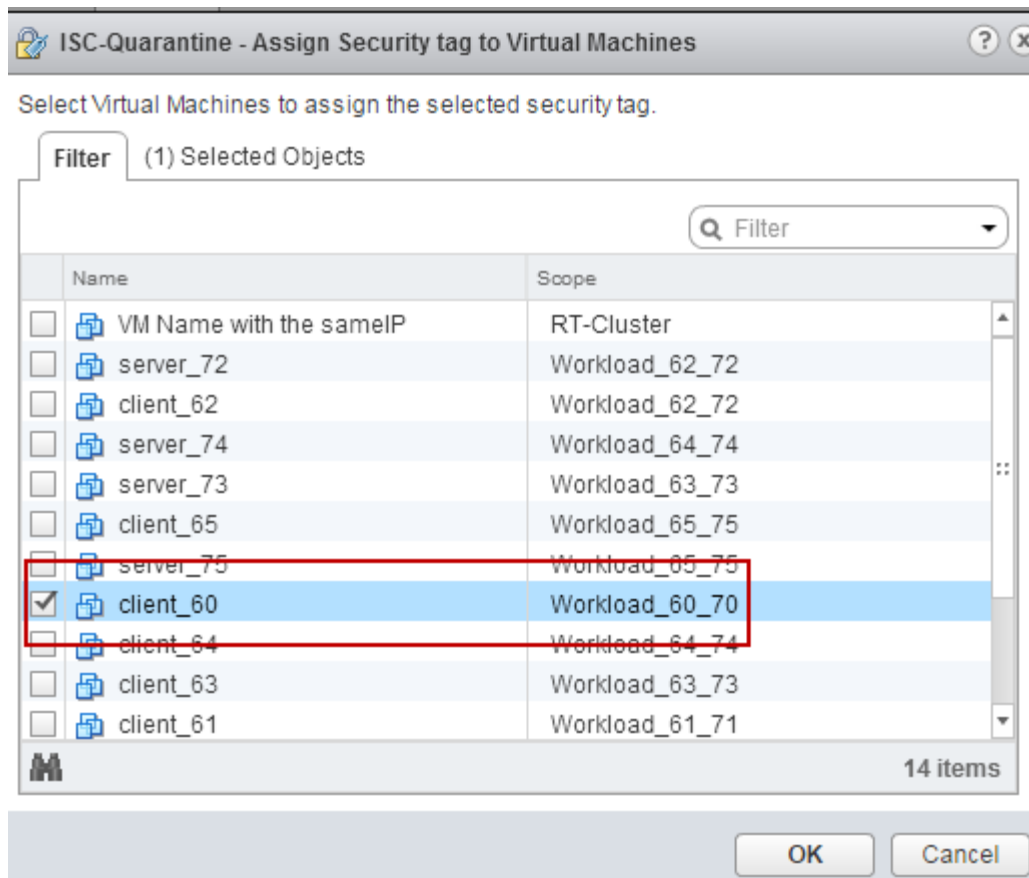


Figure 6-11 Release VMs from quarantine

Index

A

about this guide [5](#)

C

conventions and icons used in this guide [5](#)

D

documentation

- product-specific, finding [6](#)

- typographical conventions and icons [5](#)

M

McAfee ServicePortal, accessing [6](#)

S

ServicePortal, finding product documentation [6](#)

T

technical support, finding product information [6](#)

