

Firefly Host

Installation and Upgrade Guide for VMware

Release

6.0



Published: 2014-01-14

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Copyright © 2014, Juniper Networks, Inc. All rights reserved.

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Firefly Host Installation and Upgrade Guide for VMware

Release 6.0

Copyright © 2014, Juniper Networks, Inc.

All rights reserved.

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <http://www.juniper.net/support/eula.html>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Abbreviated Table of Contents

	About the Documentation	xiii
Part 1	Firefly Host Overview	
Chapter 1	Introduction to Firefly Host	3
Part 2	Firefly Host Installation and Configuration	
Chapter 2	Firefly Host Installation	7
Chapter 3	Firefly Host Upgrade	45
Chapter 4	Firefly Host Integration with vCloud Director	51
Chapter 5	Firefly Host Management	57
Part 3	Firefly Host Settings Infrastructure to Secure Hosts	
Chapter 6	Securing ESX/ESXi Hosts using Firefly Host	73
Chapter 7	VMware Auto Deploy for ESXi Servers and with Firefly Host	77
Chapter 8	Firefly Host Firewall Module	87
Chapter 9	Firefly Host Network Module	117
Part 4	Index	
	Index	127

Table of Contents

	About the Documentation	xiii
	Documentation and Release Notes	xiii
	Documentation Conventions	xiii
	Documentation Feedback	xv
	Requesting Technical Support	xv
	Self-Help Online Tools and Resources	xvi
	Opening a Case with JTAC	xvi
Part 1	Firefly Host Overview	
Chapter 1	Introduction to Firefly Host	3
	Understanding Firefly Host	3
Part 2	Firefly Host Installation and Configuration	
Chapter 2	Firefly Host Installation	7
	Understanding the Open Virtualization Format OVA Template Method	7
	Using the OVA Bundled Method to Integrate Firefly Host with the VMware Infrastructure	8
	Using the OVA Single File Method to Integrate the Firefly Host Dashboard with VMware	17
	Using the OVA Single File Method to Integrate the Firefly Host VM with VMware	19
	Setting Up Firefly Host	19
	Determining the Firefly Host Dashboard's Default IP Address	19
	Changing or Setting the IP Address for the Firefly Host Dashboard	21
	Connecting to the Firefly Host Dashboard and Configuring Basic Settings	23
	Integrating the Firefly Host with VMware Using the Settings Module	31
	Installing Firefly Host VMs on ESX/ESXi Hosts	35
	Configuring Firefly Host Installation Settings	40
	Removing Firefly Host VMs from ESX/ESXi Hosts	42
Chapter 3	Firefly Host Upgrade	45
	Updating the Firefly Host Dashboard	45
	Updating Individual Firefly Host VMs	46
	Updating Firefly Host VMs in Batch Mode	48
Chapter 4	Firefly Host Integration with vCloud Director	51
	Understanding Firefly Host Integration with vCloud Director	51
	VMware vCloud Director	51
	Firefly Host and vCloud	51

	Requirements	52
	Configuring Firefly Host Integration with vCloud Director	53
Chapter 5	Firefly Host Management	57
	Understanding Firefly Host Timeout Parameters and the Firefly Host VM Installation, Uninstallation, and Update Tasks	57
	Adding New Firefly Host Administrator Definitions, Permissions, and Authentication Using the Settings Module	59
	Configuring an Administrator Account	59
	Changing Administrator Passwords	61
	Global Administrator: Changing Your Own Password	62
	Global Administrator: Changing the Password of Another Administrator	62
	VM Administrator and Network Monitoring Administrator Accounts: Changing Your Own Password	63
	Setting Up Active Directory for Firefly Host Administrator Authentication	64
	Adding and Editing Firefly Host Machines Definitions (VMware)	66
	Adding a Machine	66
	Viewing Machine Information	68
Part 3	Firefly Host Settings Infrastructure to Secure Hosts	
Chapter 6	Securing ESX/ESXi Hosts using Firefly Host	73
	Securing and Unsecuring Virtual Machines Using the Firefly Host Dashboard	73
	Disabling the Firefly Host Suspend-Resume Process Enacted After a VM Is Unsecured	74
	Displaying the State of the vmsafe config Setting	74
	Disabling the Suspend-Resume Process	74
	Understanding Automatic Securing of VMs	75
Chapter 7	VMware Auto Deploy for ESXi Servers and with Firefly Host	77
	Understanding VMware Auto Deploy for ESXi Servers and with Firefly Host	77
	About VMware Auto Deploy	77
	Firefly Host Support for Auto Deploy	77
	Firefly Host Automatic Installation of a Firefly Host VMs	78
	Configuring VMware Auto Deploy and Firefly Host to Secure ESXi Hosts	78
	Configuring Auto Deploy in VMware	79
	Configuring Firefly Auto Deploy Support	84
Chapter 8	Firefly Host Firewall Module	87
	Understanding the Firefly Host Firewall Module	87
	The Firewall Module and the VM Tree	87
	Overview of the Firewall Policy Model	88
	Global Policy, Group Policy, and Individual VM Policy Tiers	89
	Global Policy	90
	Group Policy	91
	Individual VM Policy Rules	92
	Default Policy	92
	Quarantine Policy	92
	Firewall Policy Structure and Policy Rules Precedence	92

	Viewing the Complete Policy Rule Base for a VM	94
	The Manage Policy Tab	94
	Policy Per vNIC and Dual Stack	95
	Creating a Policy Rule	95
	The Apply Policy Tab	98
	The Logs Tab	100
	Understanding How Firefly Host Handles ICMPv6 Protocol Traffic	101
	About ICMPv6	101
	Filtering ICMPv6 Packets	101
	Default Policy Group for Allowing Inbound ICMPv6 Packets	102
	Viewing the Default ICMPv6 Protocols Group Members	102
	Editing the Default ICMPv6 Protocols Group Members	104
	Understanding Predefined Objects for Firefly Host Firewall Policy Terms	105
	Defining and Selecting Source and Destination Terms for Policy Rules	105
	Predefined Global IP Address Objects	105
	Predefined Network Objects	106
	Predefined Network Objects for Well Known IP Addresses	106
	Additional IPv4 and IPv6 Predefined Network Objects	107
	Configuring Firefly Host Firewall Policies	108
	Understanding Firefly Host Predefined Firewall Policy for Its Components	115
Chapter 9	Firefly Host Network Module	117
	Understanding the Firefly Host Network Module	117
	Network Module	117
	Manipulating Displayed Information	118
	Changing the Time Interval for Displayed Information	119
	Using Advanced Options for Filtering Network Data	121
	Sorting Table Data	121
	Using the Firefly Host Network and Firewall Modules Cooperatively	122
	Network Assessment	122
	Using the Network Module to Observe Traffic Coming Into and Going Out from VMs	123
	Detecting Unexpected and Unwanted Behavior	123
	Using the Network and Firewall Modules Together	124
Part 4	Index	127

List of Figures

Part 2	Firefly Host Installation and Configuration	
Chapter 2	Firefly Host Installation	7
	Figure 1: OVA Template Details Page	10
	Figure 2: OVA File Deployment License Agreement	11
	Figure 3: Naming the vApp	12
	Figure 4: Specifying the Host and Cluster	13
	Figure 5: Selecting the Storage	13
	Figure 6: Mapping the Firefly Host Management Networks	14
	Figure 7: Specifying the Database Disk Size	15
	Figure 8: Verifying That the Configuration Is Correct	15
	Figure 9: Displaying the Firefly Host Appliance Components	16
	Figure 10: Firefly Host Dashboard Summary Tab in vCenter	17
	Figure 11: Viewing the Firefly Host Dashboard IP Address in VMware	21
	Figure 12: Firefly Host Dashboard IP Addresses on the Firefly Host CLI Console	22
	Figure 13: Configuring an IP Address for the Firefly Host Dashboard	22
	Figure 14: Logging In to the Firefly Host Dashboard	23
	Figure 15: Firefly Host Installation Wizard Overview	24
	Figure 16: Changing the Default Password	24
	Figure 17: Configuring Network Settings for the Firefly Host Dashboard	26
	Figure 18: Configuring the Time Server	27
	Figure 19: Firefly Host Installation Wizard displaying Product Licensing	28
	Figure 20: Firefly Host Dashboard vCenter Integration	29
	Figure 21: Configuring the Firefly Host Dashboard vCenter Settings	30
	Figure 22: Securing an ESX/ESXi Host With a Firefly Host VM	36
	Figure 23: Installing a Firefly Host VM on an ESX/ESXi Host	36
	Figure 24: Specifying Firefly Host Security Parameters During Installation	37
	Figure 25: Firefly Host VM Installation Process Completion Notice	40
	Figure 26: Firefly Host VM Uninstall	42
Chapter 4	Firefly Host Integration with vCloud Director	51
	Figure 27: Firefly Host Dashboard vCenter Integration Window Showing vCloud Director Settings Pane	54
Chapter 5	Firefly Host Management	57
	Figure 28: Firefly Host CLI Console	58
	Figure 29: Creating a VM Admin Administrator Account	60
	Figure 30: Adding a New Administrator	61
	Figure 31: Changing the Global Administrator Password	62
	Figure 32: Global Administrator Changing the Password of Another Administrator	63

	Figure 33: Administrators Changing Their Password	64
	Figure 34: Enabling Active Directory	65
	Figure 35: Configuring Machines Information	68
	Figure 36: Syslog Entry Including VM Name and Log Tag	68
Part 3	Firefly Host Settings Infrastructure to Secure Hosts	
Chapter 7	VMware Auto Deploy for ESXi Servers and with Firefly Host	77
	Figure 37: Firefly Host Failure Alert	78
	Figure 38: Configuring Automatic Installation of Firefly Host VMs for Auto-Deployed ESXi Hosts	84
Chapter 8	Firefly Host Firewall Module	87
	Figure 39: Firewall Module Policy for a Single VM	88
	Figure 40: Global Policy	91
	Figure 41: VM Policy Expanded Rule Base	94
	Figure 42: Firewall Module Manage Policy Page	95
	Figure 43: Adding a Rule	96
	Figure 44: Using the Dialog Box Filter to Add Terms for policy rules	96
	Figure 45: Firewall Apply Policy Page	98
	Figure 46: Changed Policies Dialog Box	99
	Figure 47: Firewall Module Logs Tab	100
	Figure 48: Default Global Policy Showing Default ICMPv6 Allow Group	102
	Figure 49: Protocols Settings ICMPv6 Default Protocol Group	103
	Figure 50: Default Global Policy	110
	Figure 51: Adding a Global Policy Rule to Reject Telnet Connection Attempts	111
	Figure 52: VM Policy for an Individual VM	113
	Figure 53: Complete VM Policy for an Individual VM	113
	Figure 54: All Machines	114
	Figure 55: Policy Install Progress	114
Chapter 9	Firefly Host Network Module	117
	Figure 56: Network Summary Tab for All VMs	118
	Figure 57: Main Module Network Module Summary Tab for a Single VM	118
	Figure 58: Displaying Network Data for Different Time Intervals: Part 1	119
	Figure 59: Displaying Network Data for Different Time Intervals: Part 2	119
	Figure 60: Selecting a Time Interval	120
	Figure 61: Setting the Custom Time Period	120
	Figure 62: Top Protocols Across All Machines Example	122
	Figure 63: Network Module Connection Tab Information	123

List of Tables

	About the Documentation	xiii
	Table 1: Notice Icons	xiv
	Table 2: Text and Syntax Conventions	xiv
Part 2	Firefly Host Installation and Configuration	
Chapter 5	Firefly Host Management	57
	Table 3: Firefly Host Built-In Administrator User Types	59
Part 3	Firefly Host Settings Infrastructure to Secure Hosts	
Chapter 8	Firefly Host Firewall Module	87
	Table 4: Firewall Policy Configuration Settings	97
	Table 5: Firewall Policy Icons	99
Chapter 9	Firefly Host Network Module	117
	Table 6: Using Advanced Options for Filtering Network Data	121

About the Documentation

- Documentation and Release Notes on page xiii
- Documentation Conventions on page xiii
- Documentation Feedback on page xv
- Requesting Technical Support on page xv

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at <http://www.juniper.net/techpubs/>.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at <http://www.juniper.net/books>.

Documentation Conventions

Table 1 on page xiv defines notice icons used in this guide.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.

Table 2 on page xiv defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the configure command: <code>user@host> configure</code>
<code>Fixed-width text like this</code>	Represents output that appears on the terminal screen.	<code>user@host> show chassis alarms</code> <code>No alarms currently active</code>
<i>Italic text like this</i>	<ul style="list-style-type: none"> Introduces or emphasizes important new terms. Identifies guide names. Identifies RFC and Internet draft titles. 	<ul style="list-style-type: none"> A policy <i>term</i> is a named structure that defines match conditions and actions. <i>Junos OS CLI User Guide</i> RFC 1997, <i>BGP Communities Attribute</i>
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: <code>[edit]</code> <code>root@# set system domain-name <i>domain-name</i></code>
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"> To configure a stub area, include the stub statement at the <code>[edit protocols ospf area area-id]</code> hierarchy level. The console port is labeled CONSOLE.
< > (angle brackets)	Encloses optional keywords or variables.	<code>stub <default-metric <i>metric</i>>;</code>

Table 2: Text and Syntax Conventions (*continued*)

Convention	Description	Examples
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	broadcast multicast <i>(string1 string2 string3)</i>
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[] (square brackets)	Encloses a variable for which you can substitute one or more values.	community name members [community-ids]
Indentation and braces ({ })	Identifies a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop <i>address</i> ; retain; } } }
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"> In the Logical Interfaces box, select All Interfaces. To cancel the configuration, click Cancel.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select Protocols>Ospf .

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at <https://www.juniper.net/cgi-bin/docbugreport/>. If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version (if applicable)

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract,

or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://www.juniper.net/alerts/>
- Join and participate in the Juniper Networks Community Forum: <http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://tools.juniper.net/SerialNumberEntitlementSearch/>

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at <http://www.juniper.net/cm/>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <http://www.juniper.net/support/requesting-support.html>.

PART 1

Firefly Host Overview

- [Introduction to Firefly Host on page 3](#)

CHAPTER 1

Introduction to Firefly Host

- [Understanding Firefly Host on page 3](#)

Understanding Firefly Host

Firefly Host delivers complete virtualization security for multitenant public and private clouds, and clouds that are a hybrid of the two. Firefly Host is built off the vGW product line and replaces it. Firefly Host comprises the following three main components:

- The Firefly Host Dashboard that provides a central management server. It consists of a set of modules that you use to configure the Firefly Host features for your virtualized environment. It provides charts, tables, and graphs that allow you to view information that Firefly Host produces about your environment and use in determining how to adjust your security policy.

You use it to install and manage the Firefly Host VMs that you deploy to secure hosts in your virtualized environment.

- The Firefly Host VM that is installed on each host to be secured. The Firefly Host VM acts as a conduit to the Firefly Host Module that it inserts into the hypervisor of the host that Firefly Host protects. The Firefly Host VM maintains policy and logging information. A Firefly Host VM remains attached to the ESX/ESXi host that it is installed on.

The Firefly Host Dashboard pushes the appropriate security policy to the Firefly Host VM which, in turn, inserts it into the Firefly Host Module.

- The Firefly Host Module

Virtualized network traffic is secured and analyzed against the security policy for all VMs on the ESX/ESXi host in the Firefly Host Module installed on the host. All connections are processed and firewall security is enforced in the Firefly Host module.

Related Documentation

- *[Understanding the Firefly Host Architecture](#)*
- *[Understanding Cloud Computing and Firefly Host](#)*
- *[Understanding Hypervisors and Firefly Host](#)*
- *[Understanding the VMware Infrastructure and Firefly Host](#)*
- *[Understanding the Firefly Host Dashboard](#)*

- *Understanding the Firefly Host VM*
- *Firefly Host Prerequisites and Resource Requirements for the VMware Environment*

PART 2

Firefly Host Installation and Configuration

- [Firefly Host Installation on page 7](#)
- [Firefly Host Upgrade on page 45](#)
- [Firefly Host Integration with vCloud Director on page 51](#)
- [Firefly Host Management on page 57](#)

CHAPTER 2

Firefly Host Installation

This chapter explains integrating Firefly Host with VMware and setting up the Firefly Host Dashboard. It also explains installing and uninstalling the Firefly Host VMs on ESX/ESXi Hosts.

- [Understanding the Open Virtualization Format OVA Template Method on page 7](#)
- [Using the OVA Bundled Method to Integrate Firefly Host with the VMware Infrastructure on page 8](#)
- [Using the OVA Single File Method to Integrate the Firefly Host Dashboard with VMware on page 17](#)
- [Using the OVA Single File Method to Integrate the Firefly Host VM with VMware on page 19](#)
- [Setting Up Firefly Host on page 19](#)
- [Integrating the Firefly Host with VMware Using the Settings Module on page 31](#)
- [Installing Firefly Host VMs on ESX/ESXi Hosts on page 35](#)
- [Configuring Firefly Host Installation Settings on page 40](#)
- [Removing Firefly Host VMs from ESX/ESXi Hosts on page 42](#)

Understanding the Open Virtualization Format OVA Template Method

Firefly Host leverages the Open Virtualization Format (OVF) standard for packaging and delivering virtual machines (VMs). The OVF supports industry-standard content verification and integrity checking, and it provides a basic scheme for managing software licensing. As described by the standard, OVF defines an "open, secure, portable, efficient and extensible format for the packaging and distribution of software to be run in virtual machines." The standard also supports the OVA template method of packaging and distributing software in a single archive. You use the vSphere 4.x client to load the OVA file.

You can use OVA to deploy the Firefly Host VMs in the following ways:

- In a single bundled OVA package, also referred to as a Combo Package that contains the Firefly Host Dashboard and the Firefly Host VM template.

Firefly Host uses OVA to deliver a single file containing both Firefly Host components.

- In nonbundled OVA files to separately deploy the Firefly Host Dashboard and the Firefly Host VM template.

The OVA Combo Package installs a vApp, and VMware will not install a vApp on a cluster for which the Dynamic Resource Scheduler (DRS) is not enabled. You can take the nonbundled approach in this case.

The nonbundled OVA approach is also useful for installing the most current Firefly Host VM, after the initial installation, to ensure that the latest version is used for automatic Firefly Host VM instantiation on ESX/ESXi hosts.

You can also use it to create a secondary Firefly Host Dashboard for high availability. For details, see *Installing an Additional Firefly Host Dashboard and Configuring the Primary Firefly Host Dashboard to Use It for High Availability*.

Related Documentation

- [Using the OVA Single File Method to Integrate the Firefly Host VM with VMware on page 19](#)
- [Using the OVA Bundled Method to Integrate Firefly Host with the VMware Infrastructure on page 8](#)
- *Preparing to Integrate Firefly Host with the VMware Environment*
- *Understanding the VMware Infrastructure and Firefly Host*
- [Understanding Firefly Host on page 3](#)

Using the OVA Bundled Method to Integrate Firefly Host with the VMware Infrastructure

This topic explains how to integrate the Firefly Host appliances—the Firefly Host Dashboard and the Firefly Host VM template—with the VMware virtualized infrastructure.

For information on *Firefly Host Prerequisites and Resource Requirements for the VMware Environment* see *Firefly Host Prerequisites and Resource Requirements for the VMware Environment*.

This topic includes the following sections:

- [Requirements on page 8](#)
- [Overview on page 8](#)
- [Downloading the Firefly Host OVA Combo Package on page 9](#)
- [Integrating the Firefly Host with the VMware Infrastructure on page 9](#)

Requirements

For information, see *Firefly Host Prerequisites and Resource Requirements for the VMware Environment*.

Overview

The bundled OVA template allows you to deploy both the Firefly Host Dashboard and the Firefly Host VM appliances in a single OVA archive file. In this case, OVA creates a single vApp and inserts the two Firefly Host appliances into it.

You can delete the vApp after the deployment and integration process is complete. It is used only to convey the Firefly Host VMs. However, take care not to delete it before then.

In the single Combo Package file, the OVA template deploys:

- The Firefly Host Dashboard
- The Firefly Host VM

You must manually convert the Firefly Host VM to a template after you integrate the Firefly Host with the VMware infrastructure. Firefly Host uses the resulting template to instantiate a Firefly Host VM on each ESX/ESXi host when you secure that host.



NOTE: The OVA Combo Package installs a vApp, and VMware will not install a vApp on a cluster for which DRS is not enabled. In this case, you must use the nonbundled OVA method to deploy each component separately.

- For details, see “Using the OVA Single File Method to Integrate the Firefly Host Dashboard with VMware” on page 17.
- For details, see “Using the OVA Single File Method to Integrate the Firefly Host VM with VMware” on page 19.

The Firefly Host software packages are available at:

<http://www.juniper.net/support/downloads/>.

Downloading the Firefly Host OVA Combo Package

Step-by-Step Procedure To download the Juniper Networks OVA archive file that contains both the Firefly Host Dashboard and the Firefly Host VM:

1. Navigate to the Juniper Networks Support page.
2. Select **Software Downloads** from the Support box in the left column.
3. Select **Firefly Host (Altor)** in the Security pane.
4. Select the **Software** tab.
5. Click **Firefly Host 6.0 Combo Package**, and log in to the site to download the file.

Integrating the Firefly Host with the VMware Infrastructure

Step-by-Step Procedure To deploy the Firefly Host appliances—the Firefly Host Dashboard and the Firefly Host VM—and integrate them with the VMware infrastructure:

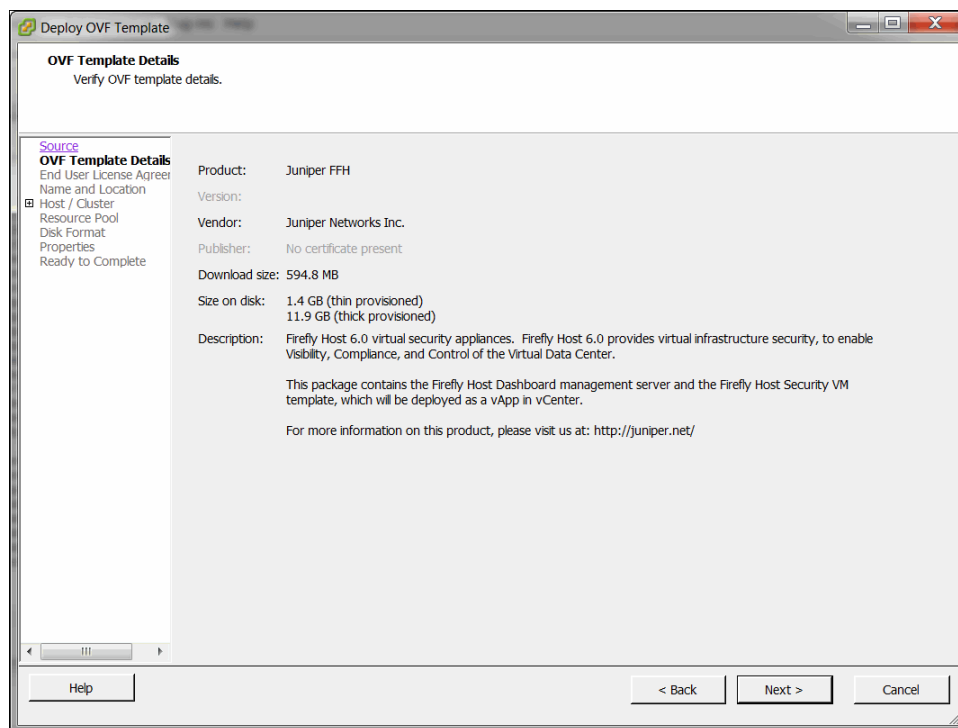
1. Using the vSphere client, load the bundled OVA file. Select **Deploy OVF Template** from the File menu.
2. Enter the download filename or its URL in the Deploy from file or URL box—for example, enter: `c:\temp\Firefly_Host_Combo_6.0_#-#-#-#-#.ova`—and click **Next**.

You use the OVF template method to deploy the OVA file. After you specify the name of the OVA file and its location, the Appliance Wizard displays the OVA template details dialog box.

3. Verify the contents of the OVA package, and click **Next**.

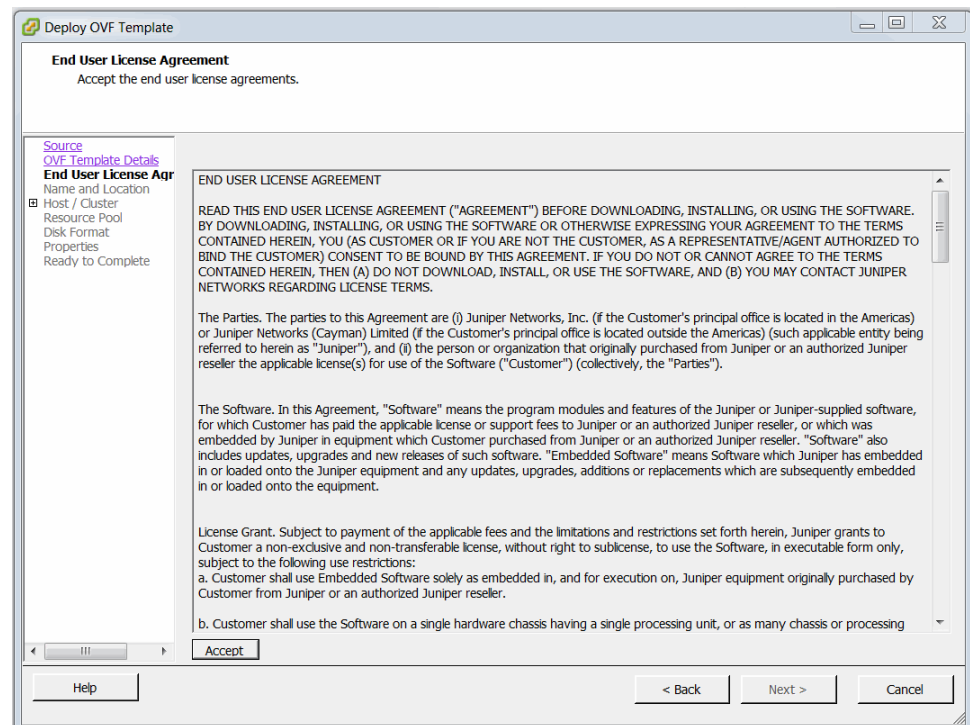
Before the wizard unbundles the OVA package, verify that it contains the Firefly Host appliances. The OVA template summary also specifies the disk space requirements for thick and thin provisioning. See [Figure 1 on page 10](#).

Figure 1: OVA Template Details Page



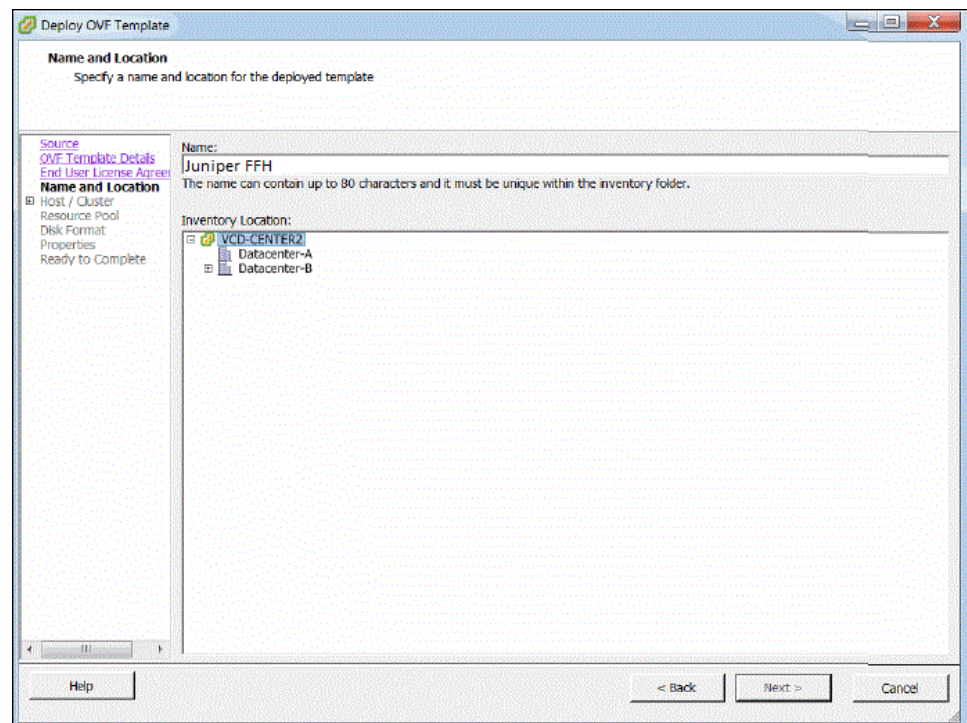
4. Accept the Firefly Host license agreement, and click **Next**. See [Figure 2 on page 11](#).

Figure 2: OVA File Deployment License Agreement



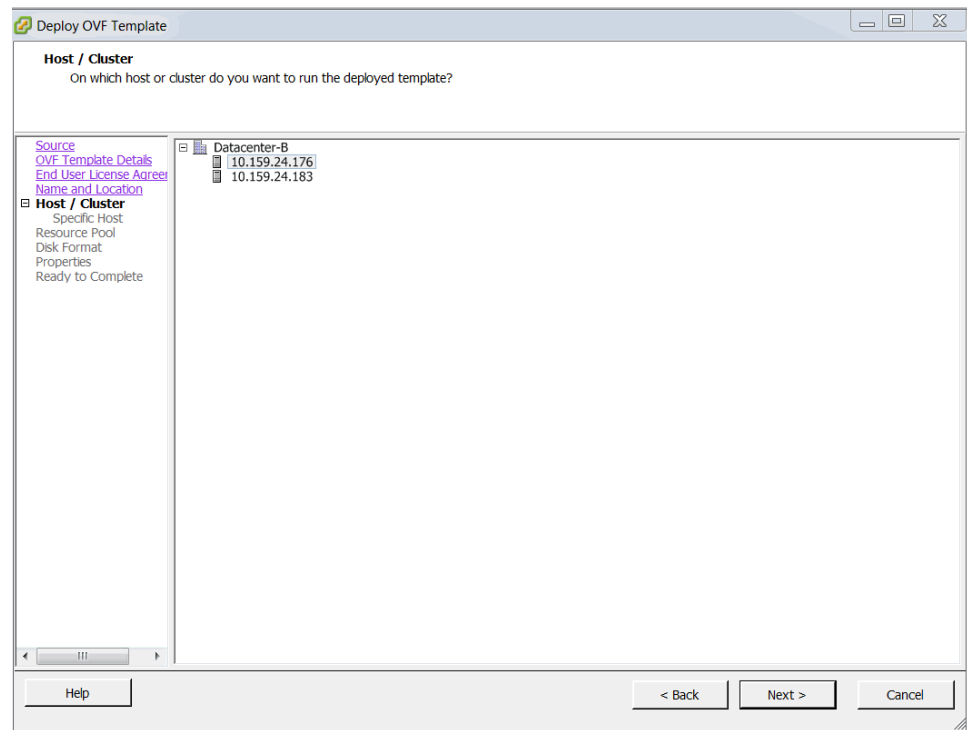
5. Specify a name for the vApp that will be created and a storage location. See [Figure 3 on page 12](#).

Figure 3: Naming the vApp



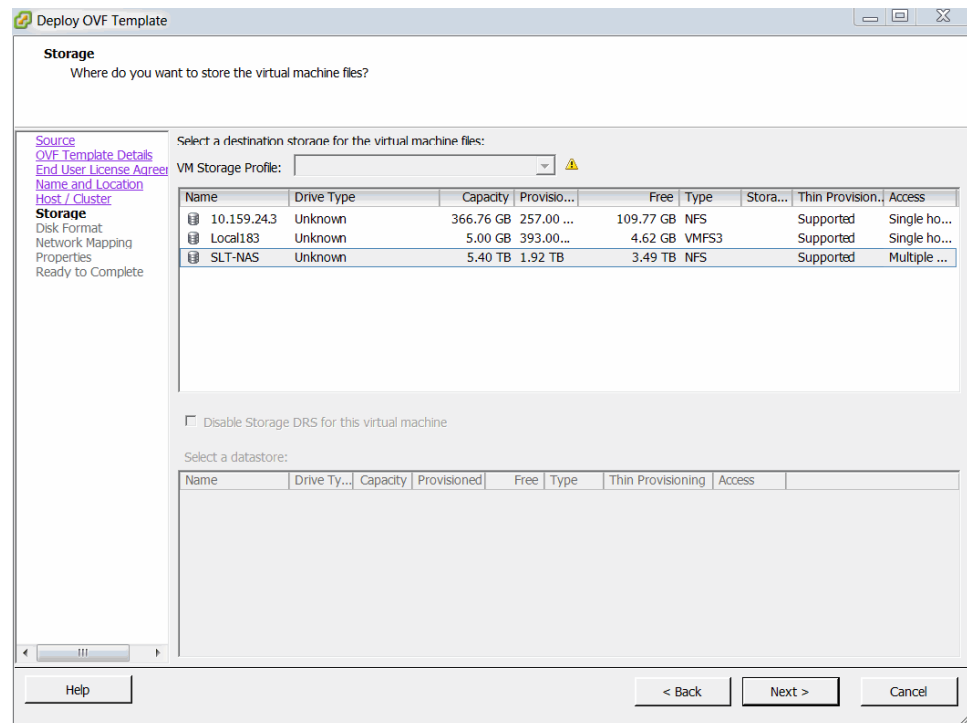
6. Specify the host or host/cluster on which to run the deployed template. We recommend that you use a network storage device (NAS) so that it can be migrated through VMotion for space optimization. See [Figure 4 on page 13](#).

Figure 4: Specifying the Host and Cluster



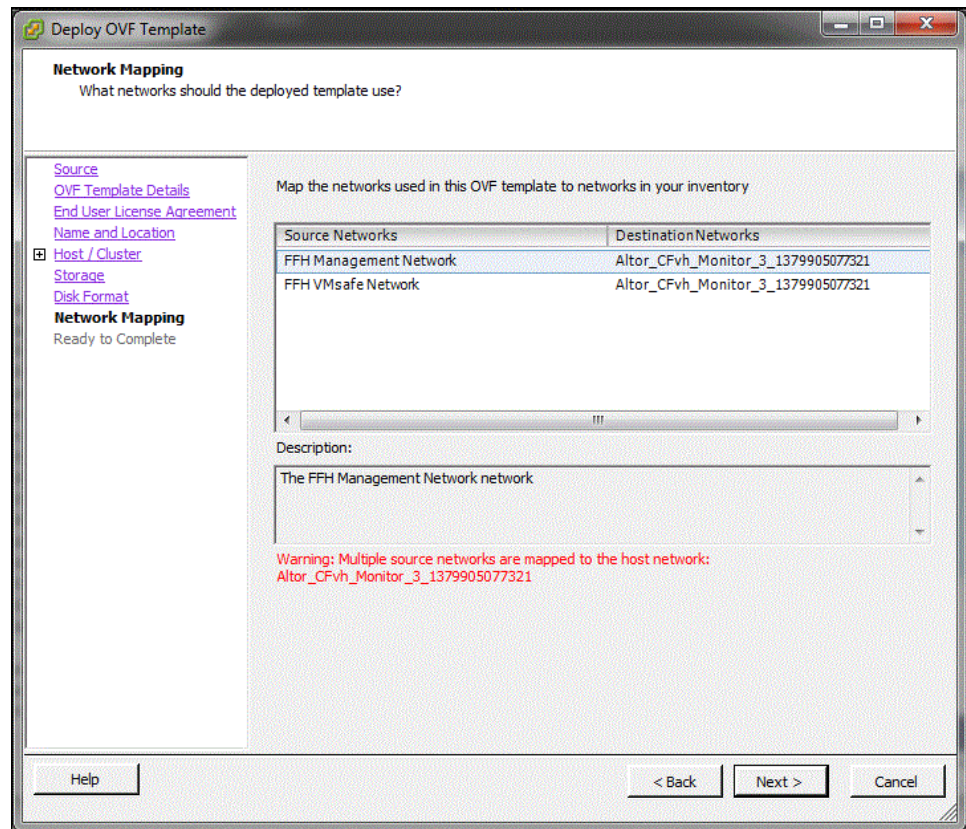
7. Select the datastore. Do not use a read-only datastore. [Figure 5 on page 13.](#)

Figure 5: Selecting the Storage



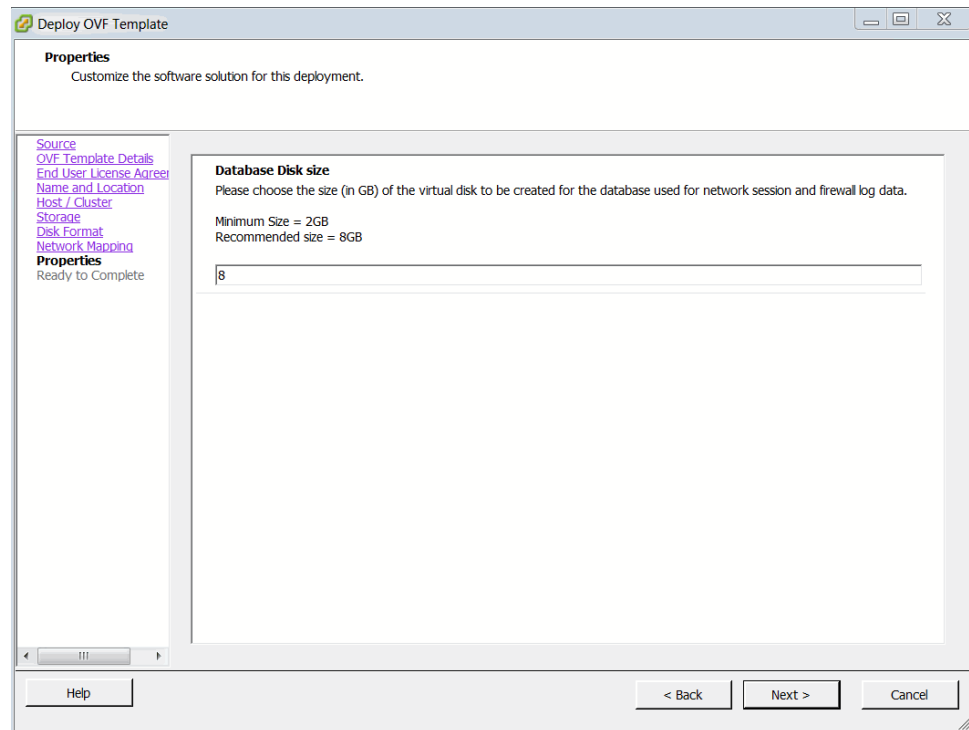
8. Select the disk format. Accept the thick provisioned format default. Thick provisioning preallocates all required space for the product.
9. Map the networks. Set the Firefly Host management network to a destination network that is accessible to vCenter and the Firefly Host Dashboard. See [Figure 6 on page 14](#).

Figure 6: Mapping the Firefly Host Management Networks



10. Specify the size of the database to use for storing Firefly Host files.
The database stores network connection records and firewall logs.
See [Figure 7 on page 15](#).

Figure 7: Specifying the Database Disk Size

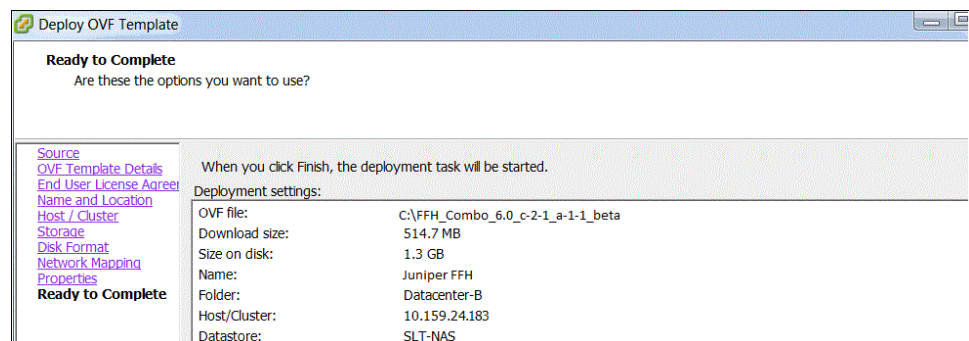


The default disk size is 8.0 GB. In a typical environment that includes 5 to 10 ESX/ESXi hosts, a database of this size can accommodate data accumulated over several months. However, for your environment you might want to deploy a database that is larger than 8.0 GB.

You can increase the database size later if you find that the current space is not adequate. Although there is no hard-coded limit, we recommend restricting the size to less than 75 GB.

11. Verify that the configuration is correct, and click **Finish** to complete the deployment. See [Figure 8 on page 15](#).

Figure 8: Verifying That the Configuration Is Correct

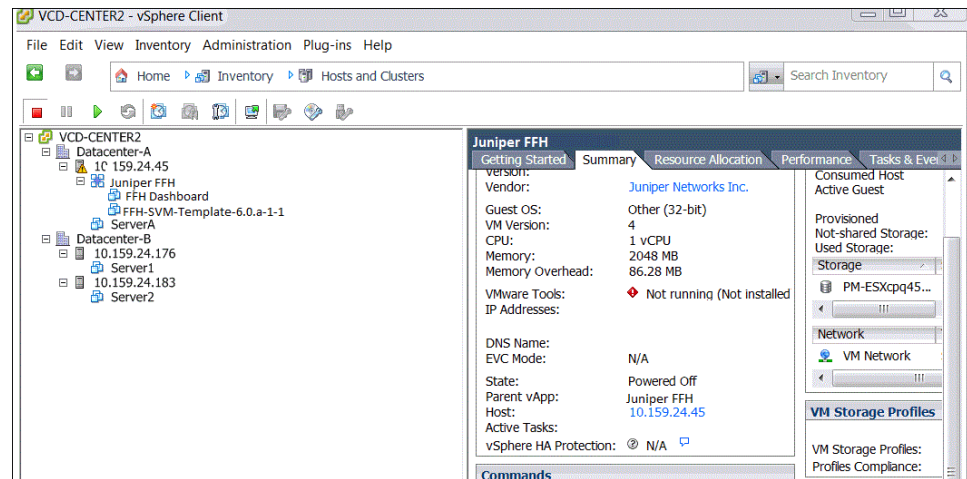


The Virtual Appliance Wizard downloads the files and inserts the Firefly Host VMs as a single virtual appliance (vApp) into the VMware infrastructure.

When the OVA import is completed, the vCenter includes the vApp containing both the Firefly Host Dashboard and the Firefly Host VM template components.

12. Expand the appliance called Juniper Firefly Host 6.0 to display the Firefly Host Dashboard and the Firefly Host VM. See [Figure 9 on page 16](#).

Figure 9: Displaying the Firefly Host Appliance Components



Move the two Firefly Host VMs out from the vAPP. Afterward you can delete the vApp if you choose to, but it is not necessary.



NOTE: Firefly Host uses the VMware vApp deployment feature as a vehicle to deliver multiple VMs in the same OVA file. The vApp structure is redundant after it is used for deployment, and therefore you can delete it. However, do not delete the vApp without first having moved the Firefly Host VMs out from it. If you do, the newly created Firefly Host VMs would be deleted when you delete the vApp.

After you remove the Firefly Host VMs from the vApp:

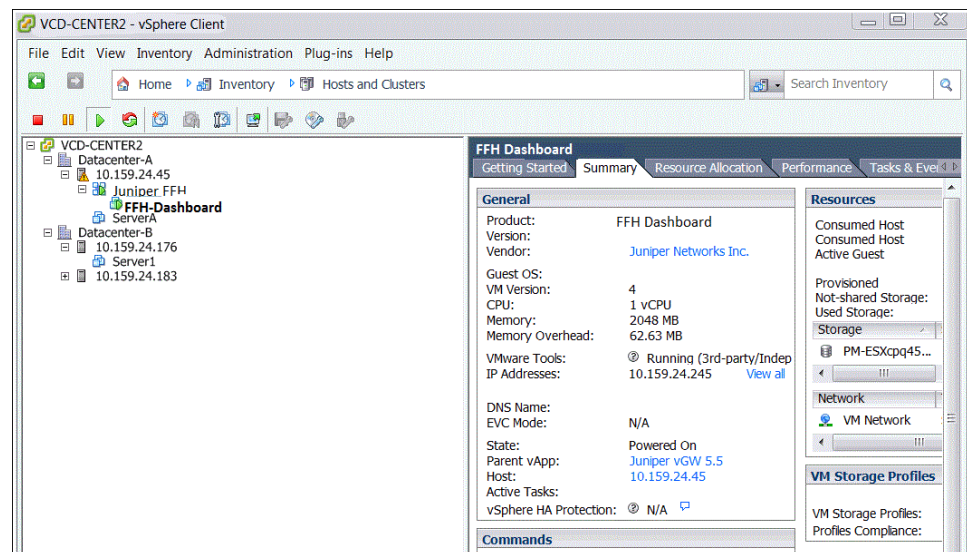
- a. Convert the Firefly Host-Firefly Host VM-Template VM to a template that the Firefly Host Dashboard and installer can use to instantiate a Firefly Host VM on each ESX/ESXi host to be secured.

Right-click the template, select **Template**, and select **Convert to Template**.

- b. Right-click the Firefly Host Dashboard and power it on. [Figure 10 on page 17](#) shows the vCenter summary information for the Firefly Host Dashboard.

[Figure 10 on page 17](#) shows the vCenter summary information for the Firefly Host Dashboard.

Figure 10: Firefly Host Dashboard Summary Tab in vCenter



Related Documentation

- [Firefly Host Prerequisites and Resource Requirements for the VMware Environment](#)
- [Understanding Firefly Host on page 3](#)
- [Understanding the VMware Infrastructure and Firefly Host](#)
- [Using the OVA Single File Method to Integrate the Firefly Host Dashboard with VMware on page 17](#)
- [Using the OVA Single File Method to Integrate the Firefly Host VM with VMware on page 19](#)
- [Understanding the Firefly Host Dashboard](#)
- [Understanding the Firefly Host VM](#)

Using the OVA Single File Method to Integrate the Firefly Host Dashboard with VMware

This topic explains how to download and deploy a single OVA file containing the Firefly Host Dashboard.

To download an OVA file containing the Firefly Host Dashboard appliance and deploy it:

1. Download the Juniper Networks Firefly Host OVA file.
 - a. Navigate to the Juniper Networks Support page.
 - b. Select **Software Downloads** from the Support box in the left column.
 - c. Select **Firefly Host (Altor)** in the Security pane.

- d. Select the **Software** tab.
- e. Click **DashboardFirefly Host 6.0**, and log in to the site to download the file.
2. Load the OVA file for the Firefly Host Dashboard using the vSphere 4.x client (File > Deploy OVF Template), and enter the name of the OVA download file in the Deploy from file or URL box.

For example, enter: `c:\temp\DashboardFireflyHost.ova`.

3. Follow the Virtual Appliance Wizard process, and select the appropriate options for your environment.
4. Click **Finish** to download the files and integrate the Firefly Host Dashboard with the VMware infrastructure.

After the Firefly Host Dashboard import process is completed, you must add a virtual hard disk for it.



NOTE: This step is not required for the bundled approach because it is done automatically.

The default disk size is 8.0 GB. In a typical environment that includes 5 to 10 ESX/ESXi hosts, a database of this size can accommodate data accumulated over several months.

For your environment you might want to deploy a database larger than 8.0 GB. Note that you can increase the database size later if you find that the current space is not adequate. The disk should not be thin-provisioned.

5. Add a disk to be used as the datastore:
 - a. Select **Firefly Host Dashboard**.
 - b. Select the **Summary** tab, and click **Edit Settings > Add a Hard Disk virtual device**.

This disk is used for the database that stores network connection records and firewall logs. Select a NAS device so that VMotion can be used to migrate the datastore.

6. Power on the Firefly Host Dashboard.

Related Documentation

- *Firefly Host Prerequisites and Resource Requirements for the VMware Environment*
- [Understanding Firefly Host on page 3](#)
- *Understanding the VMware Infrastructure and Firefly Host*
- [Using the OVA Single File Method to Integrate the Firefly Host VM with VMware on page 19](#)
- *Understanding the Firefly Host Dashboard*
- *Understanding the Firefly Host VM*

Using the OVA Single File Method to Integrate the Firefly Host VM with VMware

To download a nonbundled OVA file containing the Firefly Host VM and deploy it:

1. Load the OVA file for the Firefly Host VM using the VMware vSphere Client (File > Deploy OVF Template), and insert the template name Firefly Host-Firefly Host VM-Template in the Deploy from file or URL box. For example, enter **c:\temp\Firefly Host-Firefly Host VM-Template.ova**.

2. Select the appropriate options for your environment in each of the steps presented by the Virtual Appliance Wizard.

Configure the host/cluster, resource pool, and so on, that is appropriate for your environment.

When you are asked for network mapping information, accept the default settings. Firefly Host automatically configures these settings later.

3. When the Virtual Appliance Wizard completes, right-click the resulting VM and select **Template > Convert to Template**.

You can use the resulting template to automate installation of Firefly Host VMs on ESX/ESXi hosts to secure parts of your virtual network. The Firefly Host Dashboard and installer require the template to instantiate the Firefly Host VM on hosts to be secured.

Related Documentation

- *Firefly Host Prerequisites and Resource Requirements for the VMware Environment*
- [Using the OVA Single File Method to Integrate the Firefly Host VM with VMware on page 19.](#)
- [Using the OVA Bundled Method to Integrate Firefly Host with the VMware Infrastructure on page 8](#)
- *Preparing to Integrate Firefly Host with the VMware Environment*

Setting Up Firefly Host

After you download and integrate Firefly Host with the VMware environment and power on the Firefly Host Dashboard, you can configure its basic system parameters. This topic explains how to connect to the Firefly Host Dashboard to configure basic settings. It describes how to use the Firefly Host wizard to configure those settings initially.

This topic includes the following sections:

- [Determining the Firefly Host Dashboard's Default IP Address on page 19](#)
- [Changing or Setting the IP Address for the Firefly Host Dashboard on page 21](#)
- [Connecting to the Firefly Host Dashboard and Configuring Basic Settings on page 23](#)

Determining the Firefly Host Dashboard's Default IP Address

To access the Firefly Host Dashboard, you enter its IP address in a supported Web browser.

When you powered on the Firefly Host Dashboard during Firefly Host integration with VMware, which is described in [“Using the OVA Bundled Method to Integrate Firefly Host with the VMware Infrastructure” on page 8](#), it acquired an IP address that you can view on the vCenter Summary page.

By default, the Firefly Host Dashboard is configured to use IPv4 DHCP to acquire its address. If problems occur and it cannot obtain an IP address in this manner, it tries other methods. In order, these are the three methods that the Firefly Host Dashboard uses in an attempt to obtain an IP address:

- IPv4 DHCP
- IPv6 autoconfiguration

With stateless IPv6 autoconfiguration, the Firefly Host Dashboard acquires its IPv6 address automatically without the intervention of a DHCP server.

- IPv6 DHCPv6



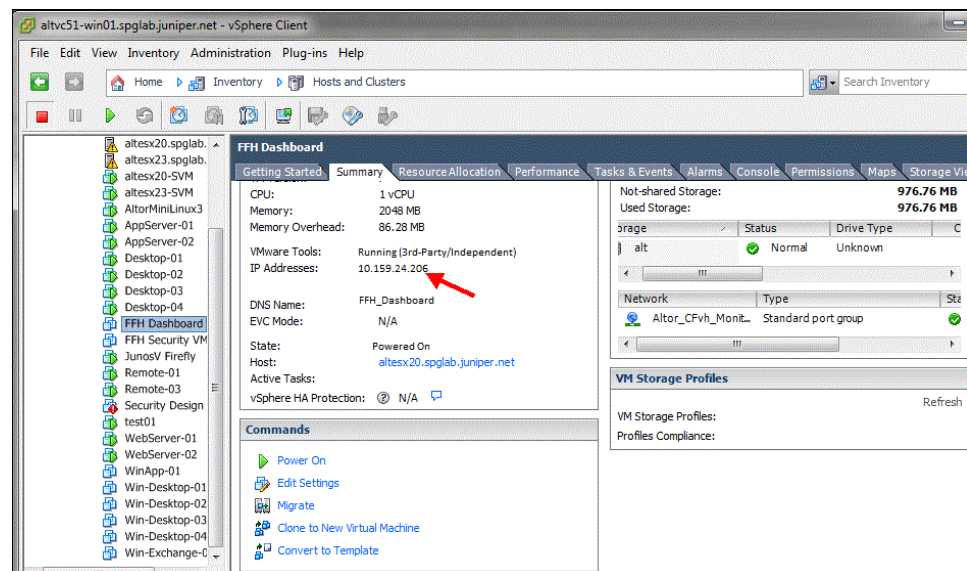
NOTE: If DHCP is not available on the Firefly Host Dashboard network, you can log into the console using admin for both the username and the password. Type config network at the command prompt and proceed through the options to assign an IP address. After an IP address is set—whether DHCP or static, you can access the Firefly Host Dashboard through a Web browser.

To view the IP address bound to the Firefly Host Dashboard:

1. Launch the VMware vSphere Client, and select the Firefly Host Dashboard icon on the left navigation pane.
2. Select the **Summary** tab.

The IP address that was acquired appears in the IP Addresses: field. See [Figure 11 on page 21](#).

Figure 11: Viewing the Firefly Host Dashboard IP Address in VMware



After you have obtained the IP address, follow the instructions in [“Connecting to the Firefly Host Dashboard and Configuring Basic Settings”](#) on page 23 to configure the basic settings.

Changing or Setting the IP Address for the Firefly Host Dashboard

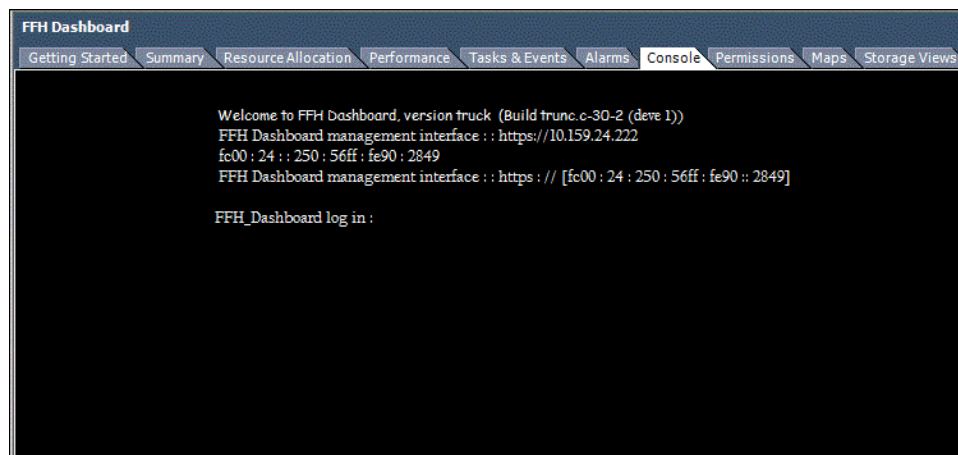
You can use the Firefly Host command-line interface (CLI) to set the IP address for the Firefly Host Dashboard.

To use the Firefly Host CLI from the vCenter console:

1. Launch the VMware vSphere Client.
2. Right-click the Firefly Host Dashboard icon on the left navigation panel to display a list of options.
3. Select the third option on the list, **Open Console**. Alternatively you can select the **Console** tab, as shown in [Figure 12 on page 22](#).

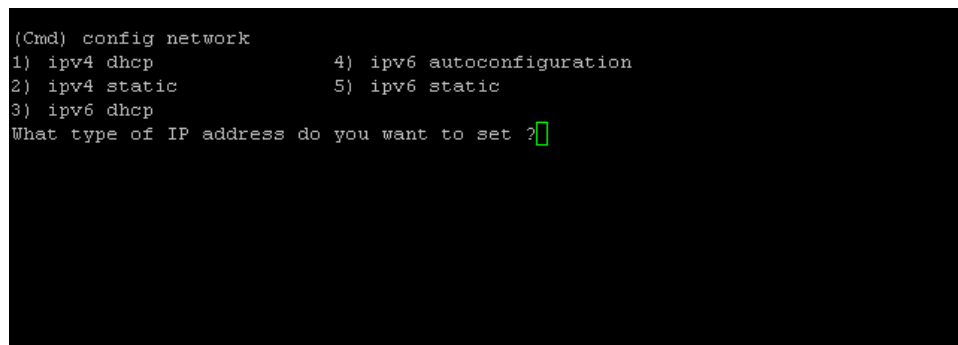
The console window appears.

Figure 12: Firefly Host Dashboard IP Addresses on the Firefly Host CLI Console



4. At the CLI prompt enter **config network**. Enter **admin** for both the username and password. In this mode you can configure the IP address for the Firefly Host Dashboard. You can specify an IP address for either IP protocol family. See [Figure 13 on page 22](#).

Figure 13: Configuring an IP Address for the Firefly Host Dashboard



5. In response to the prompt **What type of IP address do you want to set?** enter the number preceding the type of IP address that you want to be assigned to the Firefly Host Dashboard and how it is to be acquired.
For example, the administrator might enter **4** for **4) ipv6 autoconfiguration**.
6. The Firefly Host CLI gives you the opportunity to cancel by presenting the prompt **Are you sure?**. If you enter **y** for **yes**, Firefly Host shuts down the interface and brings it back up with the new IP address.

Connecting to the Firefly Host Dashboard and Configuring Basic Settings

This section explains how to set up the Firefly Host Dashboard initially.

1. Using a supported Web browser, connect to the Firefly Host Dashboard management interface through HTTPS. Enter the IP address of the Firefly Host Dashboard in the Web browser.

This is the IP address that was assigned when you powered on the Firefly Host Dashboard.

Firefly Host supports the following Web browsers:

- Microsoft Internet Explorer 7, 8, and 9
- Mozilla Firefox 3 or later

2. Enter **admin** for both the username and password. See [Figure 14 on page 23](#).

Figure 14: Logging In to the Firefly Host Dashboard



Firefly Host Dashboard

Username: admin

Password: admin

Submit

Copyright © 2013 Juniper Networks, Inc. | All rights reserved | [Legal Notices](#) | [Privacy](#)

3. Read the information message, and review the process overview shown in the Wizard Progress pane. See [Figure 15 on page 24](#).

Figure 15: Firefly Host Installation Wizard Overview

4. Change the default Firefly Host global administrator account password—admin—that you used to log in.

You must change the default password. See [Figure 16 on page 24](#). Store the new password in a secure location. It is difficult to recover a lost or forgotten global administrator account password. If you wish, you can change the password that you specify here later, but to do so you must enter your current password, which would be the one that you configured here.



TIP: You can integrate administration accounts with the Firefly Host Dashboard after the installation is completed. For information on how to do that later, see [“Adding New Firefly Host Administrator Definitions, Permissions, and Authentication Using the Settings Module” on page 59](#).

Figure 16: Changing the Default Password

5. Configure networking parameters for the Firefly Host Dashboard.



NOTE: If you changed the IP address, you must log in to the system again. Changes to the IP address take effect immediately.

Set the correct destination network for the Firefly Host Dashboard and leave the VMsafe Network unchanged. At this point you can configure other network information for the Firefly Host Dashboard, such as whether to use dual stack for it and how it obtains its management interface addresses.

A dual-stack device can connect to an IPv4-only device or an IPv6-only device, or it can connect to another device that implements dual stack.

For its management interface addressing mode, either accept the default dual stack values of DHCP for IPv4 and DHCPv6 for IPv6 or change the values by selecting:

- IPv4
 - DHCP (Default): To obtain an IPv4 address, by default the Firefly Host Dashboard is configured to use DHCP. You do not need to specify additional information.
 - Static IP. If you select **Static IP**, you must specify a static IPv4 address and its network mask routing prefix, and the default gateway to assign to the Firefly Host Dashboard.
- IPv6
 - DHCPv6 (Default): To obtain an IPv6 address, by default the Firefly Host Dashboard is configured to use DHCPv6. You do not need to specify additional information.
 - Autoconfiguration. If you select **Autoconfiguration**, stateless address autoconfiguration is used to obtain the IPv6 address. It allows network devices attached to an IPv6 network to automatically acquire IP addresses and connect to the Internet without intermediate interaction with a DHCPv6 server.
 - Static IP. If you select **Static IP**, you must specify a static IPv6 address, including the IPv6 address prefix (the initial bits of the address that denote the network address, akin to a netmask), and the default gateway to use for it.



NOTE: By default, a dual stack Firefly Host Dashboard communicates with a Firefly Host VM using the IPv4 protocol. However, you can use the Firefly Host CLI to change the default IP protocol used by setting the `center.dual.stack.default.communication.ipv4` parameter to false.

center.dual.stack.default.communication.ipv4=false

By default, this parameter is set to true.

This parameter is relevant only if the Firefly Host Dashboard is configured for dual stack and one or more Firefly Host VMs is also configured for dual stack. In all other cases, the protocol used is the one that is common to both the Firefly Host Dashboard and the Firefly Host VM, and this parameter is irrelevant.

If you do not want the Firefly Host Dashboard to be configured for dual stack which is its default configuration, you can change the configuration in the following way:

- To use only IPv4 for Firefly Host Dashboard management communication with its Firefly Host VMs, disable IPv6. On the displayed list for the IPv6: box, select **Disabled**.
- To use only IPv6 for Firefly Host Dashboard management communication with its Firefly Host VMs, disable IPv4. On the displayed list for the IPv4: box, select **Disabled**.

How you configure addressing for the Firefly Host Dashboard management center affects its communication with its Firefly Host VMs in the following way:

- In an environment in which both the Firefly Host Dashboard and the Firefly Host VM are configured for dual stack, communication problems between the Firefly Host Dashboard management interface and that of the Firefly Host VMs should not occur.
- In an environment in which the Firefly Host Dashboard is configured for dual stack but one or more of the Firefly Host VMs is not, communication problems between their management interfaces should not occur.
- In an environment in which the Firefly Host Dashboard is not configured for dual stack but all of the Firefly Host VMs are, communication problems between their management interfaces should not occur.
- In an environment in which neither the Firefly Host Dashboard nor one or more Firefly Host VM is configured for dual stack, in any case in which the IP address type of the management interfaces of the Firefly Host Dashboard and the Firefly Host VM differ—one might belong to the IPv6 protocol family and the other to the IPv4 protocol family—communication problems will occur. The Firefly Host Dashboard will not be able to connect to the Firefly Host VM to carry out any procedures.

You can make these changes during the installation process, as shown [Figure 17 on page 26](#), or you can make them later, after you complete the initial configuration.

Figure 17: Configuring Network Settings for the Firefly Host Dashboard

Wizard Progress

1. Introduction
2. Change Default Password
3. **Network Setup**
4. Time Configuration
5. Product License
6. Virtual Center Settings
7. Reports
8. Firefly Host VM Template Selection
9. Summary

Please configure the network settings for the **Firefly Host management server**.

The Firefly Host Dashboard IP address must stay the same, to allow the Firefly Host firewalls to be managed. It is recommended to use a static IP address so it doesn't change.

Network Configuration

Please specify fully qualified domain name (e.g. DashboardFireflyHost.company.com)

Host Name:

DNS Settings: ☒ Use DHCP to Get DNS

Primary DNS Server:

Secondary DNS Server:

Search Domain:

Interface 1

IPv4: IPv6:

IP Address:

Netmask: prefix

Default Gateway:

MAC Address:

[Prev Step](#) [Next Step](#)

In the latter case, you use the Settings module Appliance Settings > Network Settings page, which is the same page shown in [Figure 17 on page 26](#), only it is arrived at differently. For additional details, see *Configuring the Firefly Host Network Settings*.



NOTE: If you changed the IP address, you must log in to the system again. Changes to the IP address take effect immediately.

6. Set the system time.

Set the correct time zone, and then specify the NTP servers for your environment. See [Figure 18 on page 27](#).

Firefly Host components require that the correct system time be set on all ESX/ESXi hosts.

- If you do not have an NTP server, you can use a predefined server.
- If you do not have outbound Internet access to contact the NTP servers and you do not have an internal NTP server, then you must clear all entries shown in this window and set the time manually.

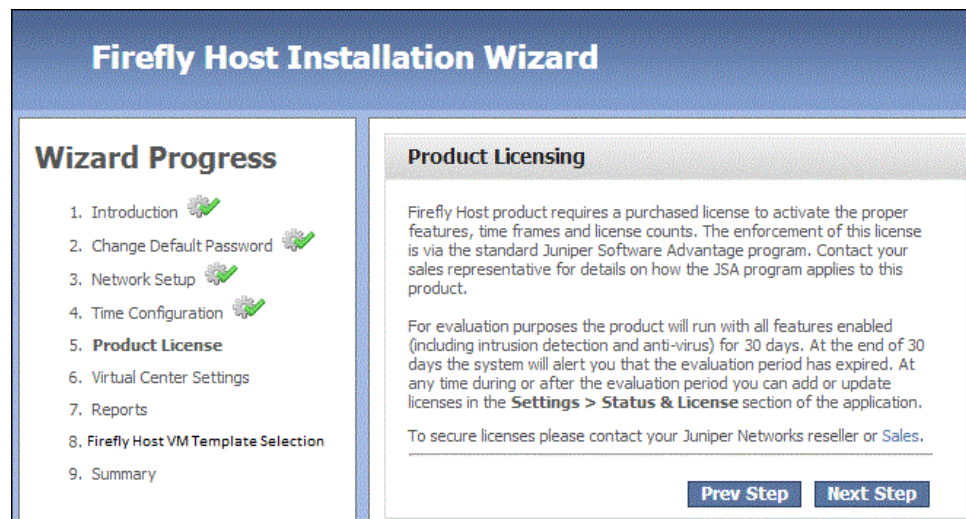
To do this, you use the Firefly Host CLI that you run from the vCenter console.

Figure 18: Configuring the Time Server

At this point, the wizard determines if the database disk was created and initialized properly. If you have not defined the database disk properly, the wizard displays a message.

The next screen explains Product Licensing. On the installation wizard, there is no option to enter purchased license information directly. See [Figure 19 on page 28](#).

Figure 19: Firefly Host Installation Wizard displaying Product Licensing



Click **Next Step**.

Licenses can be added after wizard completion. For additional information on Firefly Host licenses, see

- *Understanding Licenses for Firefly Host*
- *Viewing Status and License Information Using the Firefly Host Settings Module*
- *Adding and Managing Firefly Host Licenses*

7. Select the management domain, or scope, for this Firefly Host Dashboard to manage, and verify that the Firefly Host Dashboard can establish a connection to vCenter. Then click **Next Step**.

For the Firefly Host to query the vCenter for the VM inventory and other operations, you must have an account with read/write access.

- If the connection works properly, a message appears stating that the login was successful, and it identifies the number of ESX/ESXi hosts and VMs that were discovered.
- If there is a connection issue, you are notified. In that case, ensure that you have the correct credentials and that IP connectivity to the vCenter exists.

In some cases, you may need to insert another vNIC into the Firefly Host Dashboard. You must connect that vNIC to the network that connects to the vCenter server.

To configure a management domain:

- If this Firefly Host Dashboard will manage all of the vCenter's resources, select **Entire vCenter**.
- If this Firefly Host Dashboard will participate in a Split-Center configuration, select the data centers or the host clusters for this Firefly Host Dashboard to manage. To select host clusters, first select the data center that the host clusters belong to.

For information on Split-Center and its configuration options, see *Understanding the Firefly Host Split-Center Feature*.

Figure 21 on page 30 shows that this Firefly Host Dashboard is configured to manage two host clusters in Datacenter-B.

Figure 20: Firefly Host Dashboard vCenter Integration

The screenshot displays the Firefly Host Dashboard vCenter Integration settings page. The interface includes a top navigation bar with icons for Home, Network, Firewall, IDS, Intrusion, Compliance, Reports, and Settings. A left sidebar contains a tree view for Application Settings (Status & License, vCenter Integration, Multi-Center, Installation, Install Settings, Administrators, Active Directory, Machines, High Availability, E-Mail and Reporting, Registry Values), Security Settings (Global, Firefly Host VM Settings, IDS Settings, IDS Signatures, Alerting, Protocols, Groups, Networks, SRX Zones), and Appliance Settings (Updates, Network Settings, Proxy Settings). The main content area is divided into several sections:

- vCenter Settings:** Contains fields for Server Name or IP Address (172.30.169.35), Username (v1-trunk), and Password (masked). A note states: "Notice! Changing vCenter Settings is not recommended while performing any configuration action that interacts with the vCenter, such as install, uninstall, or update of the Firefly Host or a firewall." Below these fields is a section for "Select a scope for your Firefly Host" with radio buttons for Entire vCenter (selected), Datacenters, and Clusters. A "Save" button is at the bottom.
- Update VMs:** Includes a checkbox for "Update IP addresses as they change in vCenter. If not selected, IP addresses will not be changed once they are initially retrieved or set manually." An "Update" button is present.
- Firefly Host management server plugin:** Contains "Register" and "Unregister" buttons. A note explains: "Register or unregister vCenter Client plugin. Registration allows access to Firefly Host management server from the vCenter client and allows some Firefly Host management server actions to surface in vCenter." Below the buttons, it says "Register Firefly Host management server as a vCenter Client plugin." and "Unregister Firefly Host management server plugin."
- Deleted VMs and Groups:** Includes a checkbox for "Hide deleted VMs from view in the Inventory Tree" and a field for "Delay before purging deleted VMs and Groups in days (-1 = never):" set to 30. A "Save" button is at the bottom.
- Automatic Startup:** Includes a checkbox for "Automatic Firefly Host management server and Security VM startup" and a "Save" button.
- Synchronize machine name:** Includes a checkbox for "Sync name with vCenter" and a "Save" button.

Figure 21: Configuring the Firefly Host Dashboard vCenter Settings

Firefly Host Installation Wizard

Wizard Progress

1. Introduction
2. Change Default Password
3. Network Setup
4. Time Configuration
5. Product License
6. **Virtual Center Settings**
7. Reports
8. Firefly Host VM Template Selection
9. Summary

vCenter Settings

Establish connection to vCenter. [more](#)

Server Name or IP Address:

Username:

Password:

Select a scope for your Dashboard Firefly Host. [more](#)

☐ Entire vCenter
 ☐ Datacenters
 ☒ Clusters

Datacenter:

☒ 10.159.24.183 (Host)
 ☒ 10.159.24.176 (Host)

[Prev Step](#) [Next Step](#)

8. (Optional) Configure the e-mail server to use to send reports.

Using this option, you can configure Firefly Host to send reports on system activity through e-mail. Additionally, you can configure basic information used in the report, such as the subject and the content of standard report e-mail. After you configure these parameters, you can test the e-mail connection.

You can also use the Settings module Firefly HostApplication Settings > E-Mail and Reporting page to configure this information after the installation is completed.

9. Define a template to use to instantiate Firefly Host VMs on ESX/ESXi hosts to secure them.

If you have not downloaded the Firefly Host VM and converted it to a template, do so now. You can define how the Firefly Host responds when a VM tries to connect to an ESX/ESXi host on which the Firefly Host module cannot be loaded or is not present.

You can define whether monitoring is used. Unless you plan to deploy the product in monitor mode, leave the Monitoring-only option for VMsafe unchecked. Also, unless you want to drop network traffic to VMs when the Firefly Host fails to load, you should leave the default option of **Allow All traffic** selected. You can change this option later if you want to change the behavior for one or more VMs.

10. Click **Done** to complete the Firefly Host Dashboard setup.

The Firefly Host Dashboard appears. You use this module to deploy Firefly Host VMs to the ESX/ESXi hosts to be secured, to configure other Firefly Host features, and to view specific and summary results information and reports.

- Related Documentation**
- *Preparing to Integrate Firefly Host with the VMware Environment*
 - [Understanding Firefly Host on page 3](#)
 - *Understanding the Firefly Host Settings Module*
 - *Understanding the Firefly Host Main Module*

Integrating the Firefly Host with VMware Using the Settings Module

This topic explains the vCenter Integration settings page that allows you to configure parameters that control the interaction between Firefly Host and VMware. It covers how to change the Firefly Host VMware settings, direct VMware to update the Firefly Host Dashboard with VMs inventory information, change the settings that control how deleted VMs and information about them is handled, and how to integrate the Firefly Host with the VMware infrastructure.

You can also use it to change the management domain, or scope, for the Firefly Host Dashboard, after you configure it initially when you install the product. The management domain specifies the data centers and host clusters in the vCenter that your Firefly Host Dashboard manages.

The Firefly Host Dashboard uses the VMware Virtual Infrastructure APIs to:

- Obtain VM Inventory information
- Determine resource utilization status
- Determine events affecting the VMs

The account used for vCenter must have read-write access to the VMware Infrastructure. You can use a custom account created in VMware; this approach makes it easier to identify and monitor activities that change. In any case, the account must have administrator privileges.

The Settings module Firefly Host Application Settings > vCenter Integration page contains the following panes and their settings for which you either enter information or whose values you can change:

- **vCenter Settings**—Login information required for the Firefly Host Dashboard to communicate with the VMware vCenter and for administrator access to the vCenter. Specify the following information:
 - **Server Name or IP Address**:—Name of the vCenter or its IPv4 or IPv6 address.
 - **Username**: and **Password**:—Your administrator authentication information for accessing vCenter.
- **Scope**—Allows you to specify the vCenter's data centers and host clusters to be managed by your Firefly Host Dashboard. You set this value initially when you install the product. See [“Setting Up Firefly Host” on page 19](#) for details on initially setting the management domain.

You use this pane to change the management domain scope. The scope for your Firefly Host Dashboard can be:

- **Entire vCenter**—In this case, the Firefly Host Dashboard is able to access and manage all VMs and other entities in all data centers in the vCenter.

To use this scope, select **Entire vCenter**.

- **Datacenter**—A subset of data centers in the vCenter.

In this case, the Firefly Host Dashboard is able to access and manage only the VMs and other entities in the selected data centers.

To use this scope:

1. Select **Datacenters**.

Firefly Host displays all of the vCenter's data centers.



NOTE: To update the list of data centers at any time to show changes—datacenters that might have been added or removed—click **Refresh**.

2. Select the data centers for your Firefly Host Dashboard to manage.

Ensure that each data center is assigned to only one Firefly Host Dashboard. Otherwise, unexpected consequences can occur.

For an overview of the Split-Center feature, see *Understanding the Firefly Host Split-Center Feature*.

3. Click **Save**.

- **Clusters**—A subset of host clusters in a data center. In this case, the Firefly Host Dashboard is able to access only the VMs and other entities on the selected host clusters.



NOTE: All of the host clusters that you select to belong to a management domain (scope) must be in the *same* data center. You cannot include host clusters from two or more different data centers in the scope.

To use the Clusters scope:

1. Click **Clusters** in the *Select a scope for your Firefly Host Dashboard* area.

In response, Firefly Host displays a list of available data centers.

2. Select a data center from the displayed list whose host clusters you want the Firefly Host Dashboard to manage.
 - a. Click the arrow at the end of the box beside **Datacenter:** to display a list of data centers for the vCenter.

- b. Click the data center whose cluster(s)/host(s) you want your Firefly Host Dashboard to manage.

Firefly Host displays a list of cluster(s)/host(s) for the data center that you selected.

3. Select the check box before the names of the cluster(s)/host(s) that you want to include in your management domain.
4. Click **Save**.



NOTE: Ensure that each host cluster is assigned to only one Firefly Host Dashboard. Otherwise, unexpected consequences can occur.

You can change the cluster selection at any time. However, when you change the cluster scope, either of the following conditions can occur:

- Some Firefly Host VMs could become unmanaged—This can occur when you remove a cluster from the list of selected clusters. Any Firefly Host VM installed on an ESX/ESXi host that belongs to the removed cluster will no longer be accessible, and therefore it is no longer managed by the Firefly Host VM.
- Some unmanaged Firefly Host VMs could become accessible—If ESX/ESXi hosts that belong to a cluster that you add to your Firefly Host Dashboard management domain had a Firefly Host VM installed on them by a different Firefly Host Dashboard, you could gain access to the Firefly Host VMs. It is possible and important to gain access to an unmanaged Firefly Host VM when you add its host cluster to your Firefly Host VMs management domain for the following reason.

When a Firefly Host VM becomes inaccessible because of cluster or datacenter selection changes its original Firefly Host Dashboard, its operational state might be compromised unless it is imported into another Firefly Host Dashboard. This is because the Firefly Host VM continues to try to communicate with its original Firefly Host Dashboard, which no longer recognizes it as a managed.

To view a list of unmanaged SVMs and render them manageable again:

1. Display the Settings module > Firefly Host VM Settings page.

The unmanaged Firefly Host VMs are identified by a gray triangle status indicator.

2. To make a Firefly Host VM manageable again, click its row to select it.
3. Click **Import**.

After you save the selection, Firefly Host synchronizes all objects from vCenter. When it completes the process, Firefly Host displays a message indicating the ESX/ESXi hosts and the VMs that were found.

- Deleted VMs and Groups—Firefly Host can show information about any VMs and groups of VMs that it has encountered across time even if the VMs were deleted in VMware's vCenter system repository. This capability allows you to keep historic traffic records.

It allows you to see all activity occurring in VMware across time. The VM's information persistency in the Firefly Host Dashboard can reveal attempts by a malicious administrator or hacker to bring up a VM, perform an unauthorized activity, and then delete the VM to hide their tracks.

You can change how Firefly Host handles VMs that are deleted from vCenter using the following settings:

- **Hide deleted VMs from view in the Inventory Tree** check box.

By default, the “Hide deleted VMs from view in the Inventory Tree” check box is selected. However, if you do not want the deleted VMs appearing in the VM Tree, you can clear this menu item and they will be hidden from view.

The deleted VMs are still available to view again. By selecting the check box, they are again made visible in the VM Tree.

- **Delay before purging deleted VMs and Groups in days (-1 = never):** setting.

Enter the number of days after which Firefly Host should purge deleted VMs and groups of VMs that have been deleted from vCenter. After that time, the VMs and all information pertaining to them is permanently deleted from Firefly Host. For example, if you do not change the default value of 30 days and a VM is deleted in vCenter, at any time up to 30 days Firefly Host is still able to make the VM information visible again (unhide). On the 31st day, the VM and all information pertaining to it is permanently removed from Firefly Host.

- **Firefly Host management server plug-in**—Use this button to install the Firefly Host plug-in into the vCenter interface.
 - To install the plug-in, click **Register**.
 - To view and use the plug-in, in the **vSphere Client interface** select **Home** -> **Solutions and Applications**.
 - To remove the Firefly Host Management Plug-in, click **Unregister**.
- **Automatic Startup of the Firefly Host Dashboard and Firewall**—Use this setting to enable or disable the startup of Firefly Host components when an ESX/ESXi system reboots. Firefly Host components are set to start up automatically by default.
- **Synchronize machine name**—Changing the name of a VM in vCenter by default causes the name of the equivalent VM object in Firefly Host Dashboard to be changed to the same value. To override this setting, clear the value for this item.

For example, security administrators might want to use this override feature if they are not using the same naming convention as the VM team. The ability to override the default behavior is also useful if security administrators have created dynamic security policies using the name of the VM, and they do not want them affected by simple name changes in the vCenter.

Related Documentation

- [Understanding Firefly Host on page 3](#)
- *Understanding the VMware Infrastructure and Firefly Host*
- *Understanding the Firefly Host Dashboard*

- *About the Firefly Host Dashboard Tree*

Installing Firefly Host VMs on ESX/ESXi Hosts

A Firefly Host VM protects and secures virtual machines (VMs) on an ESX/ESXi host where it is installed. The Firefly Host VM acts as a conduit to the Firefly Host Module which it inserts into the hypervisor of the host that it protects when it is installed. The Firefly Host Dashboard pushes the appropriate security policy to the Firefly Host VM which in turn inserts it into the Firefly Host Module. All connections are processed and firewall security is enforced in the Firefly Host module. In other words, virtualized network traffic is secured and analyzed against the security policy in the Firefly Host Module.

You deploy a Firefly Host VM to each ESX/ESXi host in your environment that you want Firefly Host to secure and monitor. The Firefly Host VM protects VMs on that host and it gathers information about network traffic. It also maintains policy and logging information.

Securing an ESX/ESXi host with a Firefly Host VM entails the following two parts:

- First you must install a Firefly Host VM on the ESX/ESXi host to be secured. It is during this process that the Firefly Host VM inserts the Firefly Host module into the hypervisor of the ESX/ESXi host. This topic covers that process.
- Next you must select the VMs on the secured host that you want Firefly Host to protect with a firewall policy and other features. The Firefly Host VM obtains the policy for the VM from the Firefly Host Dashboard and provides the Firefly Host (hypervisor) module with it.

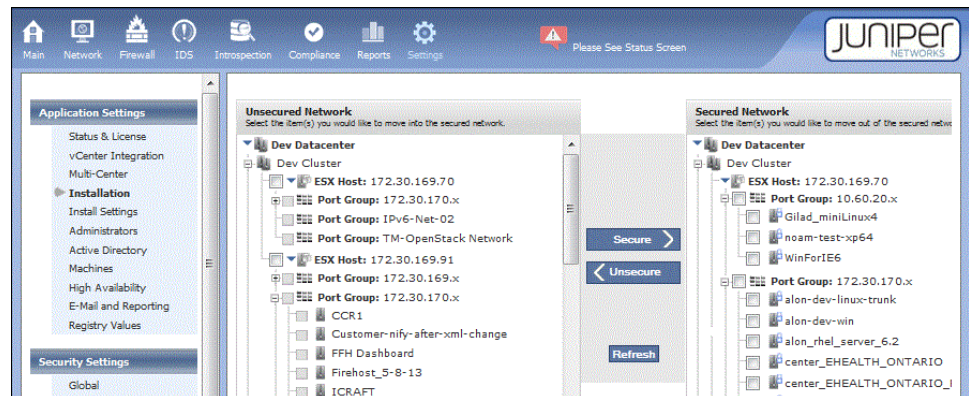
See [“Securing and Unsecuring Virtual Machines Using the Firefly Host Dashboard” on page 73](#) for details on the second part of the process.

To install the Firefly Host VM on an ESX/ESXi host:

1. Select the Settings module **Firefly Host Application Settings > Installation** page.
2. In the **Unsecured Network** pane, select the host in the data center that you want to secure with Firefly Host. See [Figure 22 on page 36](#).

You can secure only one host at a time.

Figure 22: Securing an ESX/ESXi Host With a Firefly Host VM

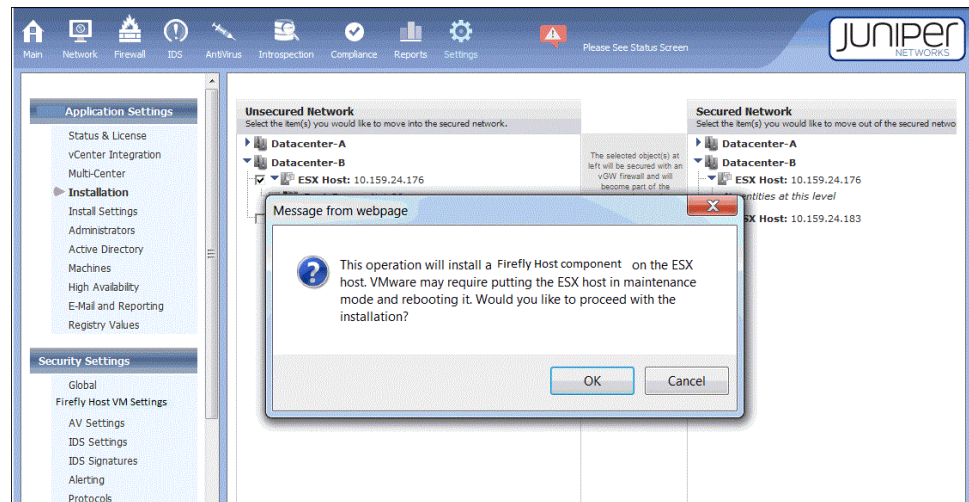


An empty check box appears before each host that is able to run the Firefly Host module. These hosts are not yet protected, but the check box indicates that you can secure them.

3. Click **Secure**.

After you initiate the installation process, a message is displayed indicating that VMware might require putting the ESX/ESXi host into maintenance mode and rebooting it. See [Figure 23 on page 36](#). Note that the message shown in this figure might differ somewhat depending on the Firefly Host version that you are installing.

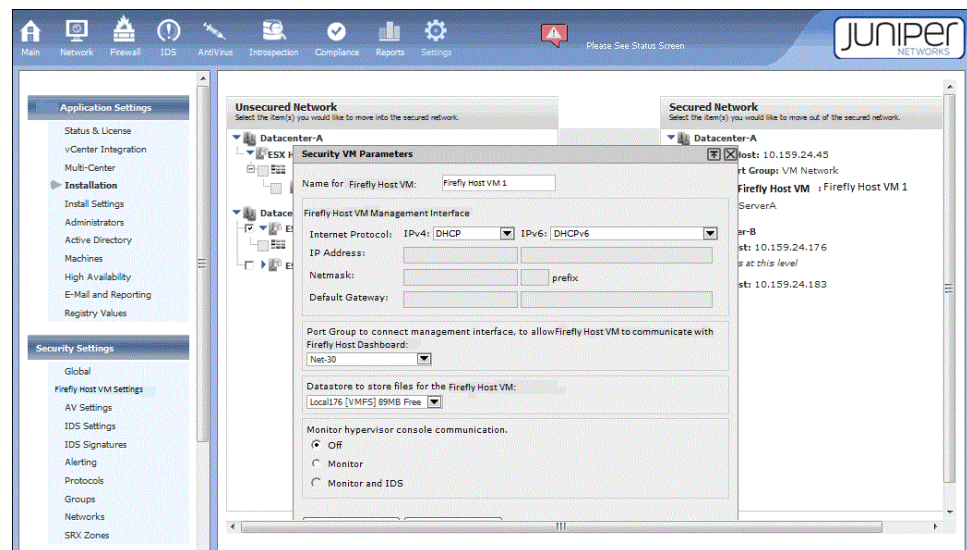
Figure 23: Installing a Firefly Host VM on an ESX/ESXi Host



4. Click **OK**.

A dialog box is displayed allowing you to enter a name and specify other parameters for the Firefly Host VM. See [Figure 24 on page 37](#).

Figure 24: Specifying Firefly Host Security Parameters During Installation



Specify or select values for the following parameters:

- Enter a name for the Firefly Host VM.
- Select the Firefly Host VM security management interface addressing mode. The Firefly Host Dashboard communicates with the Firefly Host VM management interface based on this addressing mode. This interface must be reachable by the management interface of the Firefly Host Dashboard.

Firefly Host supports both IPv4 and IPv6 address types. As such, the Installation Wizard for Firefly Host VMs allows you to enter information for both types.

Select values for:

- IPv4
 - DHCP (Default): To obtain an IPv4 address, by default the Firefly Host VM is configured to use DHCP. You do not need to specify additional information.
 - Static IP. If you select **Static IP**, you must specify a static IPv4 address and its network mask routing prefix, and the default gateway to assign to the Firefly Host VM.
- IPv6
 - DHCPv6 (Default): To obtain an IPv6 address, by default the Firefly Host VM is configured to use DHCPv6. You do not need to specify additional information.
 - Autoconfiguration. If you select **Autoconfiguration**, stateless address autoconfiguration is used to obtain the IPv6 address. It allows network devices attached to an IPv6 network to automatically acquire IP addresses and connect to the Internet without intermediate interaction with a DHCPv6 server.

- Static IP. If you select **Static IP**, you must specify a static IPv6 address, including the IPv6 address prefix (the initial bits of the address that denote the network address, akin to a netmask), and the default gateway to use for it.

By default, a dual stack Firefly Host Dashboard communicates with a Firefly Host VM using the IPv4 protocol. However, you can use the Firefly Host CLI to change the default IP protocol used by setting the `center.dual.stack.default.communication.ipv4` parameter to false.

`center.dual.stack.default.communication.ipv4=false`

By default, this parameter is set to **true**. This parameter is relevant only if the Firefly Host Dashboard is configured for dual stack and one or more Firefly Host VMs is also configured for dual stack. In all other cases, the protocol used is the one that is common to both the Firefly Host Dashboard and the Firefly Host VM, and this parameter is irrelevant.

You can configure the Firefly Host VM not to use dual stack in the following way:

- To use only IPv4 for Firefly Host Dashboard management communication with this Firefly Host VM, disable IPv6. On the displayed list for the IPv6: box, select **Disabled**.
- To use only IPv6 for Firefly Host Dashboard management communication with this Firefly Host VM, disable IPv4. On the displayed list for the IPv4: box, select **Disabled**.

How you configure addressing for the Firefly Host VM affects its communication with the Firefly Host Dashboard management center. In an environment in which neither the Firefly Host Dashboard nor the Firefly Host VM is configured for dual stack and the IP address types of their management interfaces are not the same, communication problems will occur. (For example, one interface might have an IPv6 address and the other might have an IPv4 address.) The Firefly Host Dashboard will not be able to connect to the Firefly Host VM to carry out any procedures.

- c. Specify the port group to use to connect the Firefly Host VM to the Firefly Host Dashboard.
- d. Specify the data store for the Firefly Host VM.
- e. Specify if the hypervisor communication console should be monitored and if IDS should be used.

The dialog box allows you to enable console (hypervisor) monitoring *or* console monitoring and IDS.

- If you enable console monitoring, Firefly Host monitors network traffic to the hypervisor console vNIC to ensure that inappropriate activity is not occurring.
- If you enable both console monitoring *and* IDS traffic monitoring, network traffic to the hypervisor console is monitored and IDS traffic is mirrored to the IDS engine.



WARNING: To use this option, you must first install an IDS license.

If at this point you do not enable console monitoring and IDS, you can do so later after you install a Firefly Host VM. In that case, you use the Settings module Security Settings > Firefly Host VM Settings Network Monitoring tab and the IDS tab for a particular VM.

f. Click **Secure**.

After you click **Secure**, the Firefly Host associates all virtual NICs (vNICs) for the relevant VMs with the Firefly Host module.

VMware requires that the vNICs be disconnected and reconnected through a suspend and resume process. (VMs do not have access to the network during the few seconds that this process takes.) However, you can avoid the suspend and resume process by following the instructions covered in [“Disabling the Firefly Host Suspend-Resume Process Enacted After a VM Is Unsecured”](#) on page 74.

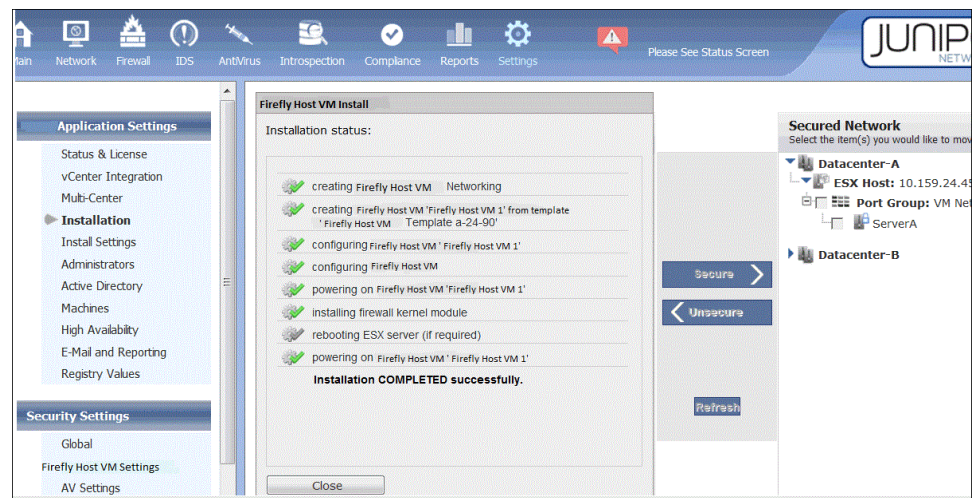
After you complete the installation, you might want to refine the configuration pertain to policy in the following ways:

- By default, each vNIC has a restrictive default security policy. You can use the Firewall module’s Manage Policy tab to make the policy less restrictive.
- You can use the Policy per vNIC feature to configure separate firewall policies for individual vNICs on the same VM. For details on the feature, see *Understanding the Firefly Host Policy per vNIC Feature* and *Configuring the Firefly Host Policy per vNIC Feature*.

After you define the Firefly Host VM, Firefly Host begins the Firefly Host VM firewall installation on the selected host. It displays a progress report as it completes each task. If problems occur during the installation process, Firefly Host displays messages describing them.

When the installation process is finished, Firefly Host displays the list of completed tasks and the successful completion notice, as shown in [Figure 25 on page 40](#). Notice that in this case, as reported, it was not necessary to reboot the host.

Figure 25: Firefly Host VM Installation Process Completion Notice



Related Documentation

- [Removing Firefly Host VMs from ESX/ESXi Hosts on page 42](#)
- [Understanding the Firefly Host VM](#)
- [Configuring Policy per vNIC to Secure Only Some of a VM's vNICs](#)
- [Installing a Secondary Firefly Host VM for High Availability](#)
- [Updating Firefly Host VMs in Batch Mode on page 48](#)
- [Understanding Firefly Host on page 3](#)

Configuring Firefly Host Installation Settings

This topic covers installation settings that you configure using the Firefly Host Dashboard. You use the Install Settings section of the Settings module for this purpose. The Install Settings page contains the following panes:

- VMsafe installation
- Automatic Securing of VMs
- Policy per vNIC

In the VMsafe installation pane, you can:

- Select the Firefly Host VM template to use to instantiate Firefly Host VMs on ESX/ESXi hosts.

From the VMsafe Template list, select the template to use.

- Specify the security behavior to follow when a Firefly Host VM is unable to attach to the Firefly Host VMsafe kernel module or retrieve firewall policy from the Firefly Host Dashboard:
 - Allow traffic to and from the Firefly Host VM without security controls enforced.

- Stop all traffic to and from the Firefly Host VM. In this case, VMware disconnects the VM's vNICs.
- Specify that the Firefly Host VM should only monitor the activity of the VM, but not secure it.

In this case firewall policies are not loaded onto the Firefly Host VM. Monitoring mode allows you to deploy a Firefly Host VM without concern that security policies will block traffic.

- Automatically secure VMs. Specify the VMs in a particular group, VMs in a policy group or with a policy applied to them, all VMs, or no VMs to be automatically secured. For details see, [“Understanding Automatic Securing of VMs” on page 75](#).

For details on installing a Firefly Host VM on an ESX, see [“Installing Firefly Host VMs on ESX/ESXi Hosts” on page 35](#).

If you enable the Auto-Secure feature, it automatically secures VMs and attaches security policies to them. If you choose to secure VMs automatically, you have the option of excluding a group within the selected group from being automatically secured.

For details on securing VMs or removing them from a secured network manually, see [“Securing and Unsecuring Virtual Machines Using the Firefly Host Dashboard” on page 73](#).

You can configure information that allows you to assign separate policies to individual vNICs.

- You use the Policy per vNIC pane to specify:
 - Whether separate policies can be configured for individual vNICs on the same VM.
 - If one or more vNICs on a VM that is configured for Policy per vNIC can be exempted from having a security policy. That is, no security policy is attached to them and they are not secured by Firefly Host.

You can use Policy per vNIC to apply policy rules to a vNIC that passes both IPv4 and IPv6 traffic.

For details on the Policy per vNIC feature, see *Configuring the Firefly Host Policy per vNIC Feature*.

For a VM with multiple vNICs, the Policy per vNIC feature allows you to use different policies for each of the vNICs. Users with VMs that connect to more than one port group/vSwitch may want different policies for each of the networks that their VMs connect to. The Policy per vNIC optional parameter, SecurePervNIC, allows you to secure some of a VM's vNICs while leaving other of its vNICs unsecured. In this case, it is the VM/port group that you secure. That is, you can use different policies for a VM based on the VM/port group. To use SecurePervNIC, you must enable Policy Per vNIC. When you use SecurePervNIC, the actual distinction is the port group, not the vNIC. That is, the vNICs of a VM are secured per VM and port group. This is due to the ambiguity of having both a secured and unsecured connection to the same Port Group. To use SecurePervNIC, you must enable Policy Per vNIC.

- Related Documentation**
- [Understanding Firefly Host on page 3](#)
 - [Understanding the Firefly Host VM](#)
 - [Understanding the Firefly Host Dashboard](#)

Removing Firefly Host VMs from ESX/ESXi Hosts

This topic explains how to remove a Firefly Host VM from an ESX or an ESXi host.

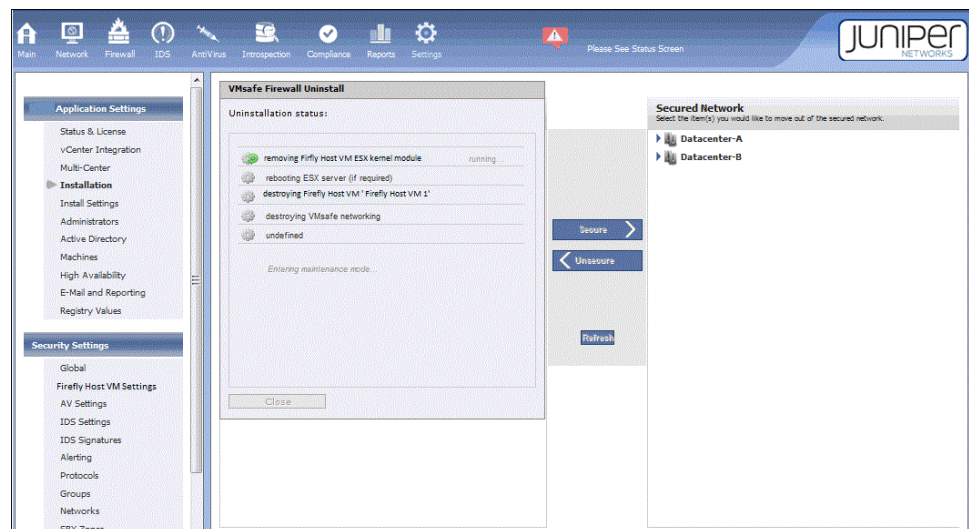
If you want to remove the VMX entries before you un-install the Firefly Host VM, then before unsecuring the entire host by removing the Firefly Host VM, unsecure the individual VMs. See [“Securing and Unsecuring Virtual Machines Using the Firefly Host Dashboard” on page 73](#).

To un-install the Firefly Host VM from a host:

1. In the Secured Network pane of the Settings module Firefly Host Application Settings > Installation page, select the host that you want to move out of the secured network.
2. Click the **Unsecure** arrow button.
3. The VMsafe Firewall Uninstall status pane is displayed. As the Firefly Host Dashboard removes the firewall from the host—or moves a specific VM out of the secured network, if you selected a VM—the status pane identifies the active process.

When you select an individual VM to remove from the secured network and click **Unsecure**, the Firefly Host Dashboard removes all relevant VMX entries for that VM, reverting the VM to its state prior to Firefly Host protection of it. [Figure 26 on page 42](#)

Figure 26: Firefly Host VM Uninstall



If you plan to un-install Firefly Host from your virtualized environment, unsecure all VMs in this manner. Afterward, select the check box for each of the ESX/ESXi hosts and click

Unsecure to remove them from Firefly Host protection. This process removes the kernel module and the related VMservice vSwitch and port groups.

Unsecuring a host before removing its VMs does not affect the VMs adversely. However, the process does not remove VMsafe VMX entries that pertain to Firefly Host. These entries are no longer required by that VM.



NOTE: You might not want the VMX entries for a VM to be removed under these conditions. For example, you might want to remove only the Firefly Host kernel module from a specific host. This might be the case if you want the VMs to be moved to a different ESX/ESXi host for protection, or you intend to reinstall Firefly Host later.

**Related
Documentation**

- [Installing Firefly Host VMs on ESX/ESXi Hosts on page 35](#)
- [Understanding Firefly Host on page 3](#)

CHAPTER 3

Firefly Host Upgrade

- [Updating the Firefly Host Dashboard on page 45](#)
- [Updating Individual Firefly Host VMs on page 46](#)
- [Updating Firefly Host VMs in Batch Mode on page 48](#)

Updating the Firefly Host Dashboard

This topic covers how to update the Firefly Host Dashboard online and offline manually.

This procedure explains how to update the Firefly Host Dashboard online. In this case, the Firefly Host Dashboard must be able to connect to the Juniper Networks update servers (HTTPS - TCP 443).

To update the Firefly Host Dashboard manually:

1. Ensure that a proper entitlement key is installed on the Firefly Host Dashboard.

If it is not already installed, insert the entitlement key in the Firefly Host Application Settings -> Status & License section of the Settings module. This section also allows you to see the update status of the Firefly Host Dashboard.

- a. In the Product Licensing section, click **Manage Licenses**.

A table showing the installed licenses is displayed.

This section also allows you to see the update status of the Firefly Host Dashboard.

Without an entitlement key, you cannot activate and install an update. You obtain the entitlement key when you purchase the product and software subscription contract.



NOTE: The entitlement key information above is applicable in case you want to upgrade from vGW Series to Firefly Host 6.0. It would not be applicable in case you upgrade from Firefly Host 6.0 to a higher version, in future.

2. Navigate to Settings > Appliance Settings > Updates.

- a. Click **Check for Updates** to query the Juniper Networks update servers.

The update server checks to determine if the component requires an update.

- b. If an update exists, click **Update Now** to apply the changes.

Firefly Host downloads the required updates from the Juniper Networks server. In some cases, the Firefly Host Dashboard will need to be rebooted.

Updating the Firefly Host Dashboard Offline

This procedure explains how to update the Firefly Host Dashboard offline, that is, without using Internet access. It uses an ISO image connected to the Firefly Host Dashboard for this purpose.



NOTE: Before you can update the Firefly Host Dashboard offline, you must obtain the update ISO from the Juniper Networks Support team and mount it on the Firefly Host Dashboard.

Before you can update the Firefly Host Dashboard offline, you must obtain the update ISO from the Juniper Networks Support team and mount it on the Firefly Host Dashboard.

To perform a manual update offline:

1. In the Settings module Appliance Settings > Updates > section, click **Advanced**.
2. Obtain the update ISO from the Juniper Networks support team, and mount it on the Firefly Host Dashboard.
3. Select the **Offline Update** check box.
4. Click **Connect Update Media**.
5. To check for updates first, click **Check for Updates**.
6. Click **Update Now**.

Related Documentation

- Understanding the Firefly Host Update Settings
- [Updating Individual Firefly Host VMs on page 46](#)
- [Updating Firefly Host VMs in Batch Mode on page 48](#)
- [Understanding Firefly Host on page 3](#)
- *Understanding the Firefly Host Settings Module*

Updating Individual Firefly Host VMs

This topic covers how to update an individual Firefly Host VM online and offline.

Before you update Firefly Host VMs, update the Firefly Host Dashboard. See [“Updating the Firefly Host Dashboard” on page 45](#)

To update an individual Firefly Host VM online, that is, with Internet access:

1. Navigate to the Settings module **Settings > Firefly Host VM Settings** page.

The Firefly Host VMs pane at the top of the page includes a table with a row for each deployed Firefly Host VM. Among other information, the table shows the version of the Firefly Host VM.

2. To display a pane that allows you to see detailed configuration information for an individual Firefly Host VM, click the row for that Firefly Host VM.
3. Select the Updates tab.
4. To check for Updates first to determine if there is a version beyond the one that is currently installed, click **Check for Updates**.
5. If an update exists, click **Update Now**.

Updating an Individual Firefly Host VM Offline.

This procedure explains how to update the Firefly Host VM offline, that is, without using Internet access. Before you can update the Firefly Host VM offline, you must obtain the update ISO from the Juniper Networks Support team.

To perform a manual update offline:

For Firefly Host VM migration

1. In VMware attach cd/dvd pointing to the ISO 2. Go to 'Settings->Updates->Advanced->' Select 'Migrate and Offline Update'

In the migrate 'Firefly Host Product Version' box, use a string of the following structure:

`vnf.altornetworks.com@altor:vf-<MAJOR VERSION STRING>[~vmsafe]`

- For example, to update to the latest version of the 6.0 release, use:

`vnf.altornetworks.com@altor:vf-6.0[~vmsafe]`

- For the latest version of the 5.5 release, use:

`vnf.altornetworks.com@altor:vf-5.5[~vmsafe]`

To perform an offline update for your SDC use a string of the following structure:

`vnf.altornetworks.com@altor:vf-<MAJOR VERSION STRING>`

- For example, to update to the latest version of the 6.0 release, use:

`vnf.altornetworks.com@altor:vf-6.0`

- For the latest version of the 5.0 release use:

`vnf.altornetworks.com@altor:vf-5.0`

2. Mount the media by selecting 'Connect Update Media' then select 'Check for Updates' you should see 6.0 listed and then you can proceed with the update.



NOTE: If you encounter problems, because, for example, Firefly Host VMs are not moved out correctly through vMotion, on the Firefly Host VM Settings page in the Settings module, click **Updates**.

This procedure explains how to update the Firefly Host VM offline, that is, without using Internet access. Before you can update the Firefly Host VM offline, you must obtain the update ISO from the Juniper Networks Support team.

To perform a manual update offline:

1. Navigate to the Appliance Settings Updates section in the Settings module.
2. Click **Updates**.
3. Click **Advanced**.
4. To check for updates first, click **Check for Updates**.
5. Select the **Offline Update** check box.

To enable offline updates (without Internet access), you must use an ISO image for the Firefly Host VM.

6. Click **Update Now**.

Related Documentation

- Understanding the Firefly Host Update Settings
- [Updating the Firefly Host Dashboard on page 45](#)
- [Updating Firefly Host VMs in Batch Mode on page 48](#)
- [Understanding Firefly Host on page 3](#)
- *Understanding the Firefly Host Settings Module*

Updating Firefly Host VMs in Batch Mode

This topic explains how to update Firefly Host VMs as a group in batch mode.

When you update Firefly Host VMs in batch mode, you can run the updates immediately or schedule them to run later.

To set up the system to update Firefly Host VMs in batch mode:

1. Navigate to the Settings module Appliance Settings > Updates page.
2. In the Firefly Host VM Batch Updates pane, enter the **Custom Product** version.
3. Select the check boxes for the Firefly Host VMs that you want to update. You can select all of them at once.
4. Specify whether you want the updates to run when the ESX/ESXi host is in Maintenance mode. Select:
 - **Always**, in which case logs are not lost.

- **As needed** for kernel driver updates only.
 - **Never**.
5. Using the **Start Time** option buttons, specify when to run the batch update process.
- To begin the batch update process immediately, select **Now**. Click **Update**.
 - To schedule the batch update, select **Later**.
 - a. Enter a start date and a start time.
 - b. Optionally, enter an end time.

If you specify an end time, Firefly Host completes any update that is in progress when the end time is reached. However, it will not begin any new Firefly Host VM updates.

- c. Optionally, enter an e-mail account to which an update status message is sent when the update either completes or is interrupted.

If you specify an e-mail address for Status email, a message reporting on the Firefly Host VMs that were updated and those that are pending is sent to the recipient.

**Related
Documentation**

- Understanding the Firefly Host Update Settings
- [Updating the Firefly Host Dashboard on page 45](#)
- [Updating Individual Firefly Host VMs on page 46](#)
- [Understanding Firefly Host on page 3](#)
- *Understanding the Firefly Host Settings Module*

CHAPTER 4

Firefly Host Integration with vCloud Director

- [Understanding Firefly Host Integration with vCloud Director on page 51](#)
- [Configuring Firefly Host Integration with vCloud Director on page 53](#)

Understanding Firefly Host Integration with vCloud Director

The Firefly Host Dashboard integrates directly with VMware's vCloud Director to allow Firefly Host to retrieve information from vCloud Director about virtual machines (VMs). After you configure vCloud in the Firefly Host Dashboard, the information about a VM that it acquires can be used to dynamically associate that VM with Firefly Host groups and policies that you create.

- [VMware vCloud Director on page 51](#)
- [Firefly Host and vCloud on page 51](#)
- [Requirements on page 52](#)

VMware vCloud Director

VMware's vCloud Director Infrastructure-as-a-Service solution allows for rapid provisioning of complete virtual software-defined datacenter services. vCloud Director implements pooling, abstraction, and automation of data center services including storage and networking services. Using it, administrators can provision infrastructure without concern for physical hardware configuration.

Although vCloud Director can be used within an enterprise infrastructure, it is commonly used by cloud-based VM hosting providers.

Firefly Host and vCloud

The Firefly Host Dashboard direct integration with vCloud Director allows it to collect information that is associated with a VM in vCloud Director. Information that Firefly Host collects includes:

- VM membership in a specific organization.

- VM tags defined in the VM metadata. vCloud Director can associate information about VMs from its Metadata tab page that is configured by an administrator or other user, based on their permissions.

The Firefly Host Dashboard obtains the VM name and value data from this configuration. The Firefly Host Dashboard can obtain multiple values, if any.

Firefly Host Dashboard allows you to define Smart Groups used as policies in which VMs that match the Smart Group criteria are dynamically associated with the group, and its policy is applied to them. The vCloud Director information used in a dynamic group is associated with the `vcd.tag` property. The information appears as comma separated *attrname=value* pairs with the organization information appearing as the value for the `OrgName` attribute, such as `OrgName=Org1`.

For example, you could define a Firewall policy to be assigned to all VMs belonging to a particular organization. If the Smart Group configuration includes that organization, the Smart Group's policy is applied to the matching VM.

You might define an Introspection Image Enforcer profile that specifies that all VMs running Windows OS that belong to a particular organization must have installed on them all applications installed on a Gold Image that they are compared to. You could also use the information acquired from vCloud Director in configuring Anitvirus scanning.

Firefly Host and vCloud Director integration is characterized as follows:

- By default, Firefly Host Dashboard integration with vCloud Director is disabled.
To enable integration with vCloud Director, you set the `center.vcd.enabled` parameter to true:**`center.vcd.enabled=true`**.
By default it is set to false.
- Firefly Host supports integration with vCloud Director 5.1 and later versions.
- Presently the Firefly Host Dashboard supports integration with only one vCloud Director server.

Requirements

For Firefly Host Dashboard to be able to integrate with vCloud Director and query it for VM inventory and other operations, the account connecting to vCloud Director must have admin privileges.

Related Documentation

- [Configuring Firefly Host Integration with vCloud Director on page 53](#)
- *Firefly Host Attributes for VMware*
- *Understanding Firefly Host Groups*
- *Creating Firefly Host Smart Groups for VMware*
- [Understanding Firefly Host on page 3](#)

Configuring Firefly Host Integration with vCloud Director

This topic covers how to integrate Firefly Host with VMware's vCloud Director using the Firefly Host Dashboard.

Before you configure Firefly Host integration with vCloud Director, you must set up vCloud Director to send relevant notifications to an Advanced Message Queuing Protocol (AMQP) broker.

vCloud Director includes an AMQP service that you can configure to work with an AMQP broker to make available notifications about events in the cloud.

There are several AMQP-compatible brokers, including:

- Red Hat MRG Messaging. See <http://www.redhat.com/products/jbossenterprisemiddleware/messaging/>
- RabbitMQ. See <http://www.rabbitmq.com/>



NOTE: On the vCloud Director Administration screen page where you configure the AMQP broker settings, you must select **Enable Notifications**. Also, set **Exchange** to **FireflyHostExchange**. If you use a different value, ensure that it matches the value of property `centre.vcd.amqp.exchange` in `centre.conf`.

After you complete this configuration and you configure the Firefly Host Dashboard for integration with vCloud Director, the Firefly Host Dashboard can register with the AMQP broker to acquire these notifications and use them for updates.

The Advanced Message Queuing Protocol (AMQP) is an OASIS open standard application layer protocol for message-oriented middleware. The defining features of AMQP are message orientation, queuing, routing (including point-to-point and publish-and-subscribe), reliability and security.

To configure Firefly Host integration with vCloud Director:

1. Enable vCloud Director integration. Set the `center.vcd.enabled` parameter to `true`:

`center.vcd.enabled=true`

By default it is set to `false`.

For this configuration parameter to take effect, you must restart Apache Tomcat.



NOTE: If you reset this value to false, all existing connections with vCloud Director are closed and the credentials are removed from the Firefly Host database. Also the pane for configuring vCloud Director credentials in Settings > Firefly Host Application Settings > vCenter Integration shown in Figure 27 on page 54 is no longer displayed.

Figure 27: Firefly Host Dashboard vCenter Integration Window Showing vCloud Director Settings Pane

- Figure 27 on page 54 shows the Settings > Firefly Host Application Settings > vCenter Integration window that you use to configure Firefly Host settings for integration with vCloud Director.

In the vCloud Director Settings pane, configure the following information:

- In the **VCD Server Name or IP Address** field, enter the IP address or DNS name of the vCloud Director server.

You can specify an IPv6 or IPv4 address.

- In the **VCD Server Port** field, if the port number differs from the default of 443, specify the port number.
- In the **vCD Username** field, enter the user type.
The user specified must have admin privileges.
- Specify a password in the **vCD Password** field

3. In the Synchronize vCloud Director pane, click **Restart**.

The Firefly Host Dashboard automatically configures information about any VM that it discovers through vCloud Director and it associates that information with the VM. You can view that information on the Settings > Firefly Host Application Settings > Machines page.

**Related
Documentation**

- [Understanding Firefly Host Integration with vCloud Director on page 51](#)
- *Firefly Host Attributes for VMware*
- *Understanding Firefly Host Groups*
- *Creating Firefly Host Smart Groups for VMware*
- [Understanding Firefly Host on page 3](#)

CHAPTER 5

Firefly Host Management

- [Understanding Firefly Host Timeout Parameters and the Firefly Host VM Installation, Uninstallation, and Update Tasks on page 57](#)
- [Adding New Firefly Host Administrator Definitions, Permissions, and Authentication Using the Settings Module on page 59](#)
- [Setting Up Active Directory for Firefly Host Administrator Authentication on page 64](#)
- [Adding and Editing Firefly Host Machines Definitions \(VMware\) on page 66](#)

Understanding Firefly Host Timeout Parameters and the Firefly Host VM Installation, Uninstallation, and Update Tasks

Configurations for the following two timeout parameters affect a variety of Firefly Host VM installation, uninstallation, and update processes:

- `center.timeout.vm.long.in.sec` (default: 10 minutes [600 seconds])
- `center.timeout.host.long.in.sec` (default: 10 minutes [600 seconds])

These Firefly Host VM processes entail individual tasks and groups of tasks. For example, the Firefly Host Module removal process that occurs when a Firefly Host VM is being uninstalled includes the "enter maintenance mode" and "remove fastpath" tasks.

If the ESX/ESXi host on which the Firefly Host VM was installed exceeded the configured timeout value while it was being put into maintenance mode during the Firefly Host VM uninstallation, the message that Firefly Host reported prior to Firefly Host 6.0 might have been misleading because it pertained to the *group* of tasks comprising the kernel module removal process.

Beginning with Firefly Host 6.0, when a task exceeds the configured timeout value that pertains to it, Firefly Host generates a log error entry that describes the individual task that was being executed when the timeout event occurred and the timeout parameter configuration that controls it, rather than giving a single task group message.

For example, the following message is generated and written to the log when the process of cloning the Firefly Host VM template exceeds the amount of time configured for `center.timeout.vm.long.in.sec`.

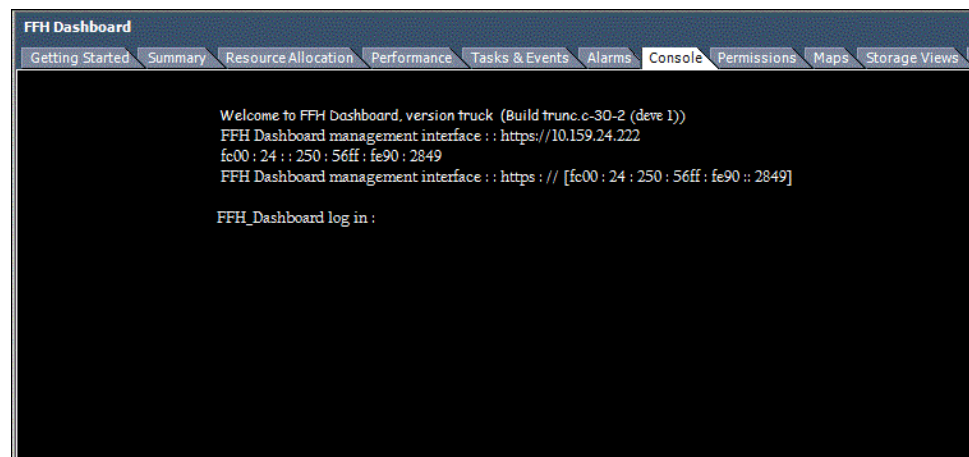
"Cancelled task (cloning Security VM X from template Y) as it was taking too long.
Timeout set by center.timeout.vm.long.in.sec"

The timeout parameters are configurable to allow you to adapt your configuration to different vCenter behaviors. For example, a log entry might indicate that a vCenter task is taking longer than expected. You can use the console to run the Firefly Host command-line interface (CLI) and change the configuration for the timeout parameter affecting the task. You can adjust the configuration appropriately and retry the process.

To use the Firefly Host CLI from the vCenter console:

1. Launch the VMware vSphere Client.
2. Right-click the Firefly Host Dashboard icon on the left navigation panel to display a list of options.
3. Select the third option on the list, **Open Console**. Alternatively you can select the Console tab, as shown in [Figure 28 on page 58](#).

Figure 28: Firefly Host CLI Console



The console window appears.

Some of the tasks affected by these timeout parameters are:

- Firefly Host VM shutdown
- ESXi reboot
- cloning Firefly Host VM template
- Firefly Host VM reporting heartbeat with new version after update

Related Documentation

- [Installing Firefly Host VMs on ESX/ESXi Hosts on page 35](#)
- [Removing Firefly Host VMs from ESX/ESXi Hosts on page 42](#)
- [Installing a Secondary Firefly Host VM for High Availability](#)
- [Updating the Firefly Host Dashboard on page 45](#)
- [Understanding the Firefly Host VM](#)
- [Understanding Firefly Host on page 3](#)

Adding New Firefly Host Administrator Definitions, Permissions, and Authentication Using the Settings Module

This topic includes the following sections:

- [Configuring an Administrator Account on page 59](#)
- [Changing Administrator Passwords on page 61](#)

Configuring an Administrator Account

Different categories of IT staff members may need to access the Firefly Host Dashboard interface for various purposes. For example, network engineers can take advantage of the network statistics charts and information on connections, top protocols used, top sources, and top destinations. Security engineers can use the Firewall module to design and apply policies for VMs and the Settings module's Firefly Host Application Settings > Installation page to deploy Firefly Host VMs to ESX/ESXi hosts to secure them.

[Table 3 on page 59](#) defines the built-in user types that Firefly Host provides to accommodate common roles and requirements, and it describes their privileges.

Table 3: Firefly Host Built-In Administrator User Types

Global Admin	<p>This administrator has the highest level of system privileges, including the ability to create accounts for additional administrators.</p> <p>The global administrator has many privileges including the ability:</p> <ul style="list-style-type: none"> • to create firewall policies and install firewalls (Firefly Host VMs) on ESX/ESXi hosts to be secured. • configure features such AntiVirus, IDS, and VM Introspection Compliance for VMs. • select port groups and VMs for insertion in and removal from a secured network. <p>This administrator can also change his own password and reset the passwords of other administrators. Having the ability to reset the password for another administrator is useful when an administrator forgets his password. For details see "Changing Administrator Passwords" on page 61.</p>
VM Admin	<p>These administrators have many privileges, including the ability to:</p> <ul style="list-style-type: none"> • modify policies and settings configurations. <ul style="list-style-type: none"> The administrator is allowed to change firewall security policies, including IDS. • configure AntiVirus and VM Introspection Compliance. • configure mirroring of inter-vm traffic, the ability to configure rules that specify external inspection devices. <p>Additionally, the global administrator can grant VM Admins "Install Firewall Policy" privilege. This privilege allows a VM Admin to distribute a policy after it has been changed and saved by any administrator who has the privilege to modify security policies.</p>

Table 3: Firefly Host Built-In Administrator User Types (*continued*)

Network Monitoring	<p>These administrators can view:</p> <ul style="list-style-type: none"> all network-related pages, for example pages that show statistics and graphs. all tabs of the Main module, including Status and Events and Alerts, and Logs. <p>These administrators are not allowed to modify any Settings pages, but they can view IDS Alerts, if IDS is configured, view AntiVirus scans, and they can view but not modify VM Introspection and Compliance results.</p>
--------------------	---

To create an administrator account:

1. From Settings module Firefly Host Application Settings > Administrators page, click **Add**.

Figure 29 on page 60 shows the Administrators page > Add Administrator pane that you use to define permissions for a new administrator and add the administrator to the system.

This example configuration specifies that authentication is performed internally by Firefly Host, not by Active Directory (AD), which could also be used. In this example, the VM Admin admin-security-example administrator is allowed to modify policy and settings and push firewall policies to Firefly Host VMs.

Figure 29: Creating a VM Admin Administrator Account

The screenshot displays the Firefly Host web interface. On the left, a sidebar menu shows 'Application Settings' with 'Administrators' selected. Below it, 'Security Settings' and 'Appliance Settings' are visible. The main area shows the 'Administrators' table with one entry: 'admin' (Default Global Admin, Global Admin, Console administrator, Internal). Below the table is the 'Add Administrator' dialog. The dialog has the following fields and options:

- Authentication Type:** Radio buttons for Internal (selected), AD Individual User, and AD Group.
- Username:** Text field containing 'admin-security-example'.
- Full Name:** Text field containing 'admin-security-example'.
- Type:** Radio buttons for Global Admin, VM Admin (selected), and Network Monitoring.
- Permissions:** A list of checkboxes:
 - ☒ Modify policy and settings
 - ☒ Allow mirroring of inter-VM traffic
 - ☒ Allow scheduling and starting VM Introspection scans
 - ☒ Allow scheduling and configuring AV scans
 - ☒ Allow configuration backup and restore
 - ☒ Install Firewall policy
- Change password:** A checkbox that is checked, with fields for 'New Password' and 'Confirm Password' (both masked with dots).

Buttons for 'Add', 'Delete', 'Save', and 'Cancel' are located at the bottom of the dialog.

2. In the **Authentication Type:** area, select the button associated with the kind of authentication to be used for this administrator. You can use Active Directory (AD) as a means of authentication rather than storing the credentials locally. In this case, Active Directory must first be enabled through the Settings module > Firefly Host

Application Settings > Active Directory page. For details on AD authentication, see [“Setting Up Active Directory for Firefly Host Administrator Authentication” on page 64](#).

3. In the **Username:** and **Full Name:** fields, enter the user names for the administrator.
4. In the **Type:** area, select the button associated with the type of administrator account that you want to create. See [Table 3 on page 59](#).
5. In the **Permissions:** area select the permissions that you want to grant to the administrator. Notice that for VM Admin you can select “Modify policy and settings” and “Install Firewall policy”, but if you select Network Monitoring you cannot select any of these permissions. See [Table 3 on page 59](#) for allowed permissions.
6. Specify a password and confirm the password.
7. Click **Save**.

After you save the configuration, the administrator definition is added to the Administrators table, as shown in [Figure 30 on page 61](#).

Figure 30: Adding a New Administrator

Administrators			
			Filter <input type="text"/>
Username	Full Name	Type	Authentication Type
admin	Default Global Admin	Global Admin, Console administrator	Internal
admin-example	admin-example	VM Admin	Internal



NOTE: At any time, you can click the table row for an administrator definition to display the Edit Administrator pane that shows the configuration. From the Edit Administrator pane you can modify the permissions and password and save the modified definition.

Changing Administrator Passwords

Whether you are a global administrator (Global Admin), an administrator whose account is defined as a VM Admin, or an administrator with Network Monitoring permissions, you can use the Settings module Firefly Host Application Settings > Administrators page to change your password.

This section includes the following sections that explain the simple process and requirements:

- [Global Administrator: Changing Your Own Password on page 62](#)
- [Global Administrator: Changing the Password of Another Administrator on page 62](#)
- [VM Administrator and Network Monitoring Administrator Accounts: Changing Your Own Password on page 63](#)

Global Administrator: Changing Your Own Password

As the global administrator (Global Admin), when you select your own row in the Administrators table, the **Edit Administrator** dialog box appears showing the configuration for your account. To change your own password, you must first enter your current password followed by the new one.

When you select the **Change password** check box, the **Current Password:** and **New Password:** boxes appear, allowing you to change your password. You must also enter the new password in the **Confirm Password:** box. After you enter the new password, click **Save**. [Figure 31 on page 62](#) shows this dialog box.

Figure 31: Changing the Global Administrator Password

The screenshot shows the Juniper Firefly Host configuration interface. On the left is a navigation pane with categories like Status & License, vCenter Integration, Multi-Center, Installation, Install Settings, Administrators, Security Settings, and Appliance Settings. The 'Administrators' section is selected. The main area displays a table of administrators:

Username	Full Name	Type	Authentication Type
admin	Default Global Admin	Global Admin, Console administrator	Internal
admin-security-examp	admin-security-example	VM Admin	Internal

Below the table are 'Add' and 'Delete' buttons. The 'Edit Administrator' dialog box is open for the 'admin' user. It shows the following fields and options:

- Authentication Type:** ☒ Internal ☐ AD Individual User ☐ AD Group
- Username:** admin
- Full Name:** Default Global Admin
- Type:** ☒ Global Admin ☐ VM Admin ☐ Network Monitoring
- Permissions:**
 - ☒ Modify policy and settings
 - ☒ Allow mirroring of inter-VM traffic
 - ☒ Allow scheduling and starting VM Introspection scans
 - ☒ Allow scheduling and configuring AV scans
 - ☒ Allow configuration backup and restore
 - ☒ Install Firewall policy
- Change password:** ☒
 - Current Password:** [text box]
 - New Password:** [text box]
 - Confirm Password:** [text box]

At the bottom of the dialog are 'Save' and 'Cancel' buttons.

Global Administrator: Changing the Password of Another Administrator

When you want to change the password of another administrator—such as an administrator whose account is defined as a VM Admin or for an administrator with Network Monitoring permissions—you are not required to enter that administrator's current password. Not having to enter the current password for another administrator allows you to provide that administrator with a new password when they forget their current one.

As the global administrator, when you select the row for another administrator in the Administrators table, the **Edit Administrator** dialog box appears, showing the configuration for that administrator's account.

As [Figure 32 on page 63](#) shows, when you select the **Change password** check box, the **New Password:** and **Confirm Password:** boxes appear, allowing you to change the password for the administrator whose account configuration is displayed. After you enter the new password, click **Save**.

Figure 32: Global Administrator Changing the Password of Another Administrator

Edit Administrator

Authentication Type: ☒ Internal ☐ AD Individual User ☐ AD Group

Username:

Full Name:

Type: ☐ Global Admin ☒ VM Admin ☐ Network Monitoring

Permissions:

- ☒ Modify policy and settings
 - ☒ Allow mirroring of inter-VM traffic
 - ☒ Allow scheduling and starting VM Introspection scans
 - ☒ Allow scheduling and configuring AV scans
 - ☒ Allow configuration backup and restore
- ☐ Install Firewall policy

☒ Change password New Password: Confirm Password:

Save **Cancel**

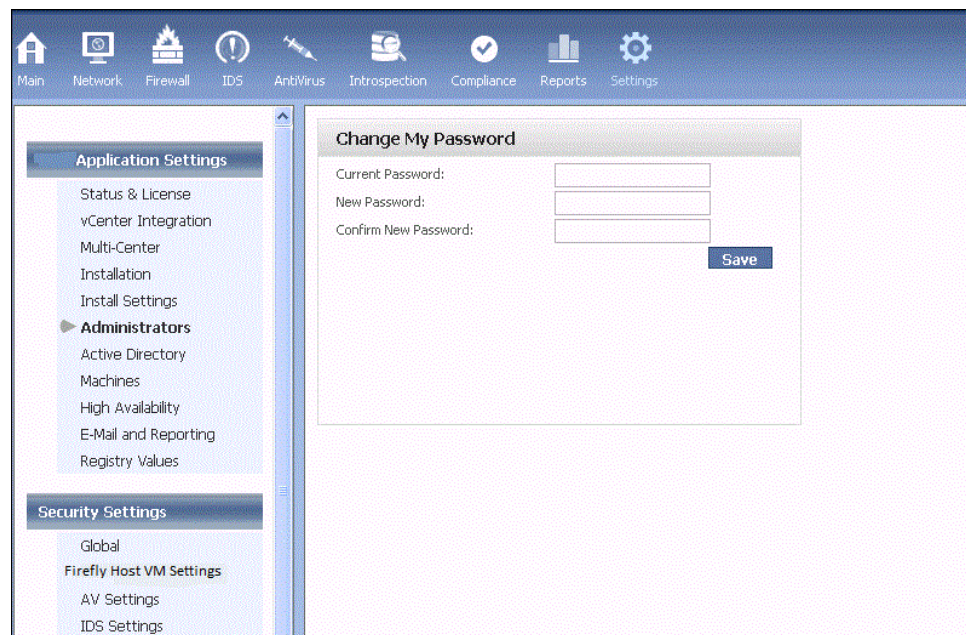
VM Administrator and Network Monitoring Administrator Accounts: Changing Your Own Password

After the global administrator (Global Admin) defines an administrator account for you, you can change the password that was specified during the configuration. In this case, the global administrator conveys the password to you. You can also change your password at any time after you change it initially.

When you select Administrators, the change password dialog box appears. To change your password, you must first enter your current password followed by the new one.

To change your password, enter your current password in the **Current Password:** box and your new password in the **New Password:** box. You must also enter the new password in the **Confirm Password:** box. Then click **Save**. See [Figure 33 on page 64](#)

Figure 33: Administrators Changing Their Password



Related Documentation

- [Understanding Firefly Host on page 3](#)
- [Setting Up Active Directory for Firefly Host Administrator Authentication on page 64](#)
- [Configuring Firefly Host Firewall Policies on page 108](#)
- [Understanding the Firefly Host VM](#)
- [Understanding the Firefly Host Dashboard](#)

Setting Up Active Directory for Firefly Host Administrator Authentication

This topic covers use of Active Directory (AD) for administrator authentication. First it explains how to enable AD support for Firefly Host, which you must do before you can configure administrator authentication to use it. Then it explains how to configure it as the authentication type for an administrator.

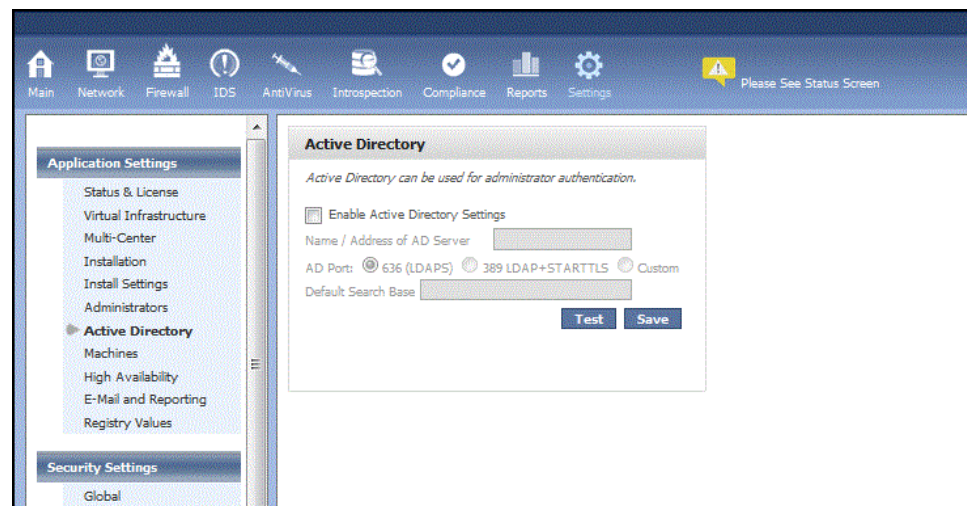
You can use AD with Firefly Host for administrator authentication instead of storing the authentication information locally in the Firefly Host Dashboard database. Firefly Host supports AD over IPv4 and IPv6 networks.

Administrators can use their AD credentials to log in to the Firefly Host Dashboard. Firefly Host checks AD for the credentials, and, based on the settings, it allows the user to log in to Firefly Host Dashboard or it denies the user access.

To set up the Firefly Host to work with AD:

1. Define the Name (or IP address) of the AD server. [Figure 34 on page 65](#) shows the Active Directory configuration page.

Figure 34: Enabling Active Directory



2. Set the appropriate port. By default, port TCP 636 (LDAPS) is used. However, you can use 389 LDAP+STARTTLS or configure a custom port.

Enable your network to give the Firefly Host Dashboard access to this port to the server.

3. After you select the name or IP address, port, and default search base, select **Test** or **Save** to view the fingerprint used to validate the communication destination and to initiate all future communication through encryption.

When you select **AD Group** for **Authentication type**, a dialog box is displayed allowing you to enter the user ID and password to use to log in to AD to get the group list.



NOTE: AD must be enabled for you to select AD Group as the authentication method. Use the Settings module Firefly Host Application Settings > Active Directory page to enable it, as described previously.

If there are more than 100 configurable groups, Firefly Host presents the following alert message:

“There are too many groups in Active Directory to be displayed in a drop-down list. Please fill in the name of the AD Group.”

Rather than displaying a drop-down list of group names, the AD Group Name field is presented as a text box in which you can enter the name of the group.

When you save the configuration, Firefly Host checks AD to ensure that the group exists, based on the name that you entered. If the group does not exist, Firefly Host displays the following message:

“The AD Group *name* does not exist in Active Directory.”

To create users or groups to be authenticated through the configured server lookup process:

1. Select the Settings module > Firefly Host Application Settings > Administrators page.
2. Add administrators. Set the authentication type to **AD Individual User** or **AD Group**.
 - For AD Individual User, the account is authenticated with AD credentials and all privileges are applied according to defined Firefly Host settings.
 - For AD Group, the name of an existing group in AD is used and privileges are assigned to it. The AD lookup is used to authenticate the user to determine that he is a member of the group. If so, he is granted access to Firefly Host.

**Related
Documentation**

- [Adding New Firefly Host Administrator Definitions, Permissions, and Authentication Using the Settings Module on page 59](#)
- [Understanding Firefly Host on page 3](#)
- [Configuring Firefly Host Firewall Policies on page 108](#)
- [Understanding the Firefly Host VM](#)
- [Understanding the Firefly Host Dashboard](#)
- [Adding and Editing Firefly Host Machines Definitions \(VMware\) on page 66](#)

Adding and Editing Firefly Host Machines Definitions (VMware)

This topic covers the Machines page that you use to define IP addresses and other information for new machines. These machines include both VMware ESX/ESXi hosts and virtual machines (VMs) that you define for your environment. You also use this page to view or edit information about machines that are already defined, including those that are discovered automatically. Machines can have IPv4 or IPv6 addresses.

This topic describes a new parameter provided with Firefly Host Release 6.0—Log Tags—that allows you to specify tags that are added to syslog output. You can use these tags to sort on syslog feed.

This topic includes the following sections:

- [Adding a Machine on page 66](#)
- [Viewing Machine Information on page 68](#)

Adding a Machine

Normally the IP address for a machine is “auto-discovered”, obtained through VMware Tools. For systems without VMware Tools, you can use the Settings module Applications Settings > Machines page to manually add addressing information for a machine. You can also specify additional information for a machine, such as Log Tags and Smart Tags.

To configure information for a machine, enter:

- **Name:** This is the name of the machine (VM). By default, it is set to synchronize with the VMware vCenter. However, you can detach it by clearing the Synchronize name with vCenter checkbox.

In Release 6.0, Firefly Host adds the name to syslog output, instead of adding just VM_ID. The name is relative to the VM that is either the source (src) or destination (dst) of the log flow. For example, dst_name="mini-5-1" or src_name="mini-5-1". hr".

- **Description:** Give a brief description of the machine.
- For the machine's address, use DNS for the machine name or enter its address explicitly.

- **DNS name:**

If you define a machine in this section, it is identified in the network tables by its name rather than by its IP address.

- Specify the machine's DNS name.
- To obtain the name through a DNS query, click **Query via DNS**.

- **IP Address:** Specify the machine's IP address explicitly.

- **Smart Tags:** Optionally, configure Smart Tags to assign identifiers to the machine that can be used for VM Smart Groups or policy creation.

The syntax for a Smart Tag is attribute-value. You can define multiple tags separated by semicolons, for example: finance;pci=true;audited=true.

- **Log Tags:** Optionally, specify Log Tags to be added to Syslog entries for this machine.

In conjunction with the VM name that is added to Syslogs as of Firefly Host Release 6.0, this option allows you to specify any tag that you want to use to be added to the syslogs. For example, you can use this tag to associate certain VMs with a Tenant or Department such as customer A's VMs are tagged with 'cust-a' and which are then sorted automatically from the syslog feed by parsing on this tag.

Similar to the VM name tag described above, these tags are relevant on direction of the flow (src_log_tag or dst_log_tag). For example, dst_log_tag="testLogTags". These logs are issued when Firefly Host processes secured VM traffic or files.

The Log Tag string pertains to this VM only. It cannot exceed 200 characters.

[Figure 35 on page 68](#) shows the edit screen that includes a log tag for a machine that was already added. [Figure 36 on page 68](#) shows the resulting syslog entry.

The Log Tag string pertains to this VM only. It cannot exceed 200 characters.

- **Type:** This is the type of machine, for example, ESX/ESXi server, external machine
- **Monitoring Groups:** Monitoring groups that the machine belongs to.
- **Policy Groups:** Policy Groups that the machine belongs to.
- **VMSafe Protected:** Whether the machine is secured by Firefly Host.

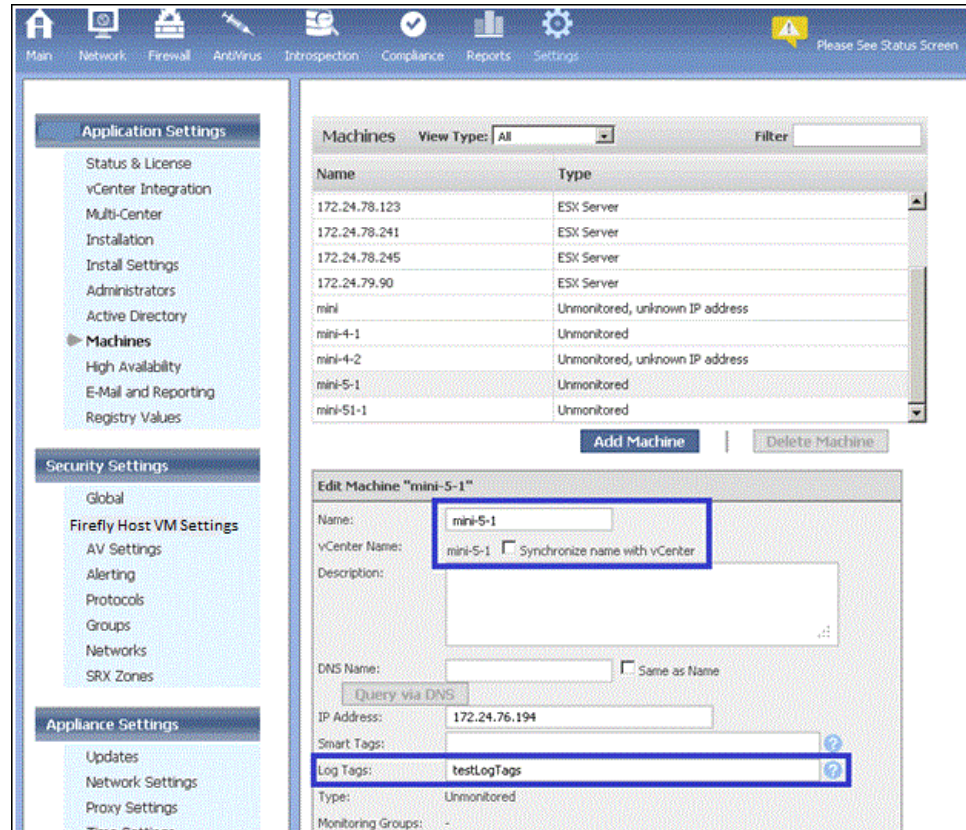
When you select a VM, as opposed to an ESX/ESXi server, and display the Edit Machine box for it, this information is displayed for it.



NOTE: If you click **Advanced...** You can change the behavior if Firefly Host fails to connect to the kernel (failopen or failclosed).

You can also use the Machines page to edit information for an existing machine. See [Figure 35 on page 68](#).

Figure 35: Configuring Machines Information



For Syslog Entry Including VMName and Log Tag, see [Figure 36 on page 68](#).

Figure 36: Syslog Entry Including VM Name and Log Tag

```
action=allow vm_id=0 ip_proto=udp rule=7 type=fw src_id=0 dst_id=29 src_id=32 src_name= dst_name="mini-5-1" src_log_tag= dst_log_tag="testLogTags"
```

Viewing Machine Information

You can view information about machines that are already defined. You can use the **View Type:** box to sort the list by machine type. You can sort by ESX servers, external machines, monitored, unmonitored, and secured machines.

You can use the Filter box to search by a portion of an IP address or machine name or type.

- Related Documentation**
- [Understanding Firefly Host on page 3](#)
 - *Firefly Host Dashboard Modules (VMware)*

PART 3

Firefly Host Settings Infrastructure to Secure Hosts

- [Securing ESX/ESXi Hosts using Firefly Host on page 73](#)
- [VMware Auto Deploy for ESXi Servers and with Firefly Host on page 77](#)
- [Firefly Host Firewall Module on page 87](#)
- [Firefly Host Network Module on page 117](#)

CHAPTER 6

Securing ESX/ESXi Hosts using Firefly Host

- [Securing and Unsecuring Virtual Machines Using the Firefly Host Dashboard on page 73](#)
- [Disabling the Firefly Host Suspend-Resume Process Enacted After a VM Is Unsecured on page 74](#)
- [Understanding Automatic Securing of VMs on page 75](#)

Securing and Unsecuring Virtual Machines Using the Firefly Host Dashboard

After you install the Firefly Host VM on an ESX/ESXi host to secure it, the Firefly Host Dashboard allows you to manually secure virtual machines (VM) on that host or remove them from the protected network. Removing a secured VM from the protected network is referred to as *unsecuring* the VM.

To secure a VM that does not belong to the Secured Network:

1. In the Firefly Host Dashboard Settings module Firefly Host Application Settings section, select **Installation**.
2. In the Unsecured Network pane, select the VM that you want to secure. Click the check box in front of its name.
3. Click **Secure**.

As it secures the VM, the Firefly Host reports on the status of each part of the process. If the VM is successfully secured, the report states that the VM was successfully secured.

4. Click **Close**.

The Firefly Host Dashboard displays a process symbol that dynamically indicates that the VM is being secured with a firewall and moved into the secured network. The VM is now protected, and it appears in the Secured Network pane.

After all Firefly Host components in your environment are upgraded to release 6.0, if you attempt to introduce components from a previous release, the process is halted and Firefly Host displays a message informing you that you must install the correct version.

Related Documentation

- [Disabling the Firefly Host Suspend-Resume Process Enacted After a VM Is Unsecured on page 74](#)
- [Installing Firefly Host VMs on ESX/ESXi Hosts on page 35](#)
- [Understanding Firefly Host on page 3](#)

Disabling the Firefly Host Suspend-Resume Process Enacted After a VM Is Unsecured

You use the Firefly Host Dashboard Settings module Installation section to secure and unsecure a VM. By default, the Firefly Host suspends and resumes a VM when you unsecure it. You can change this behavior by changing the value of the `vm-safe.config` option.

- [Displaying the State of the `vm-safe.config` Setting on page 74](#)
- [Disabling the Suspend-Resume Process on page 74](#)

Displaying the State of the `vm-safe.config` Setting

This example shows the default setting. You can use the following command to display the current state of the `center.config vm-safe.config` option:

```
(Cmd) config show center.suspend.after.vmsafe.config
# whether center should suspend and resume VM after VMsafe configuration
center.suspend.after.vmsafe.config = true
```

Disabling the Suspend-Resume Process

In some cases it might be necessary or desirable to stop Firefly Host from enacting the suspend-resume process after a VM is unsecured. For example, you might want to disable the process to allow the VM to be migrated to another host or to suspend and resume the VM later after completing the removal of protection from the VM.



TIP: Take care when you protect VMs such as the VMware vCenter Database VM and other VMs that must not be suspended.

To enable the `vm-safe.config` process to take effect after the VM is migrated to another host without suspending the VM, use the following statement. Set the option to `false` in `center.config`:

```
(Cmd) config set center.suspend.after.vmsafe.config false
```

After changing this value, either restart the Firefly Host management process or reboot the Firefly Host Dashboard. You can use the service restart command line or the Firefly Host Dashboard to restart the Firefly Host management process.

To restart the Firefly Host management process from the command line, enter the following command:

```
(Cmd) service restart tomcat
Sending 'restart' command
The following watches were affected:
```

tomcat

To restart the Firefly Host management process using the Firefly Host Dashboard:

1. Select the Settings module Support section.
2. In the Restart pane of the displayed page, click **Restart**.

Related Documentation

- [Installing Firefly Host VMs on ESX/ESXi Hosts on page 35](#)
- [Securing and Unsecuring Virtual Machines Using the Firefly Host Dashboard on page 73](#)
- [Understanding Firefly Host on page 3](#)

Understanding Automatic Securing of VMs

Firefly Host allows you to configure your system to *automatically* secure VMs. Auto-securing VMs streamlines policy application allowing you to efficiently ensure security throughout your virtual infrastructure. You can configure the Auto-Secure feature options to direct Firefly Host to automatically secure VMs in the manner most appropriate for your environment.

You use the Settings module Firefly Host Application Settings > Install Settings > Automatic Securing of VMs pane to configure Auto-Secure for your virtualized environment.

The Automatic Securing of VMs pane includes the following options:

- No VM

No individual VMs or groups of VMs are automatically secured. This is the default behavior.

- VMs in the following group

This option allows you to select either a Static Group or a Smart Group from the list of existing groups. The list contains all groups, including those configured as Policy Groups and those that are not. Using this option, you can select only one group.



NOTE: Only VMs in the selected group are automatically secured.

- If you did not configure the selected group as a Policy Group, Firefly Host automatically secures members of the group with the Global and Default policies.
- If you configured the selected group with the Policy Group option, then any policy rules that were created for the group and applied to it take effect. In this case, the Default policy is not used.
- VMs with a VM Policy or in a Policy Group

Because Default Policy and Global Policy rules tend to be restrictive, they are not appropriate for securing all VMs. This option allows you to predefine policy rules for individual VMs and groups of VMs and direct Firefly Host to use the policy rules that

you predefined to automatically secure them rather than relying on just the Default and Global policy rules. Using this option, you can automatically secure many Policy Groups and individual VMs instead of being restricted to selecting a single group.

VMs that fit any of the following criteria are automatically secured:

- Individual VMs for which you have predefined specific policy rules and applied those policies using the Firewall module Apply Policy page to install the policy.
- Groups of VMs that you created as Static Groups or Smart Groups and for which you selected the Policy Group option. You must also have created and applied a policy for the group, and that policy must contain rules.

- All VMs

All VMs are automatically secured. As described previously, any policy rules defined for Policy Groups that have been previously applied take effect for VM members of the group. If a VM is not a member of any group, then Global and Default Policies and any individual VM rules take effect for them.

You can refine this selection by excluding a specific group of VMs.

- Optionally, exclude a group of VMs from being automatically secured. You might want to exclude VMs from auto-securing that you are using for testing.



NOTE: Firefly Host auto-secure feature will not attempt to secure an FT-enabled VM. Firefly Host generates an alert telling you that you must disable FT for that VM or suspend the VM for Firefly Host to secure the VM. The auto-secure feature monitors for cases in which an FT-enabled VM is disabled and for VMs that are suspended and powered-off.

If a VM is automatically secured, you cannot use the Settings module Installation page to unsecure it. The VM is shown on this page in a dimmed box and a message is presented informing you that it is automatically secured. In this case, if you were able to unsecure the VM, Firefly Host would simply secure it again automatically.

Instead, you must first remove the VM from the automatically secured group that it belongs to, or, if it is an individual VM, remove the policy from it, and then unsecure it.

**Related
Documentation**

- [Understanding Firefly Host on page 3](#)
- [Understanding the Firefly Host VM](#)

CHAPTER 7

VMware Auto Deploy for ESXi Servers and with Firefly Host

- [Understanding VMware Auto Deploy for ESXi Servers and with Firefly Host on page 77](#)
- [Configuring VMware Auto Deploy and Firefly Host to Secure ESXi Hosts on page 78](#)

Understanding VMware Auto Deploy for ESXi Servers and with Firefly Host

Firefly Host allows you to secure automatically ESXi hosts generated through the VMware Auto Deploy feature. This topic covers Auto Deploy and Firefly Host automatic installation of Firefly Host VMs for these hosts. It includes the following sections:

- [About VMware Auto Deploy on page 77](#)
- [Firefly Host Support for Auto Deploy on page 77](#)
- [Firefly Host Automatic Installation of a Firefly Host VMs on page 78](#)

About VMware Auto Deploy

VMware Auto Deploy leverages the network Preboot Execution Environment (PXE) to rapidly provision large numbers of ESXi hosts to efficiently and easily managing their hypervisor installation and upgrades. ESXi hosts that are deployed through Auto Deploy are automatically added to a host cluster. New hosts are provisioned based on user-defined specifications. You can define specifications for various hypervisor images and host profiles to be used for different hosts.

After an ESXi host is network-booted from a central Auto Deploy server, a software image is installed on it and a vCenter host profile is then used to configure the host. When this process is done, the ESXi host is connected to vCenter, where you can create virtual machines (VMs). Apart from defining rules governing images and profiles for collective use, this process is entirely automated, allowing for quick provisioning without user intervention.

Firefly Host Support for Auto Deploy

Firefly Host is designed to work in tandem with VMware Auto Deploy. It complements VMware Auto Deploy by allowing you to automatically secure ESXi hosts. You can configure Firefly to automatically install Firefly Host VMs on these hosts based on clusters

that they belong to, on all ESXi hosts created through auto-deploy, or on none of them, effectively disabling the feature.

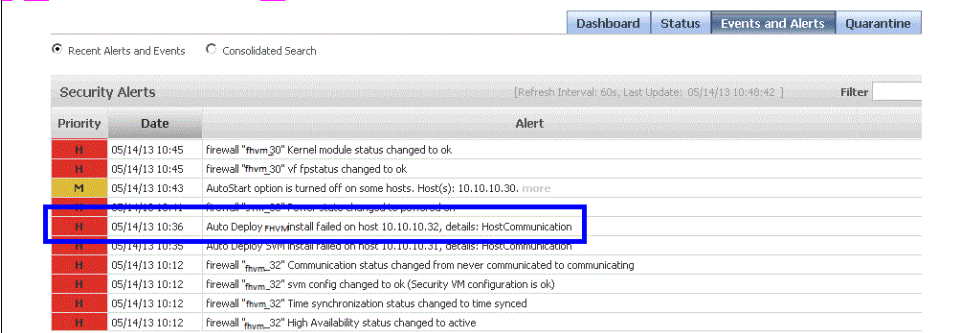
Firefly Host assigns a name to an automatically installed Firefly Host VM based on a prefix that you specify (Firefly Host VM Name prefix) when you configure Firefly Host auto deploy support and an octet derived from the host's IP address.

Firefly Host Automatic Installation of a Firefly Host VMs

Firefly Host detects if an ESXi host has been added to the clusters that you selected when you configured Firefly Host Auto Deploy support. For ESXi hosts in a selected cluster, it determines if a Firefly Host VM is already installed on that host.

- If a Firefly Host VM is already installed, Firefly Host ensures that networking is set up to properly handle hosts that have been rebooted. (Restoring the network restores connectivity between the Firefly Host V and the fastpath module.)
- If a Firefly Host VM is not installed on the host, Firefly Host treats the ESXi host as one that was added to the cluster by the VMware Auto Deploy process. In this case, it follows the same process that it uses to install a Firefly Host V under normal conditions except for the following actions:
 - It verifies that the port group and the data store exist.
 - It omits the step that installs the fastpath module and the step that reboots the ESXi host because it is assumed the fastpath module was already embedded in the image that was deployed on the host.
 - If a failure occurs, it generates an alert as shown in [Figure 37 on page 78](#).

Figure 37: Firefly Host Failure Alert



Priority	Date	Alert
H	05/14/13 10:45	firewall "fwvm_30" Kernel module status changed to ok
H	05/14/13 10:45	firewall "fwvm_30" vf fpstatus changed to ok
M	05/14/13 10:43	AutoStart option is turned off on some hosts. Host(s): 10.10.10.30, more
H	05/14/13 10:41	firewall "fwvm_30" Power state changed to powered on
H	05/14/13 10:36	Auto Deploy revm install failed on host 10.10.10.32, details: HostCommunication
H	05/14/13 10:35	Auto Deploy svm install failed on host 10.10.10.31, details: HostCommunication
H	05/14/13 10:12	firewall "fwvm_32" Communication status changed from never communicated to communicating
H	05/14/13 10:12	firewall "fwvm_32" svm config changed to ok (Security VM configuration is ok)
H	05/14/13 10:12	firewall "fwvm_32" Time synchronization status changed to time synced
H	05/14/13 10:12	firewall "fwvm_32" High Availability status changed to active

Related Documentation

- [Installing Firefly Host VMs on ESX/ESXi Hosts on page 35](#)
- [Understanding the Firefly Host VM Settings](#)
- [Understanding the Firefly Host Dashboard](#)

Configuring VMware Auto Deploy and Firefly Host to Secure ESXi Hosts

You can configure Firefly Host to monitor clusters for ESXi hosts that are provisioned through VMware Auto Deploy to install Firefly Host VMs on them automatically.

This topic first explains how to set up VMware for Auto Deploy.

- [Configuring Auto Deploy in VMware on page 79](#)
- [Configuring Firefly Auto Deploy Support on page 84](#)

Configuring Auto Deploy in VMware

VMware for Auto Deploy allows you to deploy ESXi 5.0 hosts and their associated configurations automatically.

To set up VMware Auto Deploy, you install a vCenter server, a vSphere client, the Auto Deploy service, a DHCP server, a TFTP server, and the Image Builder PowerCLI and Powershell. PowerCLI and Powershell is a commandlet and scripting language that allows you to build ESXi-based images and create rules to push out those images to your ESXi hosts.

The Auto Deploy service is a Web server that serves up ESXi images. The Auto Deploy service is embedded in the vCenter server appliance (vApp). When you install that appliance, Auto Deploy is automatically configured.

However, to configure Auto Deploy completely you specify the location for the repository where the ESXi images are stored and the repository size. You also configure an Auto Deploy connection to the vCenter server, and you specify the IP address that the Auto Deploy service should use to communicate with the network.

This topic provides information based on VMware instructions. If you encounter problems configuring VMware Auto Deploy, refer to the VMware documentation.

This process requires the following virtual machines (VMs), connectivity, and components:

- VMs. You must create VMs for:
 - VMware vCenter.
 - VMware Auto Deploy.

Install the Auto Deploy service on the same VM as vCenter, preferably.

- VMware vSphere to run PowerCLI, which requires Powershell.
- A DHCP server.
- A TFTP server.

A TFTP server is required to push the boot loader to the ESXi host. You can install it wherever you choose, including on the same VM as the vCenter server. You can install any TFTP server, for example, SolarWinds or Open TFTP.

When you install the TFTP server:

- Disable Internet Explorer ESC in MS Windows. If it is not disabled, error messages are generated reporting that you do not have access permission.
- Ensure that the timeout settings allow sufficient time to boot at least four ESXi hosts concurrently.

- Ensure that access to the TFTP server is granted.

After you complete the installation process, the TFTP folder contains the boot loader that is streamed to the ESXi host.

- There must be at least one ESXi host whose MAC address you know.
- You must have control over the IP assignment on the network.
- You must create a virtual switch (vSwitch) in VMware for Firefly Host with two port groups: one for the Firefly fastpath driver module and another for Firefly Host VM.

There are two ways to create and configure a vSwitch.

- You can use the vSphere Client Add Network wizard. It guides you through processes to create a virtual network, including how to create a vSwitch.
- You can use the VMware vSphere Configuration > Networking > Virtual Switch view for the selected ESXi host.

You must use the following names for the vSwitch and the fastpath driver port group.

- Use vmservice-vswitch as the name for the vSwitch.
- Use vmservice-vmknic-pg as the fastpath driver port group name.

There are no requirements for the name that you give to the Firefly Host VM port group. Normally the Firefly Host Dashboard generates this name based on the Firefly Host VM ID. Because the Firefly Host VM does not yet exist, this information is not available.

When you configure VMware Auto Deploy, you create one or more ESXi image profiles that are used to configure the ESXi hosts that Auto Deploy generates. You can clone an existing profile using the **new-esximageprofile** command. In that case, specify the name of the existing profile as the value of **-cloneprofile**.

You must derive the image profile name from the name of the ESXi software depot. It must follow the version number of the depot file that you retrieve during the configuration process, for example **"VMware-ESXi-5.0.0-469512-standard"**.

If the value that you specify for **-cloneprofile** generates an error, for example, because the VMware naming scheme has changed, you can retrieve a list of profiles to find the correct profile name. The name should have the same six-digit build number as that of the depot ZIP file. To get a list of profile names, in PowerCLI enter:

"Get-EsxImageProfile?"

You must configure Firefly to automatically install Firefly Host VMs on the ESXi hosts provisioned by VMware Auto Deploy.

- Install the fastpath driver version that Firefly Host installs normally when it installs Firefly Host VMs.
- Set the net.dvfilterbindipaddress (Net.DVFilterBindIpAddress) property for the selected ESXi host to 169.254.65.1. In vSphere select **Configuration > Software**, and click **Advanced Settings**.

To install the Auto Deploy service and to create an Auto Deploy image profile:

1. Install vCenter server 5.0, if it is not already installed.
2. Install the vSphere 5.0 client, if it is not already installed.
3. Install the Auto Deploy service.

To verify that the Auto Deploy service is connected and configured, in vSphere, click **Home > vCenter Service Status**.

4. Install a TFTP server.
 - a. In vCenter, select **Home > Administration > Auto Deploy**, and then click **Download TFTP Boot Zip**.
 - b. Download the ZIP file and extract the contents to the root folder on the TFTP server.
 - c. Configure the TFTP server and start the server instance.
5. Install the PowerCLI and Powershell.

Change the execution policy.

set-executionpolicy remotesigned

6. Get the required images.
 - Using PowerCLI, download the ESXi software depot (repository).

This is not the ISO image. It is a VMware file that has a name similar to the following one:

VMware-ESXi-5.0.0-469512-depot.zip
 - Get the Firefly VIB ZIP file.

There are no restrictions on where you download it.
7. Using PowerCLI, create the Auto Deploy image profile and add the ESXi image to it.

The image profile contains all modules and features that you want bundled.

All ZIP file names must include the .zip extension.

- a. Connect to vCenter.

connect-viserver localhost

- b. Add the ESXi depot.

add-esxsoftwaredepot ESXi-depot-zip-full-path

- c. Add the Firefly VIB ZIP file.

add-esxsoftwaredepot VIB-zip-full-path

Specify the full path to where you downloaded the VIB ZIP file and include the ZIP filename.

- d. Create an ESXi image profile and add the ESXi image to it.

```
new-esximageprofile -cloneprofile "VMware-ESXi-5.0.0-469512-standard" -name  
"image-profile-name"
```

- e. Add the Firefly VIB to the image profile.

```
add-esxsoftwarepackage -imageprofile "image-profile-name" --softwarepackage  
dvfilter-altor-vf
```

To obtain image profile software package names, enter:

```
get-esxsoftwarepackage
```

- f. Create a deploy rule. The deploy rule downloads and installs all of the modules for the image into the Auto Deploy repository.

```
new-deployrule -name "auto-deploy-rule-name?" -item "image-profile-name?"  
-AllHosts?
```

- Specify the name of the image profile that you created previously.
- Specify a name for the deploy rule to add to the image profile ("auto-deploy-rule-name").



NOTE: The example rule specifies that the image applies to all hosts (-AllHosts?).

- g. Create an image profile ZIP file and export it to where you want the file to reside.

```
export-esximageprofile -imageprofile "image-profile-name?" -exporttobundle  
-filepath image-profile-location-full-pathname.
```



WARNING: PowerCLI is session based. If you exit the PowerCLI session without first exporting the bundle to the repository, the image cannot be reused.

- h. Add the deploy rule that you created.

```
add-deployrule -deployrule "auto-deploy-rule-name?"
```

8. Set up DHCP to network-boot the ESXi host:

- Get the MAC address of the ESXi host.
- On the DHCP server:
 - Create an IP reservation for the ESXi host using its MAC address.
 - Add option 66 (Boot Server Host Name - TFTP server IP).
 - Add option 67 (Bootfile Name - undionly.kpxe.vmw-hardwired).

9. Boot the ESXi host.



NOTE: The ESXi host should appear in a vCenter data center automatically.

10. Verify that the Firefly VIB was installed. Select the ESXi host, click the **Hardware Status** tab, and expand **Software Components** to ensure that `dvfilter-altor-vf` exists.

You must set up a host profile for the cluster where your hosts will be booted.

1. Before you create the host profile, set up the following components.
 - The network and storage.
 - Additional vNICs.
2. If you have multiple clusters, create a separate deploy rule for each ESXi host to direct the new host to a specific cluster. For example:

```
New-DeployRule -name "HostCluster" -item cluster-name -Pattern
"ipv4=10.70.1.1-10.70.1.250"
```

```
Add-DeployRule -DeployRule HostCluster
```

3. Use **Security configuration > Administrator password** to configure the administrator password after you create the host profile.

Configuring Firefly Auto Deploy Support

Configure Firefly Host to install a Firefly Host VM on selected ESXi hosts that were deployed through VMware Auto Deploy. Use the Automatic Securing of Auto-deployed hosts pane on the Settings > Firefly Application Settings > Install Settings page. See [Figure 38 on page 84](#).

Figure 38: Configuring Automatic Installation of Firefly Host VMs for Auto-Deployed ESXi Hosts

Firefly Host automatically installs a Firefly Host VM on the selected hosts.

1. Select the ESXi hosts to secure.
 - **No hosts**—No hosts will be secured.
 - **All hosts**—All hosts will be secured.
 - **Hosts in the following clusters**—Only hosts in the clusters that you identify will be secured. Select the check box for each cluster that you want to include.
2. Specify a prefix to use as part of the name that is assigned to automatically installed Firefly Host VMs. Select the port group and the datastore to use.
 - **Firefly Host VM Name prefix**—Firefly Host automatically assigns a name to a Firefly Host VM using the value you specify as the prefix. To create the complete name, it prepends the value to the last octet of the ESXi host IP address in the format `[prefix]_[octet]`.

For example, if you used Firefly Host VM_ as the prefix, if the last octet of the ESXi host IP address to secure was 123, the name Firefly Host VM_123 would be assigned to the Firefly Host VM for that host.

- **Port Group**—From the **Port Group** list, select the network label for the port groups.

Port groups serve as anchor points for VMs that connect to labeled networks. A port group is identified by a unique network label. The same network label is used for all port groups in a datacenter that are physically connected to the same network.

When you select either All Hosts or specific clusters, Firefly Host updates the port group selection list. The list includes only port groups that are common to *all* connected hosts.

This behavior applies if you select one cluster or more than one.

- **Datastore**—From the Datastore list, select the datastore to use for the Firefly Host VMs.

When you select either All Hosts or specific clusters whose hosts are to be secured, Firefly Host updates the datastore list to include their datastores. The list includes only options that are common to *all* connected hosts. If there are no datastores that are on *all* hosts, the list is empty. However, if there is only one connected host, the list will show all of the datastores on that host.

This behavior applies to all clusters, whether you select one or more.

3. Select the method to use to acquire IP addresses for the Firefly Host VMs.

- **Method**—Select either DHCP or static.
- **IP Address**—If Method is set to static, specify the static IP address to assign to the Firefly Host VM.
- **Network Mask**—Specify the network mask to use in the IP address for the Firefly Host VM.
- **Default Gateway**—Specify the default gateway for the Firefly Host VMs.

4. Reset the error count to override the limit restricting the number of times that Firefly Host is allowed to attempt to install a Firefly Host VM on a host after repeated failures, reset the error count. Select **Force recheck on all hosts**.

Firefly Host maintains a count of the number of failed attempts for each host. When that count is exceeded, it no longer tries to install a Firefly Host Security VM on it. The installation attempts limit is set in the **center.auto.deploy.Firefly Host**

VM.install.retry.count parameter, which has a default of three times. If you select this check box, the count is reset. It is also reset if you modify configuration settings.

You can create a per-host XML configuration. If you do this, the file must reside at `/usr/lib/tomcat/webapps/ROOT/WEB-INF/autoDeploy.xml`. You can find the xsd to use at:
<http://vgw-milford.juniper.net/trac/browser/center/branches/fullers/schemas/autoDeploy.xsd>.

If the static IP and IP or netmask or gateway are not set, the fallback behavior is to use configuration information set in the Firefly Host Dashboard.

- If the static IP and IP or netmask or gateway are not set, the fallback behavior is to use configuration information set in the Firefly Host Design VM is used.

For example, if you set the IP method to DHCP in the Firefly Host Dashboard and a per-host configuration host entry does not have the IP configuration method specified, then the Firefly Host VM for that host would get DHCP.

- If the port group or datastore are not found, the installation is canceled and a message is issued in the error log.

CHAPTER 8

Firefly Host Firewall Module

- [Understanding the Firefly Host Firewall Module on page 87](#)
- [Understanding How Firefly Host Handles ICMPv6 Protocol Traffic on page 101](#)
- [Understanding Predefined Objects for Firefly Host Firewall Policy Terms on page 105](#)
- [Configuring Firefly Host Firewall Policies on page 108](#)
- [Understanding Firefly Host Predefined Firewall Policy for Its Components on page 115](#)

Understanding the Firefly Host Firewall Module

This topic covers the Firefly Host Firewall module that allows you to create reusable and individual policy rules to use in building policies for groups of VMs and individual VMs. You also use the Firewall module to apply those policies to VMs.

Before it covers the Firewall module interface, this chapter explains the policy module concepts that are fundamental to constructing firewall policies.

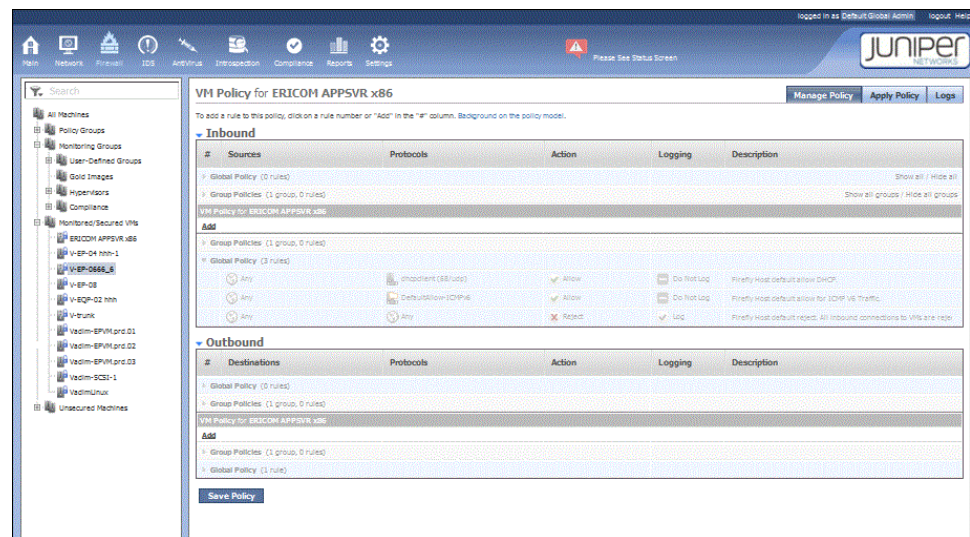
This topic contains the following sections:

- [The Firewall Module and the VM Tree on page 87](#)
- [Overview of the Firewall Policy Model on page 88](#)
- [Global Policy, Group Policy, and Individual VM Policy Tiers on page 89](#)
- [Firewall Policy Structure and Policy Rules Precedence on page 92](#)
- [Viewing the Complete Policy Rule Base for a VM on page 94](#)
- [The Manage Policy Tab on page 94](#)
- [The Apply Policy Tab on page 98](#)
- [The Logs Tab on page 100](#)

The Firewall Module and the VM Tree

The Firewall module of the Firefly Host Dashboard allows you to define, apply, and monitor security policies. To change the data displayed on a Firewall module page, select all, one, or more than one VM in the VM tree. If you select one or more VMs, but not all, information pertaining to only the selected VMs is displayed. [Figure 39 on page 88](#) shows information for a single VM.

Figure 39: Firewall Module Policy for a Single VM



Overview of the Firewall Policy Model

Security administrators of virtualized data centers invest a great deal of time and effort in planning their virtual infrastructures and building them out into group structures and categories to segment their VMs appropriately. The firewall policy model that they use to secure their virtualized infrastructure must be designed to accommodate the complexities that are intrinsic to the data center. Defining policy rules and building a firewall inside the middle of the data center differs in fundamental ways from building a perimeter firewall. Additionally, security for the virtualized data center infrastructure includes many challenges not the least of which is management of firewall policies for a large number of VMs.

The Firefly Host Firewall policy used to secure the virtualized data center is modeled on the data center infrastructure overall, and it is purpose-built to meet its requirements.

- It entails group policy constructs to address group structures.
- It provides a means of simplifying the daunting task of creating policies for a large and increasing number of individual VMs.

You can create reusable policies to apply across all VMs and groups of VMs, and you can define policy rules for individual VMs.

- It allows for flexible nesting to let you define policy rule precedence within these structures as they apply to an individual VM. You can change the order of rules within global, group, or individual sets of rules to control the effect of the policy.
- It addresses the need to build flows between different systems with greater granularity than a perimeter firewall design would entail.

Ultimately every VM has its own complete firewall policy, which is composed of some or all of these parts:

- Rules that apply to all VMs in your environment. Every VM policy contains Global Policy rules.
- Rules that apply to the individual VM *and* others like it, if a VM belongs to a group (Group Policy rules).
- Rules that apply only to that VM, if any are required (individual VM Policy rules).

If a VM contains multiple vNICs, you can define separate policy rules for individual vNICs. These policy configurations show up in the VM rules section. See *Configuring the Firefly Host Policy per vNIC Feature*.

The combination of these parts gives a VM a unique firewall rule base.

Global Policy, Group Policy, and Individual VM Policy Tiers

As with many firewall designs, the Firefly Host firewall policy rules are applied in a top-down fashion. To ease management of a large number of VMs and to give you control over when rules are applied, the Firefly Host firewall policy allows you to define policy at three tiers: the Global Policy tier, the Group Policy tier, and the VM Policy tier. You create a Global Policy and one or more Group Policy rule sets separately. Firefly Host nests them appropriately for the individual VM when you create its policy. You can move policy rules within a tier to change precedence, controlling the order in which rules are executed.

At first glance the Firefly Host firewall policy nesting model might seem complex, but its simplicity and usefulness become evident as you become familiar with the symmetry at the Global Policy and Group Policy tiers and the precedence relationship within a tier and among the tiers. The Global Policy tier has high-level and low-level sections that bound the policy; the Group Policy tier is nested within the Global Policy tier and it too has high-level and low-level sections. Individual VM Policy rules are nested at the center of a VM's policy between the Group Policy high-level and low-level sections.

Although a VM policy could contain policy rules at all three tiers, it is not necessarily the case. The following sections cover each of the policy tiers in particular, but to gain an overall sense of how they can be combined to create a policy consider the following:

Ultimately every VM has its own complete firewall policy, which is composed of some or all of these parts:

- Rules that apply to all VMs in your environment. Every VM policy contains Global Policy rules.
- Rules that apply to the individual VM *and* others like it, if a VM belongs to a group (Group Policy rules).
- Rules that apply only to that VM, if any are required (individual VM Policy rules).

If a VM contains multiple vNICs, you can define separate policy rules for individual vNICs. These policy configurations show up in the VM rules section. See *Configuring the Firefly Host Policy per vNIC Feature*.

Global Policy and Group Policy rule sets contain Inbound and Outbound parts.

Global Policy

You define a reusable Global Policy whose rules apply to every VM in your environment once—it is *global*. In that it is included in every VM's policy, the Global Policy is very powerful.



NOTE: Although it is possible to delete all rules from the Global Policy, the concept of the Global Policy as applied before any other rules in the policy remains enforced. If you deleted all global rules, an empty Global Policy would be applied to the VM.

Not to diminish their usefulness, you should take care in creating rules at the Global Policy level for the very fact that they are inherited by everyone.

Both the Inbound and Outbound parts of a firewall policy contain Global Policy sections. As is the case with many firewall configurations, by default the Global policy is restrictive. It is configured to allow inbound DHCP traffic and then to reject all other inbound traffic.

You can think of the Global Policy as a template or a container for the other nested parts that will compose the entire firewall policy for any VM, keeping in mind that the Global Policy itself consists of rules.

For both the Inbound and Outbound parts of a firewall policy, the Global Policy is segmented into the following two sections:

- High-level Global Policy rules

These rules are positioned at the top of each part of a firewall policy. They are always applied to every VM first, whether that VM belongs to a group or is an individual VM. You use high-level Global Policy rules to enforce policy that cannot be overridden by any individual VM Policy rule.

For example, in addition to enforcing corporate policy, you might use high-level Global Policy rules to prevent outbreaks and protect against vulnerabilities. You might add a Global Policy rule to block access to a vulnerable service until it is updated with all of the required patches.

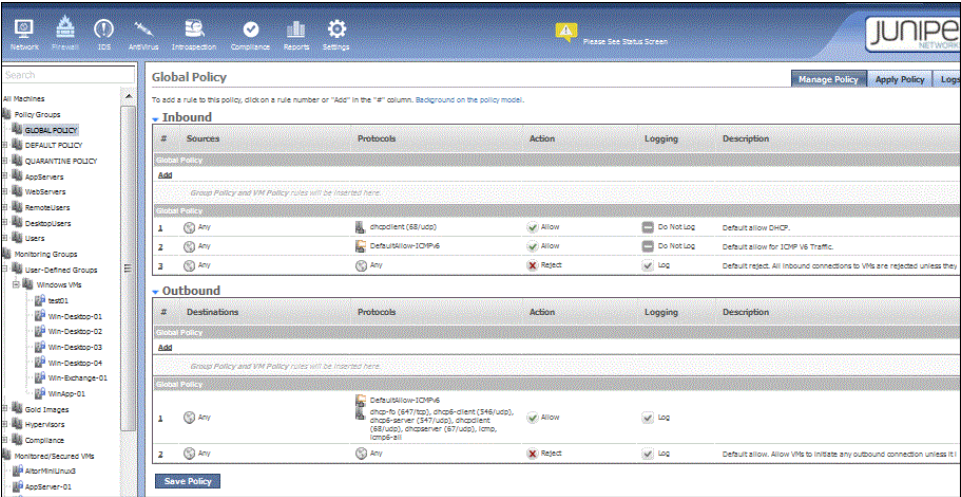
- Low-level Global Policy rules

These rules are positioned at the bottom of each part of a firewall policy. In any overall individual VM's firewall policy, they are applied last. They are applied to every VM. For example, for the Inbound part of a Global Policy, if an incoming connection is processed according to the appropriate firewall policy and it does not match any of the preceding rules, it falls through to the Inbound low-level Global Policy rules. Low-level Global policy rules are typically used as clean-up rules. By default, the Inbound low-level Global Policy rule rejects all connection attempts. It is defined as any-any-reject.

Between the high-level and low-level sets of Global Policy rules is a placeholder that allows for nesting of Group Policy rule sets and individual VM Policy rules.

To create a Global Policy, you select **GLOBAL POLICY** under Policy Groups in the VM tree. The page shown in [Figure 40 on page 91](#) is displayed.

Figure 40: Global Policy



Group Policy

Most of the daily policy management that security administrators of virtualized environments carry out is at the group level. Most likely you have structured your environment along lines of groups of VM with similar characteristics and you want to apply a similar policy to VMs that are members of a group.



NOTE: In the nested model, a VM might belong to a Policy Group and inherit the Group Policy rules defined for that group, but it also might have its own individual VM Policy rules that contribute to its overall firewall policy rule base.

For example, you might organize VMs into functional groups such as Web servers and database servers, and you might want to apply a different set of policy rules to each group. In your environment, you might create different groups for MS Windows systems versus Linux systems. To apply the appropriate security, you could define a different Group Policy for each of them.

The Group Policy concept allows you to define policy rules that are relevant to the VMs that comprise the group. As new VMs are created and added to a Policy Group, the Group Policy associated with the group is applied to them.

A VM might belong to multiple Policy Groups. For example, a VM might be a Windows VM and belong to the Windows group, but it also might be used as a Web server and belong to the Web servers group. In this case, the VM gets the Group Policy rules for both groups.

Individual VM Policy Rules

At the center of the entire firewall policy for an individual VM are any particular VM Policy rules that you define for that VM. Until this point, the firewall policy for an individual VM is composed of reusable parts—the Global Policy and, if the VM belongs to any Policy Groups, Group Policy rules.

You can apply individual VM Policy rules to a VM policy for particular purposes that distinguish that VM's policy from others. For example, you might want RADIUS access to a VM that is not applied at the Global Policy or Group Policy levels. To accomplish that, in the VM's firewall policy, you would define an Inbound VM Policy rule that allowed RADIUS access to the VM.

Default Policy

A newly created VM that does not have a group policy associated with it is automatically assigned the Default Policy. Later if it becomes a member of a policy group, then it inherits that group's Group Policy rules, and the Default Policy rules no longer apply.

Quarantine Policy

When a VM is infected by a virus and the scanning configuration specifies "Quarantine the VM", the VM is put in the Quarantine policy group. The Quarantine Policy that you define is applied to all VMs in the Quarantine policy group. When you remove the VM from the group, the Quarantine policy is removed.

To remove the VM from the Quarantine policy group, use the Main module Quarantine tab. Select the VM, and click **Un-quarantine**.

For details on how the parts of the quarantine process work together for a quarantined VM, see "Understanding Quarantined VMs and How to Manage Them" on page 152.

Firewall Policy Structure and Policy Rules Precedence

The Firefly Host Firewall policy model is premised on a pre-post concept that allows you to manage rules execution precedence.

Consider the nested structure of a firewall policy. To summarize the order, a firewall policy has inbound and outbound sections. The Inbound section contains the high-level Global Policy rules followed by, the Group Policy rules, then the individual VM Policy rules, and finally the default Global Policy rules. The default Global Policy rules consist of a rule to allow DHCP traffic, a rule to allow certain types of ICPMV6 traffic, and, at the bottom, a rule to reject all other inbound traffic. The outbound section contains the same parts in the same order, only its Global Policy section contains a single rule that allows VMs to initiate outbound connections.

high-level Global Policy— At the top of the Inbound section is the high-level Global Policy tier, containing any global policies that you add.

high-level Group Policy—Beneath it is the high-level Group Policy section containing any of Policy Groups rule sets that apply to the individual VM that you want executed *before* the individual VM Policy rules.

VM Policy—Beneath it is the high-level VM Policy section containing any individual rules that you define for the VM whose policy you are creating.

low-level Group Policy—Beneath it is the low-level Group Policy section containing any group rule sets for the VM that you want to be executed *after* its individual ones.

Default Global Policy—The default Global Policy rules consist of a rule to allow DHCP traffic, a rule to allow certain types of ICPMv6 traffic, and, at the bottom, a rule to reject all other inbound traffic.

It is this structure that allows you to manipulate the order in which rules are executed for the individual VM firewall policy. The Firefly Host Policy model affords you extensive, flexible control over the order in which rules are executed. You can move rules up and down within their sets; you can move rules from a low-level section of one tier to that tier's high-level section or the opposite, and you can reorganize individual VM Policy rules.

Rules are executed in a top-down fashion:

- High-level Global Policy rules are always executed first, and that cannot be changed. However, you can manage the order in which Global Policy rules are executed by moving them up and down in the set.
- High-level Group Policy rules are executed next. They are always executed before individual VM Policy rules, but you can also change the order in which they are executed by moving them up and down within the set.
- Individual VM Policy rules are executed next, and you can change their order to control when they are executed.
- Low-level Group Policy rules are always executed after the individual VM Policy rules.

By placing some of the Group Policy's rules in its low-level section, you are able to specify that in most cases you want these rules applied to all VMs that belong to the Policy Group *after* the individual VM Policy rules are executed. You will allow VM Policy rules for individual VMs to take precedence over these Group Policy rules.

- Finally, low-level Global Policy rules are executed for every VM.

For example:

- If you move a rule *up* from its low-level Group Policy section to its high-level counterpart, that rule is executed *before* any individual VM Policy rule, and it *cannot* be overridden by a VM Policy rule. Previously, when it resided in the low-level Group Policy section, a VM Policy rule could override it.
- If you move a rule *down* from its high-level Group Policy section to its low-level counterpart, that rule is executed *after* any individual VM Policy rule, and it *can* be overridden by a VM Policy rule. Previously, when it resided in the high-level Group Policy section, a VM Policy rule could not override it.

When you nest rules for a VM's firewall policy, take into account precedence among the various levels of the policy. For example, consider a policy for a VM whose inbound low-level Group Policy section includes a rule that allows management access to the

VM. Suppose that as the data center administrator you will always want management access to the VM. However, you understand that another administrator could create a firewall policy intended for an individual VM that is a member of the Windows VMs group as part of the group policy. That administrator could define a VM Policy rule for the individual VM that would reject management access to the VM, effectively denying you access. Because the Group Policy rule allowing access is in the low-level section of the Group Policy rule set, the individual VM Policy rule would override it.

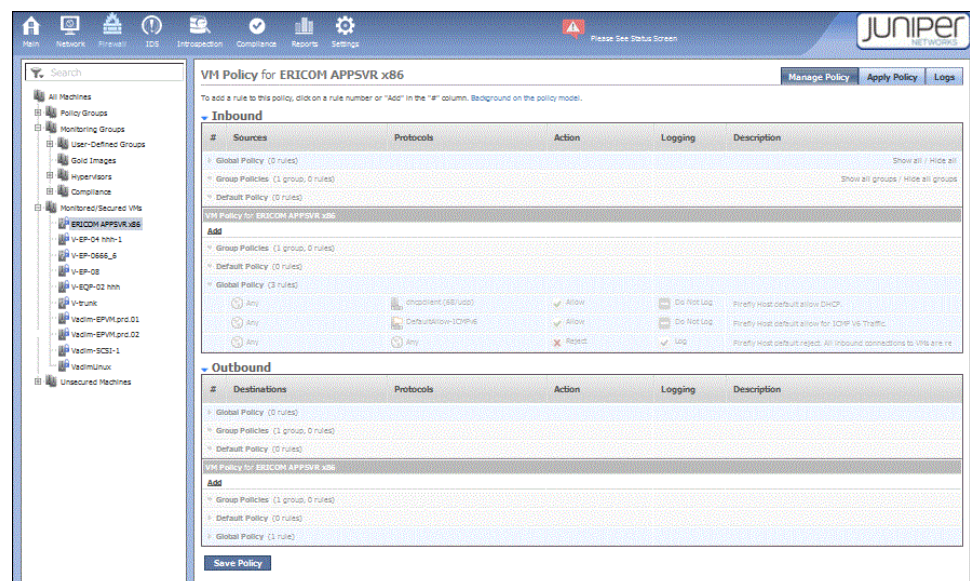
To ensure that you always have management access, you could affect the precedence in the policy for any VM that belongs to that group by moving the rule that allows management access up from the low-level Group Policy section to the high-level Group Policy section. To do so, click the rule number in the low-level Group Policy and select **Move Rule Up** from the list.

Viewing the Complete Policy Rule Base for a VM

Each VM protected by a Firefly Host firewall policy can be thought of as having its own firewall policy. The resulting full policy for a VM always includes a Global Policy, Group Policies if the VM belongs to Policy Groups, and individual VM Policy rules that are specific to it.

After you have created a firewall policy for a VM or you want to understand its policy, you can expand it to see its entire rule base. To do this, select the Firewall module. In the VM tree, select the VM. On the upper-right side of the VM Policy page, click **show-all**. See [Figure 41 on page 94](#).

Figure 41: VM Policy Expanded Rule Base

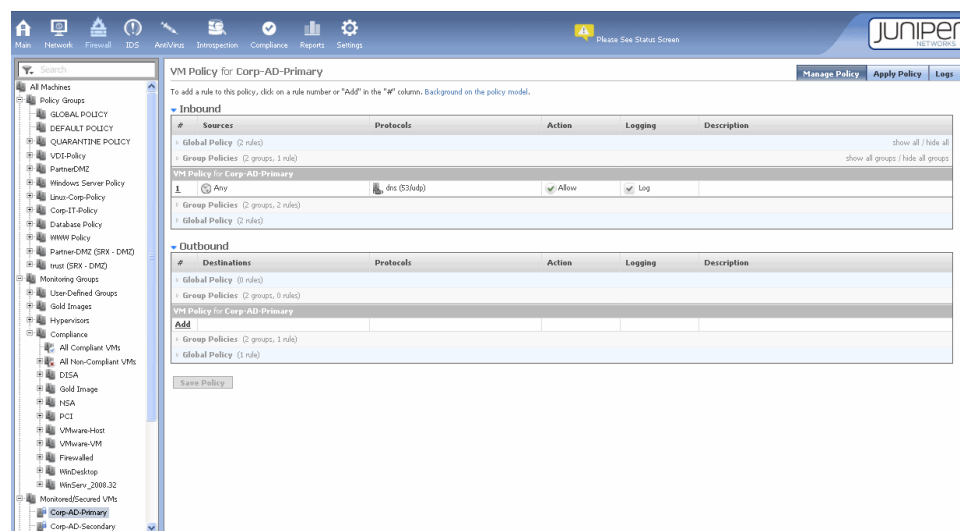


The Manage Policy Tab

The Manage Policy tab allows you to define and edit security policies. The Manage Policy page shows the policy configured for the group of VMs or the VM that is selected in the VM tree. To change the data displayed on the Manage Policy page, select a different

object in the VM tree. You can select all machines, a group, or an individual VM. [Figure 42 on page 95](#) shows the policy for the Corp-AD-Primary VM.

Figure 42: Firewall Module Manage Policy Page



This section contains the following parts:

- [Policy Per vNIC and Dual Stack on page 95](#)
- [Creating a Policy Rule on page 95](#)

Policy Per vNIC and Dual Stack

A single VM may have multiple vNICs attached to it. In the case of a dual stack, a VM would have a vNIC with an IPv4 address and an IPv6 address bound to it.

Firefly Host provides a feature called Policy per vNIC that allows you to define separate policies for individual vNICs attached to the same VM. You can configure separate policies for individual vNICs, separate policies for some of them while leaving others unsecured, or you can use the same policy for all of them.

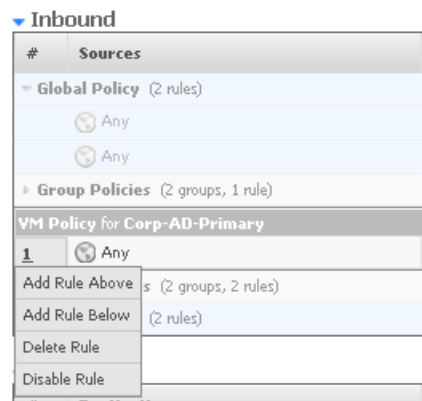
Using the Policy per vNIC feature, you can handily apply different policy rules to vNICs passing IPv4 traffic from those used for IPv6 traffic even when the vNICs are attached to the same VM. To apply the rule to all traffic of a type, you could use the predefined terms **Any-IPv4** and **Any-IPv6**.

Creating a Policy Rule

To create a policy rule:

1. Click a rule number in the rule numbers (#) column.
2. Select **Add Rule Above** or **Add Rule Below**. See [Figure 43 on page 96](#).

Figure 43: Adding a Rule



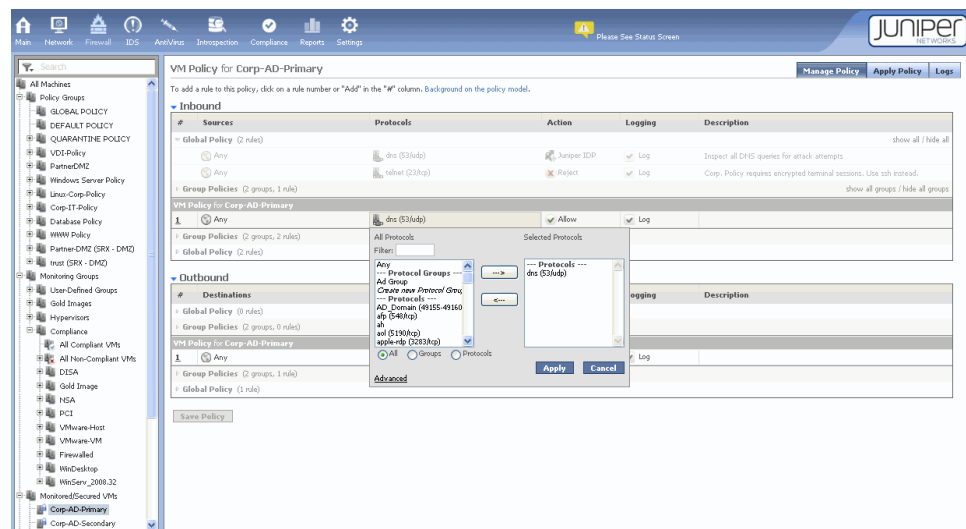
NOTE: Rules are applied in order of execution from top to bottom.

3. Configure policy settings by clicking the table cells and editing the information using the dialog box.

For example, to specify a protocol for the rule, click the default value **Any**, which displays a dialog box. To quickly make selections, type the first letter of the item that you want to select in the filter field. See [Figure 44 on page 96](#).

Typing the letter **t** in the All Protocols dialog box scrolls to the telnet selection in the list.

Figure 44: Using the Dialog Box Filter to Add Terms for policy rules



To immediately select an item, type directly into the Filter box.

To define a policy that contains all protocols except for a few:

1. Click **Advanced** at the bottom of the dialog box.
2. Click **Negate this selection**.
As a result, “All protocols except” is displayed at the top of the Selected Protocols list.
3. For each protocol or protocol group that you want to exclude from the policy rule, select the object and click the right arrow to move it to the list.
4. Click **Apply**, when you are finished.
5. When you have finished entering or editing all policy settings, click **Save** to save your changes in the Firefly Host Dashboard database.



WARNING: For new policy rules to take effect, you must apply the policy changes using the Apply Policy tab. You can apply rules immediately or during maintenance.

To delete or disable/deactivate an existing rule, click the rule number and choose the appropriate option. Disabled rules appear dimmed and are shown with a strike-through mark.

Table 4 on page 97 describes the policy configuration settings.

Table 4: Firewall Policy Configuration Settings

Field	Function
Sources	Define the object from which the connection originates.
Protocols	Define which protocols are used in the rule. You can also dynamically create a new protocol or protocol group by selecting the appropriate option.
Action	Allow the connection, drop the connection (silent drop), or reject the connection (drop traffic and send source a notification). In addition, you can redirect or duplicate packets to third-party devices using Settings > Security Settings > Global > External Inspection Devices. See <i>Configuring Global Settings Using the Firefly Host Settings Module (VMware)</i> .
Logging	Log the connection matching the rule, skip logging for this connection, or send an alert when this connection matches the rule. The Alert option directs the Firefly Host to send e-mail messages or SNMP traps. See “Alerts” on page 80.
Description	Enter a description for the policy.

The Apply Policy Tab

The Apply Policy tab allows you to push security policies out to the Firefly Host VM firewall to protect the VMs in your infrastructure. When you create or modify a policy, it is not applied to the VM automatically. For new policy rules to take effect, you must apply the policy changes using the Apply Policy tab. You can apply rules immediately or during maintenance.

You use the VM tree on the left side of the Apply Policy page to select the VMs to apply policies to.

Reflecting the hierarchy in which you create a VM policy, the Apply Policy table shows:

- That the VM has a Global Policy, its Group Policies, if it belongs to a group, and any individual policies configured specifically for it.



NOTE: If there are no Group or individual policy rules for a VM, the Global Policy is applied.

- If a VM has multiple vNICs, whether Policy per vNIC is applied to it.
- The Firefly Host VM that protects the VM.
- The date that the policy was installed.

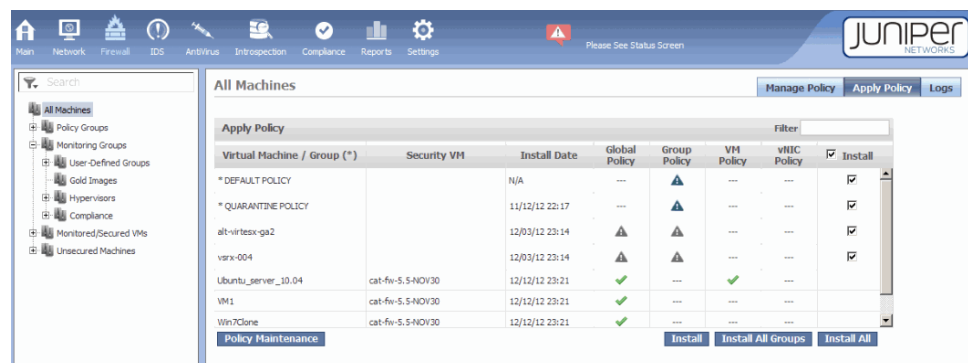
To install a policy on one or more selected VMs:

1. Select the **Install** check box at the right of the title bar.
2. Select the check box in the Install column at the right of the VM's row.
3. Click **Install** at the bottom of the page.

To install policies for all VMs, click the **Install** check box at the top of the column, then click **Install All**. To install policies for all Groups, click **Install All Groups**.

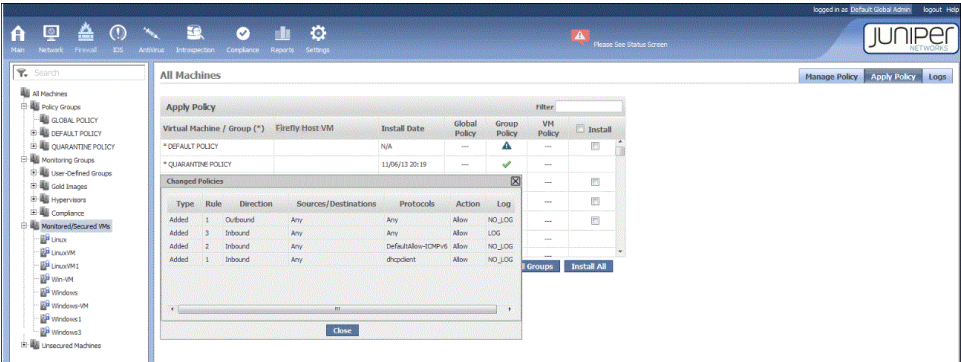
Figure 45 on page 98 shows the Apply Policy page.

Figure 45: Firewall Apply Policy Page








Click on warnings to view the changed policy rules. See [Figure 46 on page 99](#).

Figure 46: Changed Policies Dialog Box



See [Table 5 on page 99](#) for a list of icons displayed for VMs on the Apply Policy page.

Table 5: Firewall Policy Icons

Icon	Indicates that
	The policy is current and no further actions are required.
	The VM is in a policy group, but it cannot retrieve policies because it is not protected by a Firefly Host VM firewall. This usually indicates an error condition that you should investigate.
	<p>The policy type does not exist for the VM. For example, an individual VM policy for that VM is not configured.</p> <p>You are not required to build individual VM policies for each VM.</p>
	The policy has been modified, and it needs to be deployed for the VM.
	An error condition exists that prevents installation of the policy. When a policy distribution problem exists but the old policy works properly, a check mark icon might be displayed.



TIP: Place the pointer over a policy status icon to display a tool tip that describes the icon.

When you are ready to implement a policy, click either **install** or **install all** to push the policy out to the firewall. This action causes the policy to be deployed on the selected VMs or the vNICs of the VMs, if the Policy per vNIC feature is used.



NOTE: When you attempt to apply a policy to a vNIC that is not secured and that belongs to a protected VM, the policy is not applied. The following message is displayed:

“Policy was compiled and saved. This VM is currently not associated with a firewall, so the policy is not being immediately loaded on a firewall. This could be because the VMs migrated to an unprotected host or are powered off. Once the VM will be associated to a firewall, the corresponding saved policy will be enforced.”

The Logs Tab

You can define policy rules to specify Log, Don't Log, and Alert notification options. When you select **Log** or **Alert** for a rule, traffic that matches that rule is logged.

Figure 47 on page 100 shows the Logs tab.

For the Logs tab, you can use an advanced option that includes a mark verified VMs setting. Firefly Host uses the unique VMware ID/UUID in addition to an IP address to validate that connections are coming from the identified server. This feature protects the network from issues such as IP spoofing and DHCP changes. VMs for which this extra validation is allowed are flagged with an asterisk (*). You can use the mark verified VMs setting to display or hide the icon. Click **Auto-refresh** to refresh the log displayed automatically every 60 seconds.

The log entries show both IPv4 and IPv6 addresses.

Figure 47: Firewall Module Logs Tab

Start Time	Rule Id	Action	Source	Source Port	Destination	Proto	IP Proto	Record Id
09/02/11 10:47	29	Allow	Partner-SQL-eConn	46990/tcp	Partner-Web-eConn	mysql	tcp	19399997
09/02/11 10:47	5	Reject	VDI-Workstation2	65100/tcp	WWW-TT-1	http	tcp	19399996
09/02/11 10:47	5	Reject	VDI-Workstation2	65100/tcp	WWW-TT-1	http	tcp	19399995
09/02/11 10:47	5	Reject	VDI-Workstation2	65099/tcp	WWW-TT-1	http	tcp	19399994
09/02/11 10:47	5	Reject	VDI-Workstation2	65099/tcp	WWW-TT-1	http	tcp	19399993
09/02/11 10:47	5	Reject	VDI-Workstation2	65099/tcp	WWW-TT-1	http	tcp	19399992
09/02/11 10:47	5	Reject	VDI-Workstation2	65098/tcp	WWW-TT-1	http	tcp	19399991
09/02/11 10:47	5	Reject	VDI-Workstation2	65098/tcp	WWW-TT-1	http	tcp	19399990
09/02/11 10:47	2	Allow	Partner-Web-eConn	54391/tcp	Partner-SQL-eConn	mysql	tcp	19399989
09/02/11 10:47	2	Allow	Partner-Web-eConn	54390/tcp	Partner-SQL-eConn	mysql	tcp	19399988
09/02/11 10:47	2	Allow	Partner-Web-eConn	54389/tcp	Partner-SQL-eConn	mysql	tcp	19399987
09/02/11 10:47	2	Allow	Partner-Web-eConn	54388/tcp	Partner-SQL-eConn	mysql	tcp	19399986
09/02/11 10:47	29	Allow	Partner-SQL-eConn	43672/tcp	Partner-Web-eConn	http	tcp	19399985
09/02/11 10:47	29	Allow	Partner-SQL-eConn	43671/tcp	Partner-Web-eConn	http	tcp	19399984
09/02/11 10:47	29	Allow	Partner-SQL-eConn	43670/tcp	Partner-Web-eConn	http	tcp	19399983
09/02/11 10:47	29	Allow	Partner-SQL-eConn	43669/tcp	Partner-Web-eConn	http	tcp	19399982
09/02/11 10:47	29	Allow	Partner-SQL-eConn	43668/tcp	Partner-Web-eConn	http	tcp	19399981
09/02/11 10:47	29	Allow	Partner-SQL-eConn	46984/tcp	Partner-Web-eConn	mysql	tcp	19399980
09/02/11 10:47	29	Allow	Partner-SQL-eConn	46983/tcp	Partner-Web-eConn	mysql	tcp	19399979
09/02/11 10:47	29	Allow	Partner-SQL-eConn	46982/tcp	Partner-Web-eConn	mysql	tcp	19399978
09/02/11 10:47	29	Allow	Partner-SQL-eConn	46981/tcp	Partner-Web-eConn	mysql	tcp	19399977
09/02/11 10:47	29	Allow	Partner-Web-eConn	54391/tcp	Partner-SQL-eConn	mysql	tcp	19399976
09/02/11 10:47	29	Allow	Partner-Web-eConn	54390/tcp	Partner-SQL-eConn	mysql	tcp	19399975
09/02/11 10:47	29	Allow	Partner-Web-eConn	54389/tcp	Partner-SQL-eConn	mysql	tcp	19399974
09/02/11 10:47	29	Allow	Partner-Web-eConn	54388/tcp	Partner-SQL-eConn	mysql	tcp	19399973
09/02/11 10:47	33	Allow	Partner-SQL-eConn	43672/tcp	Partner-Web-eConn	http	tcp	19399972
09/02/11 10:47	33	Allow	Partner-SQL-eConn	43671/tcp	Partner-Web-eConn	http	tcp	19399971
09/02/11 10:47	33	Allow	Partner-SQL-eConn	43670/tcp	Partner-Web-eConn	http	tcp	19399970

You can use filters to refine the display of log entries. To display only those logs related to a specific VM, select the VM in the VM tree pane.

Related Documentation

- [Understanding the Firefly Host Policy per vNIC Feature](#)
- [Understanding the Firefly Host Dashboard](#)
- [Understanding the Firefly Host Dashboard Taskbar](#)
- [About the Firefly Host Dashboard Tree](#)
- [Understanding the Firefly Host Network Module on page 117](#)
- [Understanding Firefly Host on page 3](#)

Understanding How Firefly Host Handles ICMPv6 Protocol Traffic

This topic covers the Internet Control Message Protocol version 6 (ICMPv6) which is integral to IPv6 and fundamental to the proper functioning of IPv6 networks.

It describes the Firefly Host default firewall policy protocol group for handling ICMPv6 traffic.



WARNING: By default Firefly Host allows inbound and outbound ICMPv6 traffic. Juniper Networks strongly recommends that you not override this default policy because of the important role that ICMPv6 plays in establishing and maintaining communication in IPv6 networks.

- [About ICMPv6 on page 101](#)
- [Filtering ICMPv6 Packets on page 101](#)
- [Default Policy Group for Allowing Inbound ICMPv6 Packets on page 102](#)

About ICMPv6

ICMPv6 consists of a large number of messages with diverse functions which, like ICMP messages for IPv4 networks, could be categorized broadly as error and information messages.

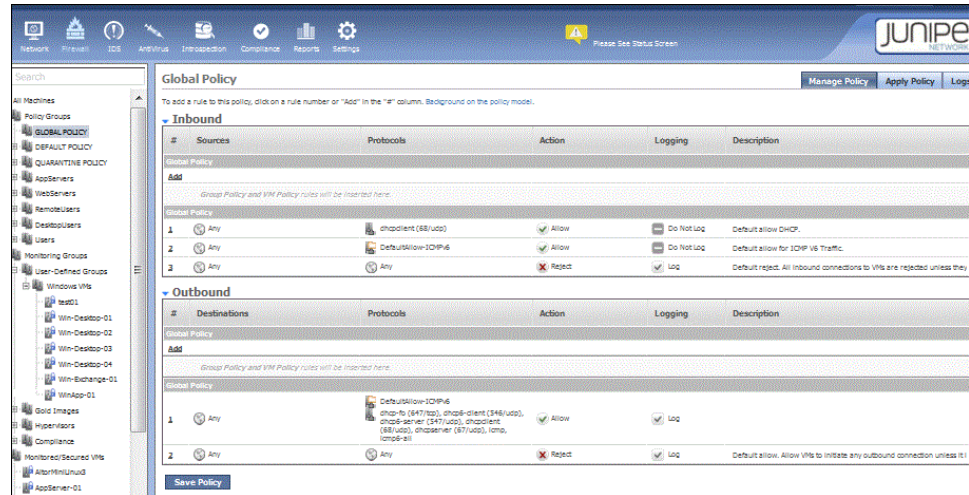
ICMP for IPv4 is an auxiliary protocol not necessarily required for IPv4 proper functioning. By contrast, ICMPv6 is an essential component in the establishment and maintenance of IPv6 communications. Among the messages it includes are those for address assignment, address resolution, and multicast group management. ICMPv6 error messages and information messages are transported by IPv6 packets in which the IPv6 Next Header value for ICMPv6 is set to 58.

Filtering ICMPv6 Packets

In IPv4 networks, it is common practice for firewalls to drop ICMP Echo Request messages to protect against scanning attacks and to minimize the risk of denial of service attacks. Port scanning in IPv6 networks is less severe, so it is not necessary to filter IPv6 Echo Requests. In practice, it is important to avoid aggressive filtering of ICMPv6 packets. Because they are fundamental to the proper functioning of IPv6 networks and tunneling, it is essential that ICMPv6 connectivity messages are allowed to pass through the firewall.

Firefly Host establishes a default protocol group called DefaultAllow-ICMPv6 that allows access to traffic from a comprehensive set of ICMPv6 protocols. A default rule for the DefaultAllow-ICMPv6 protocol is created that is applied to the inbound Global policy rule set to allow this inbound traffic. See [Figure 48 on page 102](#).

Figure 48: Default Global Policy Showing Default ICMPv6 Allow Group



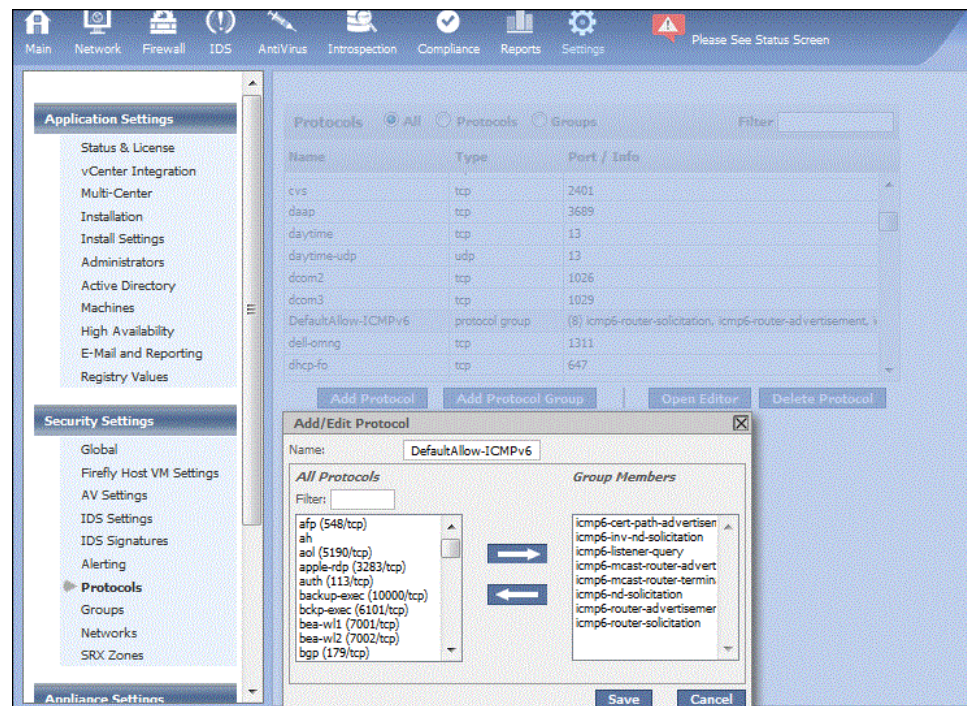
Default Policy Group for Allowing Inbound ICMPv6 Packets

Firefly Host provides the predefined DefaultAllow-ICMPv6 protocol group that allows inbound ICMPv6 traffic for all types of packets included in the group. Because ICMPv6 is critical to proper IPv6 functioning, it is important that you allow this traffic. However, if for some reason you wish to block traffic from one or more ICMPv6 protocols that are members of the default protocol group, you can edit the list to exclude them from the *allow* condition and filter the traffic. See [“Editing the Default ICMPv6 Protocols Group Members” on page 104](#).

Viewing the Default ICMPv6 Protocols Group Members

You can view the list of ICMPv6 protocols that comprise the DefaultAllow-ICMPv6 protocol group on the Settings module Security Settings > Protocols page. See [Figure 49 on page 103](#).

Figure 49: Protocols Settings ICMPv6 Default Protocol Group



To view the list:

1. Beside **Protocols**, select **Groups**.
2. Click **DefaultAllow-ICMPv6**.

The column on the right side of the Edit protocol group pane shows the group members:

- icmp6-listener-query
130. Multicast Listener Query (RFC 2710)
- icmp6-router-solicitation
133. Router Solicitation (RFC 4861)
- icmp6-router-advertisement
134. Router Advertisement (RFC 2461)
- icmp6-nd-solicitation
135. Neighbor Discovery Solicitation (RFC 4861)
- icmp6-inv-nd-solicitation
141. Inverse Neighbor Discovery Solicitation Message (RFC 3122)
- icmp6-cert-path-advertisement
149. Certification Path Advertisement Message (RFC 3971)
- icmp6-mcast-router-advertisement

151. Multicast Router Advertisement (RFC 4286)

- icmp6-mcast-router-termination

153. Multicast Router Termination (RFC 4286)

Editing the Default ICMPv6 Protocols Group Members

If you must block traffic on any of the ICMPv6 protocols in the Firefly Host DefaultAllow-ICMPv6 protocol group, you can edit the group from Settings module Security Settings > Protocol page.

To edit the list from the Settings module Security Settings > Protocol page:

1. Beside **Protocols**, select **Groups**.
2. Click **DefaultAllow-ICMPv6**.

The column on the right side of the Edit protocol group pane shows the group members:

- icmp6-cert-path-advertisement
- icmp6-inv-nd-solicitation
- icmp6-listener-query
- icmp6-mcast-router-advertisement
- icmp6-mcast-router-termination
- icmp6-nd-solicitation
- icmp6-router-advertisement
- icmp6-router-solicitation

3. Select the ICMPv6 protocol that you want to remove from the list, thereby blocking its packets, and click the left facing arrow.

Repeat this process for each protocol that you want to remove from the list.

4. Click **Save**.

Related Documentation

- [Understanding the Firefly Host Firewall Module on page 87](#)
- [Understanding Firefly Host Predefined Firewall Policy for Its Components on page 115](#)
- [Understanding Firefly Host IPv6 Support](#)
- [Understanding Firefly Host on page 3](#)
- [Understanding the Firefly Host Settings Module](#)

Understanding Predefined Objects for Firefly Host Firewall Policy Terms

This topic focuses primarily on the Firefly Host predefined objects that you can use for source and destination terms in firewall policy rules. It summarizes the various ways in which you can specify addresses for these terms.

- [Defining and Selecting Source and Destination Terms for Policy Rules on page 105](#)
- [Predefined Global IP Address Objects on page 105](#)
- [Predefined Network Objects on page 106](#)

Defining and Selecting Source and Destination Terms for Policy Rules

To create firewall policies, you specify rules. You add inbound and outbound rules to a policy to specify the source and destination of traffic. You select a value for the source or the destination of a term from the list of existing objects that is displayed when you right-click the rule numbers column in the Inbound (Sources) and Outbound (Destinations) parts of a policy.

Firefly Host provides the following ways in which you can define the addresses for a rule's source or destination terms:

- You can define these addresses dynamically as you create the rule. You can create groups or machines and then use them in the rule.

As a convenience, the Firefly Host Dashboard makes the configuration panes that you use for this purpose available from the Manage Policy page of the Firewall module that you use to define the policy. They are the same panes that you use to create the objects from other parts of the Firefly Host Dashboard.

- You can select a network or a machine that you have already defined.
- You can select any of the predefined objects that Firefly Host provides. The following sections cover these objects.

Predefined Global IP Address Objects

Firefly Host Release 6.0 introduces support for IPv6, including configuration of policies on IPv6 traffic. Firefly Host provides the following predefined objects that allow you to refer to IP addresses collectively by type—whether IPv4 addresses or IPv6 addresses—in a policy rule's source and destination terms:

Any—Matches any IPv4 and IPv6 address.

Any-IPv4—Matches any IPv4 address.

Any-IPv6—Matches any IPv6 address.

In releases earlier than version 6.0—releases before Firefly Host supported IPv6—the term Any referred to any IPv4 address. For environments in which not all Firefly Host components are at version 6.0 or later, the term Any also refers to any IPv4 address. It reverts back to the meaning it had in environments that support only IPv4 traffic. For

more information about how Any is interpreted in mixed Firefly Host components environments, see *IPv6 Support in Homogeneous and Heterogeneous Firefly Host Environments*.



WARNING: All Firefly Host components must be at version 6.0 or later for you to be able to create policies on IPv6 traffic.

Predefined Network Objects

Firefly Host provides predefined network objects for well-known IP address ranges and prefixes that you can use in policy rule terms for either source or destination addresses. It also provides network objects for other IPv6 and IPv4 addresses. This section covers both groups.



NOTE: Prior to Firefly Host Release 6.0, you used the Settings module Security Settings > Global Settings Rules pane to control broadcast and multicast settings. As of Release 6.0, you can no longer set these parameters from the Global Settings Rules pane. Rather, you must use the corresponding network object in a policy rule to control the firewall behavior.

Predefined Network Objects for Well Known IP Addresses

Firefly Host provides the following predefined network objects that you can use in policy rule terms as either source or destination addresses:

- Link Local Addresses (**fe80::/10**)

IPv6 link-local addresses are defined in section 2.5.6 of the IETF RFC 4291 standard as having a 10-bit prefix of **fe80** followed by 54 zero bits and a 64-bit interface ID.

A link-local address is an IP address that is intended for communications within the link, or segment, of a local network or a point-to-point connection that a host is connected to. These addresses are useful for establishing communication across a link in the absence of a globally routable prefix or for intentionally limiting the scope of traffic that should not be routed. IPv6 link-local addresses, therefore, can be used only within the context of a single Layer 2 domain. Packets sourced from or destined to a link-local address are not forwarded out of the Layer 2 domain by routers.

- IPv4 Mapped Addresses (**::ffff:0.0.0.0 – ::ffff:255.255.255.255**)

The IETF RFC 6052 standard *IPv6 Addressing of IPv4/IPv6 Translators* covers the algorithmic translation of an IPv6 address to a corresponding IPv4 address, and vice versa, using statically configured information. Algorithmic translation is used in IPv4/IPv6 translators and other types of proxies and gateways that are used in IPv4/IPv6 scenarios, such as DNS.



NOTE: Firefly Host accepts both IPv4 and IPv6 address formats and displays the addresses as you enter them.

- Well Known Prefix for IPv4 (**64:ff9b::/96**)

The IEFT RFC 6052 standard *IPv6 Addressing of IPv4/IPv6 Translators* covers the Well Known Prefix **64:ff9b::/96** that is used in an algorithmic mapping between IPv4 to IPv6 addresses. It is defined out of the **0000::/8** address block.

- IPv4 Local Broadcast (**255.255.255.255**)

A special definition exists for the IP broadcast address **255.255.255.255**. It is the broadcast address of the zero network or **0.0.0.0**, which in IP standards implies the local network. Transmission to this address is never forwarded by the routers connecting the local network to other networks.

Additional IPv4 and IPv6 Predefined Network Objects

- Unspecified IPv4 (all zeros)

In IPv4, an IP address of all zeroes (**0.0.0.0**) has a special meaning. It refers to the host itself. It is used when a device does not know its own address.

- Unspecified IPv6 (all zeros)

The IPv6 unicast unspecified address is equivalent to the IPv4 unspecified address. The IPv6 unspecified address is **0:0:0:0:0:0:0:0**, or a double colon (::). In IPv6, this concept has been formalized. It is typically used in the source field of a datagram sent by a device seeking to have its IP address configured.

- Loopback IPv4 (**127.0.0.1**)

The IEFT RFC 2606 standard officially reserved domain name for the IPv4 and IPv6 loopback network addresses is localhost.

In IPv4, this network has the prefix **127.0/8**, as defined in the IEFT RFC 3330 standard. The most commonly used IP address on the loopback device is **127.0.0.1** for IPv4, although any address in the range **127.0.0.0** to **127.255.255.255** is mapped to it.

- Loopback IPv6 (::1)

The IEFT RFC 2606 standard officially reserved domain name for the IPv4 and IPv6 loopback addresses is localhost. IPv6 designates only a single address for the IP loopback function, **::1**. The **::1/128** prefix is defined in the IEFT RFC 3513 standard.

- Multicast IPv4 (**224.0.0.0/4**)

A multicast address is a logical identifier for a group of hosts in a network that are available to process datagrams or frames for a designated network service. IPv4 and IPv6 multicast addressing is used at Layer 3 (OSI) for IPv4 and IPv6.

The Classless Interdomain Routing (CIDR) prefix of multicast addresses is **224.0.0.0/4**. The group includes the addresses from **224.0.0.0** to **239.255.255.255**. Address assignments from within this range are specified in the RFC 5771 standard.

- Multicast IPv6 (**ff00::/8**)

Multicast addresses in IPv6 have the prefix **ff00::/8**. IPv6 multicast addresses are generally formed from 4-bit groups, illustrated as follows:

- Prefix: The **prefix** holds the binary value 11111111 for any multicast address.
- Flags: Currently, 3 of the 4 flag bits in the **flags** field are defined. The left-most, most-significant flag bit is reserved for future use.
- Scope: IPv6 multicast addresses specify their scope. The set of possible scopes is different. The 4-bit **sc**, or scope, field (bits 12 to 15) is used to indicate whether the address is valid and unique.
- Group ID: The 112-bit **group ID** field identifies the service. For example, if **ff02::101** refers to all Network Time Protocol (NTP) servers on the local network segment, then **ff08::101** refers to all NTP servers in an organization's networks. The Group ID field may be further divided for special multicast address types.

**Related
Documentation**

- [Understanding the Firefly Host Firewall Module on page 87](#)
- [Configuring Firefly Host Firewall Policies on page 108](#)
- [Understanding the Firefly Host Policy per vNIC Feature](#)
- [Understanding Firefly Host on page 3](#)

Configuring Firefly Host Firewall Policies

This topic covers how to create a firewall policy for a VM composed of the corporate Global Policy, two Group Policies for the groups that the VM is a member of, and one VM Policy rule applicable to the individual VM.

It covers the preliminary tasks of defining the reusable Global Policy and a Group Policy for one of the groups that the VM is a member of.

Before you begin this procedure, read “[Understanding the Firefly Host Firewall Module on page 87](#)”. The procedure for composing an overall policy for a VM includes these parts:

- Define a Global Policy. The Global Policy is a reusable policy that is inherited by firewall policies for all VMs. You need to define it only once.

When you select the Firewall module and a VM in the VM tree to create a VM policy for it, the VM policy automatically inherits the Global Policy that you have created.

- Define Group Policies for the groups that the VM belongs to. You can define a Group Policy for a Policy Group any time after the Policy Group is created.

If the individual VM belongs to a Policy Group, it automatically inherits the Group Policy defined for that Policy Group, if the Group Policy is already defined.

When you select the Firewall module and a VM in the VM tree to create a VM Policy for it, the VM Policy contains the Group Policies that you created for any groups that the VM is a member of.

After you define the Group Policy for a group, it is automatically used in the individual policies that you construct for all members of the group. VMs that are created later and added to the policy group, either manually or automatically, inherit the Group Policy rules for that group.



NOTE: To illustrate precedence setting, this example assumes that the Group Policy already exists. It shows how to modify it.

- Define an individual VM Policy for the VM. At this point, you build the overall policy for the VM.

The VM Policy for a VM is composed of the Global Policy, Group Policies for any groups that it belongs to, and any individual VM Policy rules that you want to apply to that VM in particular.

When you select the Firewall module and a VM in the VM tree to create a VM Policy for it, the policy automatically inherits the Global Policy and the Group Policies for any groups that the VM is a member of. To complete the individual VM Policy, you add any VM Policy rules that you want to apply to that VM only. For example, you might need RADIUS access to a particular VM and not to others. You could apply a VM Policy rule to that VM's individual policy.

Create a reusable Global Policy to be used as part of the VM policies for all VMs in your environment.

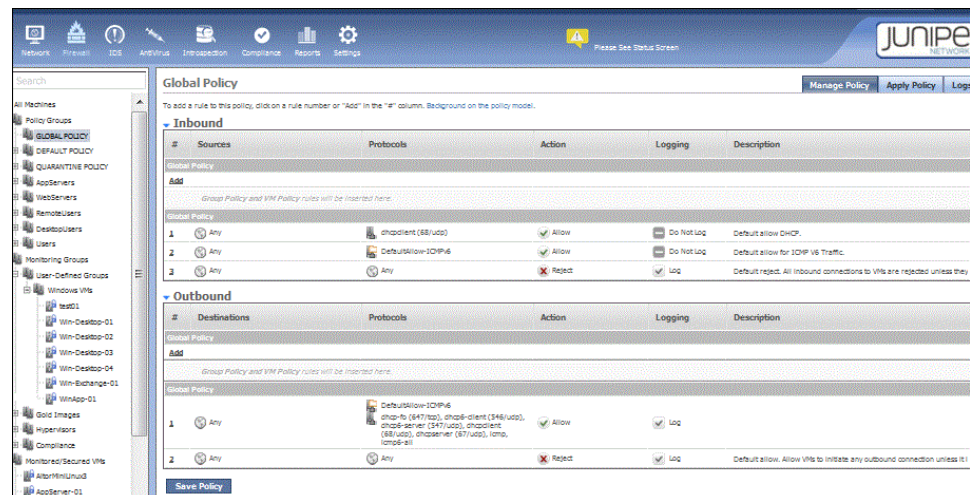


NOTE: This example focuses on defining an inbound policy only. The process of defining outbound policy mirrors it.

1. Define a Global Policy. From the Firewall module, select **Global Policy** under the Policy Groups section in the VM Tree.

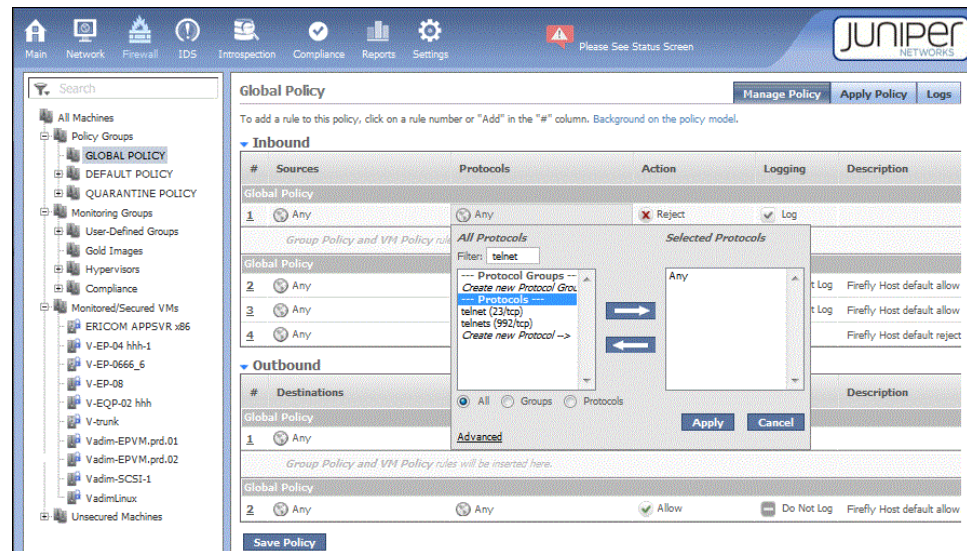
The Global Policy page appears. It contains Inbound and Outbound sections. Each section contains a high-level Global Policy section and a low-level Global Policy section with a placeholder for Group Policy rules and individual VM Policy rules in the middle. [Figure 50 on page 110](#) shows the Global Policy with its default policy rules.

Figure 50: Default Global Policy



2. Create an Inbound high-level Global Policy rule to prohibit use of Telnet.
 - a. In the Inbound section, click **Add** in the # column under the first section labeled Global Policy to add a rule.
 - b. For the Sources policy term, leave the default value Any unchanged.
You want the rule to apply to all VMs.
 - c. Click **Any** in the Protocols column, and enter **telnet** in the Filter box. The filter scrolls to **telnet**.
 - d. Select **telnet**, and click the right arrow to move telnet from the All Protocols section to the Selected Protocols section. See [Figure 51 on page 111](#).

Figure 51: Adding a Global Policy Rule to Reject Telnet Connection Attempts



- e. Click **Allow** in the actions column and select **Reject** from the Action options list. You want to reject all inbound Telnet connections attempts for all VMs in your environment.
 - f. Leave the check mark default setting for Logging unchanged. Although they are rejected, you want to log any Telnet connection attempts.
3. Leave the low-level Global Policy rule unchanged.

By default, the last rule serves as a “clean-up” rule that catches all inbound connection attempts to this VM that have fallen through the rest of the policy rule base. It rejects them, and it specifies that Firefly Host should create a log entry for the event.

4. Click **Save Policy**.

Modify the Group Policy for the Window VMs Policy Group to control rule execution precedence.

This procedure allows you to modify an existing Group Policy to change rule execution precedence. You want to ensure that a rule currently positioned in the low-level Group Policy section is not overridden by a VM Policy rule that might be inserted above it when an individual VM policy that includes the Group Policy is created. You want that rule to be executed *before* any VM Policy rules. To achieve that result, move the rule up from the low-level Group Policy section to the high-level Group Policy section.



NOTE: This example focuses on defining an Inbound policy only. An outbound policy definition process mirrors it.

1. In the Policy Groups section of the VM tree, select **Windows VMs**.

Notice that the high-level and low-level Group Policy sections are nested within the high-level and low-level Global Policy sections.

indicates the placeholder for adding VM Policy rules at the center of the Group Policy section.

2. Move the network management rule from the low-level Group Policy section to the high-level Group Policy section so that any VM Policy rule for an individual VM Policy rule added later cannot override it. See .
3. Click **Save Policy**.

Create a VM Policy for an individual VM

This procedure covers how to create individual VM policy rules for the WWW-HR-IIS VM that inherits the Global Policy and the Group Policies for the groups that it is a member of. An individual VM can belong to more than one Policy Group. When that is the case, the VM inherits the Group Policies for all of the Policy Groups that it belongs to. In this example, the WWW-HS-IIS VM is a member of two Policy Groups: WWW Servers and Windows VM.

This example focuses on the Inbound section of the VM Policy.

1. To display the VM Policy for the WWW-HR-IIS VM, select **WWW-HR-IIS** in the Windows VMs under Policy Groups in the VM Tree.



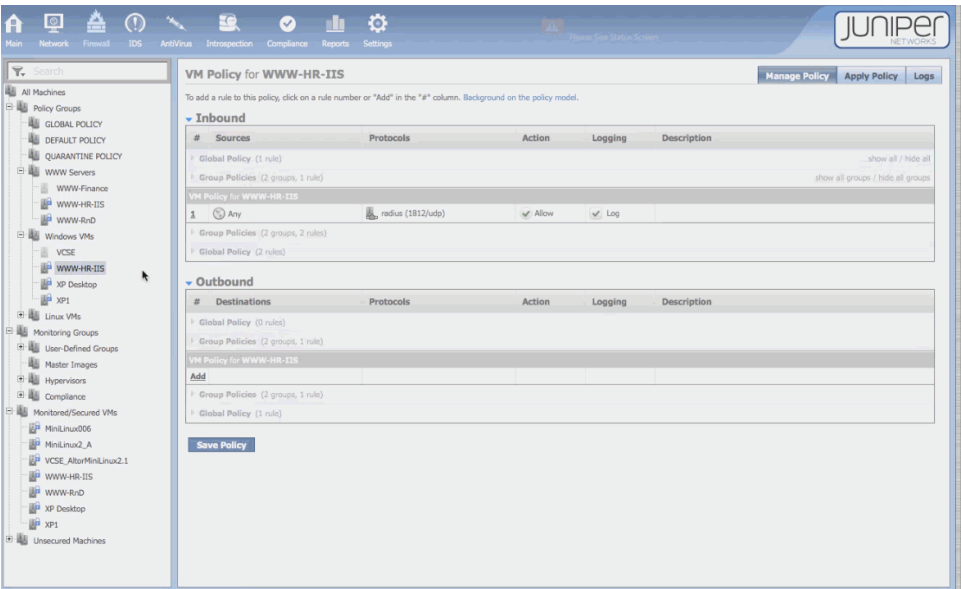
TIP: Because WWW-HR-IIS belongs to two groups, you can select it under either of its groups to display its VM Policy page.

The VM Policy for WWW-HR-IIS page is composed of the following nested parts that were previously built:

- the high-level and lower-level Global Policy rules forming the outer layer of the nest.
- a high-level Group Policy section below the high-level Global Policy. It states that the VM Policy contains two Policy Groups with a rule defined in only one of them.
- a middle section called VM Policy for WWW-HR-IIS. You can add VM Policies specifically for the VM to this section.
- the low-level Group Policy section that indicates that the VM belongs to two Policy Groups and that it inherits their Group Policies that include two rules.
- the low-level Global Policy.

Figure 52 on page 113 shows the policy.

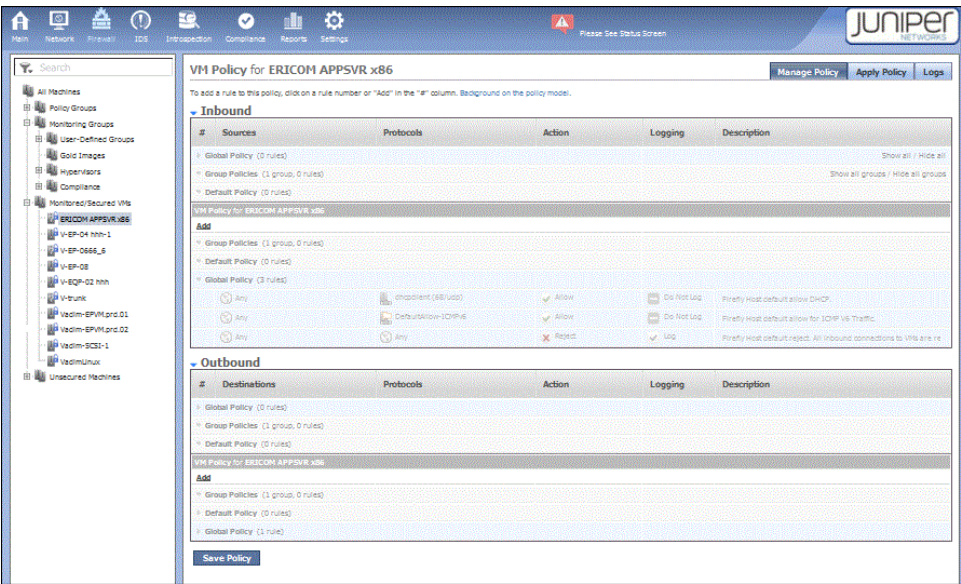
Figure 52: VM Policy for an Individual VM



2. To see the entire rule base for the VM, expanding the policies that it inherited to show their rules, click **show all** in the upper-right corner of the page.

See [Figure 53 on page 113](#).

Figure 53: Complete VM Policy for an Individual VM

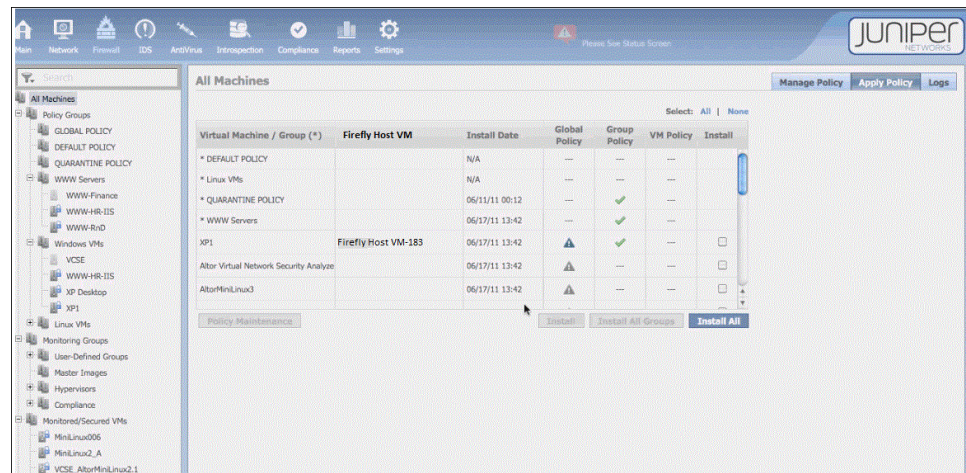


Apply the VM Policy.

When you define a firewall policy for a VM, it is not automatically applied. You must use the Firewall module Manage Policy tab to install it. This procedure installs a firewall policy for a single VM: AltorMiniLinux3.

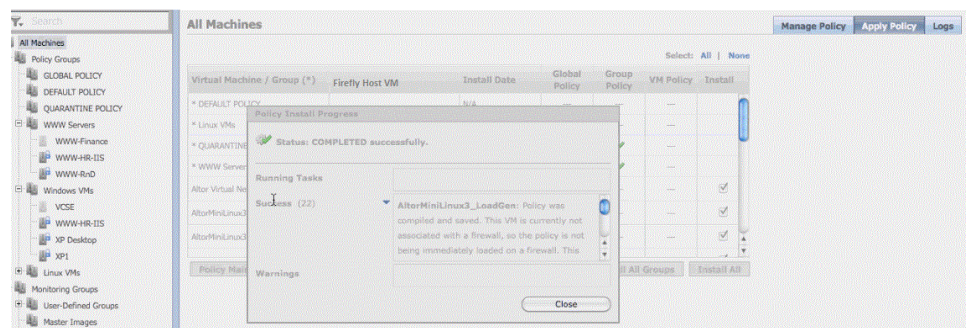
1. Select the Firewall module. Select **All Machines** in the VM Tree. The following page is displayed. See [Figure 54 on page 114](#).

Figure 54: All Machines



2. Select the VM and click **Install**. In this example, All Machines is selected. After the firewall policy is installed on the VMs, the message shown in the following figure is displayed. See [Figure 55 on page 114](#).

Figure 55: Policy Install Progress



Related Documentation

- [Understanding Firefly Host on page 3](#)
- [Using the Firefly Host Network and Firewall Modules Cooperatively on page 122](#)
- [Understanding Firefly Host Predefined Firewall Policy for Its Components on page 115](#)

Understanding Firefly Host Predefined Firewall Policy for Its Components

Firefly Host Firewall module allows you to secure virtual machines (VMs) within your virtualized infrastructure with individual policy rules, group policy rules, and global policy rules.

Not to be confused with securing VMs in your virtualized data centers, Firefly Host secures and protects its own two main components—the Firefly Host Dashboard and the Firefly Host VM—with predefined rule sets. You cannot change these predefined policy rules nor should you ever need to.

Firefly Host stateful firewall comprises the following predefined rule sets for its two components.

For the Firefly Host Dashboard, the policy rules

- allow the following connections:
 - all outgoing connections
 - all incoming TCP/8443
 - all incoming TCP/443
 - all incoming TCP/8003
 - DHCP
 - NDP on IPv6
- Otherwise all connection attempts are dropped.

For the Firefly Host VM, the policy rules

- allow the following connections:
 - all outgoing connections
 - all incoming TCP/8443
 - DHCP
 - NDP on IPv6
- Otherwise all connection attempts are dropped.

Related Documentation

- [Understanding the Firefly Host Firewall Module on page 87](#)
- [Understanding the Firefly Host Dashboard](#)
- [Understanding the Firefly Host VM](#)
- [Understanding Firefly Host on page 3](#)

CHAPTER 9

Firefly Host Network Module

- [Understanding the Firefly Host Network Module on page 117](#)
- [Using the Firefly Host Network and Firewall Modules Cooperatively on page 122](#)

Understanding the Firefly Host Network Module

The Firefly Host Dashboard Network module displays network traffic for virtual machines (VMs) that are selected in the VM tree. You can view network traffic for all VMs or specific ones.

This topic includes the following sections:

- [Network Module on page 117](#)
- [Manipulating Displayed Information on page 118](#)

Network Module

The Network module contains the following six tabs:

- Summary
- Top Protocols
- Top Sources
- Top Destinations
- Top Talkers
- Connections

To display information for a VM, the VM must have a known IP address. The IP address is determined automatically if VMware Tools is installed on the VM. If it is not set automatically, you can set the IP address manually using the Settings module Firefly Host Application Settings > Machines page.

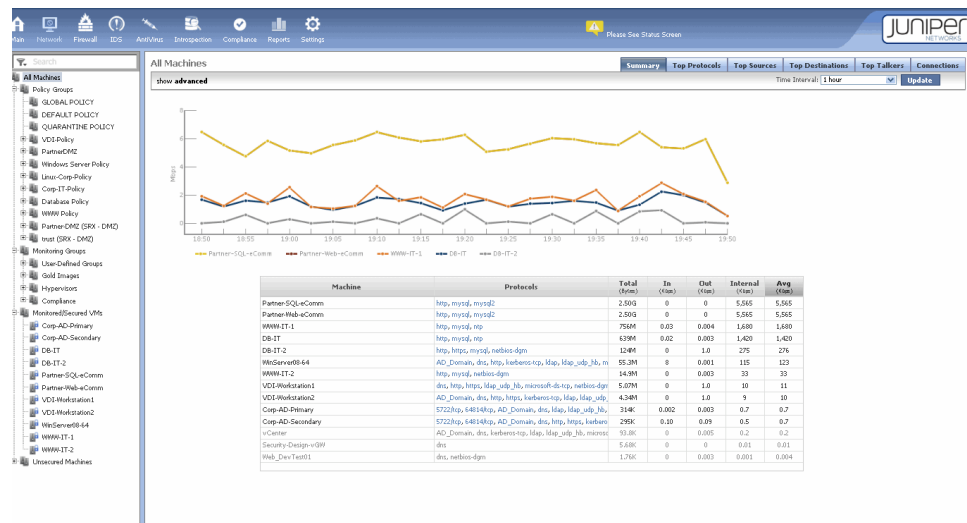
The Network module analysis takes into account IPv4 traffic and IPv6 traffic. Tables shown on the Network module tabs display information for objects with IPv4 and IPv6 addresses.

Manipulating Displayed Information

The Network Summary tab allows you to display information about all VMs, as shown in Figure 56 on page 118.

A line graph displayed at the top of the page plots bandwidth usage for the top VMs in the report. A table below the graph provides detailed network data for VMs selected in the VM tree. In this case, data for 1 hour is displayed.

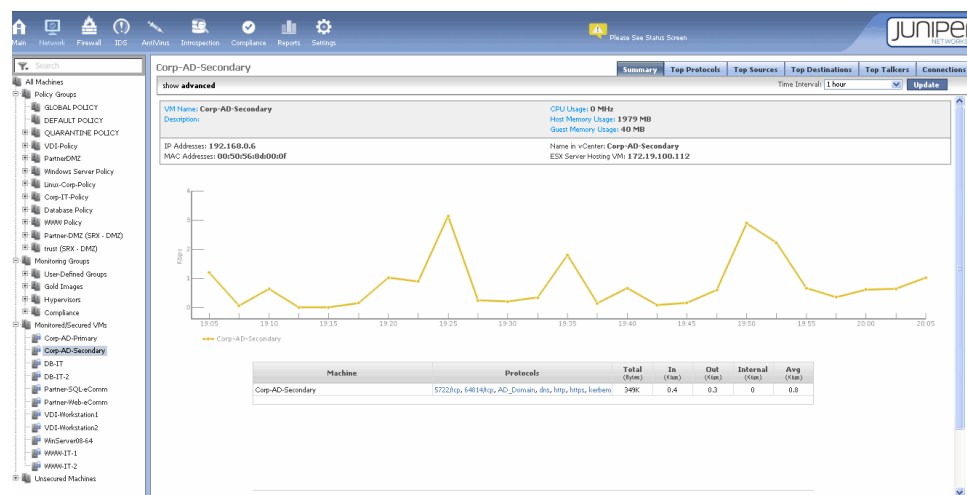
Figure 56: Network Summary Tab for All VMs



To display information about a single VM, select the VM in the VM tree.

Figure 57 on page 118 shows the information displayed for the Corp-AD-Secondary VM.

Figure 57: Main Module Network Module Summary Tab for a Single VM



To view a VM's connections, click an individual line in the graph. To display a filter for a protocol, click the protocol field.

Changing the Time Interval for Displayed Information

To change the period for which network data is plotted, use the Time Interval menu. Choose a different interval, and click **Update**. You can select a time interval or specify a custom period.



TIP: The time interval feature is also available for other Firefly Host Dashboard modules.

Figure 58 on page 119 and Figure 59 on page 119 show information for all machines for two different time periods.

Figure 58: Displaying Network Data for Different Time Intervals: Part 1

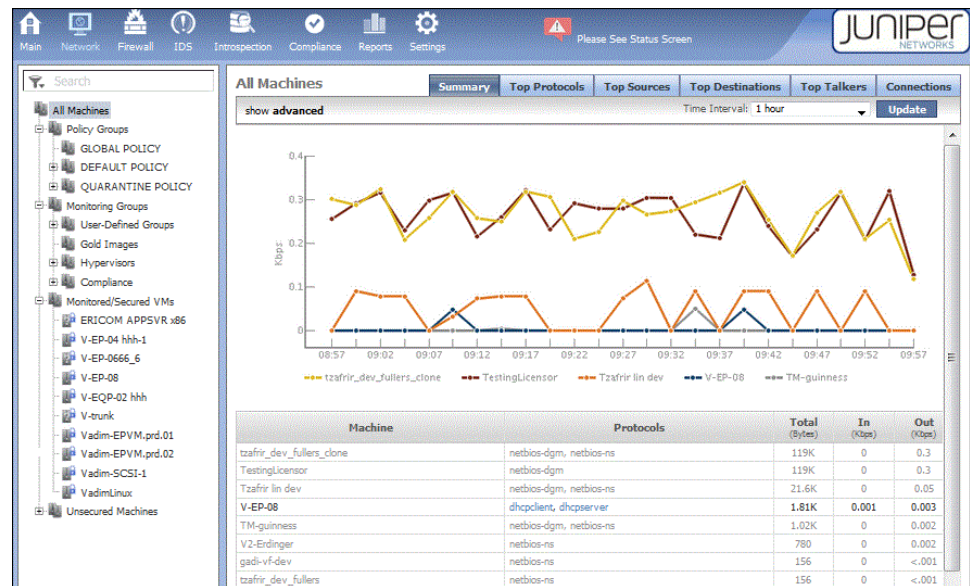
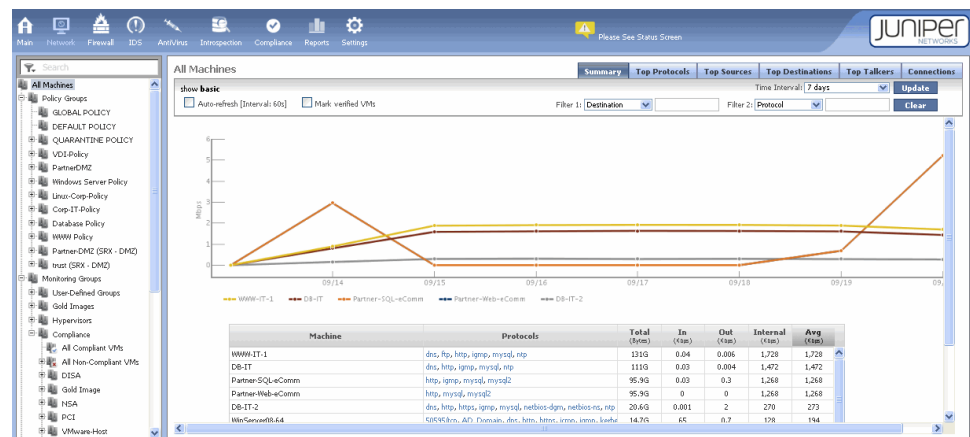


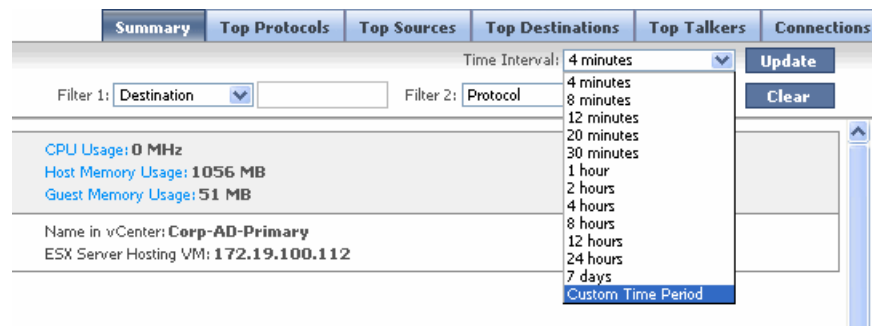
Figure 59: Displaying Network Data for Different Time Intervals: Part 2



Real-time data from the last traffic interval populates the Total, In, Out, and Internal table columns. If you are charting protocols, sources, destinations, or top talkers, the interval selected is used to calculate the minimum, maximum, and average figures in the table shown below the graph. For example, if you select 4 minutes as the time interval, the graph would show a sample of the throughput every 10 seconds. Each dot represents the average throughput value for that period.

The Custom Time Period feature allows you to view historical data. To use it, in the Time Interval menu, select **Custom Time Period**. (Figure 60 on page 120 shows the Custom Time Period menu item.)

Figure 60: Selecting a Time Interval

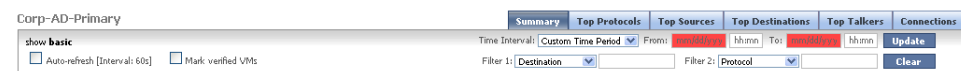


The custom time period is interpreted as follows:

- You cannot set the custom time period to a range of less than 1 minute.
If you enter the same value for the **From** and **To** fields—that is, the same beginning and end—Firefly Host automatically changes the time interval to 1 minute before the specified time.
For example, if you set the **From** field value to 01/02/13 00:00 and the **To** field value to 01/02/13 00:00, Firefly Host changes the **From** time to 01/01/13 23:59 (11:59 P.M.) to allow for a time period of 1 minute. The **To** field is still interpreted as 01/02/13 00:00, the beginning of the next day.
- If you specify a valid time range, such as the **From** field set to 01/01/13 00:00 with the **To** field set to 01/02/13 00:00, Firefly Host uses the time you specified.

Figure 61 on page 120 shows the Custom Time Period fields.

Figure 61: Setting the Custom Time Period



NOTE: Depending on the size of the database and the resources available to it, when you specify a custom time period, the Firefly Host Dashboard might take 30 minutes or more to chart the data and display it. When you want to examine a large data set, for example, data from a month or more, we recommend that you use the Reporting module.

Using Advanced Options for Filtering Network Data

You can filter the information to be displayed. To display filtering options, click **show advanced** at the left end of the time interval bar. Click the **Filter 1** and **Filter 2** menus to select filtering options and enter associated values in the related boxes. Then click **Update** to refresh the graph and data display, based on your settings. Click **Clear** to reset filter boxes.



NOTE: Configured filters affect all data in the graph and tables.

Other advanced options differ somewhat depending on the tab you are viewing. [Table 6 on page 121](#) describes the Advanced options.

Table 6: Using Advanced Options for Filtering Network Data

Select	Action
Auto-refresh	Refreshes data automatically every 60 seconds.
mark verified VMs	<p>Causes the Firefly Host to automatically use the unique VMware ID/UUID as well as the IP address to validate that connections are actually coming from the identified server. Firefly Host reports on both IPv4 and IPv6 addresses.</p> <p>Using both the VMware ID/UUID and the IP address protects against security threats such as IP spoofing. VMs for which this extra validation occurs can be displayed in the interface.</p>
multicast in table	<p>Includes multicast packets when monitoring. Because multicast packets are not destined for a specific host and they are seen by all machines on the network, they are included in the connection session list for all VMs.</p> <p>However, the amount of multicast traffic can be quite large, and it can obscure sessions specific to a selected VM. To remove multicast from this view, clear the multicast in table check box.</p>

To exit advanced view, click **show basic**.

Sorting Table Data

You can sort table data in the Network page by column. Drag the pointer over the column headings. When the pointer changes to the pointing hand, click the column heading to sort.

To display information for a single VM that is listed in the table, click its entry.

Related Documentation

- [Using the Firefly Host Network and Firewall Modules Cooperatively on page 122](#)
- [Understanding the Firefly Host Dashboard](#)
- [Understanding the Firefly Host Dashboard Taskbar](#)
- [About the Firefly Host Dashboard Tree](#)
- [Understanding Firefly Host on page 3](#)

Using the Firefly Host Network and Firewall Modules Cooperatively

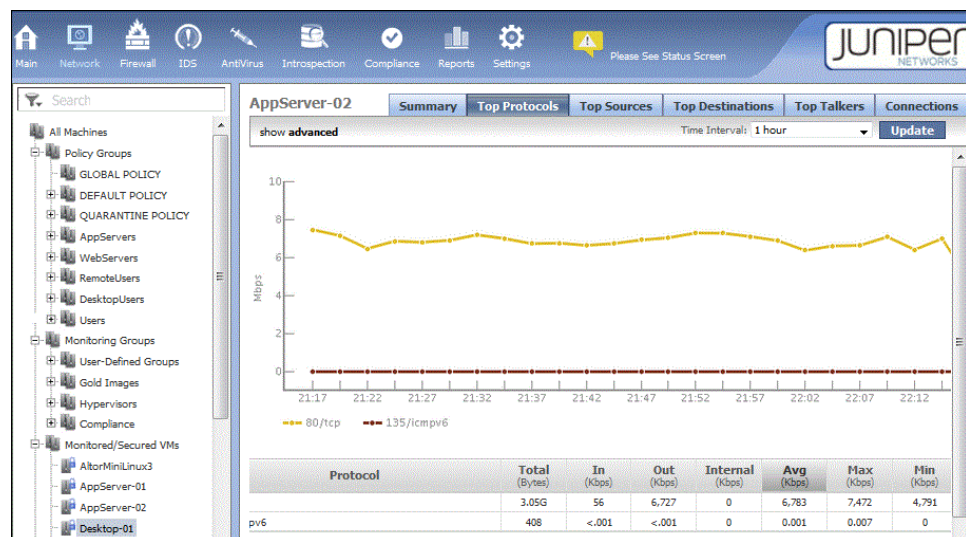
There are various ways to use the Network module in the service of the Firewall module to build a strong firewall. This topic explores some of them.

- [Network Assessment on page 122](#)
- [Using the Network Module to Observe Traffic Coming Into and Going Out from VMs on page 123](#)
- [Detecting Unexpected and Unwanted Behavior on page 123](#)
- [Using the Network and Firewall Modules Together on page 124](#)

Network Assessment

Administrators are not always aware of events that transpire on their virtualized networks because existing software for the virtualized environment does not always expose them. Firefly Host Network module addresses this problem. It gives you a clear view of all traffic flows across your virtualized network. You can view overall throughput, chart protocol usage, identify sources and destinations of traffic, and identify top talkers. You can calculate minimum, maximum, and average figures across specific time intervals for these aspects of your network. In the example shown in [Figure 62 on page 122](#), the Top Protocols assessment shows that the most heavily used protocols are Microsoft SQL Server followed by MySQL. The table beneath the graph gives details on all protocols used in top down order from most used to least.

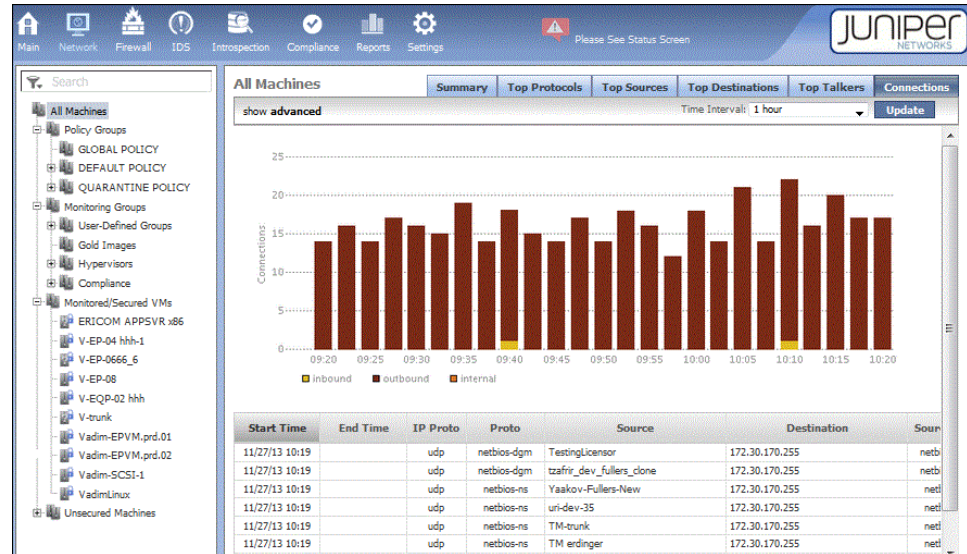
Figure 62: Top Protocols Across All Machines Example



Because the Firefly Host allows you to view activity that occurs inside the hypervisor, you can quickly discover who is communicating with whom. If you were to use only the Firefly Host ability to view connections in real time, you would still be able to make realistic network assessments. But the Firefly Host can contribute much more information to use in your network assessment.

As [Figure 63 on page 123](#) shows, the Network module's Connections tab displays the number of connections in your network across time for all machines, whether the connections are inbound, outbound, or internal. The table beneath the graph shows when the connection was set up and when it ended, the protocol used, the source and destination endpoints, and the bytes transmitted. You can view this kind of information for an individual VM by selecting the VM in the VM tree.

Figure 63: Network Module Connection Tab Information



Using the Network Module to Observe Traffic Coming Into and Going Out from VMs

The Network module contributes to your ability to create strong firewall security in many ways. It displays information about all traffic, including traffic internal to a VM, traffic in and out of its vNICs, traffic from another VM on the same host, traffic between VMs on different hosts, and even traffic transmitted through a physical connection. In its simplest sense, you can think of this aspect of the Network module as akin to a packet sniffer, but it is far more than that.

When you use the Time Interval field to select a different time period, Firefly Host redraws its graphs to let you view traffic patterns that occur during that period. You might want to use this feature to compare activity during one period of time with another, to look at past behavior, or to hone in on a VM to view its activity during a specific period.

For example, you could view all HTTP connections, the engaged workstations, and how much traffic is transmitted. You could do this for a two-day period, then a week, and then longer to observe anomalies that might exist.

Detecting Unexpected and Unwanted Behavior

The Network module can reveal unwanted behavior on your network that should be prohibited or investigated further. There are many examples of the kinds of information that the Network module might reveal. For example, you might notice that:

- Traffic might be transmitted on a particular protocol that is unusual or inappropriate, therefore raising questions.
 - The protocol 999TCP might be connecting to the finance server, an unwanted event that you want the firewall to protect against.
 - HTTP traffic might be transmitted to a VM that should not receive it.
- Some workstations might pull updates from a Microsoft server unintentionally instead of from local update servers.
- Thirty different protocols might be used, not all of which you were informed about. You might want to prohibit use of some of them.

Using the Network and Firewall Modules Together

When used together, the Network module and the Firewall module allow you to implement appropriate, strong security for your virtualized environment. By using the Network module to view how VMs behave in real time, you can better analyze your current security posture and observe its weaknesses.

As you begin to lock down your system through the Firewall module, the Network module becomes increasingly useful. After you use the Firewall module to refine your security policy, you can return to the Network module to determine if the change in policy produces the expected behavior.

You might still notice traffic that should not be allowed. In that case, you can return to the Firewall module, create a rule or modify an existing one, and then look at the behavioral results again in the Network module.

You can cycle through this process as many times as necessary to put in place the desired security policy. You can continue to use the Network module and the Firewall module together to implement the security you desire as your network expands and as its security requirements change.

Related Documentation

- [Understanding the Firefly Host Firewall Module on page 87](#)
- [Understanding the Firefly Host Network Module on page 117](#)
- *Understanding the Firefly Host Dashboard*
- *Understanding the Firefly Host Dashboard Taskbar*
- *About the Firefly Host Dashboard Tree*
- [Understanding Firefly Host on page 3](#)

PART 4

Index

- [Index on page 127](#)

Index

Symbols

#, comments in configuration statements.....	xv
(), in syntax descriptions.....	xv
< >, in syntax descriptions.....	xiv
[], in configuration statements.....	xv
{ }, in configuration statements.....	xv
(pipe), in syntax descriptions.....	xv

A

Auto Deploy.....	77
VMware.....	78

B

braces, in configuration statements.....	xv
brackets	
angle, in syntax descriptions.....	xiv
square, in configuration statements.....	xv

C

comments, in configuration statements.....	xv
configuring basic system parameters.....	19
conventions	
text and syntax.....	xiv
curly braces, in configuration statements.....	xv
customer support.....	xv
contacting JTAC.....	xv

D

documentation	
comments on.....	xv

F

Firefly.....	77
VMware Auto Deploy support.....	77
Firefly Host.....	78
VMware Auto Deploy support.....	78
Firefly Host Dashboard	
Firewall module.....	87, 122
Network module.....	117, 122
predefined firewall policy rules	115

Firefly Host VM	
predefined firewall policy rules	115
single OVA install method.....	19
Firewall module.....	87
used with Network module.....	122
firewall policy rules for Firefly Host	
components.....	115
font conventions.....	xiv

I

ICMPv6P.....	101
--------------	-----

M

machines.....	66
manuals	
comments on.....	xv

N

Network module.....	117
used with Firewall module.....	122

O

Open Virtualization Format (OVF)	
OVA template.....	7, 8
OVA bundled method.....	8
downloading package.....	9
OVA template.....	7
OVA template method	
single method for Firefly Host Dashboard.....	17

P

parentheses, in syntax descriptions.....	xv
Primary-level entry	
secondary-level entry.....	105
Primary-level entry only.....	105
Protocols	
ICPMv6.....	101

S

security zones	
interfaces.....	19
Settings module	
machines.....	66
single OVA install method	
Firefly Host VM	19
support, technical See technical support	
syntax conventions.....	xiv

T

technical support

contacting JTAC.....xv

V

vCenter

settings.....31

VMware

integrating Firefly Host.....31