

vShield Quick Start Guide

vShield Manager 4.1

vShield Edge 1.0

vShield App 1.0

vShield Endpoint 1.0

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see <http://www.vmware.com/support/pubs>.

EN-000375-00

vmware[®]

You can find the most up-to-date technical documentation on the VMware Web site at:

<http://www.vmware.com/support/>

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

docfeedback@vmware.com

Copyright © 2010 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

About This Book	5
1 Introduction to vShield	7
vShield Components at a Glance	7
vShield Manager	7
vShield Zones	7
vShield Edge	8
Standard vShield Edge Services (Including Cloud Director)	8
Advanced vShield Edge Services	8
vShield App	9
vShield Endpoint	9
Deployment Scenarios	10
Protecting the DMZ	10
Isolating and Protecting Internal Networks	10
Protecting Virtual Machines in a Cluster	11
Common Deployments of vShield Edge	11
Common Deployments of vShield App	11
2 Preparing for Installation	13
System Requirements	13
Hardware	13
Software	13
Client and User Access	14
Deployment Considerations	14
Preparing Virtual Machines for vShield Protection	14
How Are My Virtual Machines Grouped?	14
Are My Virtual Machines Still Protected if I vMotion Them to Another ESX Host?	14
How Do I Isolate a Group of Virtual Machines?	15
vShield Manager Uptime	15
Communication Between vShield Components	15
Hardening Your vShield Virtual Machines	15
vShield Manager User Interface	15
Command Line Interface	15
REST Requests	16
3 Installing the vShield Manager and vShield Zones	17
Obtain the vShield Manager OVA File	17
Install the vShield Manager Virtual Appliance	17
Configure the Network Settings of the vShield Manager	18
Log In to the vShield Manager User Interface	19
Synchronize the vShield Manager with the vCenter Server	19
Register the vShield Manager Plug-In with the vSphere Client	20
Change the Password of the vShield Manager User Interface Default Account	20
Install vShield Zones	20
Where to Go Next	21

4	Installing vShield Edge, vShield App, and vShield Endpoint	23
	Running vShield in Evaluation Mode	23
	Preparing Your Virtual Infrastructure for vShield App, vShield Edge, and vShield Endpoint	23
	Install vShield Component Licenses	24
	Prepare All ESX Hosts	24
	Prepare a vNetwork for Port Group Isolation	25
	Install a vShield Edge	25
	Installing vShield Endpoint	27
	vShield Endpoint Installation Workflow	27
	Install the Thin Agent on the Guest Virtual Machine	27
	Prerequisites	27
	Where to Go Next	28
	Index	29

About This Book

The *vShield Quick Start Guide* provides information about installing VMware® vShield™ into your VMware Virtual Infrastructure environment.

Intended Audience

This book is intended for anyone who wants to install or use VMware vShield. The information in this book is written for experienced Windows or Linux system administrators who are familiar with virtual machine technology and datacenter operations. This book also assumes familiarity with VMware Virtual Infrastructure, including vCenter™ Server 4.x, VMware ESX™ 4.x, and the vSphere Client.

VMware Technical Publications Glossary

VMware Technical Publications provides a glossary of terms that might be unfamiliar to you. For definitions of terms as they are used in VMware technical documentation go to <http://www.vmware.com/support/pubs>.

Document Feedback

VMware welcomes your suggestions for improving our documentation. If you have comments, send your feedback to docfeedback@vmware.com.

VMware Infrastructure Documentation

The following documents comprise the VMware vShield documentation set:

- *vShield Administration Guide*
- *vShield Quick Start Guide*
- *vShield API Programming Guide*

You should also have access to the combined vCenter Server and ESX documentation set.

Technical Support and Education Resources

The following sections describe the technical support resources available to you. To access the current version of this book and other books, go to <http://www.vmware.com/support/pubs>.

Online and Telephone Support

To use online support to submit technical support requests, view your product and contract information, and register your products, go to <http://www.vmware.com/support>.

Customers with appropriate support contracts should use telephone support for the fastest response on priority 1 issues. Go to http://www.vmware.com/support/phone_support.

Support Offerings

To find out how VMware support offerings can help meet your business needs, go to <http://www.vmware.com/support/services>.

VMware Professional Services

VMware Education Services courses offer extensive hands-on labs, case study examples, and course materials designed to be used as on-the-job reference tools. Courses are available onsite, in the classroom, and live online. For onsite pilot programs and implementation best practices, VMware Consulting Services provides offerings to help you assess, plan, build, and manage your virtual environment. To access information about education classes, certification programs, and consulting services, go to <http://www.vmware.com/services>.

Introduction to vShield

This chapter introduces the VMware® vShield™ components you install.

The chapter includes the following topics:

- [“vShield Components at a Glance”](#) on page 7
- [“Deployment Scenarios”](#) on page 10

vShield Components at a Glance

VMware vShield is a suite of security virtual appliances built for VMware vCenter™ Server integration. vShield is a critical security component for protecting virtualized datacenters from attacks and misuse helping you achieve your compliance-mandated goals.

vShield includes virtual appliances and services essential for protecting virtual machines. vShield can be configured through a web-based user interface, a vSphere Client plug-in, a command line interface (CLI), and REST API.

vCenter Server includes vShield Manager and vShield Zones. The following vShield packages each require a license:

- vShield Edge with Port Group Isolation
- vShield App
- vShield Endpoint

One vShield Manager manages multiple vShield Zones, vShield Edge, vShield App, and vShield Endpoint instances.

vShield Manager

The vShield Manager is the centralized network management component of vShield, and is installed as a virtual appliance on any ESX™ host in your vCenter Server environment. A vShield Manager can run on a different ESX host from your vShield agents.

Using the vShield Manager user interface or vSphere Client plug-in, administrators install, configure, and maintain vShield components. The vShield Manager user interface leverages the VMware Infrastructure SDK to display a copy of the vSphere Client inventory panel, and includes the Hosts & Clusters and Networks views.

vShield Zones

vShield Zones provides firewall protection for traffic between virtual machines. For each Zones Firewall rule, you can specify the source IP, destination IP, source port, destination port, and service.

vShield Edge

vShield Edge provides network edge security and gateway services to isolate the virtual machines in a port group, vDS port group, or Cisco® Nexus 1000V. The vShield Edge connects isolated, stub networks to shared (uplink) networks by providing common gateway services such as DHCP, VPN, NAT, and Load Balancing. Common deployments of vShield Edge include in the DMZ, VPN Extranets, and multi-tenant Cloud environments where the vShield Edge provides perimeter security for Virtual Datacenters (VDCs).

Standard vShield Edge Services (Including Cloud Director)

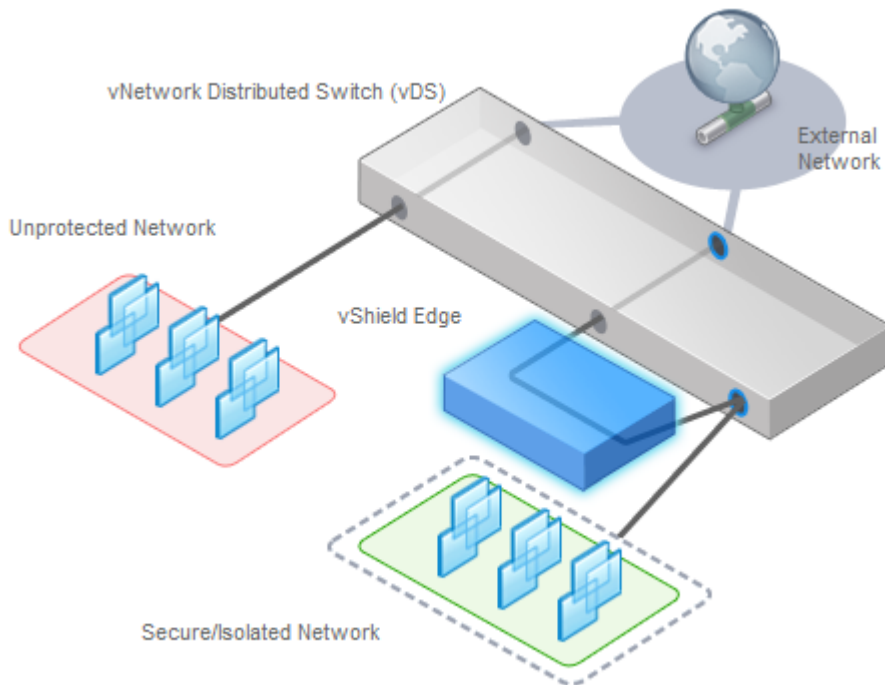
- Firewall: Supported rules include IP 5-tuple configuration with IP and port ranges for stateful inspection for TCP, UDP, and ICMP.
- Network Address Translation: Separate controls for Source and Destination IP addresses, as well as TCP and UDP port translation.
- Dynamic Host Configuration Protocol (DHCP): Configuration of IP pools, gateways, DNS servers, and search domains.

Advanced vShield Edge Services

- Site-to-Site Virtual Private Network (VPN): Uses standardized IPsec protocol settings to interoperate with all major firewall vendors.
- Load Balancing: Simple and dynamically configurable virtual IP addresses and server groups.

vShield Edge supports syslog export for all services to remote servers.

Figure 1-1. vShield Edge Installed to Secure a vDS Port Group



vShield App

vShield App is an interior, vNIC-level firewall that allows you to create access control policies regardless of network topology. A vShield App monitors all traffic in and out of an ESX host, including between virtual machines in the same port group. vShield App includes traffic analysis and container-based policy creation.

vShield App installs as a hypervisor module and firewall service virtual appliance. vShield App integrates with ESX hosts through VMsafe APIs and works with VMware vSphere platform features such as DRS, vMotion, DPM, and maintenance mode.

vShield App provides firewalling between virtual machines by placing a firewall filter on every virtual network adapter. The firewall filter operates transparently and does not require network changes or modification of IP addresses to create security zones. You can write access rules by using vCenter containers, like datacenters, cluster, resource pools and vApps, or network objects, like Port Groups and VLANs, to reduce the number of firewall rules and make the rules easier to track.

You should install vShield App instances on all ESX hosts within a cluster so that VMware vMotion™ operations work and virtual machines remain protected as they migrate between ESX hosts. By default, a vShield App virtual appliance cannot be moved by using vMotion.

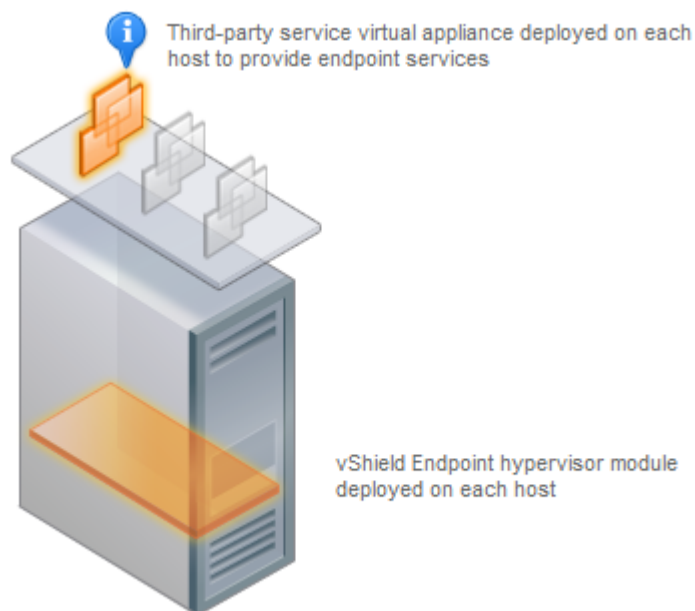
The Flow Monitoring feature displays allowed and blocked network flows at the application protocol level. You can use this information to audit network traffic and troubleshoot operational.

vShield Endpoint

vShield Endpoint delivers an introspection-based antivirus solution. vShield Endpoint uses the hypervisor to scan guest virtual machines from the outside without a bulky agent. vShield Endpoint is efficient in avoiding resource bottlenecks while optimizing memory use.

vShield Endpoint installs as a hypervisor module and security virtual appliance from a third-party antivirus vendor (VMware partners) on an ESX host.

Figure 1-2. vShield Endpoint Installed on an ESX Host



Deployment Scenarios

Using vShield, you can build secure zones for a variety of virtual machine deployments. You can isolate virtual machines based on specific applications, network segmentation, or custom compliance factors. Once you determine your zoning policies, you can deploy vShield to enforce access rules to each of these zones.

Protecting the DMZ

The DMZ is a mixed trust zone. Clients enter from the Internet for Web and email services, while services within the DMZ might require access to services inside the internal network. You can place DMZ virtual machines in a port group and secure that port group with a vShield Edge. vShield Edge provides access services such as firewall, NAT, and VPN, as well as load balancing to secure DMZ services.

A common example of a DMZ service requiring an internal service is Microsoft Exchange. Microsoft Outlook Web Access (OWA) commonly resides in the DMZ cluster, while the Microsoft Exchange back end is in the internal cluster. On the internal cluster, you can create firewall rules to allow only Exchanged-related requests from the DMZ, identifying specific source-to-destination parameters. From the DMZ cluster, you can create rules to allow outside access to the DMZ only to specific destinations using HTTP, FTP, or SMTP.

Isolating and Protecting Internal Networks

You can use a vShield Edge with the Port Group Isolation feature to isolate an internal network from the external network. A vShield Edge provides perimeter firewall protection and edge services to secure virtual machines in a port group, enabling communication to the external network through DHCP, NAT, and VPN.

Within the secured port group, you can install a vShield App instance on each ESX host that the vDS spans to secure communication between virtual machines in the internal network.

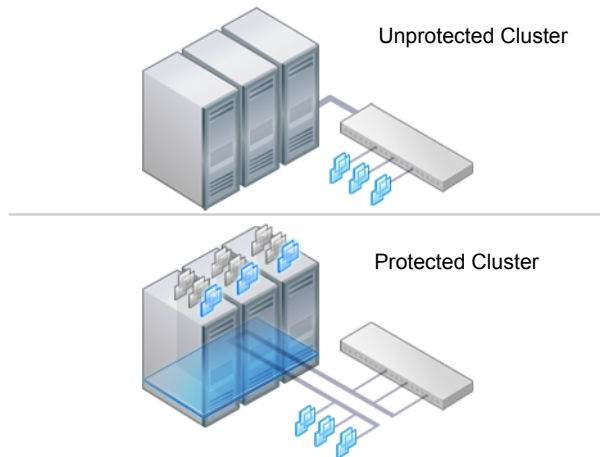
If you utilize VLAN tags to segment traffic, you can use App Firewall to create smarter access policies. Using App Firewall instead of a physical firewall allows you to collapse or mix trust zones in shared ESX clusters. By doing so, you gain optimal utilization and consolidation from features such as DRS and HA, instead of having separate, fragmented clusters. Management of the overall ESX deployment as a single pool is less complex than having separately managed pools.

For example, you use VLANs to segment virtual machine zones based on logical, organizational, or network boundaries. Leveraging the Virtual Infrastructure SDK, the vShield Manager inventory panel displays a view of your VLAN networks under the Networks view. You can build access rules for each VLAN network to isolate virtual machines and drop untagged traffic to these machines.

Protecting Virtual Machines in a Cluster

In [Figure 1-3](#), vShield App instances are installed on each ESX host in a cluster. Virtual machines are protected when moved via vMotion™ or DRS between ESX hosts in the cluster. Each vApp shares and maintains state of all transmissions.

Figure 1-3. vShield App Instances Installed on Each ESX Host in a Cluster



Common Deployments of vShield Edge

You can use a vShield Edge with the Port Group Isolation feature to isolate a stub network, using NAT to allow traffic in and out of the network. If you deploy internal stub networks, you can use vShield Edge to secure communication between networks by using LAN-to-LAN encryption via VPN tunnels.

vShield Edge can be deployed as a self-service application within VMware Cloud Director.

Common Deployments of vShield App

You can use vShield App to create security zones within a vDC. You can impose firewall policies on vCenter containers or *Security Groups*, which are custom containers you can create by using the vShield Manager user interface. Container-based policies enable you to create mixed trust zones clusters without requiring an external physical firewall.

In a deployment that does not use vDCs, use a vShield App with the Security Groups feature to create trust zones and enforce access policies.

Service Provider Admins can use vShield App to impose broad firewall policies across all guest virtual machines in an internal network. For example, you can impose a firewall policy on the second vNIC of all guest virtual machines that allows the virtual machines to connect to a storage server, but blocks the virtual machines from addressing any other virtual machines.

Preparing for Installation

This chapter introduces an overview of the prerequisites for successful vShield installation.

The chapter includes the following topics:

- [“System Requirements”](#) on page 13
- [“Deployment Considerations”](#) on page 14

System Requirements

Before installing vShield in your vCenter Server environment, consider your network configuration and resources. You can install one vShield Manager per vCenter Server, one vShield App per ESX™ host, and one vShield Edge per port group.

To install vShield, you must meet the following requirements:

Hardware

[Table 2-2](#) lists the hardware requirements for this version of vShield.

Table 2-1. Hardware Requirements

Component	Minimum
Memory	8 GB
Disk Space	<ul style="list-style-type: none"> ■ 8 GB for the vShield Manager ■ 5 GB per vShield App per ESX host ■ 100 MB per vShield Edge
NICs	2 gigabit NICs on an ESX host

Software

- VMware vCenter Server 4.0 Update 1 or later

NOTE vShield Endpoint requires vCenter Server 4.1 or later.

[Table 2-2](#) lists the vCenter versions that are compatible with this version of vShield.

Table 2-2. Supported vCenter Versions

vCenter Release	Build Number
4.0 Update 1	264050
4.1 GA	208111
4.1 GA vSphere Client	208111

- VMware ESX 4.0 Update 1 or later for each server

NOTE vShield Endpoint requires ESX 4.1 or later.

[Table 2-3](#) lists the ESX and ESXi versions that are compatible with this version of vShield.

Table 2-3. Supported ESX and ESXi Versions

ESX or ESXi Release	Build Number
4.0 Update 1	208167
4.1 GA	260247

- VMare vCloud Director 1.0

[Table 2-4](#) lists the vCloud Director versions that are compatible with this version of vShield.

Table 2-4. Supported vCloud Director Versions

vCloud Director Release	Build Number
1.0	285979

Client and User Access

- PC with the VMware vSphere Client
- Permissions to add and power on virtual machines
- Access to the datastore where you store virtual machine files, and the account permissions to copy files to that datastore
- Enable cookies on your Web browser to access the vShield Manager user interface
- Connect to the vShield Manager using one of the following supported Web browsers:
 - Internet Explorer 6.x and later
 - Mozilla Firefox 1.x and later
 - Safari 1.x or 2.x

Deployment Considerations

Consider the following recommendations and restrictions before you deploy vShield components.

Preparing Virtual Machines for vShield Protection

You must determine how to protect your virtual machines with vShield. Consider the following questions:

How Are My Virtual Machines Grouped?

You might consider moving virtual machines to port groups on a vDS or a different ESX host to group virtual machines by function, department, or other organizational need to improve security and ease configuration of access rules. You can install vShield Edge at the perimeter of any port group to isolate virtual machines from the external network. You can install a vShield App on an ESX host and configure firewall policies per container resource to enforce rules based on the hierarchy of resources.

Are My Virtual Machines Still Protected if I vMotion Them to Another ESX Host?

Yes, if you install a vShield App on each ESX host in a cluster, you can migrate machines between hosts without weakening the security posture. vShield App instances cannot be migrated to other hosts, thus each instance maintains state for existing sessions.

How Do I Isolate a Group of Virtual Machines?

You can use vShield Edge with the Port Group Isolation feature or VLANs to isolate virtual machines from the external network.

- 1 Install Port Group Isolation on each ESX host that a vDS spans.
- 2 Create a port group on the vDS.
- 3 Enable Port Group Isolation on the vDS.
- 4 Install a vShield Edge on the port group.
- 5 Move the virtual machines to the port group.
- 6 Configure vShield Edge NAT rules for traffic in and out of the port group.

NOTE You can also use VLANs to isolate virtual machines protected by a vShield Edge. If you use VLANs, the internal port group connected to a vShield Edge must have a VLAN tag that is different from the external port group.

vShield Manager Uptime

The vShield Manager should be run on an ESX host that is not affected by downtime, such as frequent reboots or maintenance mode operations. You can use HA or DRS to increase the resilience of the vShield Manager. If the ESX host on which the vShield Manager resides is expected to require downtime, vMotion the vShield Manager virtual appliance to another ESX host. Thus, more than one ESX host is recommended.

Communication Between vShield Components

The management interfaces of vShield components should be placed in a common network, such as the vSphere management network. The vShield Manager requires connectivity to the vCenter Server, as well as all vShield App and vShield Edge instances. vShield components can communicate over routed connections as well as different LANs.

NOTE The vShield Manager must be in the same vCenter Server environment as the vShield components to be managed. You cannot use the vShield Manager across different vCenter Server environments.

Hardening Your vShield Virtual Machines

You can access the vShield Manager and other vShield components by using a web-based user interface, command line interface, and REST API. vShield includes default login credentials for each of these access options. After installation of each vShield virtual machine, you should harden access by changing the default login credentials.

vShield Manager User Interface

You access the vShield Manager user interface by opening a web browser window and navigating to the IP address of the vShield Manager's management port. The default user account, admin, has global access to the vShield Manager. After initial login, you should change the default password of the admin user account. See ["Change the Password of the vShield Manager User Interface Default Account"](#) on page 20.

Command Line Interface

You can access the vShield Manager, vShield App, and vShield Edge virtual appliances by using a command line interface via vSphere Client console session. Each virtual appliance uses the same default username (**admin**) and password (**default**) combination as the vShield Manager user interface. Entering Enabled mode also uses the password **default**.

For more on hardening the CLI, see the *vShield Administration Guide*.

REST Requests

All REST API requests require authentication with the vShield Manager. Using Base 64 encoding, you identify a username-password combination in the following format: username:password. You must use a vShield Manager user interface account (username and password) with privileged access to perform requests. For more on authenticating REST API requests, see the *vShield API Programming Guide*

Installing the vShield Manager and vShield Zones

3

VMware vShield provides firewall protection, traffic analysis, and network perimeter services to protect your vCenter Server virtual infrastructure. vShield virtual appliance installation has been automated for most virtual datacenters.

The vShield Manager is the centralized management component of vShield. You use the vShield Manager to monitor and push configurations to vShield App, vShield Endpoint, and vShield Edge instances. The vShield Manager runs as a virtual appliance on an ESX host.

VMware vShield is included with VMware ESX 4.0 and 4.1. The base VMware vShield package includes the vShield Manager and vShield Zones. You can configure the vShield Zones firewall rule set to monitor traffic based on IP address-to-IP address communication.

Installing the vShield Manager is a multistep process. You must perform all of the tasks that follow in sequence to complete vShield Manager installation successfully.

This chapter includes the following topics:

- [“Obtain the vShield Manager OVA File”](#) on page 17
- [“Install the vShield Manager Virtual Appliance”](#) on page 17
- [“Configure the Network Settings of the vShield Manager”](#) on page 18
- [“Log In to the vShield Manager User Interface”](#) on page 19
- [“Synchronize the vShield Manager with the vCenter Server”](#) on page 19
- [“Register the vShield Manager Plug-In with the vSphere Client”](#) on page 20
- [“Change the Password of the vShield Manager User Interface Default Account”](#) on page 20
- [“Install vShield Zones”](#) on page 20
- [“Where to Go Next”](#) on page 21

Obtain the vShield Manager OVA File

The vShield Manager virtual machine is packaged as an Open Virtualization Appliance (OVA) file, which allows you to use the vSphere Client to import the vShield Manager into the datastore and virtual machine inventory.

Install the vShield Manager Virtual Appliance

You can install the vShield Manager virtual machine on an ESX host in a cluster configured with DRS. The target ESX host must be managed by the same vCenter instance as the ESX hosts on which you want to deploy vShield Zones or vShield App instances. A single vShield Manager serves a single vCenter Server environment.

The vShield Manager virtual machine installation includes VMware Tools. Do not attempt to upgrade or install VMware Tools on the vShield Manager.

To install the vShield Manager

- 1 Log in to the vSphere Client.
- 2 Create a port group to home the management interface of the vShield Manager.

The vShield Manager management interface must be reachable by all future vShield Edge, vShield App, and vShield Endpoint instances.

NOTE Do not place the management interface of the vShield Manager in same port group as the Service Console and VMkernel.

- 3 Go to **File > Deploy OVF Template**.
- 4 Click **Deploy from file** and click **Browse** to locate the folder on your PC containing the vShield Manager OVA file.
- 5 Complete the wizard.
The vShield Manager is installed as a virtual machine into your inventory.
- 6 Power on the vShield Manager virtual machine.

Configure the Network Settings of the vShield Manager

You must use the command line interface (CLI) of the vShield Manager to configure an IP address, identify the default gateway, and set DNS settings.

You can specify up to two DNS servers that the vShield Manager can use for IP address and host name resolution. DNS is required if any ESX host in your vCenter Server environment was added by using the hostname (instead of IP address).

To configure the vShield Manager network settings by using the vShield Manager CLI

- 1 Right-click the vShield Manager virtual machine and click **Open Console** to open the command line interface (CLI) of the vShield Manager.

The booting process might take a few minutes.

- 2 After the `manager login` prompt appears, log in to the CLI by using the user name **admin** and the password **default**.
- 3 Enter Enabled mode by using the password **default**.

```
manager> enable
Password:
manager#
```

- 4 Run the `setup` command to open the CLI setup wizard.

The CLI setup wizard guides you through IP address assignment for the vShield Manager's management interface and identification of the default network gateway. The IP address of the management interface must be reachable by all installed vShield App, vShield Edge, and vShield Endpoint instances, and by a Web browser for system management.

```
manager# setup
```

Use CTRL-D to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

```
IP Address (A.B.C.D):
Subnet Mask (A.B.C.D):
Default gateway (A.B.C.D):
Primary DNS IP (A.B.C.D):
Secondary DNS IP (A.B.C.D):
```

```
Old configuration will be lost, and system needs to be rebooted
Do you want to save new configuration (y/[n]): y
Please log out and log back in again.
```

```
manager> exit
manager login:
```

- 5 Log in to the CLI.
- 6 Ping the default gateway to verify network connectivity.


```
manager> ping A.B.C.D
```
- 7 From your PC, ping the vShield Manager IP address to validate that the IP address is reachable.

Log In to the vShield Manager User Interface

After you have installed and configured the vShield Manager virtual machine, log in to the vShield Manager user interface.

To log in to the vShield Manager user interface

- 1 Open a Web browser window and type the IP address assigned to the vShield Manager.

The vShield Manager user interface opens in an SSH session.

- 2 Accept the security certificate.

NOTE You can use an SSL certificate for authentication. Refer to the *vShield Administration Guide*.

The vShield Manager login screen appears.

- 3 Log in to the vShield Manager user interface by using the user name **admin** and the password **default**.

You should change the default password as one of your first tasks to prevent unauthorized use. See [“Change the Password of the vShield Manager User Interface Default Account”](#) on page 20.

- 4 Click **Log In**.

Synchronize the vShield Manager with the vCenter Server

Synchronize with your vCenter Server to display your VMware Infrastructure inventory in the vShield Manager user interface.

You must have a vCenter Server user account with administrative access to complete this task.

NOTE The vShield Manager virtual machine does not appear as a resource in the inventory panel of the vShield Manager user interface. The **Settings & Reports** object represents the vShield Manager virtual machine in the inventory panel.

To synchronize the vShield Manager with vCenter Server

- 1 Log in to the vShield Manager.
- 2 Click **Settings & Reports** from the vShield Manager inventory panel.
- 3 Click the **Configuration** tab.
- 4 Click the **vCenter** tab.
- 5 Type the IP address or hostname of your vCenter Server in the **IP address/Name** field.
- 6 Type your vSphere Client login user name in the **User Name** field.
- 7 Type the password associated with the user name in the **Password** field.
- 8 Click **Save**.

Register the vShield Manager Plug-In with the vSphere Client

The **vSphere Plug-in** option lets you register the vShield Manager as a vSphere Client plug-in. After the plug-in is registered, you can configure most vShield options from the vSphere Client.

To register the vShield Manager as a vSphere Client Plug-in

- 1 Click **Settings & Reports** from the vShield Manager inventory panel.
- 2 Click the **Configuration** tab.
- 3 Click **vSphere Plug-in**.
- 4 Click **Register**.
- 5 If you are logged in to the vSphere Client, log out.
- 6 Log in to the vSphere Client.
- 7 Select an ESX host.
- 8 Verify that the **vShield** tab appears as an option.

Change the Password of the vShield Manager User Interface Default Account

You can change the password of the **admin** account to harden access to your vShield Manager.

To change the admin account password

- 1 Log in to the vShield Manager user interface.
- 2 Click **Settings & Reports** from the vShield Manager inventory panel.
- 3 Click the **Users** tab.
- 4 Select the **admin** account.
- 5 Click **Update User**.
- 6 Enter a new password.
- 7 Confirm the password by typing it a second time in the **Retype Password** field.
- 8 Click **OK** to save your changes.

Install vShield Zones

The following information is required for vShield Zones installation on an ESX host:

- One IP address for the management (MGMT) port of each vShield Zones virtual appliance. Each IP address should be reachable from the vShield Manager and sit on the Management network used for vCenter and ESX host management interfaces.
- Local or network storage to place the vShield Zones disk.

vShield Zones virtual appliances include VMware Tools. Do not attempt to alter or upgrade the VMware Tools software on a vShield Zones virtual appliance.

- 1 Log in to the vSphere Client.
- 2 Select an ESX host from the inventory tree.
- 3 Click the **vShield** tab.
- 4 Accept the security certificate.
- 5 Click **Install** for the **vShield Zones** service.

- 6 Enter the following information.

Field	Action
Datastore	Select the datastore on which to store the vShield Zones virtual machine files.
Management Port Group	Select the port group to host the vShield Zone's management interface. This port group must be able to reach the vShield Manager's port group.
IP Address	Type the IP address to assign to the vShield Zone's management interface.
Netmask	Type the IP subnet mask associated with the assigned IP address.
Default Gateway	Type the IP address of the default network gateway.

- 7 Click **Install** at the top of the form.

You can follow the vShield Zones installation steps from the Recent Tasks pane of the vSphere Client screen.

- 8 After installation of all components is complete, go to the **vShield Zones > Zones Firewall** tab at the datacenter, cluster, or port group container level to configure firewall rules. Each vShield Zones instance inherits global firewall rules set in the vShield Manager. The default firewall rule set allows all traffic to pass. You must configure blocking rules to explicitly deny traffic. To configure Zones Firewall rules, see the *vShield Administration Guide*.

NOTE You can upgrade vShield Zones to vShield App by obtaining a vShield App license. vShield App enhances vShield Zones protection by offering Flow Monitoring, custom container creation (Security Groups), and container-based access policy creation and enforcement.

You do not have to uninstall vShield Zones to install vShield App. All vShield Zones instances become vShield App instances, the Zones Firewall becomes App Firewall, and the additional vShield App features are enabled.

Where to Go Next

After vShield Manager installation is complete, you can configure vShield Zones firewall settings and analyze traffic. For more, see the *vShield Administration Guide*.

To enhance your network security posture, you can obtain licenses for vShield App, vShield Endpoint, and vShield Edge. For more, see [Chapter 4, "Installing vShield Edge, vShield App, and vShield Endpoint,"](#) on page 23.

Installing vShield Edge, vShield App, and vShield Endpoint

4

After the vShield Manager and vShield Zones are installed, you can obtain licenses to activate vShield App, vShield Endpoint, and vShield Edge components. The vShield Manager OVA package includes the drivers and files required to install these add-on components.

This chapter includes the following topics:

- [“Running vShield in Evaluation Mode”](#) on page 23
- [“Preparing Your Virtual Infrastructure for vShield App, vShield Edge, and vShield Endpoint”](#) on page 23
- [“Installing vShield Endpoint”](#) on page 27
- [“Where to Go Next”](#) on page 28

Running vShield in Evaluation Mode

Before purchasing and activating licenses for vShield Edge, vShield App, an vShield Endpoint, you can install and run evaluation modes of the software. When run in evaluation mode, intended for demonstration and evaluation purposes, your vShield Edge, vShield App, and vShield Endpoint are completely operational immediately after installation, do not require any licensing configuration, and provide full functionality for 60 days from the time you first activate them.

When run in evaluation mode, vShield components can support a maximum allowed number of instances.

After the 60-day trial period expires, unless you obtain licenses for your software, you cannot use vShield. For example, you cannot power on vShield App or vShield Edge virtual appliances or protect your virtual machines.

To continue using the vShield App and vShield Edge functionality without interruptions or to restore the features that become unavailable after the 60-day trial, you need to obtain and install license files that activate the features appropriate for the vShield component you purchased.

Preparing Your Virtual Infrastructure for vShield App, vShield Edge, and vShield Endpoint

Prior to installation, the add-on components require preparation of your ESX host and vNetwork environments. You install vShield App, vShield Endpoint, and the Port Group Isolation feature on ESX hosts. You install vShield Edge on a port group, vNetwork Distributed Switch (vDS) port group, or a Cisco[®] Nexus 1000V.

If you intend to use the Port Group Isolation feature, you should install Port Group Isolation on all ESX hosts in your vCenter environment before you install any vShield Edge virtual machines. If you do not install Port Group Isolation and attempt to enable the feature during vShield Edge installation, Port Group Isolation does not work. See [“Prepare All ESX Hosts”](#) on page 24.

Install vShield Component Licenses

You must install licenses for vShield Edge, vShield App, and vShield Endpoint before installing these components. You can install these licenses after vShield Manager installation is complete by using the vSphere Client.

- 1 From a vSphere Client host that is connected to a vCenter Server system, select **Home > Licensing**.
- 2 For the report view, select **Asset**.
- 3 Right-click a vShield asset and select **Change license key**.
- 4 Select **Assign a new license key** and click **Enter Key**.
- 5 Enter the license key, enter an optional label for the key, and click **OK**.
- 6 Click **OK**.
- 7 Repeat these steps for each vShield component for which you have a license.

Prepare All ESX Hosts

You should prepare all ESX hosts in your vCenter environment for vShield add-on functionality.

The following information is required for ESX host preparation:

- One IP address for the management (MGMT) port of each vShield App virtual appliance. Each IP address should be reachable from the vShield Manager and sit on the Management network used for vCenter and ESX host management interfaces.
- Local or network storage to place the vShield App and Port Group Isolation disks.

vShield virtual appliances include VMware Tools. Do not attempt to alter or upgrade the VMware Tools software on a vShield virtual appliance.

To prepare an ESX host for vShield add-on functionality

- 1 Log in to the vSphere Client.
- 2 Select an ESX host from the inventory tree.
- 3 Click the **vShield** tab.
- 4 Accept the security certificate.
- 5 Click **Install** for the **vShield App** service.

You will be able to install all three services on the next screen.

- 6 Under vShield App, enter the following information.

Field	Action
Datastore	Select the datastore on which to store the vShield App virtual machine files.
Management Port Group	Select the port group to host the vShield App's management interface. This port group must be able to reach the vShield Manager's port group.
IP Address	Type the IP address to assign to the vShield App's management interface.
Netmask	Type the IP subnet mask associated with the assigned IP address.
Default Gateway	Type the IP address of the default network gateway.

- 7 Select the **vShield Edge Port Group Isolation Host Preparation** check box.
- 8 Select the **Datastore** on which to store the Port Group Isolation service files.
- 9 Select the **vShield Endpoint** check box.

- 10 Click **Install** at the top of the form.

You can follow the vShield App installation steps from the Recent Tasks pane of the vSphere Client screen.

- 11 After installation of all components is complete, do the following:
 - **vShield App:** At this point, vShield App installation is complete. Go to the **vShield App > App Firewall** tab at the datacenter, cluster, or port group container level to configure firewall rules. Each vShield App inherits global firewall rules set in the vShield Manager. The default firewall rule set allows all traffic to pass. You must configure blocking rules to explicitly block traffic. To configure App Firewall rules, see the *vShield Administration Guide*.
 - **Port Group Isolation:** You must enable the Port Group Isolation feature on each vDS. After enablement is complete, install a vShield Edge on each vDS port group. See [“Prepare a vNetwork for Port Group Isolation”](#) on page 25.
 - **vShield Endpoint:** To complete installation, see [“Installing vShield Endpoint”](#) on page 27.

Prepare a vNetwork for Port Group Isolation

Port Group Isolation creates a barrier between the virtual machines protected by a vShield Edge and the external network. When you enable Port Group Isolation and install a vShield Edge on a vDS port group, you isolate each secured vDS port group from the external network. When Port Group Isolation is enabled, traffic is not allowed access to the virtual machines in the secured port group unless NAT rules or VLAN tags are configured.

NOTE Port Group Isolation is an optional feature that is not required for vShield Edge operation. Port Group Isolation is available for vDS-based vShield Edge installations only.

To use Port Group Isolation, you must enable this feature on each vDS on which you will install a vShield Edge.

- 1 Enable Port Group Isolation on each vDS.
- 2 Install a vShield Edge on each vDS port group you plan to secure.
- 3 Move the virtual machines to secured vDS port groups.

After Port Group Isolation is installed on each ESX host, you must enable Port Group Isolation on each vDS where you will install a vShield Edge. This allows the Port Group Isolation service to be used on any port group in a vDS.

To enable Port Group Isolation on a vDS

- 1 Log in to the vSphere Client.
- 2 Go to **View > Inventory > Networking**.
- 3 Right-click a vDS.
- 4 Select **vShield > Enable Isolation**.

A browser window opens to confirm that Port Group Isolation has been enabled.

After Port Group Isolation installation is complete, install a vShield Edge instance on each vDS port group.

Install a vShield Edge

Each vShield Edge virtual appliance has External and Internal network interfaces. The Internal interface connects to the secured port group and acts as the gateway for all protected virtual machines in the port group. The subnet assigned to the Internal interface can be RFC 1918 private space. The External interface of the vShield Edge connects to an uplink port group that has access to a shared corporate network or a service that provides access layer networking.

Each vShield Edge requires at least one IP address to number the External interface. Multiple external IP addresses can be configured for Load Balancer, Site-to-Site VPN, and NAT services. The Internal interface can have a private IP address block that overlaps with other vShield Edge secured port groups.

You can install one vShield Edge per port group, vDS port group, or Cisco® Nexus 1000V.

If DRS and HA are enabled, a vShield Edge will be migrated dynamically.

To install a vShield Edge

- 1 Log in to the vSphere Client.
- 2 Go to **View > Inventory > Networking**.
- 3 On a vDS, create a port group.
This port group is the Internal port group.
- 4 Move a tenant's guest virtual machines to the Internal port group.
- 5 Select the new Internal port group.
- 6 Click the **Edge** tab.
- 7 Under **Network Interfaces**, enter the following information.

Field	Action
External	
Port Group	Select the external port group in the vDS. This port group homes a physical NIC and connects to the external network.
IP Address	Type the IP address of the external port group.
Subnet Mask	Type the IP subnet mask associated with the specified external IP address.
Default Gateway	Type the IP address of the default network gateway.
Internal	
Port Group	This is the selected internal port group.
IP Address	Type the IP address of the internal port group.
Subnet Mask	Type the IP subnet mask associated with the specified internal IP address.

- 8 (Optional) Select the **Isolate** check box to enable Port Group Isolation on the vShield Edge.
This prevents virtual machines on the Internal port group from communicating with systems outside of that port group.
- 9 Under **Edge deployment resource selection**, enter the following information

Field	Action
Resource Pool	Select the resource pool where the vShield Edge should be deployed.
Host	Select the ESX host on which the datastore resides.
Datastore	Select the datastore on which to store the vShield Edge virtual machine files.

- 10 Click **Install**.

After installation is complete, configure services and firewall rules to protect the virtual machines in the secured port group. To configure a vShield Edge, see the *vShield Administration Guide*.

Installing vShield Endpoint

The installation instructions that follow assume that you have the following system:

- A datacenter with vCenter Server 4.1 installed and running, and ESX 4.1 installed on each ESX host in the cluster.
- vShield Manager 4.1 installed and running.
- Anti-virus solution management server installed and running.

vShield Endpoint Installation Workflow

After preparing the ESX host for vShield Endpoint installation is complete, install vShield Endpoint in these stages:

- 1 Deploy and configure a security virtual machine (SVM) to each ESX host according to the instructions from the anti-virus solution provider.
- 2 Install the vShield Endpoint thin agent on all virtual machines to be protected. For instructions, see [“Install the Thin Agent on the Guest Virtual Machine”](#) on page 27.

Install the Thin Agent on the Guest Virtual Machine

The thin agent must be installed on each guest virtual machine to be protected. Virtual machines with the thin agent installed are automatically protected whenever they are started up on an ESX host that has the security solution installed. That is, protected virtual machines retain the security protection through shut downs and restarts, and even after a vMotion move to another ESX host with the security solution installed.

Prerequisites

- Make sure that the guest virtual machine has a supported version of Windows installed. Supported versions of the Windows operating system for vShield Endpoint 1.0 are:
 - Windows Vista (32 bit)
 - Windows 7 (32 bit)
 - Windows XP (32 bit)
 - Windows 2003 (32/64 bit)
 - Windows 2008 (32/64 bit)
- Make sure that the thin agent and the virtual machine are both either 32 or 64 bit versions. You cannot mix the two versions.
- Make sure the guest virtual machine has a SCSI controller installed.

IMPORTANT When you create a new virtual machine, the default configuration does not include a SCSI controller. You must specifically add a SCSI controller to the virtual machine. To find instructions on how to add SCSI controllers to a virtual machine, see the vSphere Client help: **vSphere Client Help > Managing Virtual Machine Hardware and Devices > Adding Virtual Devices > Add SCSI Controllers**



CAUTION BusLogic SCSI controllers are not supported.

To install the Thin Agent

- 1 The installation package is located at the same VMware customer site where you downloaded vShield Manager.

The package name has the following form:

- 32-bit

VMware-vShield-Endpoint-Driver-1.0.0-<build number>.x86-32.msi

- 64-bit

VMware-vShield-Endpoint-Driver-1.0.0-<build number>.x86-64.msi.

This is a standard Microsoft installer package.

- 2 Download and execute the installation package on the target host.
- 3 The thin agent must be installed on every guest virtual machine to be protected.
- 4 Reboot the guest virtual machine to complete the installation.

If you run a silent install using `msiexec`, the reboot will happen automatically.

Where to Go Next

After installation is complete, see the *vShield Administration Guide* for configuration, monitoring, and maintenance.

Index

C

- changing the GUI password **20**
- CLI
 - configuring vShield Manager network settings **18**
 - hardening **15**
- client requirements **14**
- cluster protection **11**
- communication between components **15**
- configuring vShield Manager network settings **18**

D

- deployment
 - cluster **11**
 - DMZ **10**
- deployment considerations **14**
- deployment scenarios **10**
- DMZ **10**

E

- enabling Port Group Isolation **25**
- ESX host preparation **24**
- evaluating vShield components **23**

F

- file system filter driver installation **27**

G

- guest driver installation **27**
- GUI, logging in **19**

H

- hardening **15**
 - CLI **15**
 - REST **16**
 - vShield Manager GUI **15**

I

- installation
 - licenses **24**
 - Port Group Isolation **24**
 - vShield App **24**
 - vShield Edge **25, 27**
 - vShield Endpoint **24**
 - vShield Endpoint thin agent **27**
 - vShield Manager **17**

- isolating networks **10**
- isolating virtual machines **15**

L

- licensing
 - evaluation mode **23**
 - installation **24**
- logging in to the GUI **19**

P

- password change **20**
- plug-in **20**
- Port Group Isolation
 - enabling **25**
 - installation **24**
 - isolating networks **10**
- preparing virtual machines for protection **14**
- protecting a cluster **11**
- protecting virtual machines **14**

R

- REST **16**

S

- synchronizing with vCenter **19**
- system requirements **13**

T

- thin agent installation **27**

V

- vCenter, syncing from vShield Manager **19**
- virtual machine isolation **15**
- vMotion **14**
- vNetwork preparation **25**
- vShield
 - component communication **15**
 - deployment scenarios **10**
 - evaluating components **23**
 - hardening **15**
 - preparing an ESX host **24**
 - vShield App **9**
 - vShield Edge **8**
 - vShield Endpoint **9**
 - vShield Manager **7**
 - vShield Zones **7**

- vShield App
 - about **9**
 - common deployments **11**
 - installation **24**
 - licensing **24**
- vShield Edge
 - about **8**
 - common deployments **11**
 - installation **25**
 - isolating networks **10**
 - licensing **24**
- vShield Endpoint
 - about **9**
 - installation **24, 27**
 - installation steps **27**
 - licensing **24**
 - thin agent installation **27**
- vShield Manager
 - about **7**
 - changing the GUI password **20**
 - installation **17**
 - logging in to GUI **19**
 - network settings **18**
 - registering plug-in **20**
 - syncing with vCenter **19**
 - uptime **15**
- vShield Manager GUI **15**
- vShield Zones
 - about **7**
 - vShield Manager **7**
- vSphere Client plug-in **20**