PGP™ Universal Server

Installation Guide

3.2

Version 3.2.0. Last updated: July 2011.

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

Symantec Home Page (*http://www.symantec.com*)

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Contents

1 About the PGP Universal Server Installation Guide

The *PGP Universal Server Installation Guide* provides important PGP™ Universal Server concepts and presents a high-level overview of the tasks required to install, set up, and use PGP Universal Server. This guide provides information about how your PGP Universal Server processes email, which helps you integrate your PGP Universal Servers into your network. There is also information on using Microsoft® Exchange Server and Lotus® Domino® Server with PGP Universal Satellite.

What is PGP Universal Server?

PGP Universal Server is a console that manages the applications that provide email, disk, and network file encryption. PGP Universal Server with PGP Universal Gateway Email provides secure messaging by transparently protecting your enterprise messages with little or no user interaction. The PGP Universal Server replaces PGP Keyserver with a built-in keyserver, and PGP Admin with PGP Desktop configuration and deployment capabilities.

PGP Universal Server also does the following:

- Automatically creates and maintains a Self-Managing Security Architecture (SMSA) by monitoring authenticated users and their email traffic.
- Allows you to send protected messages to addresses that are not part of the SMSA.
- Automatically encrypts, decrypts, signs, and verifies messages.
- Provides strong security through policies you control.

PGP Universal Satellite, a client-side feature of PGP Universal Server, does the following:

- Extends security for email messages to the computer of the email user.
- Allows external users to become part of the SMSA.
- If allowed by an administrator, gives end users the option to create and manage their keys on their computers.

PGP Desktop, a client product, is created and managed through PGP Universal Server policy and does the following:

- Creates PGP keypairs.
- Manages user keypairs.
- Stores the public keys of others.
- Encrypts user email and instant messaging (IM).
- Encrypts entire, or partial, hard drives.
- Enables secure file sharing with others over a network.

PGP Universal Server Product Family

PGP Universal Server functions as a management console for a variety of encryption solutions. You can purchase any of the PGP Desktop applications or bundles and use PGP Universal Server to create and manage client installations. You can also purchase a license that enables PGP Universal Gateway Email to encrypt email in the mailstream.

The PGP Universal Server can manage any combination of the following PGP encryption applications:

- PGP Universal Gateway Email provides automatic email encryption in the gateway, based on centralized mail policy.

  This product requires administration by the PGP Universal Server.
- **PGP Desktop Email** provides encryption at the desktop for mail, files, and AOL Instant Messenger traffic.

  This product can be managed by the PGP Universal Server.
- **PGP Whole Disk Encryption** provides encryption at the desktop for an entire disk.

  This product can be managed by the PGP Universal Server.
- **PGP NetShare** provides transparent file encryption and sharing among desktops.

  This product can be managed by the PGP Universal Server.

Who Should Read This Guide

This guide is for administrators who will install PGP Universal Server for your organization's PGP Universal Server environment.

Common Criteria Environments

To be Common Criteria compliant, see the best practices in *PGP Universal Server 2.9 Common Criteria Supplemental*. These best practices supersede recommendations made elsewhere in this and other documentation.

Using the PGP Universal Server with the Command Line

You can use the PGP Universal Server command line for read-only access to, for example, view settings, services, logs, processes, disk space, query the database, and so on.

Note: If you modify your configuration using the command line, and you do not follow these procedures, your Technical Support agreement is void.

Changes to the PGP Universal Server using command line must be:

- Authorized in writing by Technical Support.
- Implemented by a partner, reseller, or employee who is certified in the PGP Advanced Administration and Deployment Training.
- Summarized and documented in a text file in `/var/lib/ovid/customization` on the PGP Universal Server.

Changes made through the command line may not persist through reboots and may become incompatible in a future release. When troubleshooting new issues, Technical Support can require you to revert custom configurations on the PGP Universal Server to a default state.

Symbols

Notes, Cautions, and Warnings are used in the following ways.

Note: Notes are extra, but important, information. A Note calls your attention to important aspects of the product. You can use the product better if you read the Notes.

Caution: Cautions indicate the possibility of loss of data or a minor security breach. A Caution tells you about a situation where problems can occur unless precautions are taken. Pay attention to Cautions.

Warning: Warnings indicate the possibility of significant data loss or a major security breach. A Warning means serious problems will occur unless you take the appropriate action. Please take Warnings very seriously.

Getting Assistance

For additional resources, see these sections.

Getting product information

The following documents and online help are companions to the *PGP Universal Server Administrator's Guide*. This guide occasionally refers to information that can be found in one or more of these sources:

- **Online help** is installed and is available in the PGP Universal Server product.
- **PGP Universal Server Installation Guide**—Describes how to install the PGP Universal Server.
- **PGP Universal Server Upgrade Guide**—Describes the process of upgrading your PGP Universal Server.
- **PGP Universal Mail Policy Diagram**—Provides a graphical representation of how email is processed through mail policy. You can access this document via the PGP Universal Server online help.

- **Tutorials**—Provides animated introductions on how to manage the mail policy feature in PGP Universal Server 2.5 and later, and how upgraded PGP Universal Server settings migrate into the new mail policy feature.

  You can also access all the documentation and tutorials by clicking the online help icon in the upper-right corner of the PGP Universal Server screen.

- PGP Universal Satellite for Windows and Mac OS X includes online help.

PGP Universal Server and PGP Satellite release notes are also provided, which may have last-minute information not found in the product documentation.

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our Web site at the following URL:

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information

- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan	customercare_apac@symantec.com
Europe, Middle-East, Africa	semea@symantec.com
North America, Latin America	supportsolutions@symantec.com

2 Add the PGP Universal Server to Your Network

This chapter provides information about how your PGP Universal Server processes email, which can help you decide how to integrate your PGP Universal Servers into your network. It also includes information about using Microsoft Exchange Server and Lotus Domino Server with PGP Universal Satellite.

Server Placement

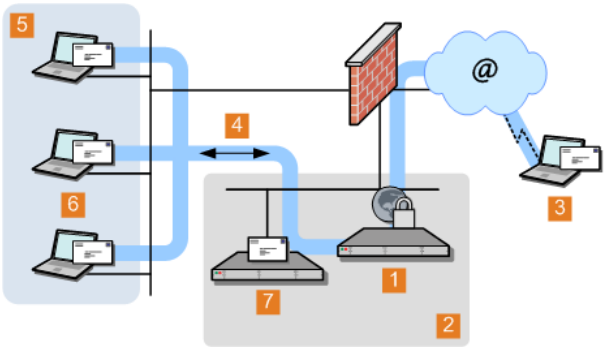
In your network, a PGP Universal Server can be placed in one of the following locations:

- **Internal placement**, where the PGP Universal Server is located between your email users and their local mail server.
- **Gateway placement**, where the PGP Universal Server is located between your external facing mail server and the Internet.

Caution: Unless it is a transparent proxy, do not place the PGP Universal Server behind a proxy server to automatically receive licensing and update information.

Gateway Placement

In a gateway placement, your PGP Universal Server sits between your mail server and the Internet in the logical flow of data.



1	PGP Universal Server gateway placement
2	Example Corp. DMZ
3	External email user
4	Logical flow of data
5	Example Corp. internal network
6	Example Corp. email users

7	Example Corp. email server

Note: The physical location of the PGP Universal Server and the mail server are not important. From a mail relay perspective, it is more important that the PGP Universal Server is between the mail server and the Internet. Both can be on the internal network or in the DMZ.

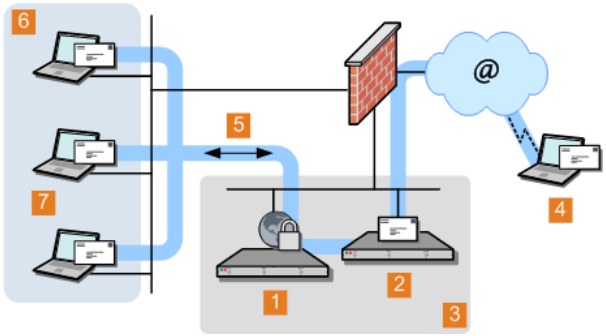
In this placement, remember the following:

- When you use SMTP, email messages are secured before they are sent to the Internet and decrypted/verified when received from the Internet.
- Email users on your internal network should not have direct access to a PGP Universal Server in the gateway placement.

  Based on your configuration, PGP Universal Server attempts to enforce this lack of access automatically .
- If you plan to use the signing features in PGP Universal Server, configure the mail server to verify the From addresses.
- Unless PGP Universal Satellite is used, messages are stored unsecured on the mail server.
- For PGP Universal Server to create the SMSA, you must configure your mail server correctly.

Internal Placement

In this placement, your PGP Universal Server sits between your email users and their email server.



1	PGP Universal Server internally placed
2	Example Corp. email server
3	Example Corp. DMZ
4	External email user
5	Logical flow of data
6	Example Corp. internal network

7	Example Corp. email users

Note: The physical location of the PGP Universal Server and the mail server are not important. From a mail relay perspective, it is more important that the PGP Universal Server is between the email users and the mail server; both can be on the internal network or in the DMZ. From a performance perspective, you should place users and the mail server next to each other on the same network.

In this PGP Universal Server placement, when messages are sent to the mail server using SMTP, they are secured based on the applicable policies. Using POP or IMAP, messages are decrypted and verified when they are retrieved from the mail server. If PGP Universal Satellite has not been deployed globally to your internal users, messages are stored secured on the mail server and are only transmitted unencrypted between the internal user and the PGP Universal Server. If your mail server is configured for SSL/TLS communications with the email client, messages are sent through that encrypted channel and remain encrypted through the entire path. For PGP Universal Server to create the SMSA, email clients must have SMTP authentication switched on when they communicate with a PGP Universal Server.

Mail Relay

After processing outgoing email, PGP Universal Server can forward the email to a central mail gateway, which acts as a mail relay. Sites that use explicit mail routing can use mail relay to forward outgoing email to a mail relay that performs explicit routing.

You cannot configure the mail relay during the initial configuration in the Setup Assistant. Instead, you have to configure the server for gateway placement and configure the mail relay in the administrative interface. For more information on configuring the relay on the Outbound or Unified SMTP proxy, see *Creating New or Editing Existing Proxies* in the *PGP Universal Server Administrator's Guide*.

Microsoft Exchange Server

Messaging Application Programming Interface (MAPI) support is available for Microsoft Exchange Server environments by using PGP Desktop or PGP Universal Satellite for Windows. MAPI support is not available in PGP Universal Satellite for Mac OS X because there are no MAPI email clients for Mac OS X.

For more information about using MAPI, see *Exchange with PGP Client Software* (on page 46) and *MAPI Support* in the *PGP Universal Server Administrator's Guide*.

Lotus Domino Server

Lotus Domino Servers and the Lotus Notes email client (versions 7.0.3 and later) are supported in PGP Desktop and PGP Universal Satellite for Windows®.

For more information about using the Lotus Notes email client, see *Lotus Domino Server with PGP Client Software* (on page 46) and *Lotus Notes Support* in the *PGP Universal Server Administrator's Guide*.

Installation Overview

This a broad overview of the process to plan, set up, and maintain your PGP Universal Server environment.

Steps 1 and 4 are described in this guide, but the other steps are described in the *PGP Universal Server Administrator's Guide*. This process applies a new, stand-alone installation of PGP Universal Server. If you plan to install a cluster, you must install and configure one PGP Universal Server following this process. Additional cluster members receive most of their configuration settings from the initial PGP Universal Server through data replication.

1 **Plan where in your network you want to locate your PGP Universal Server(s).**

Where you put PGP Universal Servers in your network, how many PGP Universal Servers you have in your network, and other factors impact how you add the PGP Universal Servers to your existing network. To help you plan, you should create a diagram of your network that includes the network components and your email flows. This diagram should also include details about the impact on your network of adding a PGP Universal Server. For more information on how to add PGP Universal Servers to your existing network, see *Adding the PGP Universal Server to Your Network* (see "*Add the PGP Universal Server to Your Network*" on page 7).

2 **Perform the necessary DNS changes.**

This involves tasks such as the following:

- Adding IP addresses for your PGP Universal Servers and an alias to your keyserver.
- Updating the MX record if necessary.
- Adding keys.<domain>, hostnames of potential Secondary servers for a cluster, and so on.

Properly configured DNS settings, such as root servers and appropriate reverse lookup records, are required to support PGP Universal Server. You host and pointer records must be correct. IP addresses must be resolvable to hostnames, and hostnames must be resolvable to IP addresses.

3 **Prepare a hardware token Ignition Key.**

To add a hardware token Ignition Key during set up, you must install the drivers and configure the token before you set up the PGP Universal Server. For information on preparing a hardware token Ignition Key, see Protecting PGP Universal Server with Ignition Keys in the *PGP Universal Server Administrator's Guide* .

Note: In a cluster, the Ignition Key that is configured on the first PGP Universal Server in the cluster also applies to subsequent members of the cluster.

4 **Install and configure PGP Universal Server.**

The Setup Assistant runs automatically when you access the PGP Universal Server administrative interface for the first time. You can set or confirm a number of basic settings, such as your network settings, administrator password, server placement option, mail server address, and so on. For more information on this process, see *Setting Up the PGP Universal Server* (see "*About Setting Up PGP Universal Server*" on page 27).

Note: To configure multiple servers as a cluster, you must first configure one server and add the additional servers as cluster members. You can do this through the Setup Assistant when you install a server that will join an existing cluster or through the PGP Universal Server administrative interface. For more information, see *Cluster Member Configuration* (see "*Configuring a Cluster Member*" on page 31).

5 **License your server.**

You must license PGP Universal Server to take it out of Learn Mode or install updates. After it is licensed, you should check for and install product updates. If you want the PGP Universal Server to provide mail proxy services, you must have a PGP Universal Server license with the mailstream feature enabled and select the **Enable Mail Proxies** checkbox on the **System Settings** page. For more information, see Licensing Your Software in the *PGP Universal Server Administrator's Guide*.

6 **Import the PGP key you want to use as your Organization Key with PGP Universal Server and back it up.**

Your Organization Key is used to sign all user keys the PGP Universal Server creates and encrypt PGP Universal Server backups. This key represents the identity of your organization and is the root of the Web-of-Trust for your users.

If your organization uses PGP Desktop and has an Corporate Key or Organization Key that you want to use with PGP Universal Server, you should import it after configuring your server. If your organization does not have a key to use as your Organization Key, you can use the Organization Key that the Setup Assistant automatically created with default values. For more information, see Managing Organization Keys in the *PGP Universal Server Administrator's Guide*.

Note: Regardless of which key you use as your Organization Key, you must back up the key.

Since PGP Universal Server's built-in back-up feature always encrypts backups to this key, you must provide a copy of your Organization Key to restore your data. For more information, see Organization Certificate in the *PGP Universal Server Administrator's Guide*.

7 **Add the PGP Additional Decryption Key (ADK) that you want to use with PGP Universal Server.**

An Additional Decryption Key (ADK) allows you to recover an email message if the recipient is unable or unwilling to do so; every message that is encrypted to the ADK can be opened by the holder(s) of the ADK. You cannot create an ADK with the PGP Universal Server, but if you have an existing PGP ADK generated by PGP Desktop, you can add it to your PGP Universal Server and use it. For more information, see the *PGP Desktop User's Guide* and Additional Decryption Key (ADK) in the *PGP Universal Server Administrator's Guide*.

8 **Create a SSL/TLS certificate or obtain a valid SSL/TLS certificate.**

The Setup Assistant automatically creates a self-signed certificate to be used with SSL/TLS traffic. Because this certificate is self-signed, it might not be trusted by email or Web browser clients. Symantec Corporation recommends that you obtain a valid SSL/TLS certificate for each of your PGP Universal Servers from a reputable Certificate Authority. This is especially important for PGP Universal Servers that are publicly accessed. Older Web browsers might reject self-signed certificates or not know how to handle them when they encounter them through PGP Universal Web Messenger or Smart Trailer. For more information, see Working with Certificates in the *PGP Universal Server Administrator's Guide*.

9 **Configure the Directory Synchronization feature if you want to synchronize an LDAP directory with your PGP Universal Server.**

If you have an existing LDAP server, Directory Synchronization provides more control over who is included in your SMSA. By default, user enrollment is set to Email enrollment. If you decide to use LDAP directory enrollment, this enrollment type assumes that you have an LDAP directory configured. You can change the client enrollment setting for Directory Synchronization in the **Directory Synchronization Settings** page.

Note: For LDAP user enrollment to work, you must have a configured LDAP directory and have enabled Directory Synchronization.

For more information, see Using Directory Synchronization to Manage Users in the *PGP Universal Server Administrator's Guide*.

10 **Configure PGP Desktop client features**.

By default, the PGP Desktop client basic license is installed with the PGP Universal Server, so you do not have to add the client license separately. However, optional features, such as messaging, PGP Whole Disk Encryption, and PGP NetShare, are disabled by default. If you purchased a license for those features, you must edit your client policy settings to enable them. For more information about consumer policy settings, see Establishing PGP Desktop Settings for Your PGP Desktop Clients in the *PGP Universal Server Administrator's Guide*.

11 **Add trusted keys, configure consumer policy, and establish mail policy.**

These settings are important to operate PGP Universal Server securely.

- For more information on adding trusted keys from outside the SMSA, see Managing Trusted Keys and Certificates in the *PGP Universal Server Administrator's Guide*.
- For more information about consumer policy settings, see Administering Consumer Policy.
- For information on setting up mail policy, see Setting Mail Policy.

When setting consumer policies, PGP Universal Server provides Out of Mail Stream (OOMS) support. This option specifies how the email is transmitted from the client to the server if PGP Desktop cannot find a key for the recipient and, therefore, cannot encrypt the message. OOMS is disabled by default, so sensitive messages that cannot be encrypted locally are sent unencrypted to PGP Universal Server "in the mail stream" like typical emails. Mail or Network administrators can read these messages by accessing the mail server's storage or monitoring network traffic. However, archiving solutions, outbound anti-virus filters, or other systems that monitor or proxy mail traffic will process these messages normally.

You can enable OOMS, which means that sensitive messages that cannot be encrypted locally are sent to PGP Universal Server "out of the mail stream." PGP Desktop creates a separate, encrypted network connection to the PGP Universal Server to transmit the message. However, archiving solutions, outbound anti-virus filters, or other systems that monitor or proxy mail traffic will not see these messages.

When you configure PGP Universal Server, you should determine the appropriate settings for your requirements. This option can be set separately for each policy group, and is set in the Consumer Policy page. For more details on the effects of enabling or disabling OOMS, see Out of Mail Stream Support in the *PGP Universal Server Administrator's Guide*.

12 **Install and configure additional cluster server members.**

You can do this through the Setup Assistant when you install a server that will join an existing cluster or through the PGP Universal Server administrative interface. You must configure one server before you can add and configure additional servers as cluster members. For more information, see Clustering your PGP Universal Servers in the *PGP Universal Server Administrator's Guide*..

13 **Reconfigure the settings of your email clients and servers, if necessary.**

Depending on how you add the PGP Universal Server to your network, some setting changes might be necessary. For example, if you are using a PGP Universal Server that is placed internally, the email clients **must** have SMTP authentication switched on. For PGP Universal Servers that are placed externally, you must configure your mail server to relay SMTP traffic to the PGP Universal Server.

14 **Enable SNMP Polling and Traps.**

You can configure PGP Universal Server to allow network management applications to monitor system information for the device on which PGP Universal Server is installed and send the information to an external destination. For more information see Configuring SNMP Monitoring in the *PGP Universal Server Administrator's Guide*.

15 **Distribute PGP Universal Satellite and/or PGP Desktop to your internal users, if appropriate.**

To provide seamless, end-to-end message security without training your users, you can use PGP Universal Satellite. Exchange/MAPI and Lotus Notes environments also require PGP Universal Satellite. PGP Desktop provides more features and user control than PGP Universal Satellite does. For more information, see PGP Universal Satellite and Configuring PGP Desktop Installations in the *PGP Universal Server Administrator's Guide*.

16 **Analyze the data from Learn Mode.**

In Learn Mode, your PGP Universal Server does the following:

- Sends messages through mail policy without taking action on the messages.
- Decrypts and verifies incoming messages when possible.
- Dynamically creates a SMSA.

You can see what the PGP Universal Server would have done without Learn Mode by monitoring the system logs. Learn Mode helps you become familiar with how the PGP Universal Server operates and allows you to see the effects of your policy settings before the PGP Universal Server goes live on your network. You can tune settings in Learn Mode, so that the PGP Universal Server is operating properly when you go live. For more information, see Operating in Learn Mode in the *PGP Universal Server Administrator's Guide*.

17 **Adjust policies as necessary.**

You should review your current policies and make the necessary changes.

18 **Back up all PGP Universal Servers before taking them out of Learn Mode.**

This gives you a baseline backup if you need to return to a clean installation. For more information, see Backing Up and Restoring System and User Data in the *PGP Universal Server Administrator's Guide*.

19 **Take your PGP Universal Servers out of Learn Mode.**

Now email messages are encrypted, signed, and decrypted/verified, based on the relevant policy rules.

20 **Monitor the system logs to ensure that your PGP Universal Server environment is operating as expected.**

3 About Open Ports

This chapter provides information on the ports a PGP Universal Server has open and on which ports it listens.

TCP Ports

Port	Protocol/Service	Comment
21	**File Transfer Protocol (FTP)**	Used to transmit encrypted backup archives to other servers. Data is sent via passive FTP, so port 20 (FTP Data) is not used.
22	**Open Secure Shell (SSH)**	Used for remote shell access to the server for low-level system administration.
25	**Simple Mail Transfer Protocol (SMTP)**	Used to send mail. In a gateway placement, the PGP Universal Server listens on port 25 for incoming and outgoing SMTP traffic.
80	**HyperText Transfer Protocol (HTTP)**	Used to allow user access to the PGP Verified Directory. If the PGP Verified Directory is disabled, access on this port is automatically redirected to port 443 over HTTPS. Also used for Universal Services Protocal (USP) keyserver connection.
110	**Post Office Protocol (POP)**	Used to retrieve mail by users with POP accounts in an internal placement. Closed to gateway placements.
143	**Internet Message Access Protocol (IMAP)**	Used to retrieve mail by users with IMAP accounts in an internal placement. Closed to gateway placements.
389	**Lightweight Directory Access Protocol (LDAP)**	Used to allow remote hosts to look up local users' public keys.
443	**HyperText Transfer Protocol, Secure (HTTPS)**	Used for PGP Desktop and PGP Universal Satellite policy distribution and PGP Universal Web Messenger access. If the Verified Directory is disabled, used for HTTPS access. Also used for Universal Services Protocal (USP)over SSL for keyserver connection.
444	**Simple Object Access Protocol, Secure (SOAPS)**	Used to cluster replication messages.

Port	Protocol/Service	Comment
465	**Simple Mail Transfer Protocol, Secure (SMTPS)**	Used to send mail securely in internal placements. Closed to gateway placements. This is a non-standard port used only by legacy mail servers. We recommend, rather than using this port, you use STARTTLS on port 25.
636	**Lightweight Directory Access Protocol, Secure (LDAPS)**	Used to securely allow remote hosts to look up public keys of local users.
993	**Internet Message Access Protocol, Secure (IMAPS)**	Used to retrieve mail securely by users with IMAP accounts in internal placements. Closed to gateway placements.
995	**Post Office Protocol, Secure (POPS)**	Used to retrieve mail securely by users with POP accounts in internal placements. Closed to gateway placements.
9000	**HyperText Transfer Protocol, Secure (HTTPS)**	Allows access to the PGP Universal Server administrative interface.

UDP Ports

Port	Protocol/Service	Comment
53	**Domain Name System (DNS)**	Used to look up a Fully Qualified Domain Name (FQDN) on the DNS server and translate to an IP address.
123	**Network Time Protocol (NTP)**	Used to synchronize the system's clock with a reference time source on a different server.
161	**Simple Network Management Protocol (SNMP)**	Used by network management applications to query the health and activities of PGP Universal Server and the computer on which it is installed.

4 About Naming your PGP Universal Server

This chapter describes how and why to name your PGP Universal Server using the **keys.<domain>** convention.

How to Name Your PGP Universal Server

Unless a valid public key is found locally, PGP Universal Servers automatically look for valid public keys for email recipients by attempting to contact a keyserver at a special hostname, **keys.<domain>**, where <domain> is the recipient's email domain.

For example, an internal user at example.com sends an email to susanjones@widgetcorp.com. If no valid public key for Susan is found on the Example PGP Universal Server, it automatically looks for a valid public key for Susan at keys.widgetcorp.com, even if there is no domain policy for widgetcorp.com on Example's PGP Universal Server. Keys are found locally if they are cached, or if Susan was an external user who explicitly supplied her key through PGP Universal Web Messenger. If the Widgetcorp PGP Universal Server is named using the keys.<domain> convention, the Example Corp. PGP Universal Server can find a valid public key for susan@widgetcorp.com at keys.widgetcorp.com.

Caution: Symantec Corporation strongly recommends you name your PGP Universal Server according to this convention, because it allows other PGP Universal Servers to easily find valid public keys for email recipients in your domain. You must also use this convention to name your externally visible PGP Universal Server.

If your organization uses email addresses, such as mingp@example.com and mingp@corp.example.com, your PGP Universal Server must be reachable at **keys.example.com** and **keys.corp.example.com.** If you have multiple PGP Universal Servers in a cluster that are managing an email domain, only one of those PGP Universal Servers needs to use the keys.<domain> convention.

Note: Keys that are found using the keys.<domain> convention are treated as valid and trusted.

Keys.<domain> should be the address of a load-balancing device, which distributes connections to your PGP Universal Server's keyserver service. The ports that need to be load balanced are the ports on which you are running your keyserver service, port 389 for LDAP and 636 for LDAPS. You can also name your PGP Universal Server according to your company's required naming convention and ensure that the server has a DNS alias of keys.<domain>.com.

If you are administering multiple email domains, you should establish the keys.<domain> convention for each email domain. If your PGP Universal Server is behind your corporate firewall, you must ensure that ports 389 (LDAP) and 636 (LDAPS) are open to support the keys.<domain> convention.

Naming Methods

To support the keys.<domain> convention, you can name your PGP Universal Server in one of the following ways:

- In the Setup Assistant, name your PGP Universal Server with the keys.<domain> convention in the **Host Name** field on the **Network Setup** page.
- On the **Network Settings** page, change the host name of your PGP Universal Server to keys.<domain> .
- Create a DNS alias to your PGP Universal Server that uses the keys.<domain> convention that is appropriate for your DNS server configuration.

5 About Installing PGP Universal Server

This chapter provides information about the following:

- Setting up your PGP Universal Server
- System requirements

Installing your PGP Universal Server For a higher-level view of this process, see *Installation Overview* (on page 10).

Installation Considerations

You must install and test the installation in a lab or staging environment before you integrate the PGP Universal Server into your network. PGP Universal Server is a customized Linux installation and cannot be installed on a Windows server. Every PGP Universal Server requires a dedicated system that meets the system requirements described in the *PGP Universal Server Release Notes*. When you install PGP Universal Server, the data is deleted and the system is reconfigured as a PGP Universal Server.

Warning: Before you install, you must back up all the data on the system. The installation erases all data from the destination disk.

The installation software is included on the Server Installation DVD, which also includes documentation, software license, PGP Universal Satellite and PGP Desktop software installers, and release notes. Symantec strongly recommends that you locate your PGP Universal Servers in secured areas with restricted access. Only authorized individuals should be granted physical access to PGP Universal Servers.

Warning: If you are performing this installation as part of a cluster migration from version 2.12 SP4, before you begin the migration, you must run the pgpSyncUsers utility on this cluster to ensure the user data is consistent. For more information, see the *PGP Universal Server Upgrade Guide* for details.

Warning: If you have a hardware token Ignition Key or a Hardware Security Module (HSM), you must contact Technical Support before you migrate to PGP Universal Server 3.2.0.

Migrating to version 3.2.0 requires that you create a new setting on the upgraded (3.2.0) version of PGP Universal Server before you restore the backup file from your previous system. This setting can only be added through SSH access with the help of Technical Support. If you migrate to version 3.2.0 without adding this preference, you will be locked out of the user interface after the upgrade. As a result, you cannot use your hardware token Ignition Key to unlock your PGP Universal Server.

System Requirements

For the latest system requirements, see the *PGP Universal Server Release Notes*.

You must install the PGP Universal Server software on PGP Universal Server Certified Hardware. You can find the latest PGP Universal Server Certified Hardware List available on Symantec Corporation's website.

PGP Universal Server on a VMware ESX Virtual Machine

Before you install PGP Universal Server version 3.2.0 on a virtual machine, ensure that:

- VMware ESXi 4.1, Update 1 is installed.
- You are an administrator with sufficient privileges to perform the required functions.
- You have used the **New Virtual Machine Wizard** to create a virtual machine on the host VMware ESX server with the following requirements:
  - Guest operating system is Linux:
    - Other Linux kernel 2.6 (32 bit)

    This is a required setting.
  - Symantec Corporation recommends that you configure at least two virtual CPUs for PGP Universal Server.
  - Have the following as minimums for memory:
    - 4GB of memory on a single server instance
    - 8GB on a two server cluster configuration
    - For additional servers, Symantec Corporation recommends additional memory.

    The minimum requirements may also increase depending upon the features in use upon the PGP Universal Servers, such as Gateway Email, PGP Whole Disk Encryption or PGP NetShare.
  - LSI Logic SCSI Adapter as the I/O Adapter type.
    This is a required setting.

    PGP Universal Server does not support the BusLogic SCSI Adapter. If you configure your virtual machine to use this adaptor, a partitioning error occurs during installation.

The remaining options can be configured as appropriate. Symantec Corporation recommends that you configure the VMware hardware as if you were configuring a physical server.

Note: Using PGP Universal Server with VMware VMotion is not currently supported.

Installing VMware Tools for PGP Universal Server

Before you use these commands on the PGP Universal Server, see *Using the PGP Universal Server with the Command Line* (on page 2).

After installing PGP Universal Server, you must install VMware Tools.

To install VMware Tools:

1 Access the PGP Universal Server using the command line with SSH and log in to the server as `root`.

To set up command line access to the PGP Universal Server, see the instructions in *Accessing the PGP Universal Server using SSH* (on page 21).

2 Run this script:

```
# /usr/bin/install-vmware-tools.sh --version 4.1
```

3 When prompted, type `reboot`.

During reboot, the console messages should indicate that the VMware modules have been loaded correctly (`[OK]`).

4 Run `# lsmod | grep vm` to confirm that the modules have been installed.

This step should list the VMware modules for ESX 4.1.

5 Run the following commands to confirm that the appropriate processes are running:

- `# chkconfig --list vmware-tools`

  This step shows whether the VMware modules are correctly set to load during system startup. They should be ON for runlevel 3.

- `# ps aux | grep guestd`

  This should show that /usr/sbin/vmware-guestd is running.

Accessing the PGP Universal Server using SSH

To access PGP Universal Server through the command line, you must create an SSHv2 key and add it to the superuser administrator account in PGP Universal Server. You can do this, for example, by using PuTTYgen to create an SSHv2 key and PuTTY to log in to the command line interface. You add the SSHv2 key to your superuser administrator account through the PGP Universal Server administrative interface.

PuTTY is a free suite of SSH tools that includes the following:

- PuTTYgen
- PuTTY
- PSFTP
- Pageant, the PuTTY authentication agent

The PuTTYgen and PuTTY.exe files can be downloaded separately from the Internet. To set up command line access to the PGP Universal Server, see the Knowledge Base.

Installation Materials

PGP Universal Server is distributed on one DVD, which you can use to install the server on PGP Universal Server Certified Hardware. The DVD also contains PGP Universal Server documentation and installers for PGP Universal Satellite and PGP Desktop.

Installation Options

Note: Your system must be set to boot from the DVD.

When you insert the installation DVD and reboot the server, you can select **customnet** as the installation boot option, . This option installs the PGP Universal Server using a standard partitioning scheme and configures the network settings based on your inputs during installation. Symantec Corporation recommends you perform the default installation to ensure that your PGP Universal Server runs properly when you finish. If the media is invalid, you can use the **mediacheck** boot option to verify the DVD contents before you begin the installation. For more information, see *Performing a Media Verification on your DVD* (see "*Verifying the Media on Your DVD*" on page 23).

During the default installation, you are prompted to provide the following information:

- IP address
- Subnet mask
- Default gateway
- DNS information
- Hostname

For more information on the information you need to provide, see *Default Installation Procedure* (on page 22).

If you provide the network information during installation, it is pre-loaded into the Setup Assistant. The default installation also simplifies the steps to connect to the PGP Universal Server and continue with the setup. Other installation boot options provide combinations of installation and configuration steps for expert system administrators. If you are considering one of these installation boot options, talk to your Technical Support representative. These options may complicate your ability to connect to and set up your PGP Universal Server. For more information about these options, see *Alternate Installation Procedures* (on page 24).

Default Installation Procedure

Before you install PGP Universal Server using the default process, you must do the following:

1. In a secure location, set up the system that will host the server.
2. Attach a keyboard and monitor to the server on which you will install PGP Universal Server.
3. Make sure the system is set to boot from the DVD.
4. Insert the PGP Universal Server Installation DVD.
5. Reboot the system.

To install the PGP Universal Server software with the default process

1. At the prompt, do one of the following:
   - Press **Enter** to run the default installation without verifying the DVD.

- If there are problems with the DVD, type `customnet mediacheck` and press **Enter** to verify the DVD before you install.

  For more information on mediacheck, see *Performing a Media Verification on your DVD* (see "*Verifying the Media on Your DVD*" on page 23).

A warning appears stating that the installation process erases and repartitions the system's disk.

2 Click **Continue** or **Cancel**.

After the pre-installation, if your system contains multiple network interfaces, these interfaces are displayed on the **Network Configuration** page. All the network interfaces are set to **Active on boot**. If you plan to use multiple interfaces, you should configure them all with IP addresses.

3 Select the network interface you want to configure and click **Edit**.

4 Type the IP address and Prefix/Netmask for the selected network interface and click **OK**.

You can type the Netmask in dotted quad notation (for example, `255.255.255.0`) or in Classless Inter-Domain Routing (CIDR) notation (/24). As you configure each interface, its IP address appears in the list of interfaces.

5 After you configure the IP address and Netmask for all the network interfaces, click **OK**.

6 Type the IP addresses of the Gateway, Primary DNS, and Secondary DNS, and click **OK**.

7 Type the hostname for the PGP Universal Server and click **OK**.

The hostname must be the name of the first network interface, because by default, the PGP Universal Server listens on the first interface. Symantec Corporation strongly recommends that you name your externally visible PGP Universal Server according to the *keys.<domain>* convention, which allows other PGP Universal Servers to easily find valid public keys for email recipients in your domain. For more information, see *Naming your PGP Universal Server* (see "*About Naming your PGP Universal Server*" on page 17).

After the PGP Universal Server is installed, the system automatically ejects the DVD and reboots.

Note: **Do not** log in at the login prompt. You do not need to log in at this point to complete the setup.

---

8 Type `https:// <hostname>:9000 or https: //<IP address>:9000` to connect to the server through the Setup Assistant

For more information on the installation and setup, see *Initial Configuration with Setup Assistant* (on page 28).

Verifying the Media on Your DVD

Before you install PGP Universal Server, verify that the media from which you are installing is error-free by adding **mediacheck** to your installation command.

To complete the media verification:

1 In a default installation, type `customnet mediacheck` and press **Enter**.

2 Click **OK**.

If you click **Skip**, proceed to step 3.

3 Click **Test**.

If the DVD does not pass, eject it, and insert another DVD, but if the DVD passes, click **OK**.

Alternate Installation Procedures

Depending on your PGP Universal Server installation needs, there are a variety of installation options, which offer alternate options for partitions, driver installation, and network configuration. To access the alternate installation options, after the installation starts, press **F2** at the initial prompt.

The following installation options are available:

- **customnet**, which does the following:
  - Clears the disk partitions.
  - Creates default partitions.
  - Prompts for network configuration information.

  For more information about this installation option, see *Default Installation Procedure* (on page 22).
- **pgp**, which does the following:
  - Clears the disk partitions.
  - Makes default partitions.
  - Assigns IP address 192.168.1.100.
- **standard**, which does the following:
  - Clears disk partitions but does not make default partitions.
  - Prompts for network configuration information.
- **ks**, which behaves the same way as the s**tandard** option.
- **expert**, which does the following:
  - Clears disk partitions.
  - Does not make default partitions.
  - Allows partitioning of removable media.
  - Prompts for a driver disk.
  - Prompts for network configuration information.
- **noautopart**, which does the following:
  - Clears disk partitions but does not make default partitions.
  - Assigns IP address 192.168.1.100.
- **memtest86**, which does the following:
  - Runs, but does not install, *memtest86+* to test the RAM.

  This test is recommended if you are installing on new hardware.

You can verify your media before you run the installation by adding the **mediacheck** keyword after any of these installation commands. For more information, see *Performing a Media Verification on your DVD* (see "*Verifying the Media on Your DVD*" on page 23).

Caution: Some of these options may make it more complicated to connect and continue the configuration using a Web browser. Symantec Corporation strongly recommends that you contact Technical Support before you attempt another installation procedure.

Set Up after "pgp" Install

If you select the default installation option (**customnet**) or the **standard**, **ks**, or **expert** options, see *Initial Configuration with Setup Assistant* (on page 28). These options configure your network settings as part of the installation process.

If you select the **pgp** or **noautopart** installation, gather materials and information before you can continue with the setup.

Hardware

Before you configure your PGP Universal Server using the Setup Assistant, you must have the following:

- A Web browser on a Windows or Mac OS X computer, which allows you to run Setup Assistant.
- A crossover Ethernet cable to connect a Windows or Mac OS X computer to the PGP Universal Server.

System Information

To configure your PGP Universal Server, you need the following:

- The temporary IP address and subnet of the newly installed PGP Universal Server, which is used to initially configure the Setup Assistant:
  - **IP:** `192.168.1.100:9000`
  - **Subnet:** `255.255.255.0`

  This data helps you connect to the PGP Universal Server during the initial configuration of the Setup Assistant, but before the PGP Universal Server is available through a Web browser.
- IP address, name, gateway, and DNS server information.
- A license or license authorization from Symantec Corporation:
  - If your PGP Universal Server can connect to the PGP Licensing Server over the Internet, the license server authorizes your PGP Universal Server license.

  - If your PGP Universal Server cannot connect to the PGP Licensing Server over the Internet, you need the License Authorization text file to license your PGP Universal Server.
- Depending on your setup, your Organization Key or a saved backup.

Connecting to the PGP Universal Server

To continue the installation and setup, you must have a crossover Ethernet cable to connect to the PGP Universal Server. Configure the client computer with a fixed IP address and access the PGP Universal Server from this computer.

To connect to the PGP Universal Server

1 Type the following information to configure the client computer:

IP: `192.168.1.99`

Subnet: `255.255.255.0`

If you are using a Mac OS X client computer, save this temporary setup as a separate location in **Network Preferences** (for example, `setup`).

2 Continue your set up as described in *Initial Configuration with Setup Assistant* (on page 28).

6 About Setting Up PGP Universal Server

This chapter describes how to access and use Setup Assistant to configure your PGP Universal Server.

The Setup Assistant

The Setup Assistant appears the first time you access the PGP Universal Server. You are prompted for information about your network and how you want your PGP Universal Server to work. The Setup Assistant performs most of the configuration for your PGP Universal Server. In the PGP Universal Server's administrative interface, you can change any Setup Assistant settings after you run it. You can also use the administrative interface to configure the features not covered in the Setup Assistant.

The Setup Assistant supports the following types of setups:

- **New Installation**, which allows you to configure a PGP Universal Server to be your only PGP Universal Server or the first server in a cluster.
- **Cluster Member**, which allows you to add this PGP Universal Server to an existing cluster.
- **Restore**, which allows you to restore backed up data from another PGP Universal Server to a new PGP Universal Server.

  You need the backed up data file and the Organization Key that was used to encrypt the backup file. For more information about configuring a PGP Universal Server with data from a backup, see the *PGP Universal Server Upgrade Guide*.
- **Keyserver**, which allows you to migrate the keys and data from a PGP Keyserver to a PGP Universal Server.

  For more information about configuring a PGP Universal Server with the keys from a PGP Keyserver, see the *PGP Universal Server Upgrade Guide*.

For each setup type, you must do the following:

1. Read and agree to the End User License Agreement.
2. Specify the type of setup.
3. Configure the network settings for your PGP Universal Server.
4. Restart the PGP Universal Server.

After the PGP Universal Server restarts, you can connect to it using a Web browser and continue with the Setup Assistant.

Initial Configuration with Setup Assistant

The Setup Assistant helps you establish the PGP Universal Server's network configuration and setup type. After the software installs and the server restarts, you can connect to the PGP Universal Server using a Web browser at the configured IP address and complete the Setup Assistant.

To initially configure PGP Universal Server with the Setup Assistant:

1 In a Web browser, connect to the PGP Universal Server in one of the following ways:

If you selected **customnet, standard, ks**, or **expert** installation options, type: `https://<hostname>:9000` using the hostname or IP address you assigned to the PGP Universal Server.

- If you selected **pgp** or **noautopart** installation options, and you are using a client computer with a fixed IP address, type:

https://192.168.1.100:9000.

For more information, see *Preparing for Setup after pgp Install* (see "*Set Up after "pgp" Install*" on page 25).

2 Read the text and click **Forward**.

3 Read the License Agreement and click **I Agree**.

4 Select an installation option:

- **New Installation** if this is a new PGP Universal Server installation and this server is the only PGP Universal Server in your network, or it is the first server in a cluster.
- **Cluster Member** if this PGP Universal Server will join an existing PGP Universal Server cluster.

Because the first PGP Universal Server acts as the sponsor for the second PGP Universal Server, you must have one PGP Universal Server already installed and configured before you can install a second PGP Universal Server as a cluster member. For more information, see Clustering your PGP Universal Servers.

- **Restore** if you want to restore the data from a server backup.

You need your Organization Key and access to the backup file to proceed with this installation. For more information, see the *PGP Universal Server Upgrade Guide*.

- **Keyserver** if you want to migrate the keys on an existing PGP Keyserver to the PGP Universal Server you are configuring. For more information, see the *PGP Universal Server Upgrade Guide*.

5 Click **Forward**.

6 Select the appropriate date and time settings.

Since your server completes many time-based operations, you must select the correct time and date.

7 (Optional) Specify an NTP time server.

The PGP Universal Server automatically synchronizes the time when the Setup Assistant is finished.

8 Click **Forward**.

9 If you selected **standard**, review the displayed information.

10 If you selected an option other than **standard**, type the appropriate information:

a In **Hostname**, type a name for this PGP Universal Server.

This must be a fully-qualified domain name of the external, untrusted interface. Symantec Corporation strongly recommends you name your externally visible PGP Universal Server according to the *keys.<domain> convention*, which allows other PGP Universal Servers to easily find valid public keys for email recipients in your domain. For example, Example Corporation names its externally visible PGP Universal Server *keys.example.com*. For more information, see *Naming your PGP Universal Server* (see "*About Naming your PGP Universal Server*" on page 17).

b Type an IP address.

c Type a subnet mask.

d Type the IP address of the default gateway for the network.

e Type the IP address(es) of the DNS servers for your network.

11 Click **Forward**.

12 Review the information and click **Done**.

Your server restarts automatically.

- If you selected **customnet**, **standard, ks**, or **expert** installation options, skip step 13 and proceed to the next section.
- If you selected **pgp** or **noautopart** installation options, proceed to step 13.

Your PGP Universal Server has accepted the new network settings, so you can disconnect the temporary setup.

13 Disconnect the cable between the client computer and the PGP Universal Server, revert the settings of the client computer, reconnect the two computers to the original network, and continue with the Setup Assistant.

Configuring a New Installation

This procedure helps you configure your newly installed PGP Universal Server.

To configure your new installation of PGP Universal Server:

1 After your PGP Universal Server reboots, log in to the administrative interface.

If you selected **New Installation**, the Licensing page appears automatically.

2 To license your PGP Universal Server, do one of the following:

- To license later, click **Skip**, which takes you to step 6.

You can add your license later through the PGP Universal Server's administrative interface.

- To license now, type your PGP Universal Server license information.

  The user name, organization name, user email, and the license number are provided by the PGP order management system.

3 If your license includes PGP Universal Gateway Email, select **Enable Mail Proxies** and click **Forward.**

If you do not select this checkbox, you cannot configure a mail server in the Setup Assistant .

4 Type the administrator's login name and passphrase.

5 Retype the administrator's passphrase to confirm it.

6 (Optional) Type the administrator's email address.

This allows the administrator to receive daily status emails.

7 Click **Forward**.

One of the following occurs:

- If you selected the **Enable Mail Proxies** checkbox with a valid PGP Universal Gateway Email license, the **Mail Processing** page appears.
- If you left the **Enable Mail Proxies** checkbox deselected, the **Managed Domain Selection** page appears.

  This only allows you to type the primary domain to be managed by your PGP Universal Server. You cannot configure PGP Universal Server placement or mail or proxy servers. Proceed to step 15.
- If you do not configure your mail proxy, you can enter a license that includes PGP Universal Gateway Email and enable and configure mail server and mail proxy settings in the PGP Universal Server administrative interface.

8 Specify the placement of this PGP Universal Server in your network:

- Select **Gateway Placement** if your PGP Universal Server is located between your mail server and the Internet.
- Select **Internal Placement** if your PGP Universal Server is located between your email users and your mail server, or if your PGP Universal Server is out of the mailstream.

9 Click **Forward**.

10 Type the hostname or IP address of the mail server with which this PGP Universal Server interacts.

11 Type an optional additional mail server to which all outbound mail is sent.

This step only applies if you are installing your PGP Universal Server in gateway placement.

12 Type the email domain that the PGP Universal Server manages.

13 Click **Forward**.

Ignition keys protect the data on your PGP Universal Server. If you want to use a hardware ignition key, prepare the token before you add it to the system. For more information on preparing a hardware token ignition key, see Protecting PGP Universal Server with Ignition Keys in the *PGP Universal Server Administrator's Guide*.

Note: If this PGP Universal Server will be used as the initial member in a cluster, this ignition key is replicated to all additional cluster members. New cluster members that are sponsored by this PGP Universal Server will be initially locked with this ignition key.

14 Click **Skip** to proceed without configuring an ignition key.

15 To configure an ignition key, select the type of ignition key, and click **Forward**.

16 Type a name for the ignition key, a passphrase, confirm the passphrase, and click **Forward**.

The PGP Universal Server automatically generates an Organization Key for you. You can generate an S/MIME Organization Certificate after the setup is finished. For more information about the Organization Key and Organization Certificate, see Managing Organization Keys in the *PGP Universal Server Administrator's Guide*.

17 (Optional) Type and confirm a passphrase to protect the organization key and click **Backup Key**.

This step is optional but strongly recommended. If you do not back up your Organization Key, you cannot restore your PGP Universal Server from backed up data.

18 Click **Forward**, review your PGP Universal Server's configuration, and **Done**.

The server restarts automatically, and you are redirected to the newly configured administrative interface.

Your PGP Universal Server is initially configured in Learn Mode. For more information, see Operating in Learn Mode in the *PGP Universal Server Administrator's Guide*.

Configuring a Cluster Member

To set up a PGP Universal Server as a cluster member, it must be sponsored by an existing PGP Universal Server. On the sponsoring server, you must perform an **Add Cluster Membe**r request, specifying that the PGP Universal Server you are installing will be as a cluster member. The joining server is added as a pending member of the cluster, with a **Contact** button that allows the sponsor to initiate the join process. You can configure a cluster member after PGP Universal Server reboots.

For more information on adding a cluster member, see *Clustering your PGP Universal Servers* in the *PGP Universal Server Administrator's Guide*.

To configure a cluster member

1 After the PGP Universal Server reboots, log in to the administrative interface.

If you selected **Cluster Member** as the configuration type for the PGP Universal Server, the Licensing page appears automatically.

2 To license your PGP Universal Server later, click **Skip**, and proceed to step 5.

You can add your license later in the PGP Universal Server's Administrative interface.

3 To license your PGP Universal Server now, type your PGP Universal Server the user name, organization name, user email, and the license number as provided by the PGP order management system.

4 Click **Forward**.

The PGP Universal Server verifies and authorizes your license.

5 Type the Hostname or IP Address of the PGP Universal Server that is acting as the sponsor for this joining server and click **Forward**.

The PGP Universal Server reboots again. The *Waiting for Cluster Host* message appears until you log in to the sponsoring server's administrative interface and click **Contact** to initiate the join with the server you are installing. When contact is received from the sponsoring PGP Universal Server, you can monitor the data replication process with the progress bar. The configuration settings for the PGP Universal Server you are installing as a cluster member are replicated from the sponsoring server. When the replication process is complete, the PGP Universal Server administrative interface login page is displayed.

Note: The replication process copies configuration settings, such as the administrator login name(s), password(s), and so on, from the sponsor PGP Universal Server.

Mail processing is not enabled on the cluster member after it is installed. To enable it you must configure one or more mail routes and proxies on the cluster member. Mail domains and the mail placement setting (Gateway or Internal) are global. Routes and proxies are local to each PGP Universal Server that will be processing email.

- To configure a mail route, select **Mail > Mail Routes** and click **Add Mail Route.**

  For more information, see Specifying Mail Routes in the *PGP Universal Server Administrator's Guide*.

- To configure a mail proxy or proxies, select **Mail > Proxies** and click **Add Proxy.**

Note: You must have a PGP Universal Gateway Email license and select the **Enable Mail Proxies** checkbox on the **System Settings** page. For more information, see Configuring Mail Proxies in the *PGP Universal Server Administrator's Guide*.

If the sponsoring server was configured to use an Ignition Key, this key is replicated to this PGP Universal Server. When the server restarts, it is automatically locked and must be unlocked using the ignition key or organization key (also a global key).

In a **New Installation** configuration, your PGP Universal Server is initially configured in Learn Mode. This is a global setting and is determined by the setting that is replicated from the sponsoring server. For more information, see Operating in Learn Mode in the *PGP Universal Server Administrator's Guide*.

Restore From a Server Backup

To configure a PGP Universal Server with data that you backed up, you need to have the appropriate backup file and the Organization Key on the setup computer. When you restore from a backup, everything that was configured, including network, proxy and policy settings, keys, and user information is restored.

For information on configuring a PGP Universal Server through the Setup Assistant with data from a backup, see the *PGP Universal Server Upgrade Guide*.

Migrate Keys from a PGP Keyserver

When you migrate keys from an old PGP Keyserver to PGP Universal Server, the following occurs:

- The PGP Keyserver are exported into a format that can be imported into a PGP Universal Server.
- In the Setup Assistant, you can configure a PGP Universal Server and add the PGP keys from the PGP Keyserver.

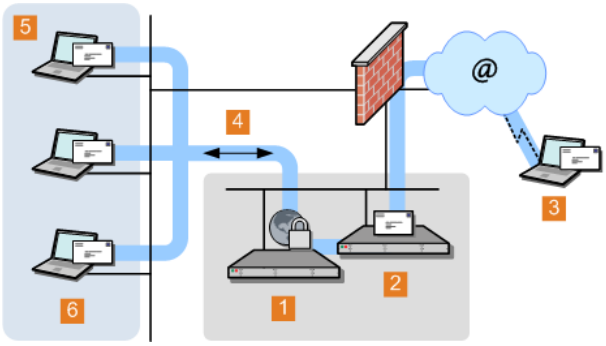
You can find more information about moving to PGP Universal Server on the Symantec Corporation Web site.

7 Configuration Examples

This chapter provides information on the potential configurations for PGP Universal Server:

Internal Placement Configuration

In this example, Example Corporation has one main office but wants to support external email users.



1	PGP Universal Server internally placed
2	Example Corp. email server
3	External email user

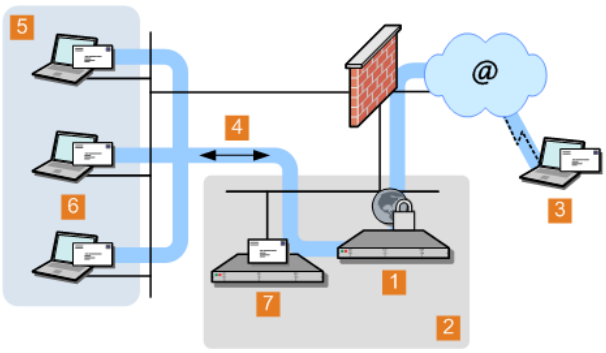
4	Logical flow of data
5	Example Corp. internal network
6	Example Corp. email users

Settings for 1:	Notes
Server type: **New Installation** Mail processing: **Internal placement** Hostname: **mail.example.com** Mail server: **mail-1.example.com** IP Address, Subnet Mask, Gateway, and DNS Servers: **As appropriate**	Change **mail.example.com** to **mail-1.example.com** and the PGP Universal Server becomes **mail.example.com**. End users might require no changes to their configuration; SMTP Authentication might need to be enabled for end users. Create a DNS alias for **keys.example.com** to also point to the PGP Universal Server.

By placing the server in the DMZ, the company can use an internal placement, which means that its messages are encrypted while on its mail server, and still support external email users via Smart Trailers, PGP Universal Web Messenger mail, or PGP Universal Satellite.

Gateway Placement Configuration

In this example, Example Corporation has its PGP Universal Server in a gateway placement.



1	PGP Universal Server gateway placement
2	Example Corp. DMZ
3	External email user
4	Logical flow of data

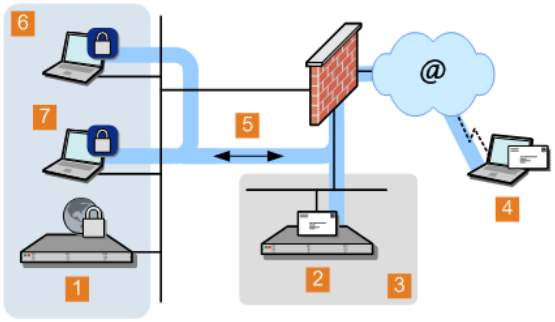
5	Example Corp. internal network
6	Example Corp. email users
7	Example Corp. email server

Settings for 1:	Notes:
Server type: **New Installation** Mail processing: **Gateway placement** Hostname: **mail-gw.example.com** Mail server: **mail.example.com** IP Address, Subnet Mask, Gateway, and DNS Servers: **As appropriate**	Add or modify the MX record for **example.com** to point to PGP Universal Server's IP address on **mail-gw.example.com**. Also in DNS, create an alias **keys.example.com** that points to **mail-gw.example.com**. Mail server must be configured to relay through the PGP Universal Server.

Gateway placement also supports external email users via Smart Trailers or PGP Universal Web Messenger mail.

Non-mailstream Placement Configuration

In this example, Example Corporation has a PGP Universal Server placed outside the mailstream. The PGP Universal Server integrates with PGP Desktop to provide automated user enrollment and real-time end-user security policy management. This is a common configuration for a PGP Universal Server managing client installations without PGP Gateway Email.



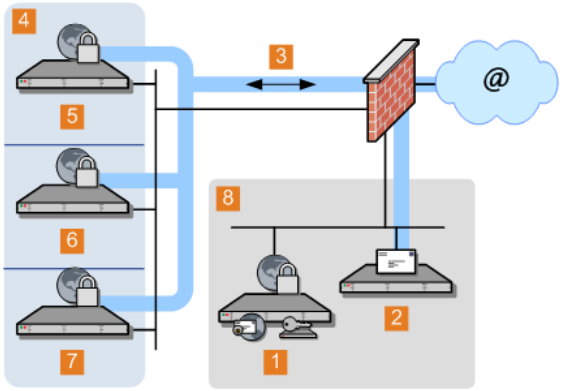
1	PGP Universal Server policy/management
2	Example Corp. email server
3	Example Corp. DMZ
4	External email user
5	Logical flow of data
6	Example Corp. internal network

7	Example Corp. PGP Desktop & email users

Settings for 1:	Notes:
Server type:**New Installation** Mail processing: **None** IP Address, Subnet Mask, Gateway, and DNS Servers: **As appropriate**	PGP Universal Server is outside of mailstream. All encryption, decryption, signing, and verification is done through PGP Desktop.

Cluster Configuration

In this example, Example Corporation has a cluster, with multiple PGP Universal Servers proxying messages on its internal network, and another server in the DMZ that performs keyserver and PGP Universal Web Messenger functions only.



1	PGP Universal Server Keyserver/Web Messenger
2	Example Corp. email server
3	Logical flow of data
4	Example Corp. internal network
5	Manufacturing - PGP Universal Server internally placed
6	Development - PGP Universal Server internally placed
7	Administration - PGP Universal Server internally placed
8	Example Corp. DMZ

Notes:
One internally placed PGP Universal Server configured as the first server in the cluster; the other and the keyserver configured as cluster members.

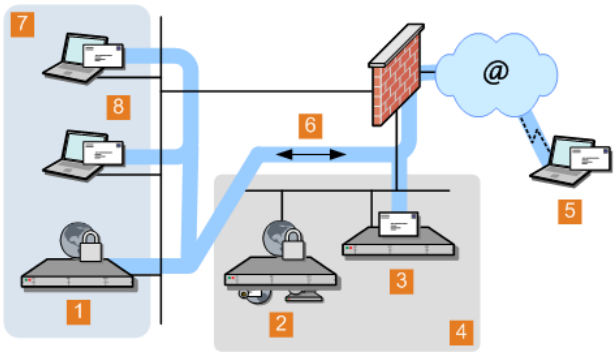
Mail server does not relay through the keyserver PGP Universal Server.

Cluster port (444) on firewall between the internally placed servers and the keyserver must be opened.

No mail proxies configured on the keyserver.

Clustered Proxy and Keyserver Configuration

In this example, Example Corporation has a cluster, with one PGP Universal Server proxying messages on its internal network, and another server in the DMZ that performs keyserver and PGP Universal Web Messenger functions only.



1	PGP Universal Server internally placed
2	PGP Universal Server Keyserver/Web Messenger
3	Example Corp. email server
4	Example Corp. DMZ
5	External email user
6	Logical flow of data
7	Example Corp. internal network
8	Example Corp. email users

Settings for 1:

Server type: **New Installation** (first server in cluster)

Mail processing: **Internal placement**

Hostname: **mail.example.com**

Mail server: **mail-1.example.com**

IP Address, Subnet Mask, Gateway, and DNS Servers: **As appropriate**

Settings for 2:

Server type: **Cluster Member**

Mail processing: **Disabled**

Hostname: **keys.example.com**

IP Address, Subnet Mask, Gateway, and DNS Servers: **As appropriate**

Notes:

mail.example.com becomes **mail-1.example.com**. PGP Universal Server becomes **mail.example.com**.

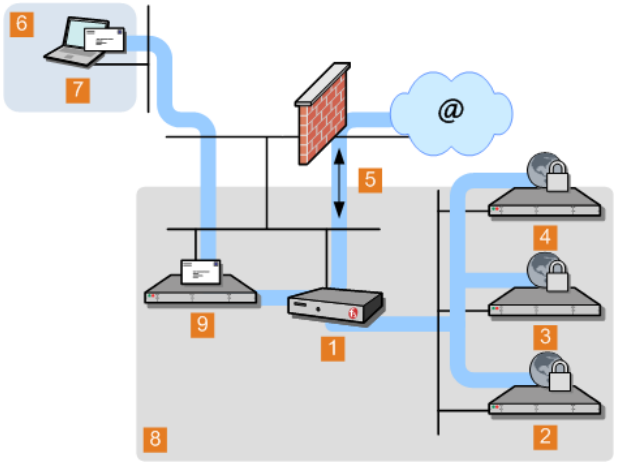
Mail server does not relay through **2**.

Cluster port (444) on firewall between the two servers *must* be opened.

To support external users via PGP Universal Web Messenger, designate the keyserver as a PGP Universal Web Messenger server.

Gateway Cluster with Load Balancer

In this example, Example Corporation is using an F5 BIG-IP load balancer to handle address rotation between the PGP Universal Servers in the cluster, ensuring that traffic goes through all of them.



1	F5 BIG-IP Load Balancer
2	PGP Universal Server 1
3	PGP Universal Server 2
4	PGP Universal Server 3
5	Logical flow of data
6	Example Corp. internal network
7	Example Corp. email users
8	Example Corp. DMZ
9	Example Corp. email server

Settings for 1:	Settings for 2:
Virtual server for trusted interface: **cluster-gw-internal.example.com** Virtual server addresses: **Trusted interfaces for hosts 2, 3, and 4, port 25** Virtual server for untrusted interface: **cluster-gw.example.com** Virtual server addresses: **Untrusted interfaces for hosts 2, 3, and 4, ports 25 and 389** IP Address, Subnet Mask, Gateway, and DNS Servers: **As appropriate**	Server type: **New Installation** Mail processing: **Gateway placement** Hostname: **cluster1-gw.example.com** Mail server: **mail.example.com** IP Address, Subnet Mask, Gateway, and DNS Servers: **As appropriate**

Settings for 3:	Settings for 4:
Server type: **Cluster Member** Hostname: **cluster2-gw.example.com** IP Address, Subnet Mask, Gateway, and DNS Servers: **As appropriate**	Server type: **Cluster Member** Hostname: **cluster3-gw.example.com** IP Address, Subnet Mask, Gateway, and DNS Servers: **As appropriate**

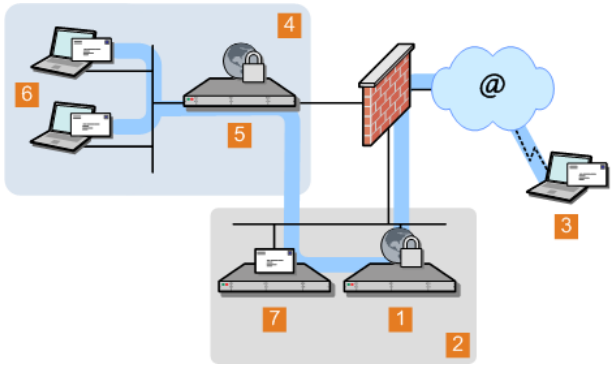
Notes:
Add DNS MX record that points to **cluster-gw.example.com**. Also in DNS, create an alias from **cluster-gw.example.com** to **keys.example.com**. The mail server must be reconfigured to relay through **cluster-gw-internal.example.com**.

Gateway and Internal Placement Cluster

You can have a cluster that includes both a PGP Universal Server internally placed and a PGP Universal Server in a gateway placement managing a single mail server, but you should carefully consider why you need both at a single location.

One good reason would be for the PGP Universal Server in gateway placement to act exclusively as a keyserver or as a PGP Universal Web Messenger server, while the PGP Universal Server(s) internally placed handles message processing.

The most common usage for this configuration is when you have internal MAPI clients running PGP Universal Satellite in addition to non-MAPI clients using POP, IMAP, and SMTP. In such a scenario, those using standards-based protocols connect to the internally placed PGP Universal Server while the PGP Universal Server in gateway placement ensures proper handling of PGP Universal Web Messenger and Smart Trailer messages for the MAPI clients.



1	PGP Universal Server gateway placed
2	Example Corp. DMZ
3	External email user
4	Example Corp. internal network
5	PGP Universal Server internally placed
6	Example Corp. email users
7	Example Corp. email server

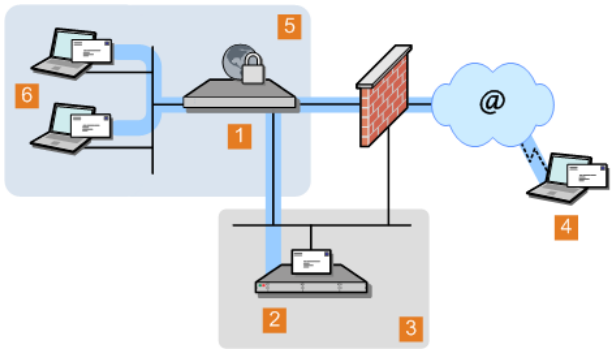
Notes:

If the same user sends messages from different locations (such as from the internal network using a desktop computer, then from a remote location using a laptop), they can create multiple user accounts and/or keys.

The first server (cluster member) is internally placed, with PGP Universal Web Messenger disabled. The second server cluster member is in the DMZ, in gateway placement, with PGP Universal Web Messenger enabled.

Encircled Configuration

Using PGP Universal Server in an encircled configuration is an alternative to placing two PGP Universal Servers in a clustered internal/gateway placement, when you have internal MAPI clients running PGP Universal Satellite in addition to non-MAPI clients using POP, IMAP, and SMTP.

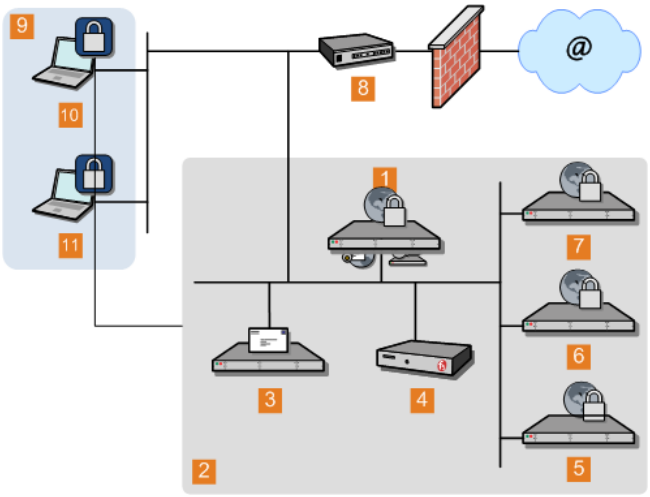


1	PGP Universal Server internally placed
2	Example Corp. email server
3	Example Corp. DMZ
4	External email user
5	Example Corp. internal network
6	Example Corp. email users

Settings for 1:	Notes:
Server type: **New Installation** Mail processing: **Internal placement** Hostname: **mail.example.com** Mail server: **mail-1.example.com** IP Address, Subnet Mask, Gateway, and DNS Servers: **As appropriate** PGP Universal Web Messenger and keyserver functionality enabled	Add DNS MX record that points to **mail.example.com**. Optional: to hide internal PGP Universal Server IP from outside, use 2nd IP in the DMZ.

Large Enterprise Configuration

As a large enterprise, Example Corporation has a sophisticated network that includes multiple PGP Universal Servers that are load balanced, PGP Universal Satellite users, a separate PGP Universal Server for PGP Universal Web Messenger and keyserver support, and a standalone Mail Transfer Agent (MTA).



1	PGP Universal Server Keyserver/Web Messenger
2	Example Corp. DMZ
3	Example Corp. email server
4	F5 BIG-IP Load Balancer
5	PGP Universal Server 1
6	PGP Universal Server 2
7	PGP Universal Server 3
8	MTA
9	Example Corp. internal network
10, 11	Example Corp. email user with PGP Universal Satellite

The company uses its MTA to perform static email routing and to establish rules that govern which email messages are processed by PGP Universal Server and which are not. Naturally, the features of the MTA being used govern what it can be used for.

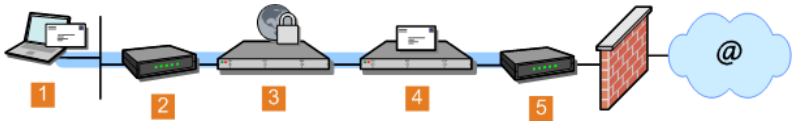
Note: PGP Corporation does not recommend any specific MTA for use with PGP Universal Server. Make sure the MTA you decide to use is correctly configured for use with PGP Universal Server.

Spam Filters and PGP Universal Server

Example Corporation has both a content-based and a Realtime Blackhole List (RBL) spam filter that it wants to use in conjunction with its PGP Universal Server. (An RBL is a list of servers that are known to send out spam or to be open relays.)

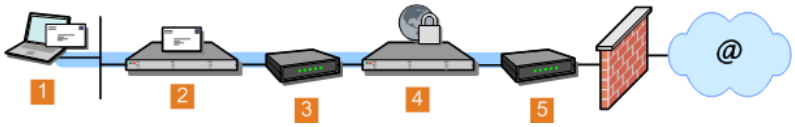
The company is careful to locate the respective spam filters in the appropriate locations in the logical flow of data and to configure them correctly.

PGP Universal Server internally placed



1	Example Corp. email user
2	Content-based spam filter
3	PGP Universal Server internally placed
4	Example Corp. email server
5	RBL-based spam filter

PGP Universal Server in gateway placement



1	Example Corp. email user
2	Example Corp. email server
3	Content-based spam filter
4	PGP Universal Server externally placed
5	RBL-based spam filter

Notes:

The content-based spam filter sits between the internal email users and the PGP Universal Server in the logical flow of data so that messages are decrypted before they are checked for spam. This allows even PGP Universal Server–encrypted messages to be checked. Other SMTP filtering devices (such as a standalone antivirus gateway, for example) would be placed in the same location.

Both spam filters must be correctly configured. For example, the content-based spam filter must not treat the PGP Universal Server as a "trusted mail relay" to avoid creating an open relay; this might require disabling the spam filter's reverse MX lookups feature.

For the gateway placement scenario, the content-based spam filter must be configured on the PGP Universal Server as a mail server. This is done on the inbound or Unified SMTP proxy.

With an internal placement, the content-based spam filter is not filtering SMTP, only POP/IMAP, so no special configuration on the PGP Universal Server is required.

Alternatively, put both spam filters between the PGP Universal Server and the firewall in the logical flow of data. This configuration assumes PGP Universal Server–encrypted messages do not contain spam because they are scanned while encrypted. However, spam in unencrypted messages is still detected.

Caution: If you begin receiving encrypted spam, relocate or add another content-based spam filter to sit between the internal email users and the PGP Universal Server. Receiving unencrypted spam is unlikely because it is CPU-intensive and inefficient.

Note: You might require this alternative configuration if the content-based spam filter requires reverse MX lookups.

Exchange with PGP Client Software

Microsoft Exchange Server environments (MAPI) are supported in PGP Desktop for internal and external PGP Universal Server users and in PGP Universal Satellite for Windows for external users.

For more information about Microsoft Exchange Server environments and MAPI support, see MAPI Support in the PGP Universal Server Administrator's Guide.

Lotus Domino Server with PGP Client Software

Lotus Domino Server environments, including the Lotus Notes email client, are supported in PGP Desktop and PGP Universal Satellite for Windows for both internal and external PGP Universal Server users.

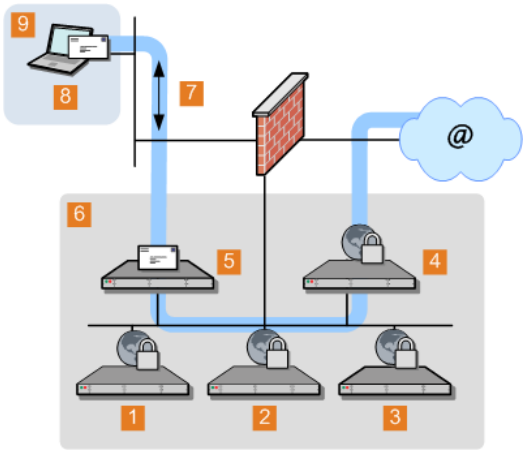
For more information about Lotus Domino Server environments and Lotus Notes email client support, see "Lotus Notes Support" in the *PGP Universal Server Administrator's Guide*.

Unsupported Configurations

The following PGP Universal Server deployment scenario is an unsupported configuration.

Multiple Gateway–Placed Servers

You cannot have multiple PGP Universal Servers operating in gateway placements in one DMZ.



1	PGP Universal Server 1
2	PGP Universal Server 2
3	PGP Universal Server 3
4	PGP Universal Server 4
5	Acmecorp email server
6	Example Corp. DMZ
7	Logical flow of data
8	Example Corp. email user
9	Example Corp. internal network

Notes:

This configuration will not work as expected because the mail server will only route outbound email through one of the PGP Universal Servers.

You can use load balancing to achieve a similar result. For more information, see *Gateway Cluster with Load Balancer* (on page 40).