PGP® Universal Server

Administrator's Guide

Rest Secured.™

Version Information

PGP Universal Server Administrator's Guide. PGP Universal Server (TM) and PGP Universal Satellite version 2.6.3. Released August 2007.

Copyright Information

Trademark Information

Licensing and Patent Information

Acknowledgments

This product includes or may include:

• The Zip and ZLib compression code, created by Mark Adler and Jean-Loup Gaill, is used with permission from the free Info-ZIP implementation, developed by zlib (http://www.zlib.net). • Libxml2, the XML C parser and toolkit developed for the Gnome project and distributed and copyrighted under the MIT License found at http://www.opensource.org/licenses/mit-license.html. Copyright © 2007 by the Open Source Initiative. • bzip2 1.0, a freely available high-quality data compressor, is copyrighted by Julian Seward, © 1996-2005. • Application server (http://www.jakarta.apache.org/), web server (http://www.apache.org/), Jakarta Commons (http://jakarta.apache.org/commons/license.html) and log4j, a Java-based library used to parse HTML, developed by the Apache Software Foundation. The license is at www.apache.org/licenses/LICENSE-2.0.txt. • Castor, an open-source, data-binding framework for moving data from XML to Java programming language objects and from Java to databases, is released by the ExoLab Group under an Apache 2.0-style license, available at http://www.castor.org/license.html. • Xalan, an open-source software library from the Apache Software Foundation that implements the XSLT XML transformation language and the XPath XML query language, is released under the Apache Software License, version 1.1, available at http://xml.apache.org/xalan-j/#license1.1. • mx4j, an open-source implementation of the Java Management Extensions (JMX), is released under an Apache-style license, available at http://mx4j.sourceforge.net/docs/ch01s06.html. • jpeglib version 6a is based in part on the work of the Independent JPEG Group. (http://www.ijg.org/) • libxslt the XSLT C library developed for the GNOME project and distributed under the MIT License http://www.opensource.org/licenses/mit-license.html. • PCRE version 4.5 Perl regular expression compiler, copyrighted and distributed by University of Cambridge. ©1997-2006. The license agreement is at http://www.pcre.org/license.txt. • BIND Balanced Binary Tree Library and Domain Name System (DNS) protocols developed and copyrighted by Internet Systems Consortium, Inc. (http://www.isc.org) • Free BSD implementation of daemon developed by The FreeBSD Project, © 1994-2006. • Simple Network Management Protocol Library developed and copyrighted by Carnegie Mellon University © 1989, 1991, 1992, Networks Associates Technology, Inc, © 2001- 2003, Cambridge Broadband Ltd. © 2001- 2003, Sun Microsystems, Inc., © 2003, Sparta, Inc, © 2003-2006, Cisco, Inc and Information Network Center of Beijing University of Posts and Telecommunications, © 2004. The license agreement for these is at http://net-snmp.sourceforge.net/about/license.html. • NTP version 4.2 developed by Network Time Protocol and copyrighted to various contributors. • Lightweight Directory Access Protocol developed and copyrighted by OpenLDAP Foundation. OpenLDAP is an open-source implementation of the Lightweight Directory Access Protocol (LDAP). Copyright ©

Export Information

Export of this software and documentation may be subject to compliance with the rules and regulations promulgated from time to time by the Bureau of Export Administration, United States Department of Commerce, which restricts the export and re-export of certain products and technical data.

Limitations

The software provided with this documentation is licensed to you for your individual use under the terms of the End User License Agreement provided with the software. The information in this document is subject to change without notice. PGP Corporation does not warrant that the information meets your requirements or that the information is free of errors. The information may include technical inaccuracies or typographical errors. Changes may be made to the information and incorporated in new editions of this document, if and when made available by PGP Corporation.

Contents

An Overview of the PGP Universal Server

Deploying your Server

Installing the PGP Universal Server Software

Organization Information

Managing Mail Processing

Managing Users

Managing Your PGP Universal Server

SECTION 1

An Overview of the PGP Universal Server

This section provides a high-level overview of the components, concepts, and terminology of the PGP Universal Server. It also provides a high-level overview of the entire installation and setup process.

1 Introduction

This Administrator's Guide describes both the **PGP Universal Server** and PGP Universal Satellite. It tells you how to get them up and running on your network, how to configure them, and how to maintain them. This section provides a high-level overview of PGP Universal Server. Topics include:

- "What is PGP Universal Server?"
- "PGP Universal Server Product Family" on page 2
- "Who Should Read This Guide" on page 2
- "Improvements in This Version of PGP Universal Server" on page 2
- "Symbols" on page 3
- "Getting Assistance" on page 4

What is PGP Universal Server?

PGP Universal Server provides multiple encryption solutions managed from a single console.

PGP Universal Server with PGP Universal Gateway Email gives you secure messaging: it transparently protects your enterprise messages with little or no user interaction.

The PGP Universal Server also replaces the PGP Keyserver product with a built-in keyserver, and the PGP Admin product with PGP Desktop configuration and deployment capabilities.

It automatically creates and maintains a Self-Managing Security Architecture (SMSA) by monitoring authenticated users and their email traffic. You can also send protected messages to addresses that are *not* part of the SMSA. The PGP Universal Server encrypts, decrypts, signs, and verifies messages automatically, providing strong security through policies you control.

PGP Universal Satellite, a client-side feature of PGP Universal Server, extends PGP security for email messages all the way to the computer of the email user, it allows external users to become part of the SMSA, and it gives end users the option to create and manage their keys on their own computer (if allowed by the PGP administrator).

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 Gateway Email to encrypt email in the mailstream.

The PGP Universal Server can manage any combination of PGP encryption applications. PGP encryption applications are:

- **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 level 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 level 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 Administrator's Guide is for the person or persons who will be implementing and maintaining your organization's PGP Universal Server environment. These are the PGP administrators.

This guide is also intended for anyone else who wants to learn about how PGP Universal Server works.

Improvements in This Version of PGP Universal Server

This release of PGP Universal introduces the following new features:

- "General" on page 3
- "PGP Messaging" on page 3
- "PGP Whole Disk Encryption" on page 3
- "PGP Keys" on page 3

General

Changes in this release

Microsoft Internet Explorer 7 support. The PGP Universal Server administrative interface now runs in Internet Explorer 7.

PGP Messaging

Changes in this release

PGP Verified Directory enhancements. You can now specify a “From” address that will display on all PGP Verified Directory-initiated email messages.

Benefits

The customized sender address prevents your PGP Universal Server’s hostname from appearing in the “From” email line.

Where to find

Services>Verified Directory screen.

For more information

See Chapter 31, “Configuring the PGP Verified Directory” for more information.

PGP Whole Disk Encryption

Changes in this release

PGP Whole Disk Encryption (WDE) Recovery Token encryption. Whole Disk Recovery Tokens are now encrypted to the PGP Universal Server Ignition Key.

Benefits

Improves user data security.

PGP Keys

Changes in this release

Key Reconstruction for Mac OS X. Key reconstruction is now available in PGP Desktop for Mac OS X.

Where to find

Policy>Internal User Policy screen.

For more information

See Chapter 28, “Configuring PGP Desktop Installations” and Chapter 32, “Managing Internal User Accounts” for more information on key reconstruction.

Symbols

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

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

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

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

Refer to these sections for additional resources.

Getting product information

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

- **PGP Universal Upgrade Guide**—Describes the process of upgrading your PGP Universal Server to version 2.6
- **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, 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.
- The administrative interface and PGP Universal Satellite for Windows and Mac OS X include online help.
- PGP Universal and PGP Satellite release notes are also provided, which may have last-minute information not found in the product documentation.

Once PGP Universal is released, additional information regarding the product is added to the online Knowledge Base available on PGP Corporation's Support Portal at www.pgpsupport.com.

Contact information

All PGP customers have access to the comprehensive set of tools and discussion forums available on the PGP Support Portal.

The PGP Support Portal provides access to tutorials, recent support briefs, the Knowledge Base, and other valuable technical information.

You must have a valid support agreement to request Technical Support.

Contacting Technical Support

- To access the PGP Support Knowledge Base or request PGP Technical Support: https://support.pgp.com. Note that you must have a valid support agreement to request Technical Support.
- To learn about PGP support options and how to contact PGP Technical Support: http://www.pgp.com/support/
- To access the PGP Universal section of the PGP Support forums: http://forums.pgpsupport.com
- For any other contacts at PGP, please visit the PGP Contacts Page: http://www.pgp.com/company/contact/index.html.
- For general information about PGP Corporation, please visit the PGP Web Site: http://www.pgp.com.

2 The Big Picture

This chapter describes some important terms and concepts and gives you a high-level overview of the things you need to do to set up and maintain your PGP Universal Server environment.

Topics include:

- "Important Terms"
- "Installation Overview" on page 11

Important Terms

PGP Products

- **PGP Universal Server:** A device you add to your network that provides secure messaging with little or no user interaction. The PGP Universal Server automatically creates and maintains a security architecture by monitoring authenticated users and their email traffic. You can also send protected messages to addresses that are *not* part of the security architecture.
- **PGP Universal Satellite:** The PGP Universal Satellite software resides on the computer of the email user. It allows email to be encrypted end to end, all the way to and from the desktop (for both internal and external users). Using PGP Universal Satellite is one of the ways for external users to participate in the SMSA. It also allows users the option of controlling their keys on their local machines (if allowed by the PGP administrator).

PGP Universal Server Concepts

- **Security Architecture:** Behind the scenes, the PGP Universal Server creates and manages its own security architecture for the users whose email domain it is securing. Because the security architecture is created and managed automatically, we call this a *self-managing* security architecture (SMSA).
- **keys.<domain> convention:** PGP Universal Server automatically looks for valid public keys for email recipients at a special hostname, if no valid public key is found locally to secure a message. This hostname is keys.<domain> (where <domain> is the email domain of the recipient). For example, Example Corporation's externally visible PGP Universal Server is named **keys.example.com**.

  PGP Corporation strongly recommends you name your externally visible 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.

  Refer to Appendix 5, "Naming your PGP Universal Server" for more information about this convention.

PGP Universal Server Features

- **Server Placement:** A PGP Universal Server can be placed in one of two locations in your network to process email.

  With an internal placement, the PGP Universal Server logically sits between your email users and your mail server. It encrypts and signs outgoing SMTP email and decrypts and verifies incoming mail being picked up by email clients using POP or IMAP. Email stored on your mail server is stored secured (encrypted).

  With a gateway placement, the PGP Universal Server logically sits between your mail server and the Internet. It encrypts and signs outgoing SMTP email and decrypts and verifies incoming SMTP email. Email stored on your mail server is stored unsecured.

  Refer to Chapter 3, "Adding the PGP Universal Server to Your Network" and Chapter 22, "Configuring Mail Proxies" for more information about server placement.

- **Administrative Interface:** Each PGP Universal Server is controlled via a Web-based administrative interface. The administrative interface gives you control over the PGP Universal Server's operation. While many settings are initially established using the web-based Setup Assistant, all settings of a PGP Universal Server can be controlled via the administrative interface.

- **Setup Assistant**: When you attempt to log in for the first time to the administrative interface of a PGP Universal Server, the Setup Assistant takes you through the configuration of that PGP Universal Server.

- **Learn Mode:** When you finish configuring a PGP Universal Server using the Setup Assistant, it begins operation in Learn Mode, which is a special mode where the PGP Universal Server proxies traffic normally but does not encrypt or sign any messages.

  Learn Mode gives the PGP Universal Server a chance to build its SMSA (creating keys for authenticated users, for example) so that when the it goes live — that is, when Learn Mode is turned off — the PGP Universal Server knows the environment and can immediately begin securing messages. It's also an excellent way for PGP administrators to learn about the product.

  You should check the logs of the PGP Universal Server while it is in Learn Mode to see what it would be doing to email traffic if it were live on your network. You can make changes to the PGP Universal Server's policies while it is in Learn Mode until things are working as expected.

- **Mail Policy:** The PGP Universal Server processes email messages based on the policies you establish. Mail policy applies to inbound and outbound email for both PGP Universal Server traffic and email processed by PGP client software. Mail policy consists of multiple policy chains, comprised of sequential mail processing rules.

- **Dictionary:** Dictionaries are lists of terms to be matched. The dictionaries work with mail policy to allow you to define content lists that can trigger rules.

- **Cluster:** When you have two or more PGP Universal Servers in your network, you configure them to synchronize with each other; this is called a "cluster."

In a cluster, one PGP Universal Server is designated Primary for the cluster; all other PGP Universal Servers in the cluster are designated Secondary. The Secondary servers synchronize their users, keys, managed domains, and policies with the Primary.

- **Organization Key:** The Setup Assistant automatically creates an Organization Key (actually a keypair) when it configures a PGP Universal Server. The Organization Key is used to sign all PGP user keys the PGP Universal Server creates and to encrypt PGP Universal Server backups.

> ⚠ It is extremely important to back up your Organization Key: all of the keys the PGP Universal Server creates are signed by the Organization Key, and all backups are encrypted to the Organization Key. If you lose your Organization Key and have not backed it up, the signatures on those keys will be meaningless and you will not be able to restore from backups encrypted to the Organization Key.

If your organization has one PGP Universal Server, back up the Organization Key from that PGP Universal Server; if you have multiple PGP Universal Servers in a cluster, back up the Organization Key from the Primary server in the cluster, as this Organization Key will be synchronized with the Secondary servers in the cluster.

- **Organization Certificate:** Create or obtain an Organization Certificate to enable S/MIME support by PGP Universal Server. The Organization Certificate signs all X.509 certificates the server creates.
- **Directory Synchronization:** If you have an LDAP directory in your organization, your PGP Universal Server can be synchronized with this directory. The PGP Universal Server will automatically import user information from the directory when users send and receive email; it will also create internal user accounts for them, including adding and using X.509 certificates if they are contained in the LDAP directory.
- **Integrated Virus Scanning and File Blocking:** Each PGP Universal Server in your organization can be configured with integrated virus scanning from Symantec such that messages and attachments can be scanned for viruses. You can also block attachments based on filenames you specify.
- **Keyserver:** Each PGP Universal Server includes an integrated keyserver populated with the public keys of your internal users. When an external user sends a message to an internal user, the external PGP Universal Server will go to the keyserver to find the public key of the recipient to use to secure the message. The PGP administrator can enable or disable the service, and control access to it via the administrative interface.
- **PGP Verified Directory:** The PGP Verified Directory supplements the internal keyserver by letting internal and external users manage the publishing of their own public keys. The PGP Verified Directory also serves as a replacement for the PGP Keyserver product. The PGP Verified Directory uses next-generation keyserver technology to ensure that the keys in the directory can be trusted.
- **Backup and Restore:** Because full backups of the data stored on your PGP Universal Server are critical in the case of a natural disaster or other unanticipated loss of data or hardware, you can schedule automatic backups of your PGP Universal Server data or manually perform a backup.

Naturally, you can fully restore a PGP Universal Server from a backup. In the event of a minor problem, you can restore the PGP Universal Server to any saved backup. In the event that a PGP Universal Server is no longer usable, you can restore its data from a backup onto a new PGP Universal Server during initial setup of the new PGP Universal Server using the Setup Assistant. All backups are encrypted to the Organization Key and may thus be stored securely off the PGP Universal Server.

- **Ignition Keys:** You can protect the contents of a PGP Universal Server, even if the hardware is physically stolen, by requiring the use of a hardware token or a software passphrase, or both, on start.

PGP Universal Server User Types

- **Internal and External Users:** Internal users are email users from the domains being managed by your PGP Universal Server; external users are email users from other domains (domains *not* being managed by your PGP Universal Server) who have been added to the SMSA.
- **Multiple Administrators:** Only PGP administrators are allowed to access the administrative interface that controls PGP Universal Server. A PGP Universal Server supports multiple PGP administrators, each of which can be assigned one of five levels of authority: from read-only access to full control over every feature and function.
- **Management of PGP Desktop Users:** PGP Universal Servers allow you to manage PGP Desktop deployments to your internal users. The PGP administrator can control which PGP Desktop features are automatically implemented at install, and establish and update mail security policy for PGP Desktop users that those users cannot override (except on the side of being more secure).
- **Other Email Users:** Users within your organization can securely send email to recipients outside the SMSA.

  First, the PGP Universal Server will attempt to find a key for the recipient. If that fails, there are four fallback options, all controlled by mail policy: bounce the message back to the sender (so it’s not sent unencrypted), send unencrypted, Smart Trailer, and PGP Universal Web Messenger mail.

  Smart Trailer sends the message unencrypted and adds text giving the recipient the option of joining the SMSA by installing PGP Universal Satellite, using an existing key or certificate, or using PGP Universal Web Messenger. PGP Universal Web Messenger lets the recipient securely read the message on a secure website; it also gives the recipient options for handling subsequent messages from the same domain: read the messages on a secure website using a passphrase they establish, install PGP Universal Satellite, or add an existing key or certificate to the SMSA.

Installation Overview

The following steps are a broad overview of what it takes to plan, set up, and maintain your PGP Universal Server environment.

All of the steps described briefly here are described in detail in later chapters.

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 all have a major impact on how you add them to your existing network.

It's a good idea to create a diagram of your network that includes all network components and shows how email flows; having this diagram may help you understand how adding a PGP Universal Server will impact your network.

Refer to Chapter 3, "Adding the PGP Universal Server to Your Network" for information that will help you plan how to add PGP Universal Servers to your existing network.

2. Perform necessary DNS changes.

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

Properly configured DNS settings (including root servers and appropriate reverse lookup records) are required in all cases to support PGP Universal Server. Make sure both host and pointer records are correct. IP addresses must be resolvable to hostnames, as well as hostnames resolvable to IP addresses.

3. Prepare a hardware token Ignition Key.

If you want to add a hardware token Ignition Key during setup, install the drivers and configure the token before you begin the PGP Universal Server setup process. See Chapter 46, "Protecting PGP Universal Server with Ignition Keys" for information on how to prepare a hardware token Ignition Key.

4. If you are going to have more than one PGP Universal Server in your network, install and configure the Primary server of the cluster first.

The Setup Assistant runs automatically when you first access the administrative interface for the PGP Universal Server.

To configure the Secondary servers in the cluster, you must configure the Primary server first and then add the Secondary servers on the Primary server before you can actually configure the Secondary servers.

Refer to Chapter 7, "Setting Up the PGP Universal Server" for more information on the Setup Assistant.

5. License your Primary server.

You cannot take a PGP Universal Server out of Learn Mode or install updates until the product is licensed. Once it is licensed, you should check for product updates and install them if found. See Chapter 9, “Licensing Your Software” for more information.

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. See Chapter 9, “Licensing Your Software” for more information.

If you want to implement virus scanning and file blocking, make sure to use a PGP Universal Server license with the Symantec AntiVirus feature enabled. You will also need a license from Symantec; see Chapter 20, “Scanning Email for Viruses” for more information.

6. If you have a PGP key you want to use as your Organization Key with PGP Universal Server, import it and then back it up on your Primary server.

Your Organization Key does two important things: it is used to sign all user keys the PGP Universal Server creates and it is used to 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 already has an Corporate Key or Organization Key, and you want to use that key with PGP Universal Server, you should import it as soon as you have configured your Primary server and then create a backup of the key.

If your organization does not have an existing key that you want to use as your Organization Key, use the Organization Key the Setup Assistant automatically creates with default values. See Chapter 12, “Managing Organization Keys” for more information.

No matter which key you use as your Organization Key, it is very important to make a backup of the key in case of a problem with your PGP Universal Server. Since PGP Universal Server’s built-in back-up feature always encrypts backups to this key, you will need to provide a copy of your Organization Key to restore your data.

Refer to “Organization Certificate” on page 88 for more information on Organization Certificates.

7. If you have a PGP Additional Decryption Key (ADK) that you want to use with PGP Universal Server, add it on your Primary server.

An ADK is a way to recover an email message if the recipient is unable or unwilling to do so; every message that is also 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, an ideal scenario for a split key; refer to the *PGP Desktop User’s Guide* for more information), you can add it to your PGP Universal Server and use it. You can only have one ADK. Refer to “Additional Decryption Key (ADK)” on page 93 for more information.

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

You can create a self-signed certificate for use with SSL/TLS traffic. Because this certificate is self signed, however, it may not be trusted by email or Web browser clients. PGP Corporation recommends that you obtain a valid SSL/TLS certificate for each of your PGP Universal Servers from a reputable Certificate Authority, such as GeoTrust, available at the PGP Online Store (www.pgpstore.com).

This is especially important for PGP Universal Servers that will be accessed publicly. Older Web browsers may reject self-signed certificates or not know how to handle them correctly when they encounter them via PGP Universal Web Messenger or Smart Trailer.

Refer to "Working with Certificates" on page 377 for more information.

9. Add trusted keys, configure internal and external user policy, and establish mail policy.

All of these settings are important for secure operation of PGP Universal Server. Refer to Chapter 13, "Managing Trusted Keys and Certificates" for information on adding trusted keys from outside the SMSA. Read Chapter 26, "Setting Internal User Policy" and Chapter 29, "Setting External User Policy" for information about user policy settings. See Chapter 15, "Setting Mail Policy" to learn about setting up mail policy.

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

Using the Directory Synchronization feature gives you more control over who is included in your SMSA, if you have an existing LDAP server.

If you are going to use the Directory Synchronization feature, it's best to configure it before you install and configure your Secondary servers. Refer to Chapter 27, "Using Directory Synchronization to Manage Users" for more information about the Directory Synchronization feature.

11. Install and configure the Secondary servers.

The Setup Assistant runs automatically when you first access a PGP Universal Server. Remember that you must configure the Primary server in the cluster first and tell it about the Secondary servers before you can configure them. See Chapter 45, "Clustering your PGP Universal Servers" to learn more about Clustering.

12. License and configure virus scanning and file blocking on those PGP Universal Servers for which you want them enabled.

You must be using a PGP Universal Server license that supports these features. Once enabled (on a per-service basis), virus scanning and file blocking are active, even while the PGP Universal Server is in Learn Mode. In a cluster, you only need to enter the virus scanning license once for the Primary server in the cluster.

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

Depending on how you are adding the PGP Universal Server to your network, some setting changes may be necessary. For example, if you are using a PGP Universal Server placed internally, the email clients **must** have SMTP authentication turned on. For PGP Universal Servers 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 to send system and application information to an external destination. See Chapter 43, “Configuring SNMP Monitoring” for more information.

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

If you want to provide seamless, end-to-end PGP message security without the need for any user training, have them use PGP Universal Satellite. Exchange/MAPI and Lotus Notes environments also require the use of PGP Universal Satellite. PGP Desktop provides more features and user control than PGP Universal Satellite. Refer to Chapter 36, “PGP Universal Satellite” and Chapter 28, “Configuring PGP Desktop Installations” for more information.

16. Analyze the data from Learn Mode.

In Learn Mode, your PGP Universal Server monitors email traffic and dynamically creates a SMSA; in fact, it does everything it would ordinarily do except encrypt and sign. You can see what the PGP Universal Server would have done without Learn Mode by monitoring the system logs.

Learn Mode lets you become familiar with how the PGP Universal Server operates and it lets you see the effects of the policy settings you have established before the PGP Universal Server actually goes live on your network. Naturally, you can fine tune settings while in Learn Mode, so that the PGP Universal Server is operating just how you want before you go live.

See Chapter 10, “Operating in Learn Mode” for more information.

17. Adjust policies as necessary.

It may take a few tries to get everything working just the way you want. For example, you may decide to revise your mail policy.

18. Perform backups of all PGP Universal Servers before you take them out of Learn Mode.

This gives you a baseline backup in case you need to return to a clean installation. To learn how to back up the PGP Universal Server, refer to Chapter 47, “Backing Up and Restoring System and User Data” for more information.

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

Once this is done, email messages will be encrypted, signed, and decrypted/verified, according to the relevant policy rules. Make sure you have licensed each of your PGP Universal Servers; you cannot take a PGP Universal Server out of Learn Mode until it has been licensed.

20. Monitor the system logs to make sure your PGP Universal Server environment is operating as expected.

SECTION 2

Deploying your Server

This section describes what you need to know to plan how to incorporate your PGP Universal Server into your network.

3 Adding the PGP Universal Server to Your Network

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

These topics are covered in the following sections:

- "Server Placement"
- "Using a Mail Relay" on page 19
- "Microsoft Exchange Server" on page 19
- "Lotus Domino Server" on page 19
- "Configuration Examples" on page 20

Server Placement

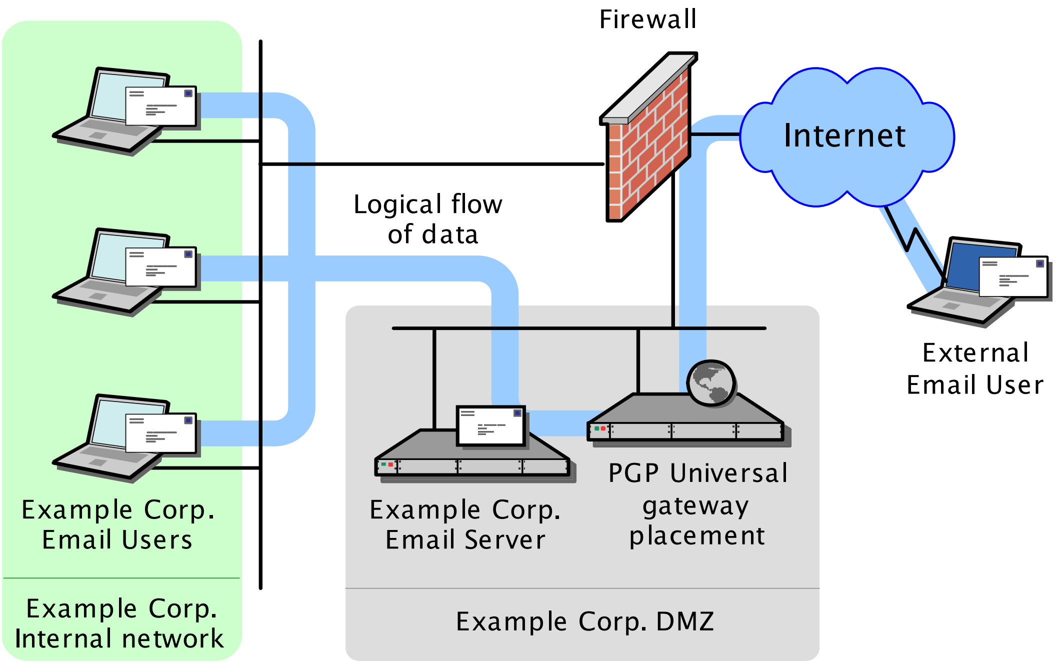
A PGP Universal Server can be placed in your network in either of two locations in the logical flow of data:

- **Internal placement**. The PGP Universal Server is located between your email users and their local mail server in the logical flow of data.
- **Gateway placement**. The PGP Universal Server is located between your external facing mail server and the Internet in the logical flow of data.

> ! The PGP Universal Server must not be behind a proxy server, unless it is a transparent proxy, to receive licensing and update information automatically. This is true for both gateway and internal placement.

Gateway Placement

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


Firewall
Internet
Logical flow of data
External Email User
Example Corp. Email Users
Example Corp. Email Server
PGP Universal gateway placement
Example Corp. Internal network
Example Corp. DMZ

The physical location of the PGP Universal Server and the mail server are not important. What is important is that, from a mail relay point of view, the PGP Universal Server is between the mail server and the Internet. Both could be on the internal network or in the DMZ.

With a gateway placement, email messages are secured before they are sent to the Internet (on the way to their destination) and decrypted/verified when received from the Internet, over SMTP in both cases.

Be sure to require authentication of incoming mail, or you risk creating an open relay.

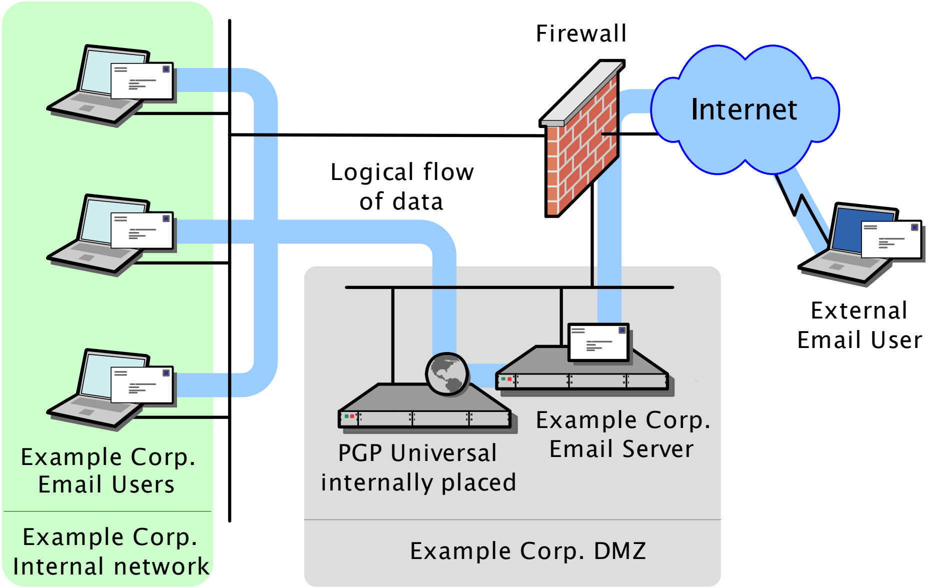
Email users on your internal network should not be allowed direct access to a PGP Universal Server in gateway placement. PGP Universal Server will attempt to enforce this automatically based on your configuration. The mail server should also be configured to verify From addresses if you intend to use the signing features of PGP Universal Server.

With a gateway placement, messages are stored unsecured on the mail server (unless PGP Universal Satellite is being used).

For PGP Universal Server to create the SMSA, you must make sure to correctly configure your mail server when you are using PGP Universal Servers in gateway placements.

Internal Placement

With an internal placement, your PGP Universal Server sits between your email users and their email server in the logical flow of data.


Firewall
Internet
Logical flow of data
External Email User
Example Corp. Email Server
PGP Universal internally placed
Example Corp. Email Users
Example Corp. Internal network
Example Corp. DMZ

The physical location of the PGP Universal Server and the mail server are not important. What is important is that, from a mail relay point of view, the PGP Universal Server is between the email users and the mail server. Both could be on the internal network or in the DMZ. From a performance perspective, it is generally advisable to put them next to each other on the same network.

With an internal placement of your PGP Universal Server, messages are secured based on the applicable policies when they are sent to the mail server using SMTP; they are decrypted and verified when they are retrieved from the mail server using POP or IMAP.

With an internal placement, messages are stored secured on the mail server. Messages are only transmitted unencrypted between the internal user and the PGP Universal Server, and then only if PGP Universal Satellite has not been deployed globally to your internal users. If your mail server is configured for SSL/TLS communications with the email client, the messages can be passed through that encrypted channel thus maintaining encryption along the entire path.

For PGP Universal Server to create the SMSA, email clients must have SMTP authentication turned on when they are communicating with a PGP Universal Server in an internal placement.

Using a Mail Relay

PGP Universal Server can forward outgoing email, after processing, to a central mail gateway acting as a mail relay. Sites that use explicit mail routing can use the mail relay feature to forward outgoing email to a mail relay that performs this explicit routing.

You cannot configure the mail relay when you initially configure the server using the Setup Assistant. Instead, you have to configure the server for gateway placement and then use the administrative interface to configure the mail relay.

Configure the relay on the Outbound or Unified SMTP proxy. Refer to "Creating New or Editing Existing Proxies" on page 184 for more information.

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 31 and "MAPI Support" on page 342.

Lotus Domino Server

Lotus Domino Servers and the Lotus Notes email client (versions 5.x and above) 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 31 and "Lotus Notes Support" on page 344.

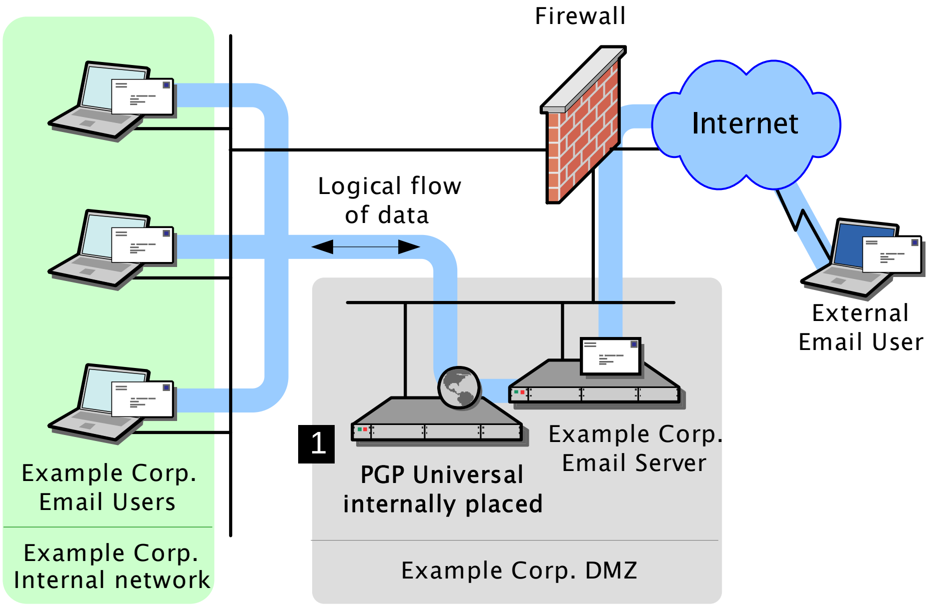
Configuration Examples

This section shows and describes potential configurations for PGP Universal Server:

- “Internal Placement Configuration”
- “Gateway Placement Configuration”
- “Non-mailstream Placement Configuration”
- “Cluster Configuration”
- “Clustered Proxy and Keyserver Configuration”
- “Gateway Cluster with Load Balancer”
- “Gateway and Internal Placement Cluster”
- “Encircled Configuration”
- “Large Enterprise Configuration”
- “Spam Filters and PGP Universal Server”
- “Exchange with PGP Client Software”
- “Lotus Domino Server with PGP Client Software”
- “Unsupported Configurations”

Internal Placement Configuration

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


Firewall
Internet
Logical flow of data
External Email User
1
PGP Universal internally placed
Example Corp. Email Server
Example Corp. Email Users
Example Corp. Internal network
Example Corp. DMZ

Settings for 1:

Server type: **Primary**

Mail processing: **Internal placement**

Hostname: **mail.example.com**

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

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

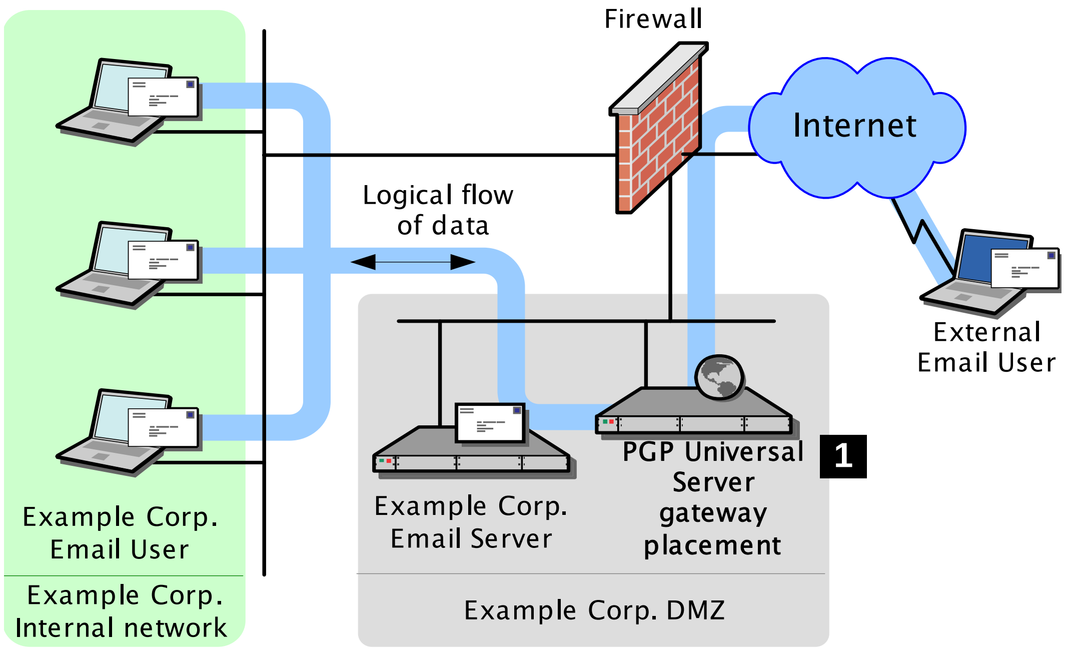
Notes:

- Change **mail.example.com** to **mail-1.example.com** and the PGP Universal Server becomes **mail.example.com**.
- End users may require no changes to their configuration; SMTP Authentication may 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 its messages are encrypted even 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.



Settings for 1:

Server type: **Primary**

Mail processing: **Gateway placement**

Hostname: **mail-gw.example.com**

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

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

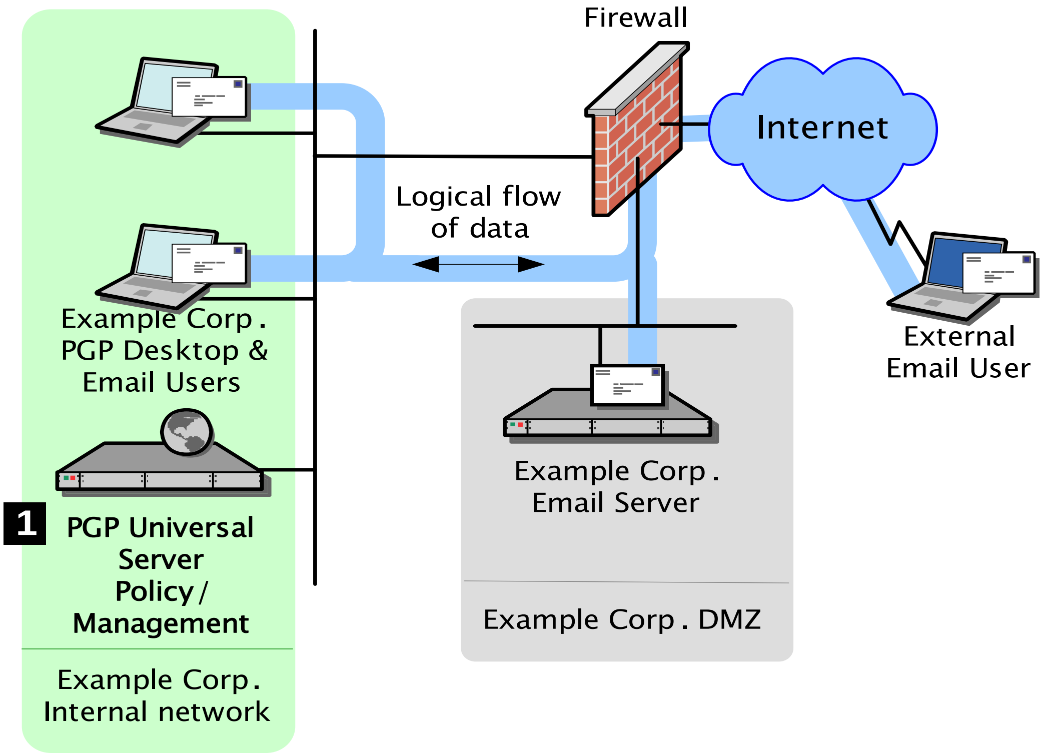
Notes:

- 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.


Firewall
Internet
Logical flow of data
External Email User
Example Corp. PGP Desktop & Email Users
1
PGP Universal Server Policy/ Management
Example Corp. Internal network
Example Corp. Email Server
Example Corp. DMZ

Settings for 1:

Server type: **Primary**

Mail processing: **None**

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

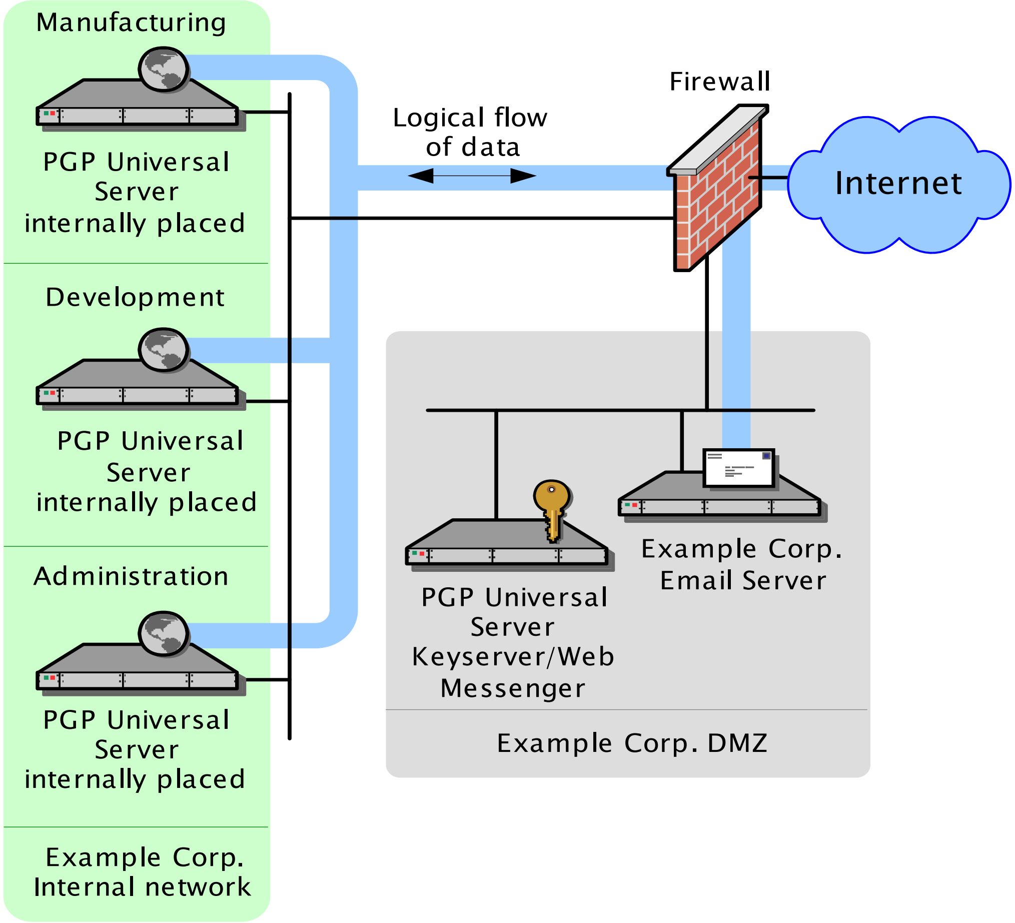
Notes:

• 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.

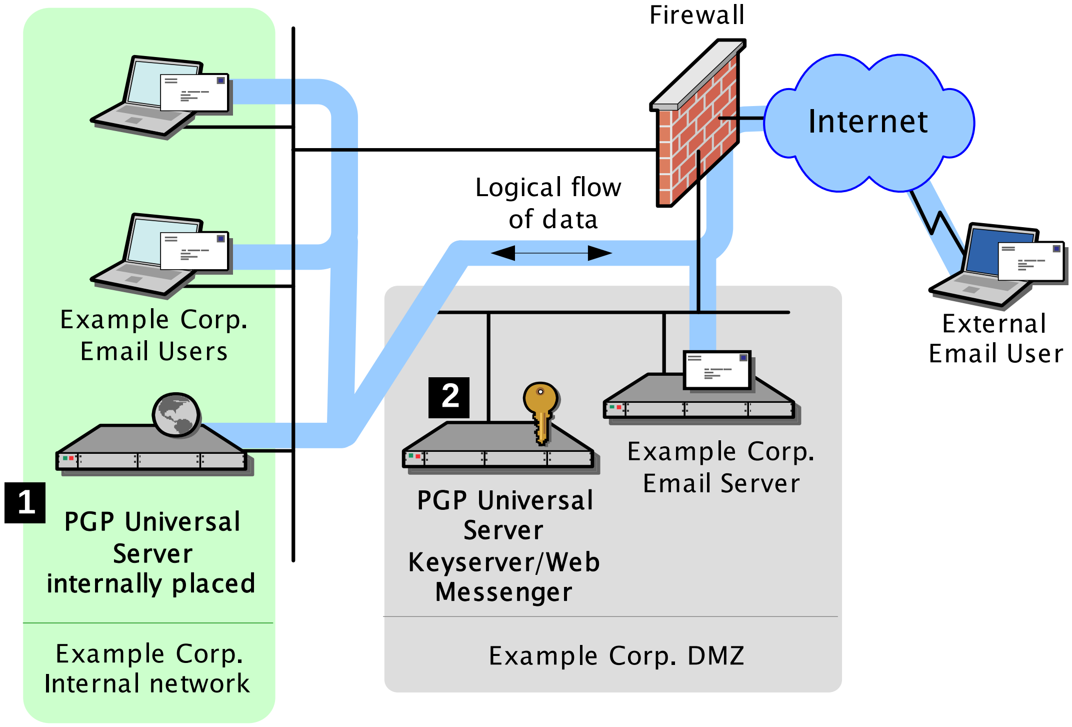

Manufacturing
PGP Universal Server internally placed
Development
PGP Universal Server internally placed
Administration
PGP Universal Server internally placed
Example Corp. Internal network
Logical flow of data
Firewall
Internet
PGP Universal Server Keyserver/Web Messenger
Example Corp. Email Server
Example Corp. DMZ

Notes:

- One internally placed PGP Universal Server configured as Primary in the Cluster; the other and the keyserver configured as Secondary.
- 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.


Firewall
Internet
Logical flow of data
External Email User
Example Corp. Email Users
2
Example Corp. Email Server
1
PGP Universal Server internally placed
PGP Universal Server Keyserver/Web Messenger
Example Corp. Internal network
Example Corp. DMZ

Settings for 1:

Server type: **Primary**

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: **Secondary**

Mail processing: **Disabled**

Hostname: **keys.example.com**

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

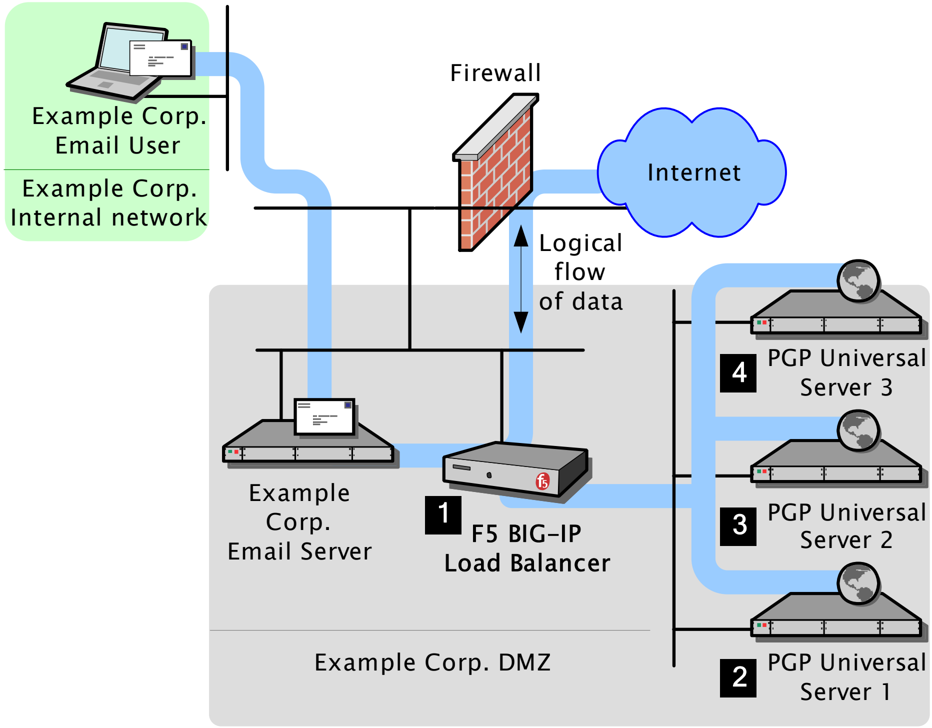
Notes:

- **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, Example Corp. could also 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.



Settings for 1:

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**

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**.

Settings for 2:

Server type: **Primary**

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:

Server type: **Secondary**

Hostname: **cluster2-gw.example.com**

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

Settings for 4:

Server type: **Secondary**

Hostname: **cluster3-gw.example.com**

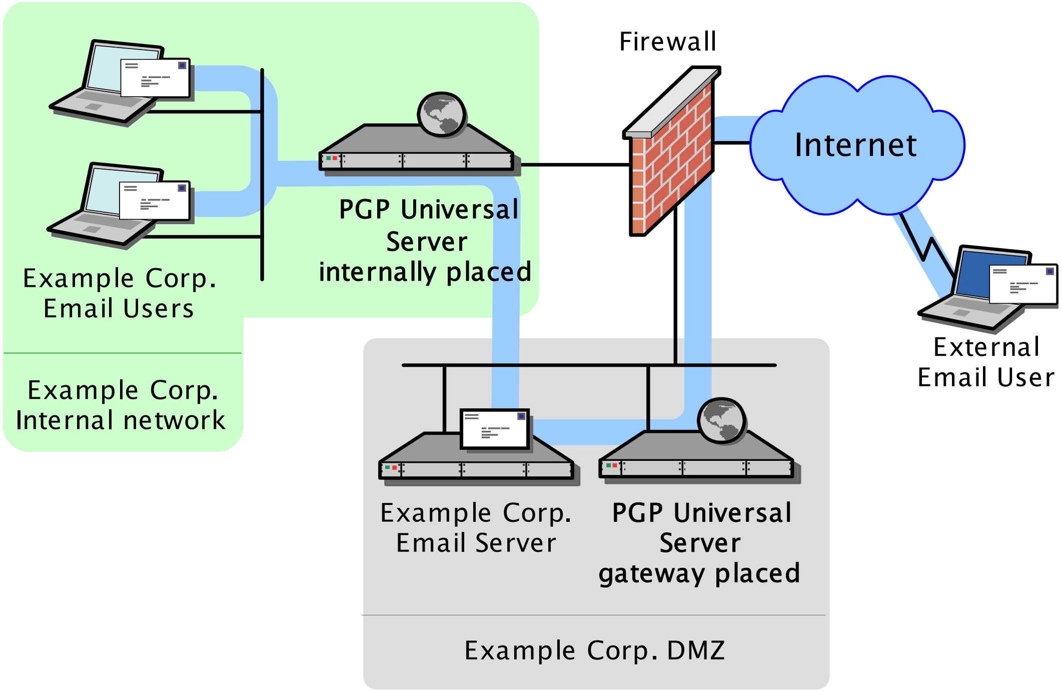
IP Address, Subnet Mask, Gateway, and DNS Servers: **As appropriate**

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.


Firewall
Internet
PGP Universal Server internally placed
Example Corp. Email Users
Example Corp. Internal network
External Email User
Example Corp. Email Server
PGP Universal Server gateway placed
Example Corp. DMZ

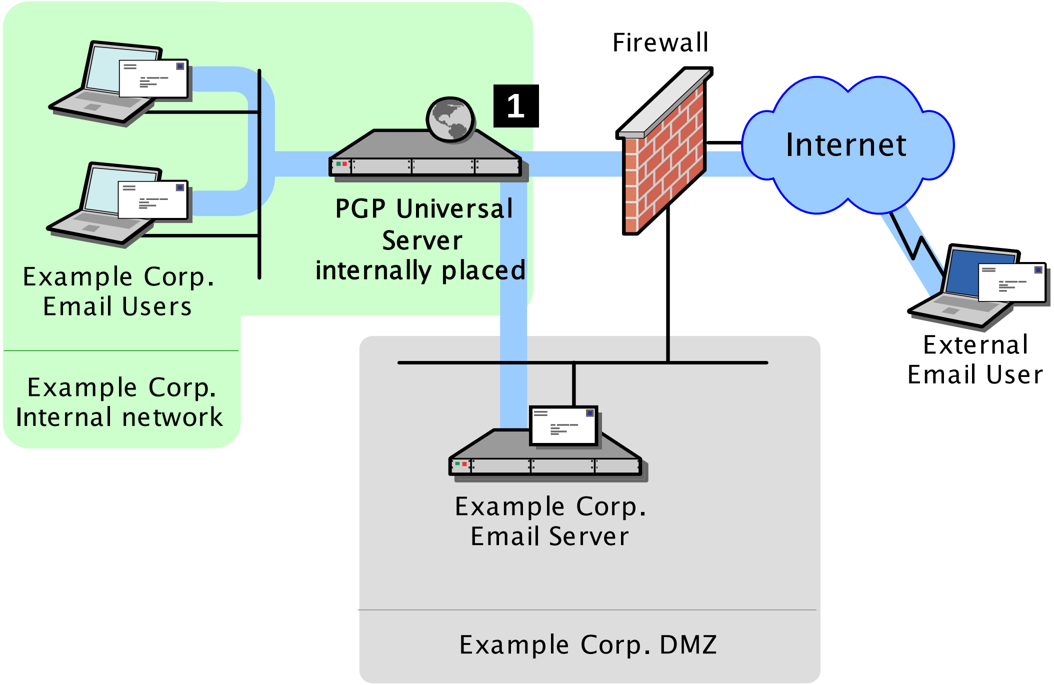
Notes:

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

• The Primary server is internally placed, with PGP Universal Web Messenger disabled. The Secondary server 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.


Firewall
1
Internet
PGP Universal Server internally placed
Example Corp. Email Users
Example Corp. Internal network
External Email User
Example Corp. Email Server
Example Corp. DMZ

Settings for 1:

Server type: **Primary**

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

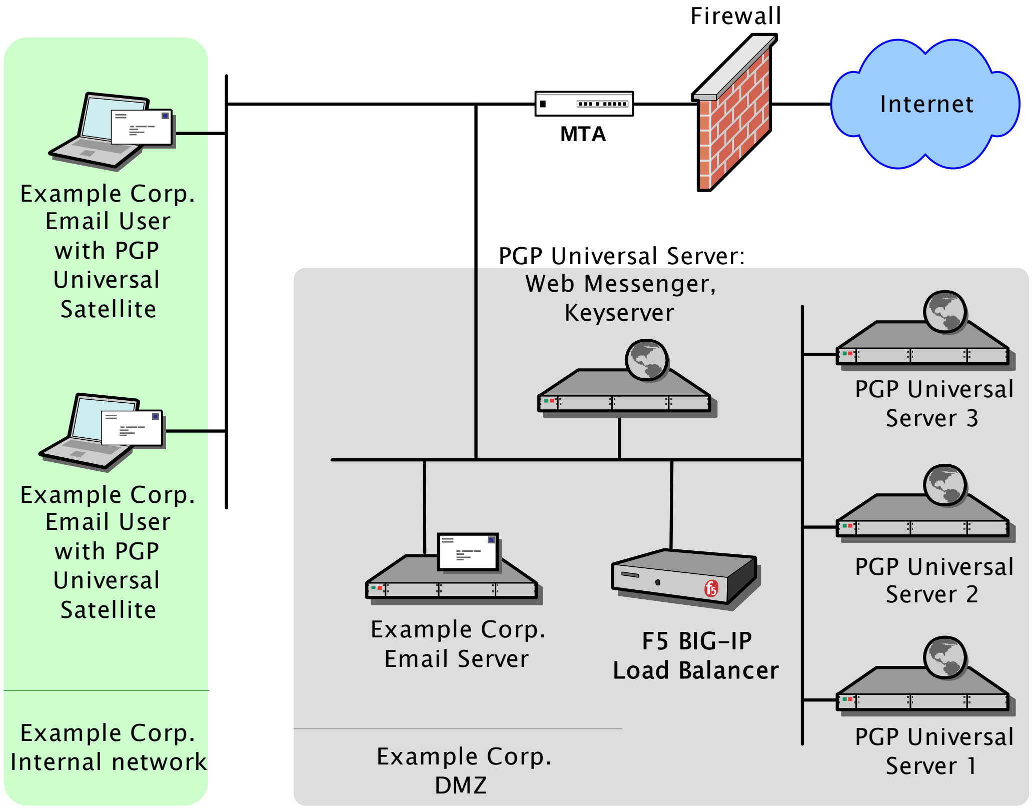
Notes:

• 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).


Firewall
Internet
MTA
Example Corp. Email User with PGP Universal Satellite
Example Corp. Email User with PGP Universal Satellite
Example Corp. Internal network
PGP Universal Server: Web Messenger, Keyserver
PGP Universal Server 3
PGP Universal Server 2
PGP Universal Server 1
Example Corp. Email Server
F5 BIG-IP Load Balancer
Example Corp. DMZ

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.

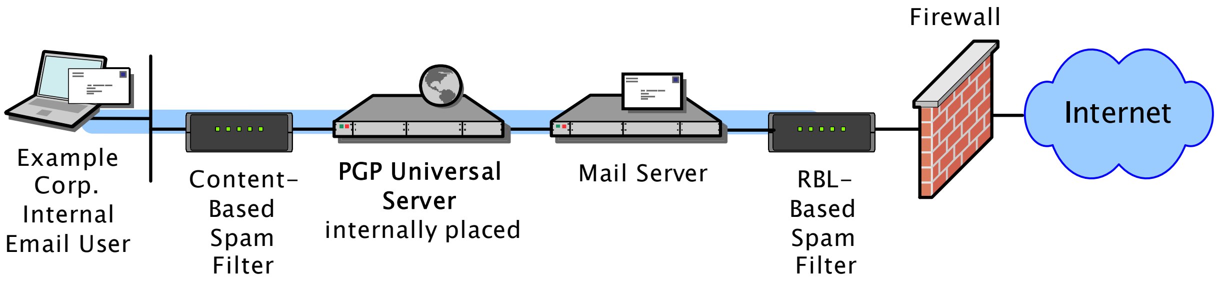
PGP Corporation does not recommend any specific MTA for use with PGP Universal Server. Make sure the MTA you decide to use is correctly configured for use with PGP Universal Server.

Spam Filters and PGP Universal Server

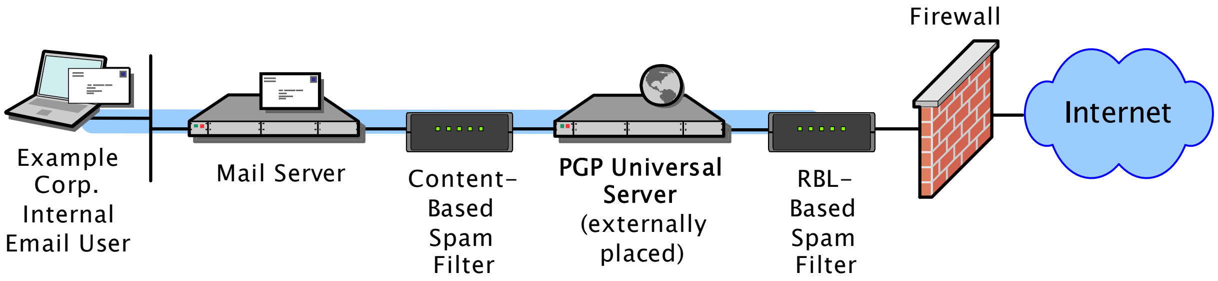
Example Corporation has both a content-based and a Realtime Blackhole List (RBL) spam filter that it wants to use in conjunction with its PGP Universal Server. (An RBL is a list of servers that are known to send out spam or to be open relays.)

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


Firewall
Internet
Example Corp. Internal Email User
Content-Based Spam Filter
PGP Universal Server internally placed
Mail Server
RBL-Based Spam Filter

PGP Universal Server in gateway placement


Firewall
Internet
Example Corp. Internal Email User
Mail Server
Content-Based Spam Filter
PGP Universal Server (externally placed)
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 requirement could mean the spam filter must disable its 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.

As an alternative configuration, Example Corporation could put both spam filters between its PGP Universal Server and its firewall in the logical flow of data. Although PGP Universal Server–encrypted messages would still be scanned for spam, because they would not yet be decrypted, it is unlikely that any spam would be found.

This alternative configuration would catch any spam that was not in a PGP Universal Server–encrypted message, however. So it would be effective if Example Corp. assumes that its PGP Universal Server–encrypted messages are free of spam or if another factor requires the content-based spam filter to be in this location; for example, if the content-based spam filter requires the use of reverse MX lookups.

> ! If Example Corporation began receiving encrypted spam, it could relocate its content-based spam filter to sit between its internal email users and its PGP Universal Server, or it could add another content-based spam filter there. Because spam encryption is CPU-intensive and therefore inefficient, it is unlikely that Example Corporation would receive any.

Exchange with PGP Client Software

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

For more information about Microsoft Exchange Server environments and MAPI support, refer to "MAPI Support" on page 342.

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.

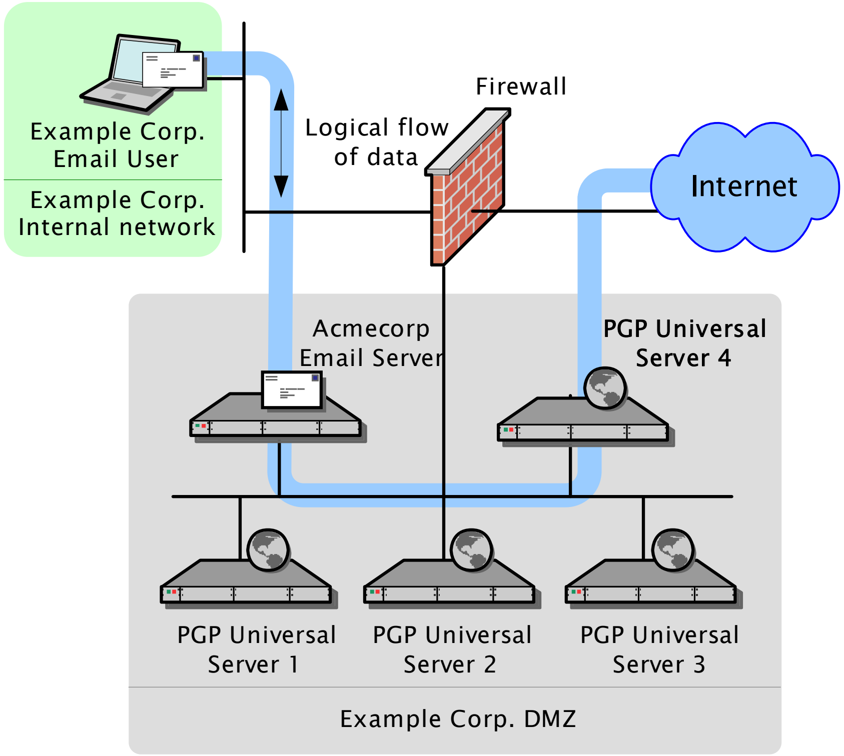
For more information about Lotus Domino Server environments and Lotus Notes email client support, refer to "Lotus Notes Support" on page 344.

Unsupported Configurations

Not every PGP Universal Server deployment scenario is a supported configuration.

Multiple Gateway–Placed Servers

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



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; refer to "Gateway Cluster with Load Balancer" on page 26 for more information.

4 Open Ports

This chapter lists and describes the ports a PGP Universal Server has open and on which it is listening.

All of the protocols listed are described in the Glossary.

TCP Ports

Port	Protocol/Service	Comment
21	FTP (File Transfer Protocol)	Used for transmitting encrypted backup archives to other servers. Data is sent via passive FTP, so port 20 (FTP Data) is not used.
22	Open SSH (Secure Shell)	Used for remote shell access to the server for low-level system administration.
25	SMTP (Simple Mail Transfer Protocol)	Used for sending mail. With a gateway placement, the PGP Universal Server listens on port 25 for both incoming and outgoing SMTP traffic
80	HTTP (HyperText Transfer Protocol)	Used to allow user access to the Verified Directory. If the Verified Directory is not enabled, access on this port will automatically be redirected to port 443 over HTTPS.
110	POP (Post Office Protocol)	Used for retrieving mail by users with POP accounts with internal placements only. Closed for gateway placements.
143	IMAP (Internet Message Access Protocol)	Used for retrieving mail by users with IMAP accounts with internal placements only. Closed for gateway placements.
389	LDAP (Lightweight Directory Access Protocol)	Used to allow remote hosts to look up public keys of local users.
443	HTTPS (HyperText Transfer Protocol, Secure)	Used for PGP Universal Satellite policy distribution and PGP Universal Web Messenger access.
444	SOAPS (Simple Object Access Protocol, Secure)	Used for clustering, and communication with PGP Desktop installations.

Port	Protocol/Service	Comment
465	SMTPS (Simple Mail Transfer Protocol, Secure)	Used for sending mail securely with internal placements only. Closed for gateway placements. This is a non-standard port used only by legacy mail servers. We recommend not using this port, and instead always using STARTTLS on port 25.
636	LDAPS (Lightweight Directory Access Protocol, Secure)	Used to securely allow remote hosts to look up public keys of local users.
993	IMAPS (Internet Message Access Protocol, Secure)	Used for retrieving mail securely by users with IMAP accounts with internal placements only. Closed for gateway placements.
995	POPS (Post Office Protocol, Secure)	Used for retrieving mail securely by users with POP accounts with internal placements only. Closed for gateway placements.
9000	HTTPS (HyperText Transfer Protocol, Secure)	Used to allow access to the PGP Universal Server administrative interface.

UDP Ports

Port	Protocol/Service	Comment
123	NTP (Network Time Protocol)	Used to synchronize the system's clock with a reference time source on a different server.
161	SNMP (Simple Network Management Protocol)	Used by network management applications to query the health and activities of PGP Universal Server software and the computer on which it is installed.

5 Naming your PGP Universal Server

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

Overview

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 a special hostname, **keys.<domain>**, where <domain> is the email domain of the recipient.

For example, let’s assume an internal user at example.com is sending email to “susanjones@widgetcorp.com.” If no valid public key for Susan is found on the Example Corp. PGP Universal Server (keys would be found locally if they are cached, or if Susan was an external user who explicitly supplied her key via the PGP Universal Web Messenger service), it will automatically look 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.

Naturally, the Example Corp. PGP Universal Server will only be able to find a valid public key for “susan@widgetcorp.com” at keys.widgetcorp.com if the Widgetcorp PGP Universal Server is named using the keys.<domain> convention.

! PGP Corporation strongly recommends you name your PGP Universal Server according to this convention, because doing so allows other PGP Universal Servers to easily find valid public keys for email recipients in your domain. Make sure to name your externally visible PGP Universal Server using this convention.

If your organization uses email addresses like “mingp@example.com” as well as “mingp@corp.example.com,” then you need your PGP Universal Server to be reachable at both **keys.example.com** and **keys.corp.example.com**.

If you have multiple PGP Universal Servers in a cluster managing an email domain, only one of those PGP Universal Servers needs to use the keys.<domain> convention.

i Keys that are found using the keys.<domain> convention are treated as valid and trusted by default.

Alternately, keys.<domain> should be the address of a load-balancing device which then distributes connections to your PGP Universal Server’s keyserver service. The ports that would need to be load-balanced are the ones on which you’re running your keyserver service (typically port 389 for LDAP and 636 for LDAPS).

Another acceptable naming convention would be to name your PGP Universal Server according to the required naming convention your company uses, and make sure 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 (as it should be), you will need to make sure that ports 389 (LDAP) and 636 (LDAPS) are open to support the keys.<domain> convention.

Configuration

There are three ways to name your PGP Universal Server to support the keys.<domain> convention:

- Name your PGP Universal Server "keys.<domain>" on the Host Name field of the Network Setup screen in the Setup Assistant
- Change the Host Name of your PGP Universal Server to keys.<domain> using the administrative interface on the Network Settings card of the System>Network screen
- Create a DNS alias to your PGP Universal Server that uses the keys.<domain> convention that is appropriate for your DNS server configuration

SECTION 3

Installing the PGP Universal Server Software

This section describes how to install the software on your server hardware, how to set up PGP Universal Server, and provides a description of the user interface.

6 Installing the PGP Universal Server

This chapter tells you how to set up your PGP Universal Server; it lists the system requirements and tells you how to install the software. Topics include:

- "About the Installation Procedure"
- "System Requirements" on page 39
- "Installation Materials" on page 40
- "Installation Options" on page 40
- "Standard Installation Procedure" on page 40
- "PGP Installation Procedure" on page 41

Refer to "Installation Overview" on page 11 for an overview of the entire installation procedure.

About the Installation Procedure

You should install and test the upgrade in a lab or staging environment before integrating the upgrade into your network.

Every PGP Universal Server requires a dedicated computer that meets the system requirements listed below. The installation process deletes all data on the system and reconfigures it as a PGP Universal Server.

⚠ Make sure there is no data on the system that you need to save before you begin the installation process.

The installation software is included on the Server Installation CD. PGP Universal Server also includes a second CD with documentation, software license, PGP Universal Satellite and PGP Desktop software installers, necessary USB token drivers, and Release Notes.

ℹ PGP Corporation strongly recommends locating your PGP Universal Servers in secured areas with restricted access. Only authorized individuals should be granted physical access to PGP Universal Servers.

System Requirements

Refer to the *Release Notes* for the latest system requirement information.

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 PGP Corporation's website (www.pgp.com).

Installation Materials

PGP Universal Server is distributed on two CDs. One CD contains the installer. Use this CD to install the server on PGP Universal Server Certified Hardware. The other CD contains documentation, PGP Universal Satellite and PGP Desktop software installers, and the necessary USB token drivers to initialize PGP Universal Server Ignition Keys.

Installation Options

When you insert the installation CD and reboot the server, you can choose a **standard** or **pgp** installation.

If you choose to run a standard installation, during installation you will be asked to provide the following information for the PGP Universal Server:

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

Refer to “Standard Installation Procedure” on page 40.

If you provide the network information during installation, you will not have to enter it into the Setup Assistant interface later in the configuration procedure. The standard installation also simplifies the steps necessary to connect to the PGP Universal Server during setup.

If you choose to run a **pgp** installation, you will enter network information after the installation process, through the browser-based Setup Assistant. Refer to “PGP Installation Procedure” on page 41. The **pgp** installation, while simpler initially, requires a more complicated procedure to connect and continue setting up your PGP Universal Server.

Standard Installation Procedure

To install the PGP Universal Server software using the standard installation:

1. Set up the system that will be hosting the server in a secure location.

2 Attach a keyboard and monitor to the server on which you are installing PGP Universal Server.

3 Insert the PGP Universal Server Installation CD into the drive.

4 Reboot the system.

When the system reboots, the install begins.

5 At the prompt, press **Enter**.

The pre-installation will run for approximately 2 minutes.

The **Network Configurations** screen will appear.

6 Enter the IP address and Netmask for the PGP Universal Server, and select **OK**.

The **Miscellaneous Network Settings** screen appears.

7 Enter the Gateway, Primary DNS, Secondary DNS, and an optional Tertiary DNS, and select **OK**.

The **Hostname Configuration** screen appears.

8 Enter the Hostname for the PGP Universal Server, and select OK.

PGP 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. Refer to Chapter 5, "Naming your PGP Universal Server" for more information.

Installation will take approximately 15 minutes.

When the software is installed, the system will automatically reboot. After the system reboots, you will see a login prompt. Do not log in here. You will not need to log in to complete the setup.

9 Connect to the server through the Setup Assistant browser interface at https://<hostname>:9000 or https://<IP address>:9000. See Chapter 7, "Initial Configuration with Setup Assistant" to continue with the installation and setup.

PGP Installation Procedure

To install the PGP Universal Server software using the pgp option:

1 Set up the system that will be hosting the server in a secure location.

2 Attach a keyboard and monitor to the server on which you are installing PGP Universal Server.

3 Insert the PGP Universal Server Installation CD into the drive.

4 Reboot the system.

When the system reboots, the install begins.

5 Type **pgp** at the prompt and press **Enter** at the first installation screen to choose the pgp installation.

The pre-installation will run for approximately 2 minutes.

Installation will take approximately 15 minutes.

When the software is installed, the system will automatically reboot. After the system reboots, you will see the prompt “pgpuniversal login.” Do not log in here. You will not need to log in to complete the setup.

6 Connect to the server through the Setup Assistant browser interface. See “Preparing for Setup after **pgp** Install” on page 44 to continue with the installation and setup.

7 Setting Up the PGP Universal Server

This chapter describes how to access and use the Setup Assistant, which is a set of screens you use to configure your PGP Universal Server. Topics include:

- "About the Setup Assistant"
- "Preparing for Setup after **pgp** Install" on page 44
- "Initial Configuration with Setup Assistant" on page 45
- "Primary or Secondary Configuration" on page 51
- "Restoring From a Server Backup" on page 61
- "Migrating the Keys from a PGP Keyserver" on page 61

Refer to "Installation Overview" on page 11 for an overview of the entire installation procedure.

About the Setup Assistant

The Setup Assistant only appears the first time you access the PGP Universal Server. The Setup Assistant displays a series of screens that ask you questions about your network and about how you want your PGP Universal Server to work; the Setup Assistant uses the answers to those questions to configure your PGP Universal Server.

In many cases, the Setup Assistant will do the majority of the configuration for your PGP Universal Server. You can change any settings you establish with the Setup Assistant anytime after you run it using the administrative interface of the PGP Universal Server; you can also use the administrative interface to configure those features not covered in the Setup Assistant.

The Setup Assistant supports four types of setups:

- **Primary**. You are configuring a PGP Universal Server that will be your only PGP Universal Server or the Primary server in a cluster.
- **Secondary**. You are configuring a PGP Universal Server that will be a Secondary server in a cluster. *You must have already set up the Primary server in the cluster or this setup will not work.*
- **Restore**. You are restoring backed-up data from another PGP Universal Server onto a new PGP Universal Server. You will need the backed-up data file and the Organization Key used to encrypt the backup file.

  Refer to the *PGP Universal Server Upgrade Guide* for more information about configuring a PGP Universal Server with data from a backup.
- **Keyserver**. You are migrating the keys and data from a PGP Keyserver to a PGP Universal Server.

Refer to the *PGP Universal Server Upgrade Guide* for more information about configuring a PGP Universal Server with the keys from a PGP Keyserver.

All four setup types have a common beginning: you read the End User License Agreement, specify the type of setup, and configure the network settings for your PGP Universal Server, then the PGP Universal Server is restarted. Once the PGP Universal Server is restarted, you can connect to it via a Web browser and continue with the rest of the Setup Assistant.

Preparing for Setup after pgp Install

If you chose the **standard** installation option, you can skip this procedure and refer to "Initial Configuration with Setup Assistant" on page 45. If you chose the **pgp** installation, you must gather some necessary materials and information before you can continue with the setup.

Hardware

To configure your PGP Universal Server using the Setup Assistant, you need to have the following:

- A Windows or Mac OS X computer from which you will connect to the PGP Universal Server using a Web browser so that you can run the Setup Assistant.
- A crossover Ethernet cable to connect a Windows or Mac OS X computer to the PGP Universal Server.

System Information

You will also need some information to configure your PGP Universal Server:

- Connect through the temporary IP address and subnet of the newly installed PGP Universal Server, which will be used for the initial configuration portion of the Setup Assistant:

  IP: 192.168.1.100:9000

  Subnet: 255.255.255.0

  You will use this data to connect to the PGP Universal Server you are configuring in the initial configuration portion of the Setup Assistant, before the PGP Universal Server is available via a Web browser.
- An IP address, name, gateway, and DNS server information for the PGP Universal Server.
- A license or license authorization from PGP Corporation. Which one you need depends on your Internet connection:
  - If your PGP Universal Server can connect to the PGP Licensing Server over the Internet, the license server will authorize your PGP Universal Server license.

  - If your PGP Universal Server cannot connect to the PGP Licensing Server over the Internet, you will need the License Authorization file to correctly license your PGP Universal Server. The License Authorization file is a text file you will need during the configuration process.

- Other data, such as your Organization Key or a saved backup, may also be needed, depending on the type of setup you are performing.

Connect to the PGP Universal Server

Connect to the PGP Universal Server to continue the installation and setup. Configure the client machine with a fixed IP address and access the PGP Universal Server from this machine.

You will need a crossover Ethernet cable when connecting the PGP Universal Server.

1. Configure the client machine:

   IP: 192.168.1.99

   Subnet: 255.255.255.0

   If you are using a Mac OS X client machine, you can save this temporary setup as a separate location in Network Preferences (such as "setup") for future use.

2. Continue setup as described in the section "Initial Configuration with Setup Assistant" on page 45.

Initial Configuration with Setup Assistant

The Setup Assistant guides you through establishing the PGP Universal Server's network configuration and setup type.

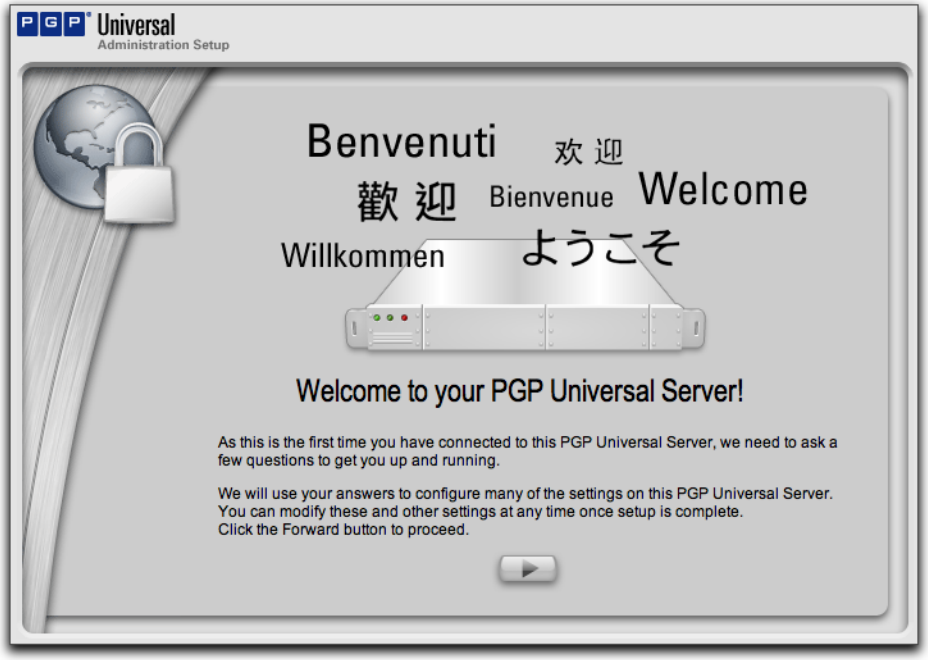
After the software installs and the server restart, you can connect to the PGP Universal Server via a Web browser at the configured IP address and finish running the Setup Assistant.

1. Open a Web browser and connect to the PGP Universal Server:

   - If you chose the **standard** installation, connect to **https://<hostname>:9000**, using the hostname or IP address you assigned to the PGP Universal Server.

   - If you chose the **pgp** installation, and you are using a client machine with a fixed IP address, connect to **https://192.168.1.100:9000,** as explained in the section "Preparing for Setup after **pgp** Install" on page 44.

   The Welcome screen of the Setup Assistant appears.



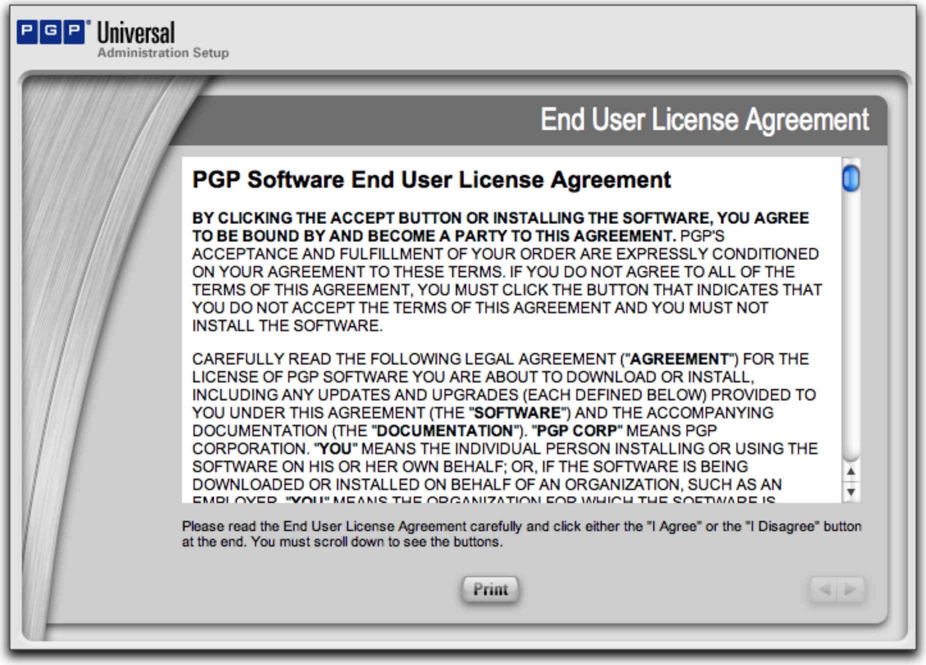
Welcome to your PGP Universal Server!

As this is the first time you have connected to this PGP Universal Server, we need to ask a few questions to get you up and running.

We will use your answers to configure many of the settings on this PGP Universal Server. You can modify these and other settings at any time once setup is complete. Click the Forward button to proceed.

2 Read the text, then click the **Forward** arrow to continue.

The End User License Agreement screen appears.



PGP Software End User License Agreement

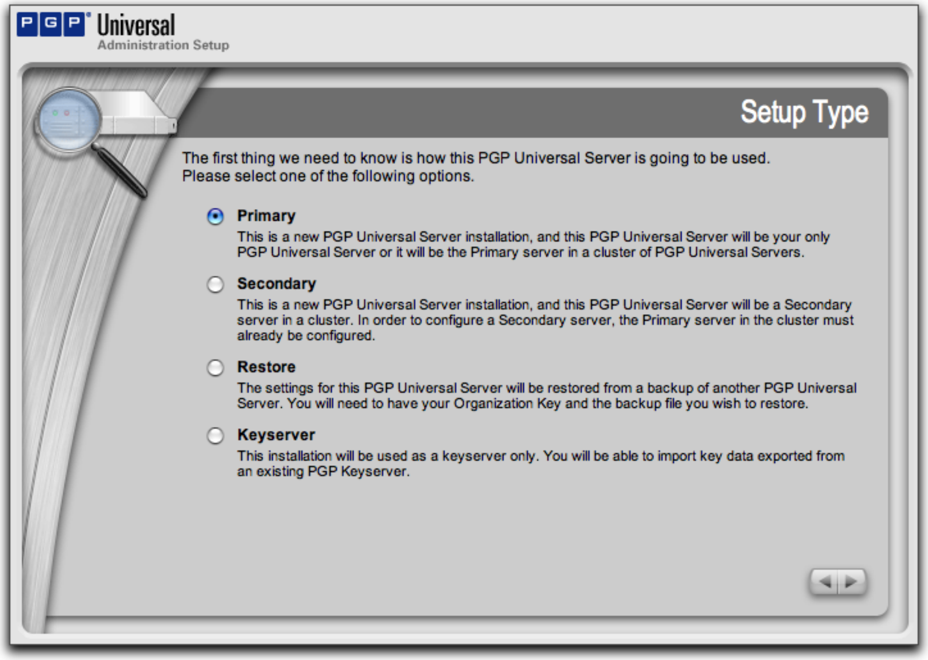
BY CLICKING THE ACCEPT BUTTON OR INSTALLING THE SOFTWARE, YOU AGREE TO BE BOUND BY AND BECOME A PARTY TO THIS AGREEMENT. PGP'S ACCEPTANCE AND FULFILLMENT OF YOUR ORDER ARE EXPRESSLY CONDITIONED ON YOUR AGREEMENT TO THESE TERMS. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, YOU MUST CLICK THE BUTTON THAT INDICATES THAT YOU DO NOT ACCEPT THE TERMS OF THIS AGREEMENT AND YOU MUST NOT INSTALL THE SOFTWARE.

CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT ("**AGREEMENT**") FOR THE LICENSE OF PGP SOFTWARE YOU ARE ABOUT TO DOWNLOAD OR INSTALL, INCLUDING ANY UPDATES AND UPGRADES (EACH DEFINED BELOW) PROVIDED TO YOU UNDER THIS AGREEMENT (THE "**SOFTWARE**") AND THE ACCOMPANYING DOCUMENTATION (THE "**DOCUMENTATION**"). "**PGP CORP**" MEANS PGP CORPORATION. "**YOU**" MEANS THE INDIVIDUAL PERSON INSTALLING OR USING THE SOFTWARE ON HIS OR HER OWN BEHALF; OR, IF THE SOFTWARE IS BEING DOWNLOADED OR INSTALLED ON BEHALF OF AN ORGANIZATION, SUCH AS AN EMPLOYER, "**YOU**" MEANS THE ORGANIZATION FOR WHICH THE SOFTWARE IS

Please read the End User License Agreement carefully and click either the "I Agree" or the "I Disagree" button at the end. You must scroll down to see the buttons.

3 Read the text of the License Agreement, then click the **I Agree** button at the end of the agreement.

The Setup Type screen appears.



The first thing we need to know is how this PGP Universal Server is going to be used.
Please select one of the following options.

● **Primary**
This is a new PGP Universal Server installation, and this PGP Universal Server will be your only PGP Universal Server or it will be the Primary server in a cluster of PGP Universal Servers.

○ **Secondary**
This is a new PGP Universal Server installation, and this PGP Universal Server will be a Secondary server in a cluster. In order to configure a Secondary server, the Primary server in the cluster must already be configured.

○ **Restore**
The settings for this PGP Universal Server will be restored from a backup of another PGP Universal Server. You will need to have your Organization Key and the backup file you wish to restore.

○ **Keyserver**
This installation will be used as a keyserver only. You will be able to import key data exported from an existing PGP Keyserver.

4 Make the appropriate selection:

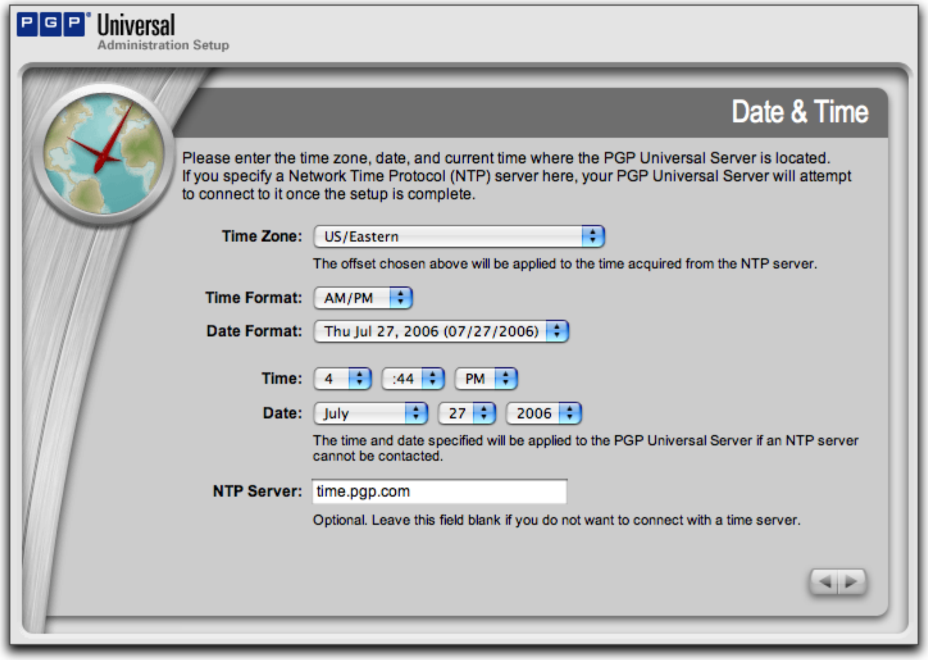
- Select **Primary** if you want this to be the Primary PGP Universal Server in a cluster or if this is the only PGP Universal Server in your network.
- Select **Secondary** if this is a Secondary PGP Universal Server in a cluster (secondary servers synchronize their settings with the Primary).

  If you are setting up a cluster of PGP Universal Servers, you must configure the Primary first, then the Secondary servers. Refer to Chapter 45, "Clustering your PGP Universal Servers" for more information.

  If you are upgrading a Secondary cluster member, you will need to recreate certain settings manually after installation and setup. Follow the procedure in the *PGP Universal Server Upgrade Guide* for more details.
- Select **Restore** if you want to restore the data from a server backup. You will need your Organization Key and access to the backup file to proceed with this installation. Refer to the *PGP Universal Server Upgrade Guide* for more information.
- Select **Keyserver** if you want to migrate the keys on an existing PGP Keyserver to the PGP Universal Server you are configuring. See the *PGP Universal Server Upgrade Guide* for more information.

5 Click the **Forward** arrow to continue.

The Date & Time screen appears.



Please enter the time zone, date, and current time where the PGP Universal Server is located. If you specify a Network Time Protocol (NTP) server here, your PGP Universal Server will attempt to connect to it once the setup is complete.

Time Zone: US/Eastern

The offset chosen above will be applied to the time acquired from the NTP server.

Time Format: AM/PM

Date Format: Thu Jul 27, 2006 (07/27/2006)

Time: 4 :44 PM

Date: July 27 2006

The time and date specified will be applied to the PGP Universal Server if an NTP server cannot be contacted.

NTP Server: time.pgp.com

Optional. Leave this field blank if you do not want to connect with a time server.

Your server preforms many time-based operations, so it is important to set up the correct time.

6 Pull down the **Time Zone** drop-down list and select your location.

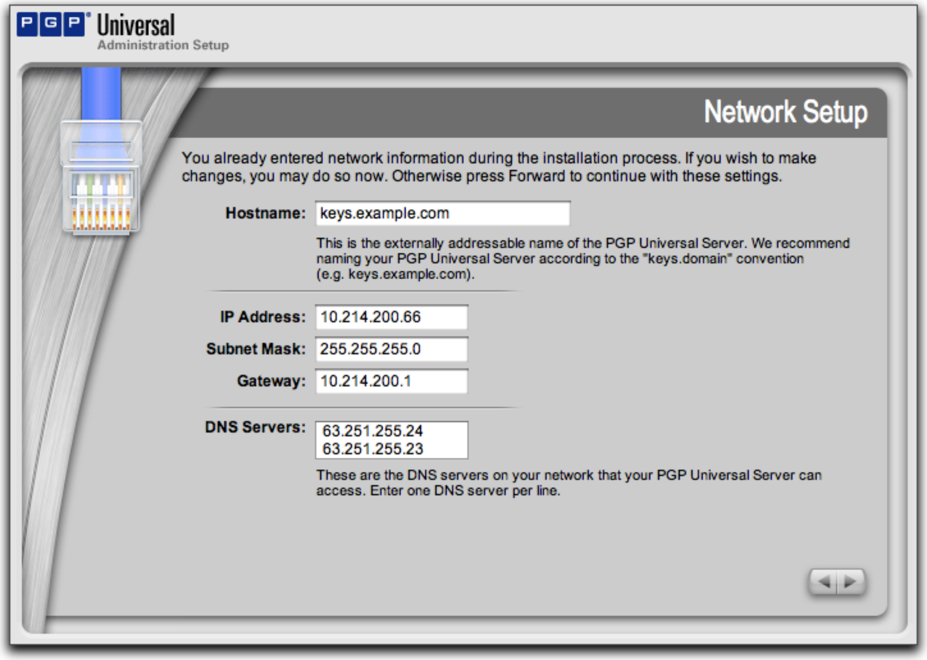
7 Choose **Time Format** and **Date Format** settings.

8 Set the correct **Time** and **Date**.

9 Optionally, specify an NTP time server in the **NTP Server** field. The PGP Universal Server will automatically synchronize the time when the Setup Assistant is finished.

10 Click the **Forward** arrow to continue.

The Network Setup screen appears.



Network Setup

You already entered network information during the installation process. If you wish to make changes, you may do so now. Otherwise press Forward to continue with these settings.

Hostname: keys.example.com

This is the externally addressable name of the PGP Universal Server. We recommend naming your PGP Universal Server according to the "keys.domain" convention (e.g. keys.example.com).

IP Address: 10.214.200.66

Subnet Mask: 255.255.255.0

Gateway: 10.214.200.1

DNS Servers: 63.251.255.24
63.251.255.23

These are the DNS servers on your network that your PGP Universal Server can access. Enter one DNS server per line.

11 If you chose the **standard** installation, this information is already present. Otherwise, enter the appropriate information:

– In the **Hostname** field, enter a name for this PGP Universal Server. This must be a fully-qualified domain name of the external, untrusted interface.

PGP 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." Refer to Chapter 5, "Naming your PGP Universal Server" for more information.

a In the **IP Address** field, enter an IP address for this PGP Universal Server.

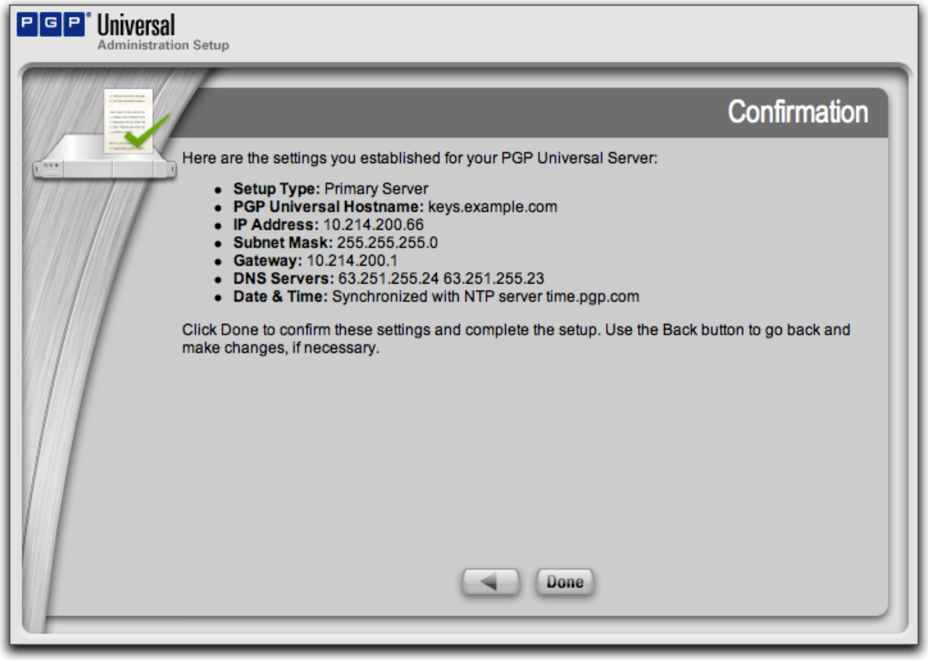
b In the **Subnet Mask** field, enter a subnet mask for this PGP Universal Server.

c In the **Gateway** field, enter the IP address of the default gateway for the network.

d In the **DNS Servers** field, enter the IP address(es) of the DNS servers for your network.

12 Click the **Forward** arrow to continue.

The Confirmation screen appears.



Here are the settings you established for your PGP Universal Server:

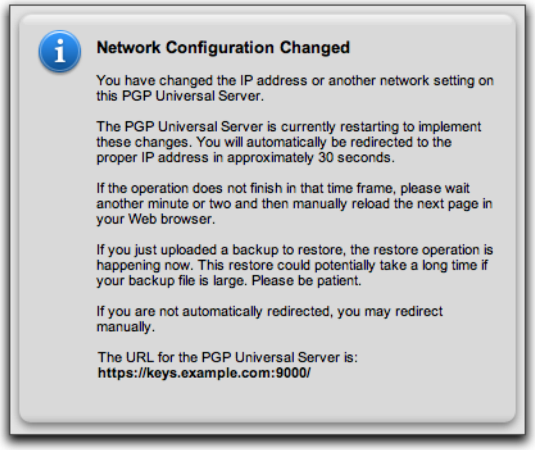
- **Setup Type:** Primary Server
- **PGP Universal Hostname:** keys.example.com
- **IP Address:** 10.214.200.66
- **Subnet Mask:** 255.255.255.0
- **Gateway:** 10.214.200.1
- **DNS Servers:** 63.251.255.24 63.251.255.23
- **Date & Time:** Synchronized with NTP server time.pgp.com

Click Done to confirm these settings and complete the setup. Use the Back button to go back and make changes, if necessary.

13 Make sure the information is correct, then click **Done**.

Click the **Back** arrow if you need to go back and make any changes.

The Network Configuration Changed dialog appears, while the server restarts automatically.



Network Configuration Changed

You have changed the IP address or another network setting on this PGP Universal Server.

The PGP Universal Server is currently restarting to implement these changes. You will automatically be redirected to the proper IP address in approximately 30 seconds.

If the operation does not finish in that time frame, please wait another minute or two and then manually reload the next page in your Web browser.

If you just uploaded a backup to restore, the restore operation is happening now. This restore could potentially take a long time if your backup file is large. Please be patient.

If you are not automatically redirected, you may redirect manually.

The URL for the PGP Universal Server is:
https://keys.example.com:9000/

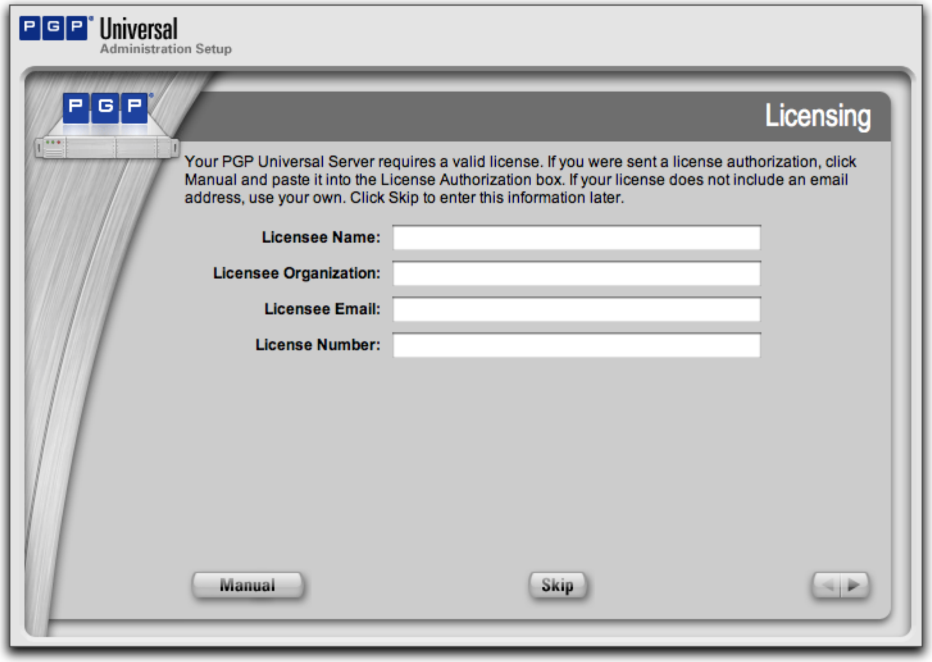
If you chose the **standard** installation, skip step 14 and go on to the next section.

If you chose the **pgp** installation, go on to the next step. At this point, your PGP Universal Server has accepted the new network settings you entered, so you can disconnect the temporary setup.

14 Disconnect the cable between the client machine and the PGP Universal Server, return the settings of the client machine back to what they were, connect the two machines back to the original network, and continue with the Setup Assistant.

Primary or Secondary Configuration

If you selected a Primary or Secondary configuration for the PGP Universal Server you are configuring with the Setup Assistant, the Licensing screen appears automatically.



Your PGP Universal Server requires a valid license. If you were sent a license authorization, click Manual and paste it into the License Authorization box. If your license does not include an email address, use your own. Click Skip to enter this information later.

Licensee Name:

Licensee Organization:

Licensee Email:

License Number:

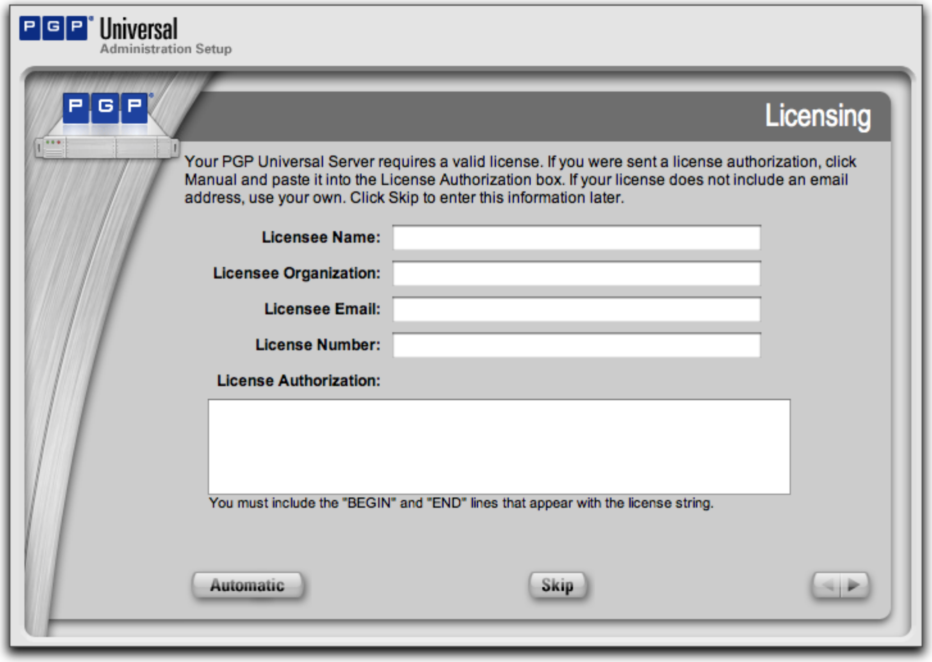
1 Enter your PGP Universal Server license information, then click the **Forward** arrow.

If your PGP Universal Server has an active connection to the Internet, the PGP Universal Server license will be authorized.

2 If your PGP Universal Server does *not* have an active connection to the Internet, for example because it is behind a proxy server, your license authorization will be needed; click **Manual**.

The Manual Licensing screen appears.

3 If you want to license your PGP Universal Server at a later time, click **Skip**, and go on to step 9.



Your PGP Universal Server requires a valid license. If you were sent a license authorization, click Manual and paste it into the License Authorization box. If your license does not include an email address, use your own. Click Skip to enter this information later.

Licensee Name:

Licensee Organization:

Licensee Email:

License Number:

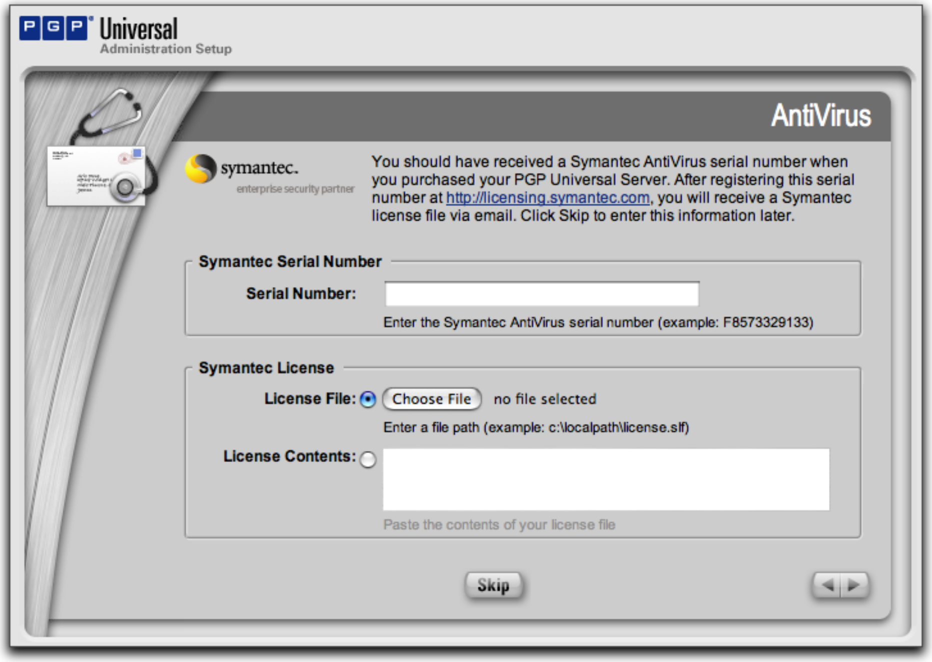
License Authorization:

You must include the "BEGIN" and "END" lines that appear with the license string.

4 Enter the appropriate license information, paste your license authorization information in the License Authorization box, then click the **Forward** arrow.

5 If you want to license your PGP Universal Server at a later time, click **Skip**.

If your PGP Universal Server license supports the Symantec AntiVirus option, the AntiVirus screen appears. See Chapter 9, "Licensing Your Software" for more information on AntiVirus licensing.



AntiVirus

You should have received a Symantec AntiVirus serial number when you purchased your PGP Universal Server. After registering this serial number at http://licensing.symantec.com, you will receive a Symantec license file via email. Click Skip to enter this information later.

Symantec Serial Number

Serial Number:

Enter the Symantec AntiVirus serial number (example: F8573329133)

Symantec License

License File: ● Choose File no file selected

Enter a file path (example: c:\localpath\license.slf)

License Contents: ○

Paste the contents of your license file

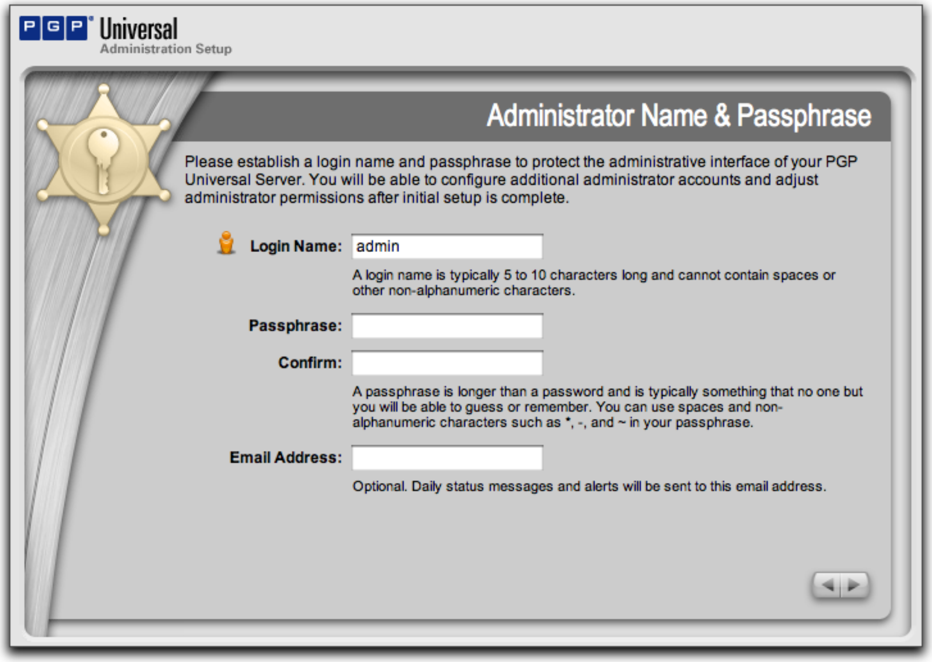
6 Enter your Symantec AntiVirus serial number in the **Serial Number** field.

Click **Skip** to continue with the Setup Assistant without licensing the AntiVirus feature.

7 In the **License File** field, locate your Symantec license file using the **Choose File** button or paste the contents of your Symantec license file into the **License Contents** box.

8 Click the **Forward** arrow to continue.

The Administrator Name & Passphrase screen appears.



Administrator Name & Passphrase

Please establish a login name and passphrase to protect the administrative interface of your PGP Universal Server. You will be able to configure additional administrator accounts and adjust administrator permissions after initial setup is complete.

Login Name: admin

A login name is typically 5 to 10 characters long and cannot contain spaces or other non-alphanumeric characters.

Passphrase:

Confirm:

A passphrase is longer than a password and is typically something that no one but you will be able to guess or remember. You can use spaces and non-alphanumeric characters such as *, -, and ~ in your passphrase.

Email Address:

Optional. Daily status messages and alerts will be sent to this email address.

9 In the **Login Name** field, enter the administrator's login name.

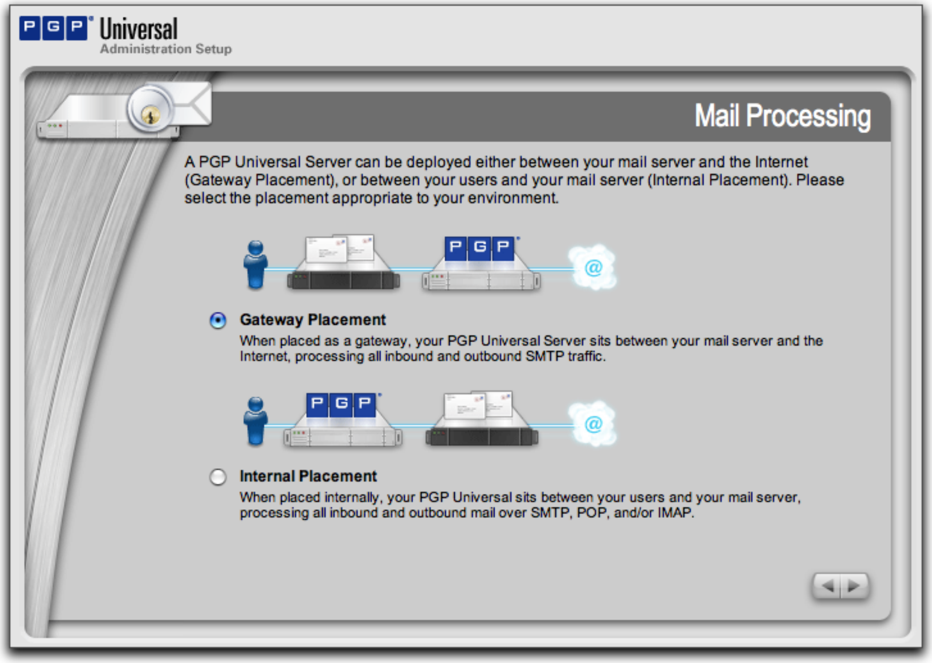
10 In the **Passphrase** field, enter the administrator's passphrase.

11 In the **Confirm** field, re-enter the same passphrase.

12 In the **Email Address** field, enter the administrator's email address. This is optional and enables the administrator to receive a daily status email.

13 Click the **Forward** arrow to continue.

The Mail Processing screen appears.



Mail Processing

A PGP Universal Server can be deployed either between your mail server and the Internet (Gateway Placement), or between your users and your mail server (Internal Placement). Please select the placement appropriate to your environment.

● **Gateway Placement**
When placed as a gateway, your PGP Universal Server sits between your mail server and the Internet, processing all inbound and outbound SMTP traffic.

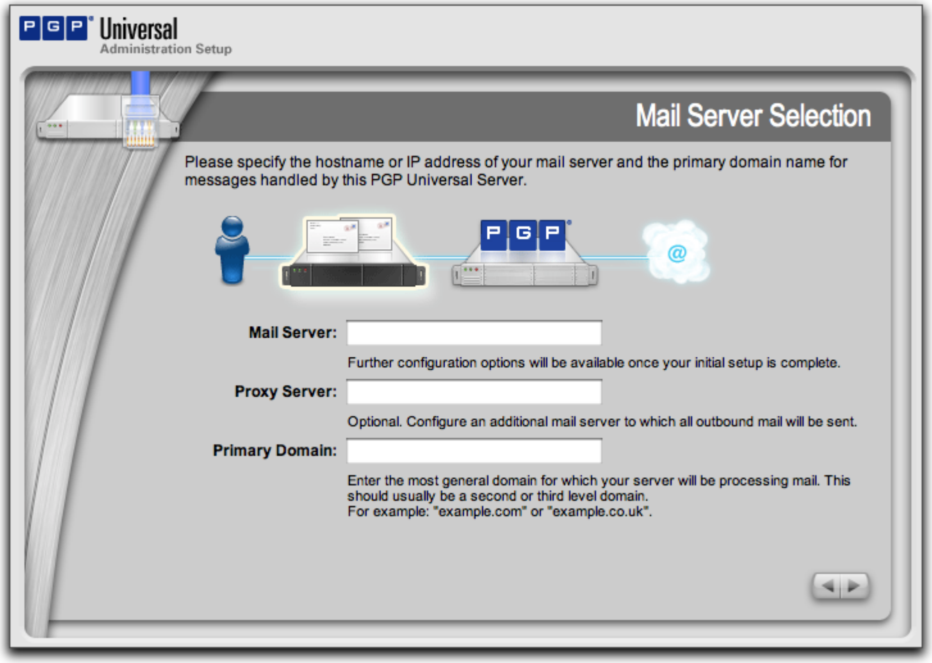
○ **Internal Placement**
When placed internally, your PGP Universal sits between your users and your mail server, processing all inbound and outbound mail over SMTP, POP, and/or IMAP.

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

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

15 Click the **Forward** arrow to continue.

The Mail Server Selection screen appears.



Mail Server Selection

Please specify the hostname or IP address of your mail server and the primary domain name for messages handled by this PGP Universal Server.

Mail Server:

Further configuration options will be available once your initial setup is complete.

Proxy Server:

Optional. Configure an additional mail server to which all outbound mail will be sent.

Primary Domain:

Enter the most general domain for which your server will be processing mail. This should usually be a second or third level domain.
For example: "example.com" or "example.co.uk".

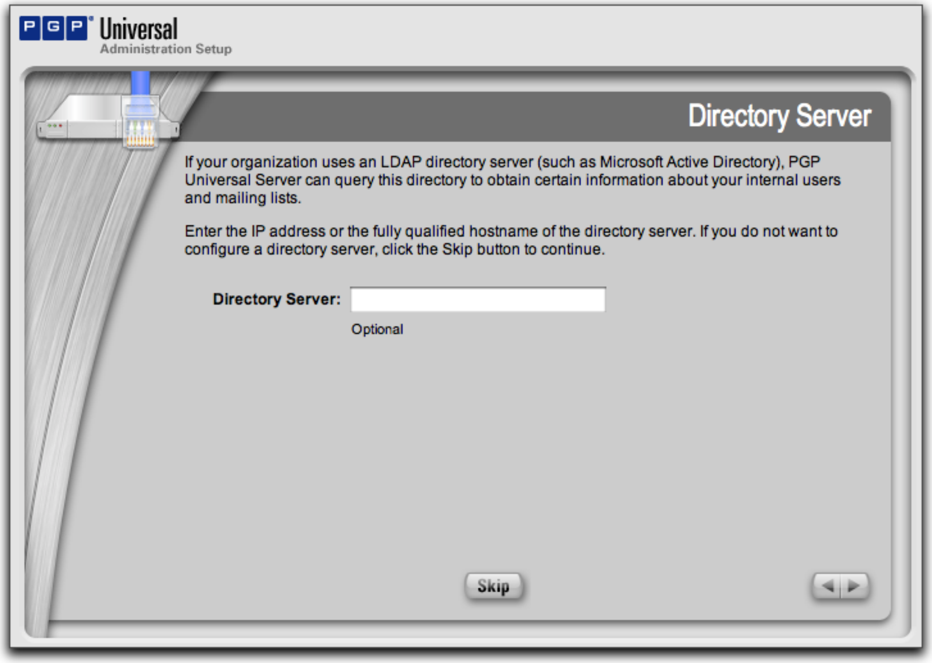
16 In the **Mail Server** field, enter the hostname or IP address of the mail server that this PGP Universal Server will be interacting with.

17 In the **Proxy Server** field, enter an optional additional mail server to which all outbound mail will be sent. This only applies if you are installing your PGP Universal server in gateway placement.

18 In the **Primary Domain** field, enter the email domain that the PGP Universal Server is going to be managing.

19 Click the **Forward** arrow to continue.

The Directory Server screen appears.



If your organization uses an LDAP directory server (such as Microsoft Active Directory), PGP Universal Server can query this directory to obtain certain information about your internal users and mailing lists.

Enter the IP address or the fully qualified hostname of the directory server. If you do not want to configure a directory server, click the Skip button to continue.

Directory Server: Optional

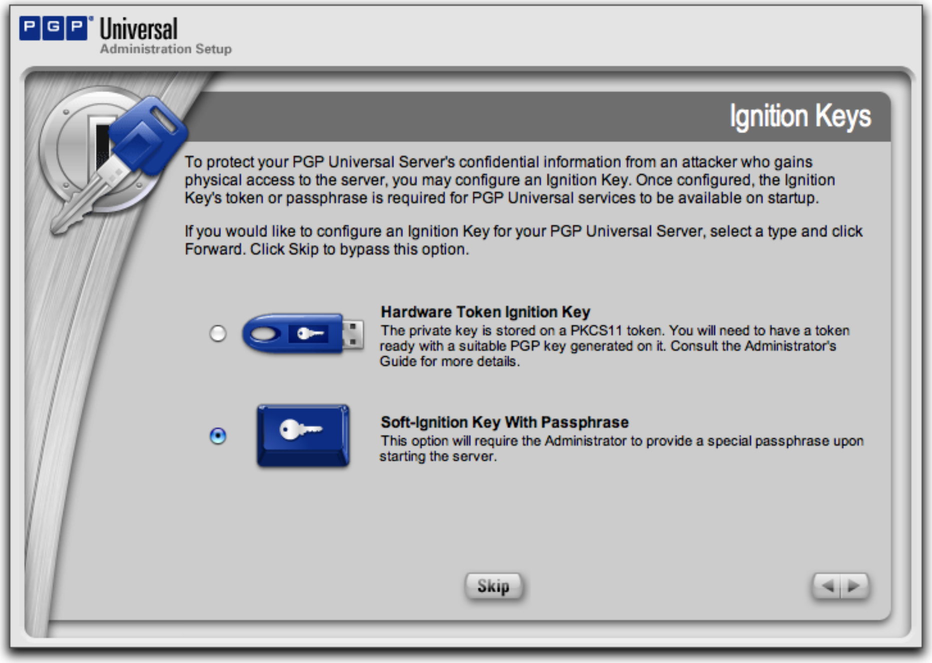
20 In the **Directory Server** field, enter the hostname or IP address of your corporate LDAP directory so that PGP Universal Server can synchronize user information with that LDAP directory.

By default, PGP Universal Server adds your LDAP directory as an Active Directory. If your directory is OpenLDAP-based, when you log in for the first time after setup, go to Policy>Internal User Policy, click Directory Synchronization, and select the correct LDAP directory type from the drop-down menu. Refer to "Enabling Directory Synchronization" on page 228 for more information.

Using a directory server is optional. If you do not have one on your network or do not wish to use one, leave the **Directory Server** field empty and click **Skip** to continue with the Setup Assistant.

21 Click the **Forward** arrow to continue.

The Ignition Keys screen appears.



To protect your PGP Universal Server's confidential information from an attacker who gains physical access to the server, you may configure an Ignition Key. Once configured, the Ignition Key's token or passphrase is required for PGP Universal services to be available on startup.

If you would like to configure an Ignition Key for your PGP Universal Server, select a type and click Forward. Click Skip to bypass this option.

○ **Hardware Token Ignition Key**
The private key is stored on a PKCS11 token. You will need to have a token ready with a suitable PGP key generated on it. Consult the Administrator's Guide for more details.

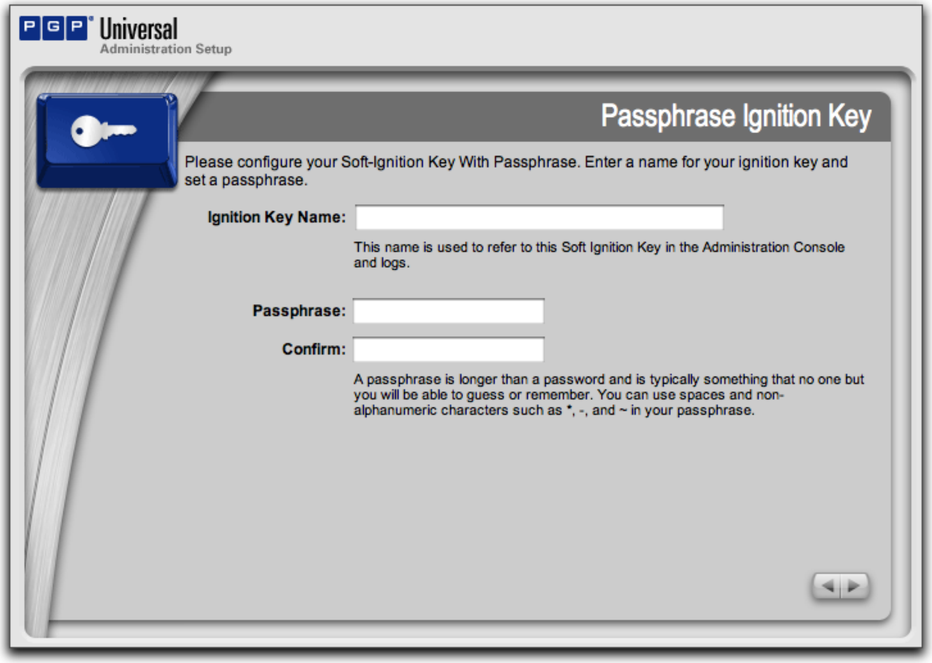
● **Soft-Ignition Key With Passphrase**
This option will require the Administrator to provide a special passphrase upon starting the server.

Ignition Keys protect the data on your PGP Universal Server if an unauthorized person gets control of it. If you want to use a hardware Ignition Key, you will need to prepare the token before you add it to the system here. See Chapter 46, “Protecting PGP Universal Server with Ignition Keys” for information on how to prepare a hardware token Ignition Key.

22 Select the type of Ignition Key you would like to use, then click the **Forward** arrow.

Click **Skip** to proceed with the Setup Assistant without configuring an Ignition Key.

The appropriate Ignition Key screen appears. The Passphrase Ignition Key screen is shown here.



Please configure your Soft-Ignition Key With Passphrase. Enter a name for your ignition key and set a passphrase.

Ignition Key Name:

This name is used to refer to this Soft Ignition Key in the Administration Console and logs.

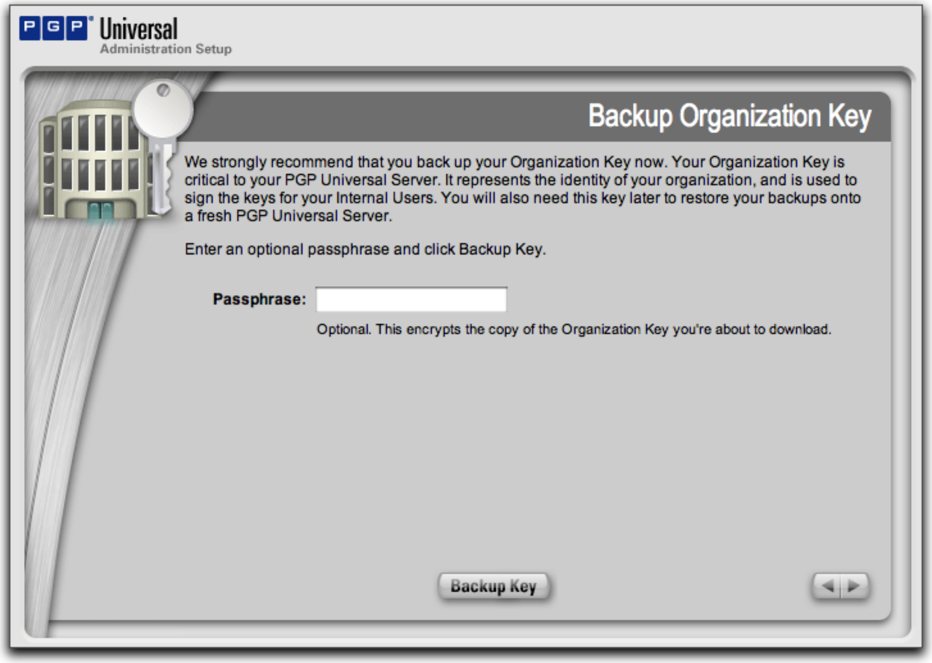
Passphrase:

Confirm:

A passphrase is longer than a password and is typically something that no one but you will be able to guess or remember. You can use spaces and non-alphanumeric characters such as *, -, and ~ in your passphrase.

23 Enter a name for the Ignition Key, a passphrase, confirm the passphrase, then click the **Forward** arrow.

The Backup Organization Key screen appears.



We strongly recommend that you back up your Organization Key now. Your Organization Key is critical to your PGP Universal Server. It represents the identity of your organization, and is used to sign the keys for your Internal Users. You will also need this key later to restore your backups onto a fresh PGP Universal Server.

Enter an optional passphrase and click Backup Key.

Passphrase:

Optional. This encrypts the copy of the Organization Key you're about to download.

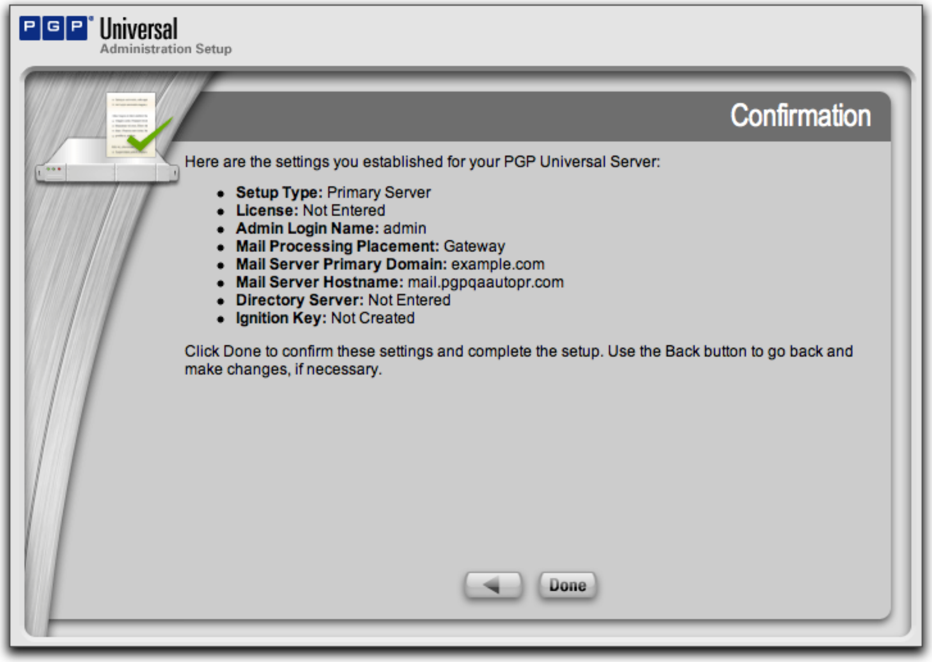
The PGP Universal Server generates an Organization Key for you. If you want to generate an S/MIME Organization Certificate, you should do so immediately after finishing setup. Refer to Chapter 12, "Managing Organization Keys" for information about the Organization Key and Organization Certificate.

24 If desired, enter the passphrase that will protect the Organization Key (this is optional, but highly recommended), then click **Backup Key** to back up the key. Be aware that without a backup of your Organization Key, you will not be able to restore your PGP Universal Server from backed-up data.

To skip backing up your Organization Key (not recommended), click **Forward** without backing up the key.

25 Click the **Forward** arrow to continue.

The Confirmation screen appears.



Here are the settings you established for your PGP Universal Server:

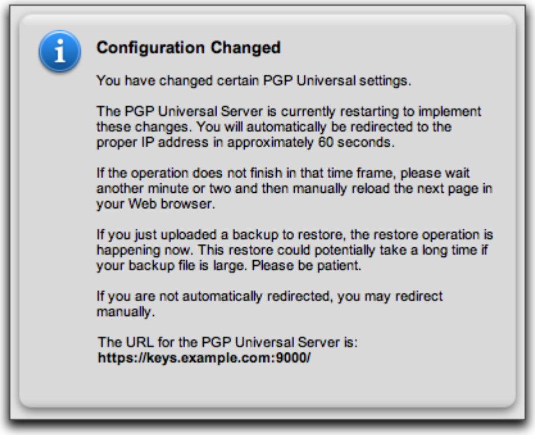
- **Setup Type:** Primary Server
- **License:** Not Entered
- **Admin Login Name:** admin
- **Mail Processing Placement:** Gateway
- **Mail Server Primary Domain:** example.com
- **Mail Server Hostname:** mail.pgpqaautopr.com
- **Directory Server:** Not Entered
- **Ignition Key:** Not Created

Click Done to confirm these settings and complete the setup. Use the Back button to go back and make changes, if necessary.

This screen summarizes the configuration of your PGP Universal Server.

26 Click **Done** to finish setup.

The Configuration Changed screen appears, and the server restarts automatically.



Configuration Changed

You have changed certain PGP Universal settings.

The PGP Universal Server is currently restarting to implement these changes. You will automatically be redirected to the proper IP address in approximately 60 seconds.

If the operation does not finish in that time frame, please wait another minute or two and then manually reload the next page in your Web browser.

If you just uploaded a backup to restore, the restore operation is happening now. This restore could potentially take a long time if your backup file is large. Please be patient.

If you are not automatically redirected, you may redirect manually.

The URL for the PGP Universal Server is:
https://keys.example.com:9000/

You will be redirected to the administrative interface of the PGP Universal Server you just configured.

Your PGP Universal Server is initially configured in Learn Mode. Refer to Chapter 10, "Operating in Learn Mode" for more information about Learn Mode.

Restoring From a Server Backup

To configure a PGP Universal Server with the data from the backup, you need to have both the appropriate backup file and the Organization Key on the setup machine. Restoring from a backup restores everything configured, including proxy and policy settings, as well as keys and user information.

Refer to the *PGP Universal Server Upgrade Guide* for complete information about how to configure a PGP Universal Server with the data from a backup.

Migrating the Keys from a PGP Keyserver

The process that allows you to migrate the keys on a PGP Keyserver to a PGP Universal Server includes two steps: getting the keys out of the PGP Keyserver into a format that can be imported into a PGP Universal Server and then using the Setup Assistant to configure a PGP Universal Server and add the PGP keys from the PGP Keyserver.

Refer to the *PGP Universal Server Upgrade Guide* for complete information about migrating PGP keys from a PGP Keyserver to a PGP Universal Server.

You can find more information online about moving to PGP Universal Server at the PGP Corporation website. The latest version of that document is always available at www.pgp.com/products/upgrade/index.html.

8 Understanding the Administrative Interface

This chapter tells you about the PGP Universal Server's Web-based administrative interface: it lists the following:

- "System Requirements"
- "Logging In"
- "Administrative Interface Map" on page 66
- "Icons" on page 67

System Requirements

The PGP Universal Server administrative interface has been fully tested with the following Web browsers:

- Windows: Internet Explorer 6, Mozilla Firefox 1.0 (or greater)
- Mac OS X: Safari 1.0 (or greater), Mozilla Firefox 1.0 (or greater)

While you may find that the administrative interface works with other Web browsers, we recommend these browsers for maximum compatibility.

Logging In

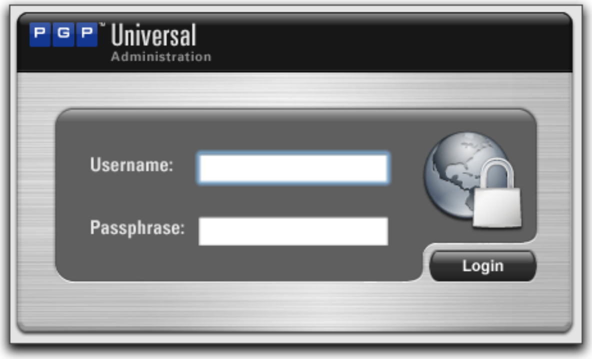
The login name and password for the administrative interface were originally established when you configured the server using the Setup Assistant.

To log in to your server's administrative interface:

1 In a Web browser, enter **https://<domain name of server>:9000/** and press **Enter**.

> If you see a Security Alert dialog relating to the security certificate, it means you need to replace the self-signed certificate created automatically with a certificate from a public Certificate Authority.

The Login screen appears.

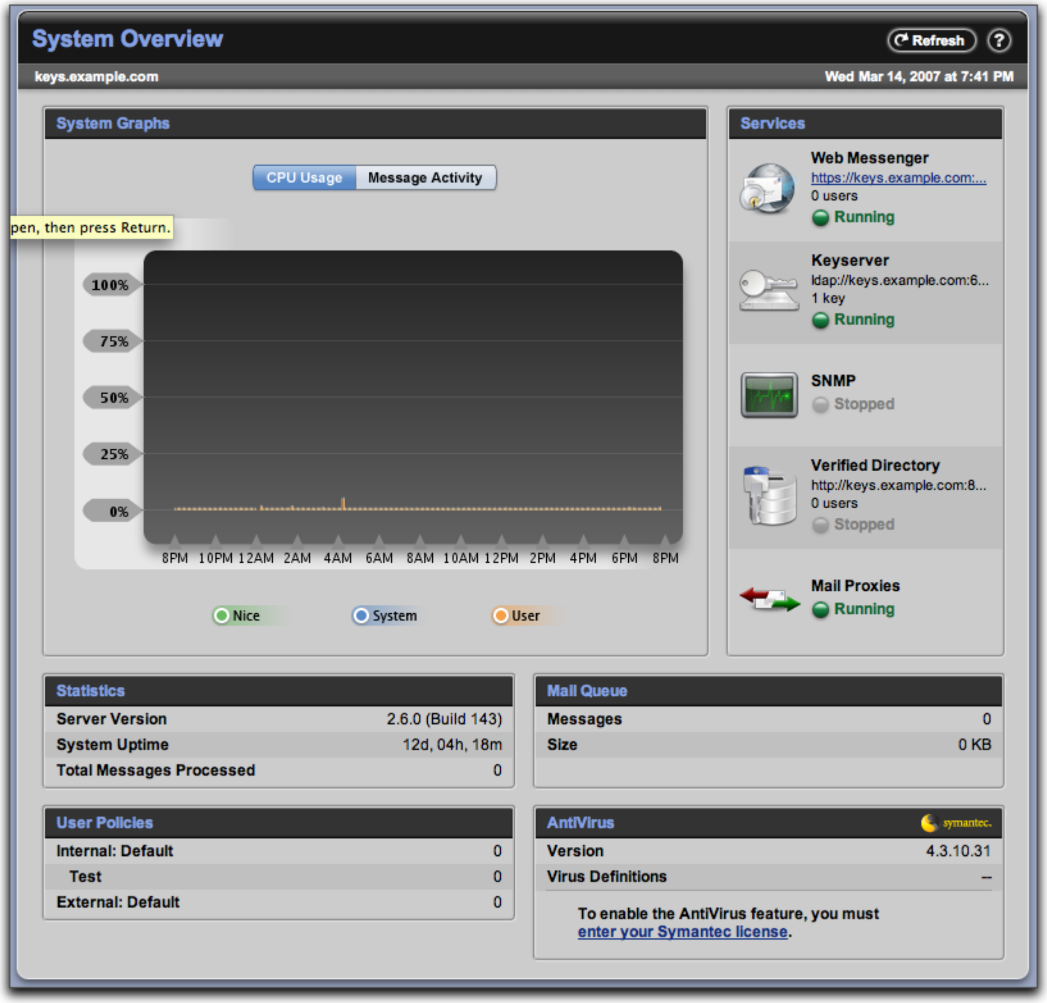


2 Enter the current login name in the **Username** field.

3 Enter the current passphrase in the **Passphrase** field.

4 Click the **Login** button or press **Enter**.

The System Overview screen is the first screen you see when you log on to PGP Universal Server. You can also view it from **Reporting>Overview**.



keys.example.com Wed Mar 14, 2007 at 7:41 PM

Web Messenger
https://keys.example.com:...
0 users
Running

Keyserver
ldap://keys.example.com:6...
1 key
Running

SNMP
Stopped

Verified Directory
http://keys.example.com:8...
0 users
Stopped

Mail Proxies
Running

Statistics	
Server Version	2.6.0 (Build 143)
System Uptime	12d, 04h, 18m
Total Messages Processed	0

Mail Queue	
Messages	0
Size	0 KB

User Policies	
Internal: Default	0
Test	0
External: Default	0

AntiVirus	symantec.
Version	4.3.10.31
Virus Definitions	–

To enable the AntiVirus feature, you must enter your Symantec license.

The screen provides a general report of system information and statistics. The information displayed includes:

- System graphs for CPU usage and message activity. Click the buttons to switch the graphs. See Chapter 40, "System Graphs" for more information about system graphs.
- Services information, including which services are running or stopped.
- Statistics, including software version number, system uptime, and total messages processed.
- Number of users in each user policy group.
- Number of email messages in the queue waiting to be processed, if applicable.
- AntiVirus information, if licensed, including Symantec AntiVirus version, date of latest virus definitions, number of viruses found and repaired, and number of scan requests.
- Number of messages in the mail queue.

Click **Refresh** (at the top of the System Overview screen) to refresh the information.

Logging In For the First Time

The first time you log in to the PGP Universal Server, you will see a welcome dialog. The welcome dialog provides access to tutorials and documentation. You can choose to have the welcome dialog appear every time you log in.

- **What's New**—Lists the new features in PGP Universal Server 2.6.
- **Mail Policy Diagram**—Provides a graphical representation of how email is processed through mail policy.
- **PGP Universal Upgrade Guide**—Provides instructions on how to migrate PGP Keyserver data, how to upgrade your PGP Universal Server, and how version 2.0.6 settings migrate into the 2.6 environment.
- **Tutorials**—Provides animated introductions on how to manage the mail policy feature in PGP Universal Server, 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.

Administrative Interface Map

The administrative interface is organized as follows:

Sections	**Screens**
Reporting	Overview
	Graphs
	Logs
Policy	Mail Policy
	Internal User Policy
	External User Policy
	Dictionaries
	Servers
Users	Internal
	External
	Verified Directory (If enabled)
	Administrators
Mail	Proxies
	AntiVirus*****
	File Blocking*****
	Mail Queue
	Mail Routes
	Message Templates
Organization	Organization Keys
	Trusted Keys
	Managed Domains
Services	Web Messenger
	Keyserver
	SNMP
	Verified Directory
System	General Settings
	Backups
	Updates
	Network
	Clustering
	Ignition Keys
	Key Cache

***** Requires a PGP Universal Server license that supports these features.

Icons

The administrative interface uses the following icons.

Type	Icon	Description
Actions	⊕	Add
	⊖	Remove
	⇌	Connect
	⊘	Delete
	⊗	Clear Search
	⬇	Install/Export
	↻	Reinstall/Regenerate
	⬆	Restore
	⦸	Revoke
	▶	Forward
	◀	Back
	⏮	First
	⏭	Last
	⏶	Move priority up
	⏷	Move priority down
	▶	Closed Action
	▼	Opened Action

Type	Icon	Description
	?	Help
	⬆	Update software
	🖨	Print
Users	👤	Internal user
	👤	Administrative user
	👤	Disabled user
	👤⊘	Internal user, revoked
	👤🕓	Expired internal user
	🌐👤⊘	External user, revoked
	🌐👤	External user
	🌐👤⏸	External user, pending
	🌐👤🕓	Expired external user
	🗄👤	Directory user
	🗄👤🕓	Expired directory user
	🗄👤⏸	Directory user, pending
Keys and Certificates	🔑	Key
	🔑🕓	Key, expired
	🔑⊘	Key, revoked
	🔑⚙	Key reconstruction

Type	Icon	Description
		Whole Disk Recovery Token
		Keypair
		Keypair, expired
		Keypair, revoked
		Certificate
		Expired certificate
		Revoked certificate
		Expired certificate pair
		Certificate pair
		Revoked certificate pair
		ADK (Additional Decryption Key)
		Organization Key
		Verified Directory Key
Mail Policy		Default policy chain
		Policy chain
		Policy rule
	Aa	Dictionary term
		Excluded address
		Pending excluded address

Type	Icon	Description
	🗄	Keyserver
	✓🗄	Default keyserver
User Policy	📋✓	Default internal user policy
	📋🚫	Excluded internal user policy
	📋🌐	External user policy
	📋👤	Internal user policy
Backup	💼	Backup successful
	💼	Backup pending
	⚠💼	Backup failed
Update	■	Successful install
	⬇📦	Update ready to be installed
	⚠📦	Failed install
Clustering	▬	Cluster
	🟢	Active cluster
	⚪	Inactive cluster
Logs	ℹ	Info
	★	Notice
	⚠	Warning
	⛔	Error

Type	Icon	Description
Miscellaneous	🌐	Domain
	⇄	Mail proxy (SMTP, POP, IMAP)
	⬇	Inbound mailserver
	⬆	Outbound mailserver
	⇆	SMTP server
	✉	Mail route
	🔌	Network interface
	?	Learn mode
	✓	Access control enabled

9 Licensing Your Software

This chapter tells you about how to license your PGP Universal Server.

Topics include:

Overview

Your PGP Universal Server must have a valid license to be taken out of Learn Mode. In other words, without a valid license, your PGP Universal Server will never encrypt or sign any email messages.

If you licensed your PGP Universal Server using the Setup Assistant, you do not have to license it again. If you did not, then you can license it at any time afterwards using the administrative interface.

Some of the features available on the PGP Universal Server can only be used if you have the appropriate license. These features include:

- Email proxying
- Virus scanning
- File blocking

To enable mail proxying, you must have a Gateway Email license. The PGP Universal Server can provide security for email messaging by inserting itself into the flow of email traffic in your network, intercepting, or proxying, that traffic, and processing it (encrypt, sign, decrypt, verify) based on the applicable policies.

You also have the option of licensing the Symantec AntiVirus™ Scan Engine feature, either while using the Setup Assistant or later using the administrative interface.

To license the Symantec AntiVirus feature, you will need both a license from PGP Corporation that includes support for the Symantec AntiVirus feature (this license is different from the standard PGP Universal Server license, which does not activate the Symantec AntiVirus feature) and a license from Symantec to enable virus scanning and LiveUpdate.

You should have received a Symantec AntiVirus serial number when you purchased your PGP Universal Server. Register that serial number with Symantec at http://licensing.symantec.com, and Symantec will email you a license file to enter through the Setup Assistant, or later through the AntiVirus interface.

If you have a license for the Symantec AntiVirus feature, you can also enable the File Blocking feature. File Blocking lets you block attachments that match any of the filenames you specify. For example, if a new virus application appears, you can quickly prevent it from entering your network using File Blocking.

License Changes for PGP Universal Server 2.5 and Later

The PGP Universal Server product line has been updated. The PGP Universal Server 100/200/500 family has been replaced with more flexible options. When you upgrade to PGP Universal Server 2.5 and later, your options are preserved but your license has been renamed. The following table explains how your previous PGP Universal Server license has changed:

2.0/9.0 License	2.6/9.6 License
PGP Whole Disk Encryption for Enterprises 9.0	PGP Universal Server 2.6 and PGP Whole Disk Encryption 9.6
PGP Universal Server 100 Gateway Email	PGP Universal Server 2.6 with PGP Gateway Email 2.6
PGP Universal Server 200 with PGP Desktop 9.0	PGP Universal Server 2.6 and PGP Desktop Email 9.6
PGP Universal Server 200 with PGP Desktop 9.0 and PGP Whole Disk Encryption	PGP Universal Server 2.6 and PGP Desktop Professional 9.6
PGP Universal Server 500 Gateway Mail with PGP Desktop 9.0	PGP Universal Server 2.6 with PGP Gateway Email 2.6, and PGP Gateway Email 2.6, and PGP Desktop Mail 9.6
PGP Universal Server 500 with PGP Desktop 9.0 and PGP Whole Disk Encryption	PGP Universal Server 2.6 with PGP Gateway Email 2.6 and PGP Whole Disk Encryption 9.6
PGP Universal Server 500 with PGP Whole Disk Encryption	PGP Universal Server 2.6 with PGP Gateway Email 2.6 and PGP Desktop Professional 9.6

PGP Universal Server is no longer being bundled with PGP Desktop. 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 Gateway Email to encrypt email in the mailstream.

Manual and Automatic Licensing

When you enter your license number, the PGP Universal Server will contact PGP Corporation's authorization servers to automatically authorize the license number. If your PGP Universal Server does not have an active connection to the Internet, you must contact PGP Support to acquire a manual authorization block.

> ! The PGP Universal Server must not be behind a proxy server, unless it is a transparent proxy, to receive licensing information automatically. If the PGP Universal Server is behind a proxy server, you will need to use manual license authorization.

Licensing a PGP Universal Server

Refer to "Licensing a PGP Universal Server" on page 368 for information about how to license a PGP Universal Server using the administrative interface.

Licensing the AntiVirus Feature

Refer to "AntiVirus Licensing" on page 170 for information about how to license the AntiVirus feature.

Licensing the File Blocking Feature

Refer to Chapter 21, "Blocking Files" for information about how to license the File Blocking feature.

Licensing the Mail Proxy Feature

You must have a PGP Universal Gateway Email license or you will not be able to use the Mail Proxies feature on the administrative interface. Refer to Chapter 22, "Configuring Mail Proxies" for information about the Mail Proxies feature.

10 Operating in Learn Mode

This chapter describes Learn Mode. When you finish configuring a PGP Universal Server using the Setup Assistant, it begins operation in Learn Mode.

In this mode, PGP Universal Servers with PGP Gateway Email proxy traffic normally but do not encrypt or sign any messages. PGP Universal Satellite also will not encrypt and sign mail when the PGP Universal Server is in Learn Mode.

ℹ You must license a PGP Universal Server before you can take it out of Learn Mode.

Topics include:

- "Purpose of Learn Mode"
- "Checking the Logs" on page 78
- "Managing Learn Mode" on page 78

Purpose of Learn Mode

Learn Mode has three purposes:

- It gives you a chance to see (by examining the logs) how the policies you established would affect email traffic if they were implemented.
- It allows the PGP Universal Server a chance to build its SMSA (creating keys for authenticated users, for example) so that when the server goes live—when Learn Mode is turned off—the server can immediately begin securing messages.
- It provides the PGP Universal Server a chance to identify mailing lists your users send messages to and add those mailing list addresses to the dictionaries of Excluded Email Addresses. It does this because you normally do not want to send encrypted messages to a mailing list.

  PGP Universal Server decrypts and verifies incoming email while operating in Learn Mode.

  PGP Universal Server still automatically detects mailing lists when Learn Mode is off, but unless the addresses were retrieved via the Directory Synchronization feature, they will require approval from the PGP Universal Server administrator to be added to the list of excluded email addresses. Refer to Chapter 17, "Using Dictionaries with Policy" for more information.

  Mailing lists are identified per RFC 2919, List-Id: A Structured Field and Namespace for the Identification of Mailing Lists, as well as by using default exclusion rules.

Checking the Logs

The effects of your policies can be checked while Learn Mode is on, even though the server isn't actually encrypting or signing messages.

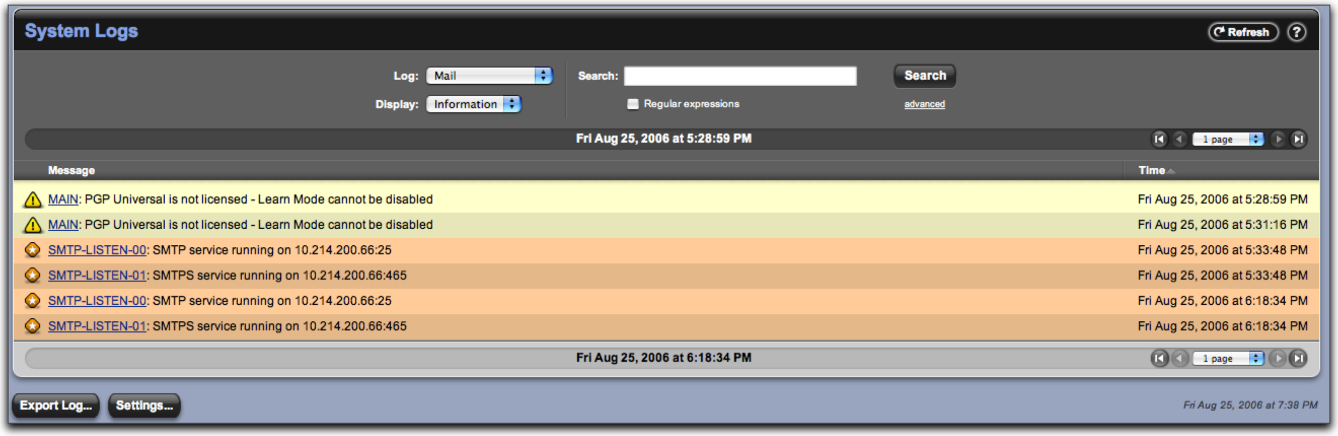
To check the server's logs:

1 Access the administrative interface for the server.

The administrative interface appears.

2 Click **Reporting**, then **Logs**.

The System Logs card appears.



System Logs

Log: Mail

Display: Information

Search:

□ Regular expressions

Fri Aug 25, 2006 at 5:28:59 PM

Message	Time
MAIN: PGP Universal is not licensed - Learn Mode cannot be disabled	Fri Aug 25, 2006 at 5:28:59 PM
MAIN: PGP Universal is not licensed - Learn Mode cannot be disabled	Fri Aug 25, 2006 at 5:31:16 PM
SMTP-LISTEN-00: SMTP service running on 10.214.200.66:25	Fri Aug 25, 2006 at 5:33:48 PM
SMTP-LISTEN-01: SMTPS service running on 10.214.200.66:465	Fri Aug 25, 2006 at 5:33:48 PM
SMTP-LISTEN-00: SMTP service running on 10.214.200.66:25	Fri Aug 25, 2006 at 6:18:34 PM
SMTP-LISTEN-01: SMTPS service running on 10.214.200.66:465	Fri Aug 25, 2006 at 6:18:34 PM

Fri Aug 25, 2006 at 6:18:34 PM

Fri Aug 25, 2006 at 7:38 PM

3 Check the logs to see what effect your policies are having on email traffic.

Managing Learn Mode

A PGP Universal Server is put into Learn Mode by the Setup Assistant. If your server is in learn mode, you will see a yellow icon, the **Change Mode** button, in the upper right corner of your browser screen.

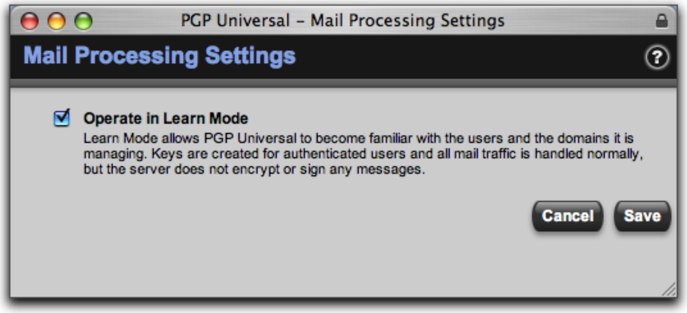
To turn Learn Mode off:

1 Access the administrative interface for the server.

The administrative interface appears.

2 Click the **Change Mode** button in the upper right corner of the screen.

The Mail Processing Settings dialog appears.



☑ **Operate in Learn Mode**
Learn Mode allows PGP Universal to become familiar with the users and the domains it is managing. Keys are created for authenticated users and all mail traffic is handled normally, but the server does not encrypt or sign any messages.

3 Clear the checkbox next to **Operate in Learn Mode**.

4 Click the **Save** button.

Learn Mode is turned off.

To turn Learn Mode on:

1 Access the administrative interface for the server.

The administrative interface appears.

2 Click the **Change Mode** button in the upper right corner of the screen.

The Mail Processing Settings dialog appears.

3 Put a check in the checkbox next to **Operate in Learn Mode**.

4 Click the **Save** button.

Learn Mode is turned on.

SECTION 4

Organization Information

This section describes how to manage the information that forms the basis of your Self-Managing Security Architecture, including your managed domains and your Organization Key. The section also describes options for recovering encrypted data.

11 Managed Domains

This chapter describes how to create and manage the internal domains for which your PGP Universal Server will protect email messages.

Topics in this chapter include:

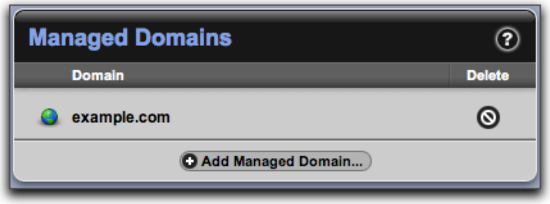
- "Overview"
- "Working with Managed Domains" on page 83

Overview

The Managed Domains card gives you control over the domains for which the PGP Universal Server is handling email.

> The Managed Domains card only appears on the administrative interface for Primary server in a cluster; it is not shown on Secondary servers.

Email users from domains being managed by your server are called "internal users." Conversely, email users from domains not being managed by your server but who are part of the SMSA are called "external users."



For example, if your company is "Example Corporation," you could have the domain "example.com" and your employees would have email addresses something like "jsmith@example.com."

If this were the case, you would want to establish "example.com" as a domain to be managed by your server. You use the Managed Domains card to do that.

Managed domains automatically include sub-domains, so in the example above, users such as "mingp@**corp**.example.com" would also be considered internal users. Multi-level domain structures as used by some countries are also acceptable: for example, the domain "example.co.uk."

The Managed Domains card accepts only Internet DNS domain names. WINS names (for example, \\EXAMPLE) and Notes domains (O=notes6@notes6) do not belong here.

Mail to and from your managed domains is processed according to your mail policy. You can also create mail policy rules specifically for your managed domains. See Chapter 15, "Setting Mail Policy" for more information on creating mail policies.

Managed domains entered on the Managed Domains card populate the Managed Domains dictionary. The dynamic Managed Domains dictionary automatically includes subdomains. See Chapter 17, "Using Dictionaries with Policy" for more information on dictionaries.

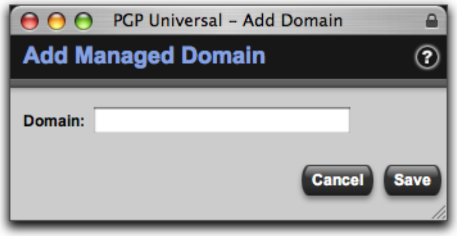
Working with Managed Domains

Adding Managed Domains

To add a domain to the list of managed domains:

1 Click **Add Managed Domain**.

The **Add Managed Domain** dialog appears.



2 Enter a domain name in the **Domain** field.

Do not enter WINS names (for example, \\EXAMPLE) and Notes domains (O=notes6@notes6) here. Enter only Internet DNS domain names.

3 Click **Save**.

Deleting Managed Domains

If you delete a managed domain, all the user IDs within that domain will remain in the system. Users will still be able to encrypt and sign messages with their keys.

To remove a domain name already on the list of managed domains:

1 Click the icon in the **Delete** column of the domain you want to remove from the list.

A confirmation dialog appears.

2 Click **OK**.

The confirmation dialog disappears and the selected domain name is removed from the list of managed domains.

12 Managing Organization Keys

This chapter describes the various keys and certificates you can configure and use with your PGP Universal Server.

Topics in this chapter include:

- "Overview"
- "Organization Key" on page 84
- "Organization Certificate" on page 88
- "Additional Decryption Key (ADK)" on page 93
- "Verified Directory Key" on page 95

Overview

There are multiple keys and certificates you can use with your PGP Universal Server:

- **Organization Key**. Used to sign all user keys the PGP Universal Server creates and to encrypt server backups.
- **Organization Certificate**. Required to support S/MIME environments.
- **Additional Decryption Key (ADK)**. Used to reconstruct messages if the recipient is unable or unwilling to do so. Every message encrypted to an external recipient by an internal user is also encrypted to the ADK, allowing the PGP administrator to decrypt any message sent by internal users, if required to do so by regulations or security policy.
- **Verified Directory Key.** Used to sign keys submitted to the PGP Verified Directory by external users.

The Organization Keys card gives you access to all of these.

Organization Key

Your Organization Key is used to sign all user keys the PGP Universal Server creates and to encrypt server backups. The Organization Key is what was referred to as the Corporate Key in the old PGP Keyserver environment.

You **must** make a backup of your Organization Key, in case of a problem with the server. That way, you can restore your server from a backup using the backup Organization Key.

Each PGP Universal Server is pre-configured with a unique Organization Key generated by the Setup Assistant. If you would like to use different settings for this key, you may regenerate the key with the settings you prefer. This should only be done prior to live deployment of the server or creation of user keys by the server.

The Organization Key will automatically renew itself one day before its expiration date. It will renew with all the same settings.

If you have multiple PGP Universal Servers in a cluster, the Organization Keys on the Secondary servers in the cluster will be synchronized with the Primary server in the cluster.

An Organization Key's identification is based on the name of the managed domain for which the key was created. Organization Keys by convention have one ID per managed domain so that they can be easily found via a directory lookup.

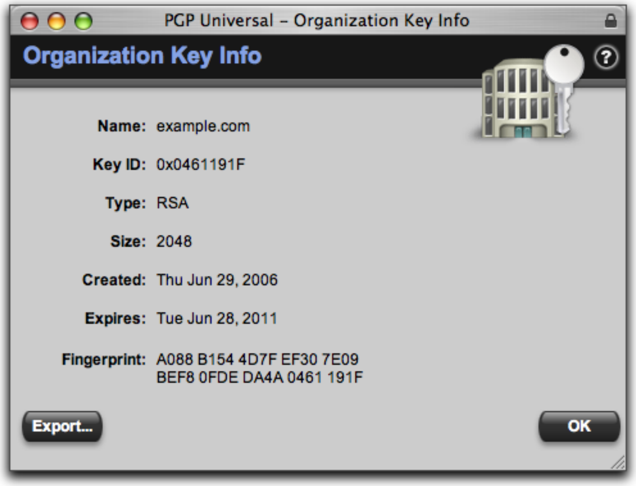
The Organization Key information includes the Public Keyserver URL, as specified on the Services>Keyserver page. Anytime the Public Keyserver URL changes, that information on the Organization Key will immediately change.

Inspecting the Organization Key

To inspect the properties of an Organization Key:

1 Click the name of the Organization Key.

The Organization Key Info dialog appears.



Name: example.com

Key ID: 0x0461191F

Type: RSA

Size: 2048

Created: Thu Jun 29, 2006

Expires: Tue Jun 28, 2011

Fingerprint: A088 B154 4D7F EF30 7E09 BEF8 0FDE DA4A 0461 191F

2 Inspect the properties of the Organization Key.

3 To export either just the public key portion of the Organization Key or the entire keypair, click the **Export** button and save the file to the desired location.

When you export the Organization Key you also get the Organization Certificate. You can use PGP Desktop to extract the Organization Certificate from the Organization Key.

4 Click the **OK** button.

The Organization Key Info dialog disappears.

If you are going to regenerate your Organization Key, you should use a fairly high bit size, such as 2048. However, if you are going to be using X.509 certificates and S/MIME, be aware that many clients only support up to 1024 bits; thus you may want to use 1024 bits for maximum compatibility with S/MIME. All PGP clients can be expected to support at least 4096 bits.

Regenerating the Organization Key

⚠ Changing the Organization Key makes all previous backups undecryptable and all of the validity signatures on the keys of internal users will be unverifiable until they are automatically renewed. *Only change the Organization Key if you fully understand the consequences of this action.*

❗ Changing the Organization Key deletes Ignition Keys. If you have hard or soft token Ignition Keys configured, regenerating the Organization Key will delete them. Deleting the Ignition Key stops PGP Universal Web Messenger from being stored encrypted.

ℹ The Organization Key signs all Trusted Keys and Certificates. If you regenerate the Organization Key, the signature on the Trusted Keys and Certificates becomes invalid. You must re-import all Trusted Keys and Certificates to have them signed by the new Organization Certificate. Refer to Chapter 13, "Managing Trusted Keys and Certificates" for more information on Trusted Keys.

To regenerate an Organization Key:

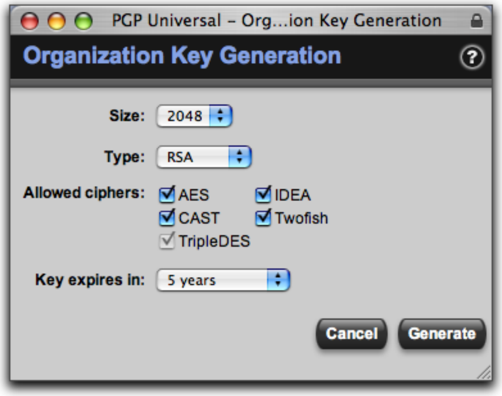
1 Click the Regenerate icon in the Action column of the Organization Key whose properties you want to change.

2 The following warning dialog appears:

Regenerating the Organization Key will cause problems with existing key signatures and backups. Any existing Ignition Keys and Organization Certificate will also be removed. Are you sure you want to proceed?

3 Click **OK**.

The Organization Key Generation dialog appears.



PGP Universal – Org...ion Key Generation

Organization Key Generation

Size: 2048

Type: RSA

Allowed ciphers: ☑ AES ☑ IDEA ☑ CAST ☑ Twofish ☑ TripleDES

Key expires in: 5 years

4 Make the desired changes to the properties of the Organization Key.

5 Click the **Generate** button.

The Organization Key Generation dialog disappears.

Importing an Organization Key

You also have the option of importing an existing PKCS #12 key and using that as your Organization Key.

Importing an Organization Key deletes Ignition Keys. If you have hard or soft token Ignition Keys configured, importing an Organization Key will delete them. Deleting the Ignition Key stops PGP Universal Web Messenger from being stored encrypted

To import an Organization Key:

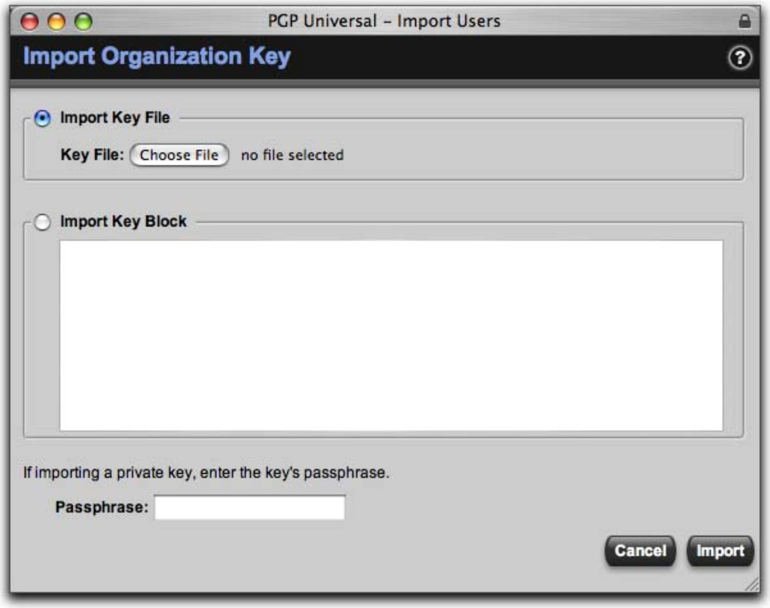
1 Click the icon in the Import column of the Organization Key row.

2 The following warning dialog appears:

Importing a new Organization Key will cause the current key (and Organization Certificate, if any) to be deleted, and will cause problems with existing key signatures and backups. Any existing Ignition Keys will also be removed. Are you sure you want to proceed?

3 Click **OK**.

The Import Organization Key dialog appears.



● Import Key File

Key File: no file selected

○ Import Key Block

If importing a private key, enter the key's passphrase.

Passphrase:

4 If you want to import a key that has been saved as a file, locate the file of the key you want to import using the **Browse** button.

Enter the passphrase for the key, if required.

5 If you want to import a key by cutting and pasting, copy the key you want to be your Organization Key to the Clipboard and paste it into the **Key Block** box.

6 Click the **Import** button.

The Import Organization Key dialog disappears. The Organization Key you imported appears in the Organization Key row.

Organization Certificate

An Organization Certificate is required for S/MIME support. You can only have one Organization Certificate attached to your Organization Key. You will not be able to restore from a backup with more than one Organization Certificate associated with your Organization Key.

The PGP Universal Server will automatically generate certificates as well as keys for new internal users created after you import or generate an Organization Certificate. All internal users will receive a certificate added to their keys within 24 hours. However, the old Organization Certificate will remain on users' keys until the certificate expires.

You have several options for dealing with Organization Certificates. You can:

- Create a self-signed Organization Certificate. Unfortunately, a self-signed Organization Certificate will not be universally recognized, so PGP Corporation recommends using a certificate from a recognized Certificate Authority (CA). Self-signed X.509 Organization Certificates are version 3.

- Create a Certificate Signing Request for a certificate authorized by an existing CA. When you receive the certificate back from the CA as a file, you will need to import that file.

  This certificate is a "subsidiary CA certificate," sometimes called a "subordinate CA." A CA delegates to the PGP Universal Server the right to issue certificates under the root CA's signing hierarchy, meaning the Basic Constraints certificate extension is *not* set.

- Import an existing certificate to use as your Organization Certificate. Imported X.509 certificates must be version 3.

To enable S/MIME support, the certificate of the issuing Root CA, and all other certificates in the chain between the Root CA and the Organization Certificate, are on the list of trusted keys and certificates on the Trusted Keys and Certificates card.

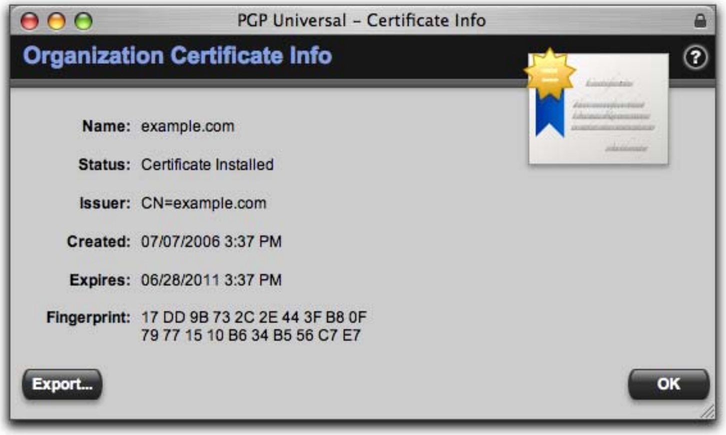
A self-signed Organization Certificate will have the same expiration date as the Organization Key, unless the Organization Key is set never to expire. If the Organization Key will never expire, the Organization Certificate will expire 10 years from the date you generate it. You must regenerate the Organization Certificate before it expires and distribute the new Certificate to anyone who uses your old Organization Certificate as a trusted root CA.

Inspecting the Organization Certificate

To inspect the settings of an Organization Certificate:

1. Click the name of the Organization Certificate.

   The Organization Certificate Info dialog appears.


PGP Universal – Certificate Info
Organization Certificate Info
?
Export...
OK

Name: example.com
Status: Certificate Installed
Issuer: CN=example.com
Created: 07/07/2006 3:37 PM
Expires: 06/28/2011 3:37 PM
Fingerprint: 17 DD 9B 73 2C 2E 44 3F B8 0F 79 77 15 10 B6 34 B5 56 C7 E7

2. Inspect the settings of the Organization Certificate.
3. Click **OK**.

Exporting the Organization Certificate

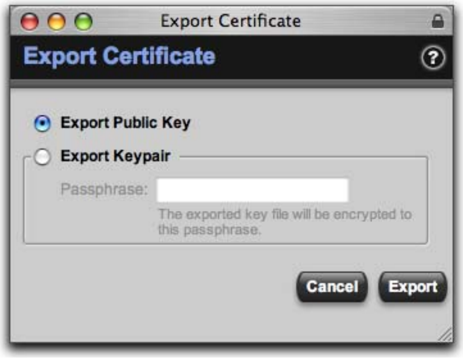
To export an Organization Certificate to a file:

1 Click on the Organization Certificate.

The Organization Certificate Info dialog appears.

2 Click **Export**.

The Export Certificate dialog appears.



● Export Public Key

○ Export Keypair

Passphrase:

The exported key file will be encrypted to this passphrase.

3 To export just the public key portion of the certificate, select **Export Public Key**.

4 To export the public and private key portions of the certificate, select **Export Keypair** and enter a passphrase that will be used to protect the private key once it is exported.

The resulting file will be PKCS #12 format.

5 Click the **Export** button.

6 At the prompt that appears, click **Save**.

7 Specify a name and location to save the file, then click **Save**.

The Organization Certificate Info dialog appears.

8 Click **OK**.

Deleting the Organization Certificate

To delete an Organization Certificate:

1 Click the icon in the Action column of the Organization Certificate.

A confirmation dialog appears.

2 Click **OK**.

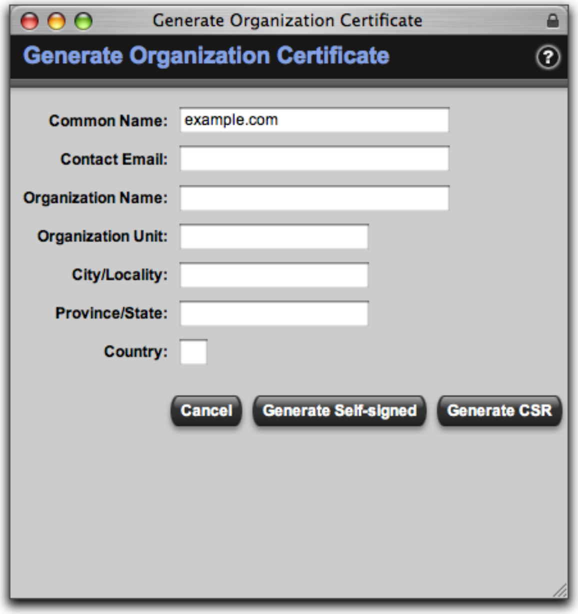
The Organization Certificate is deleted.

Generating the Organization Certificate

To create a Certificate Signing Request (CSR):

1 Click the icon in the Action column of the Organization Certificate row.

The Generate Organization Certificate dialog appears.



Generate Organization Certificate
Generate Organization Certificate
Cancel
Generate Self-signed
Generate CSR

Common Name:	example.com
Contact Email:	
Organization Name:	
Organization Unit:	
City/Locality:	
Province/State:	
Country:	

2 Enter a name for the certificate in the **Common Name** field.

3 Enter an email address in the **Contact Email** field.

4 Enter your organization's name in the **Organization Name** field.

5 Enter your organization's unit designation in the **Organization Unit** field.

6 Enter a city or locality, as appropriate, in the **City/Locality** field.

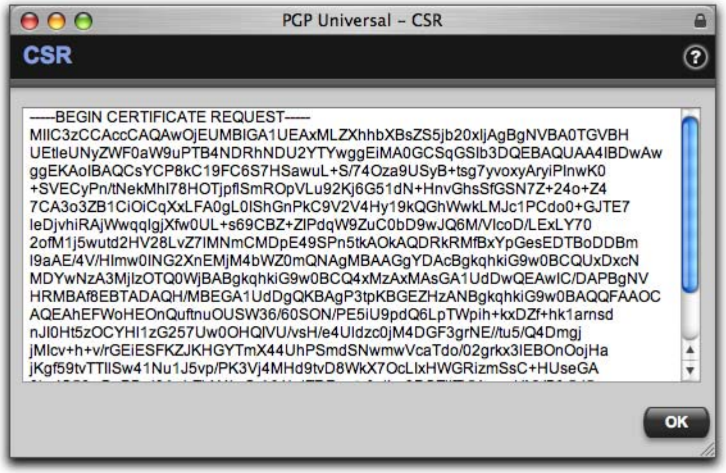
7 Enter a state or province, as appropriate, in the **Province/State** field.

8 Enter a country in the **Country** field.

9 If you want to generate a self-signed certificate, click **Generate Self-signed**. PGP Universal Server will generate a certificate. To generate a Certificate Request instead, go on to the next step.

10 Click the **Generate CSR** button.

The CSR dialog appears, showing the certificate request.



```
-----BEGIN CERTIFICATE REQUEST-----
MIIC3zCCAccCAQAwOjEUMBIGA1UEAxMLZXhhbXBsZS5jb20xljAgBgNVBA0TGVBH
UEtleUNyZWF0aW9uPTB4NDRhNDU2YTYwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
ggEKAoIBAQCsYCP8kC19FC6S7HSawuL+S/74Oza9USyB+tsg7yvoxyAryiPInwK0
+SVECyPn/tNekMhI78HOTjpflSmROpVLu92Kj6G51dN+HnvGhsSfGSN7Z+24o+Z4
7CA3o3ZB1CiOiCqXxLFA0gL0IShGnPkC9V2V4Hy19kQGhWwkLMJc1PCdo0+GJTE7
leDjvhiRAjWwqqlgjXfw0UL+s69CBZ+ZlPdqW9ZuC0bD9wJQ6M/VlcoD/LExLY70
2ofM1j5wutd2HV28LvZ7IMNmCMDpE49SPn5tkAOkAQDRkRMfBxYpGesEDTBoDDBm
l9aAE/4V/HImw0ING2XnEMjM4bWZ0mQNAgMBAAGgYDAcBgkqhkiG9w0BCQUxDxcN
MDYwNzA3MjIzOTQ0WjBABgkqhkiG9w0BCQ4xMzAxMAsGA1UdDwQEAwIC/DAPBgNV
HRMBAf8EBTADAQH/MBEGA1UdDgQKBAgP3tpKBGEZHzANBgkqhkiG9w0BAQQFAAOC
AQEAhEFWoHEOnQuftnuOUSW36/60SON/PE5iU9pdQ6LpTWpih+kxDZf+hk1arnsd
nJI0Ht5zOCYHI1zG257Uw0OHQlVU/vsH/e4UIdzc0jM4DGF3grNE//tu5/Q4Dmgj
jMIcv+h+v/rGEiESFKZJKHGYTmX44UhPSmdSNwmwVcaTdo/02grkx3IEBOnOojHa
jKgf59tvTTIlSw41Nu1J5vp/PK3Vj4MHd9tvD8WkX7OcLIxHWGRizmSsC+HUseGA
```

11 Copy the contents of the CSR dialog to a file, then click **OK**.

12 Paste the CSR into the appropriate field on your third-party CA interface.

The CA will send the certificate back to you when it has approved it.

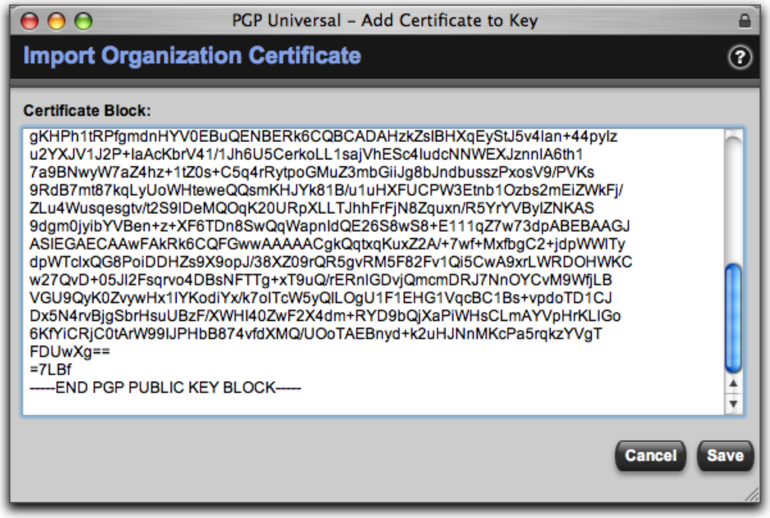
13 When you get the certificate from the CA, use the Import feature to import it as your Organization Certificate.

Importing the Organization Certificate

To import a certificate to be your Organization Certificate:

1 Click the icon in the Import column of the Organization Certificate row.

The Import Organization Certificate dialog appears.


PGP Universal – Add Certificate to Key
Import Organization Certificate
?
Cancel
Save

Certificate Block:

```
gKHPh1tRPfgmdnHYV0EBuQENBERk6CQBCADAHzkZsIBHXqEyStJ5v4Ian+44pylz
u2YXJV1J2P+IaAcKbrV41/1Jh6U5CerkoLL1sajVhESc4IudcNNWEXJznnIA6th1
7a9BNwyW7aZ4hz+1tZ0s+C5q4rRytpoGMuZ3mbGiiJg8bJndbusszPxosV9/PVKs
9RdB7mt87kqLyUoWHteweQQsmKHJYk81B/u1uHXFUCPW3Etnb1Ozbs2mEiZWkFj/
ZLu4Wusqesgtv/t2S9IDeMQOqK20URpXLLTJhhFrFjN8Zquxn/R5YrYVByIZNKAS
9dgm0jyibYVBen+z+XF6TDn8SwQqWapnIdQE26S8wS8+E111qZ7w73dpABEBAAGJ
ASIEGAECAAwFAkRk6CQFGwwAAAAACgkQqtxqKuxZ2A/+7wf+MxfbgC2+jdpWWlTy
dpWTclxQG8PoiDDHZs9X9opJ/38XZ09rQR5gvRM5F82Fv1Qi5CwA9xrLWRDOHWKC
w27QvD+05Jl2Fsqrvo4DBsNFTTg+xT9uQ/rERnIGDvjQmcmDRJ7NnOYCvM9WfjLB
VGU9QyK0ZvywHx1lYKodiYx/k7oITcW5yQlLOgU1F1EHG1VqcBC1Bs+vpdoTD1CJ
Dx5N4rvBjgSbrHsuUBzF/XWHI40ZwF2X4dm+RYD9bQjXaPiWHsCLmAYVpHrKLIGo
6KfYiCRjC0tArW99IJPHbB874vfdXMQ/UOoTAEBnyd+k2uHJNnMKcPa5rqkzYVgT
FDUwXg==
=7LBf
-----END PGP PUBLIC KEY BLOCK-----
```

2 Copy the certificate you want to be your Organization Certificate.

3 Paste the text into the Certificate Block box.

4 Click the **Save** button.

The Import Organization Certificate dialog disappears. The Organization Certificate you imported appears in the Organization Certificate row.

Additional Decryption Key (ADK)

An Additional Decryption Key (ADK) is a way to retrieve an email message if the recipient is unable or unwilling to do so and if required by regulation or security policy; every message sent by an internal user is also encrypted to the ADK. Messages encrypted to the ADK can be opened by the recipient and/or by the holder(s) of the ADK.

If you have an Additional Decryption Key uploaded, all outbound email will be encrypted to it when mail policy is applied. This setting appears in the *Send (encrypted/signed)* action and the setting cannot be disabled. Refer to Chapter 15, "Setting Mail Policy" for more information.

You can create an ADK with PGP Desktop, and then add it to your PGP Universal Server and use it. You can only have one ADK.

> S/MIME messages are not encrypted to the ADK.

If you use an ADK, PGP Universal Server adds the ADK to all new keys that it generates and all outbound email messages are automatically encrypted to it.

If you are going to use an ADK on your PGP Universal Server, you should import it prior to generating any user keys. You should also try to avoid changing to a different ADK later on, because doing so will result in some keys being associated with the old ADK and some with the new ADK. If you add or change an ADK, it will only be associated with the keys of new users. Existing users will not get that ADK added to their key.

Only PGP keys can be used as ADKs.

For information on using an ADK in a split key scenario, refer to the *PGP Desktop User's Guide*.

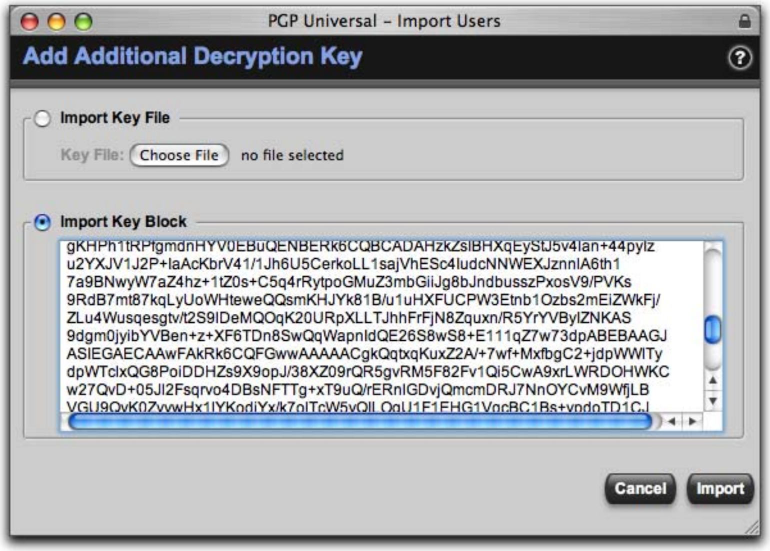
Importing the ADK

To import an ADK to your PGP Universal Server:

1 Copy the key of the ADK you are adding to the Clipboard using PGP Desktop.

2 Click the Add icon in the Action column of the Additional Decryption Key row.

The Add Additional Decryption Key dialog appears.



PGP Universal – Import Users

Add Additional Decryption Key

○ Import Key File

Key File: Choose File no file selected

● Import Key Block

```
gKHPh1tRPfgmdnHYV0EBuQENBERk6CQBCADAHzkZsIBHXqEyStJ5v4Ian+44pyIz
u2YXJV1J2P+IaAcKbrV41/1Jh6U5CerkoLL1sajVhESc4IudcNNWEXJznnIA6th1
7a9BNwyW7aZ4hz+1tZ0s+C5q4rRytpoGMuZ3mbGiiJg8bJndbusszPxosV9/PVKs
9RdB7mt87kqLyUoWHteweQQsmKHJYk81B/u1uHXFUCPW3Etnb1Ozbs2mEiZWkFj/
ZLu4Wusqesgtv/t2S9IDeMQOqK20URpXLLTJhhFrFjN8Zquxn/R5YrYVByIZNKAS
9dgm0jyibYVBen+z+XF6TDn8SwQqWapnIdQE26S8wS8+E111qZ7w73dpABEBAAGJ
ASIEGAECAAwFAkRk6CQFGwwAAAAACgkQqtxqKuxZ2A/+7wf+MxfbgC2+jdpWWITy
dpWTclxQG8PoiDDHZs9X9opJ/38XZ09rQR5gvRM5F82Fv1Qi5CwA9xrLWRDOHWKC
w27QvD+05JI2Fsqrvo4DBsNFTTg+xT9uQ/rERnIGDvjQmcmDRJ7NnOYCvM9WfjLB
VGU9QvK0ZvvwHx1IYKodiYx/k7oITcW5vQILOqU1F1FHG1VqcBC1Bs+vpdoTD1CJ
```

3 Paste the key of the ADK into the **Import Key Block** box.

4 Click the **Import** button.

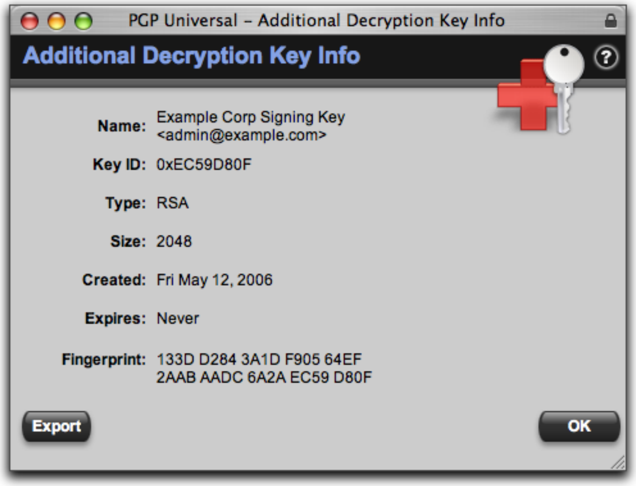
The Add Additional Decryption Key dialog disappears. The ADK you added appears in the Additional Decryption Key row.

Inspecting the ADK

To inspect the properties of an ADK:

1 Click the name of the ADK.

The Additional Decryption Key Info dialog appears.



PGP Universal – Additional Decryption Key Info

Additional Decryption Key Info

Name: Example Corp Signing Key <admin@example.com>

Key ID: 0xEC59D80F

Type: RSA

Size: 2048

Created: Fri May 12, 2006

Expires: Never

Fingerprint: 133D D284 3A1D F905 64EF 2AAB AADC 6A2A EC59 D80F

2 Inspect the properties of the ADK.

3 To export the ADK, click **Export** and save the file to the desired location.

4 Click the **OK** button.

The ADK Info dialog disappears.

Deleting the ADK

To delete an ADK:

All keys generated while the ADK was present will continue to reference the ADK even after you delete the ADK. The change will apply only to keys that are generated after the ADK is deleted.

1 Click the delete icon in the Action column of the ADK.

A confirmation dialog appears.

2 Click the **OK** button.

The ADK is deleted.

Verified Directory Key

The Verified Directory Key is the signing key for PGP Verified Directory users outside your managed domain. It must consist of both private and public keys. Once you choose the setting to allow external users to submit their keys through the PGP Verified Directory, you must upload a Verified Directory Key. External users will not be able to submit their keys to PGP Verified Directory until you have added the Verified Directory Key. Refer to Chapter 31, “Configuring the PGP Verified Directory” for information on the PGP Verified Directory.

If you have multiple PGP Universal Servers in a cluster, the Verified Directory Keys on the Secondary servers in the cluster will be synchronized with the Primary server in the cluster.

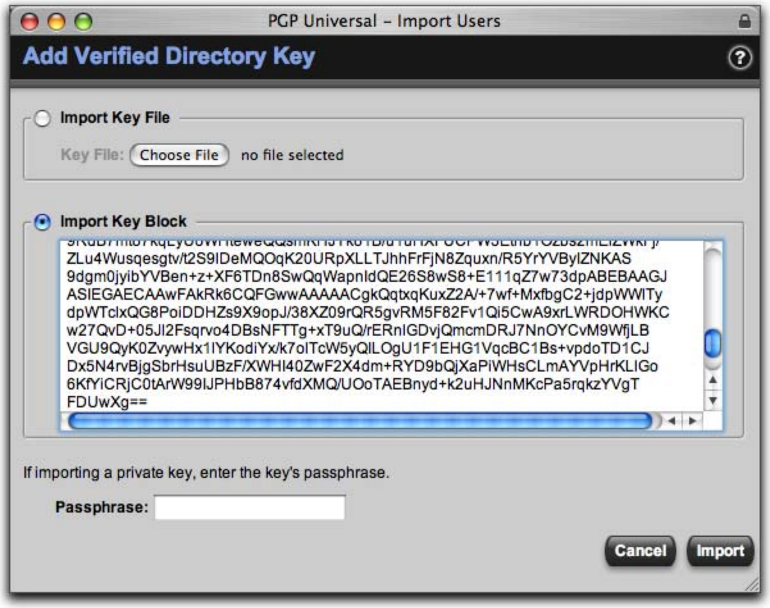
Importing the Verified Directory Key

To import a **Verified Directory Key** to your PGP Universal Server:

1 Copy the key of the **Verified Directory Key** you are adding to the Clipboard using PGP Desktop.

2 Click the **Add** icon in the **Action** column of the **Verified Directory Key** row.

The **Add Verified Directory Key** dialog appears.


PGP Universal – Import Users
Add Verified Directory Key
○ Import Key File
Key File: Choose File no file selected
● Import Key Block
Cancel
Import

```
ZLu4Wusqesgtv/t2S9IDeMQOqK20URpXLLTJhhFrFjN8Zquxn/R5YrYVByIZNKAS
9dgm0jyibYVBen+z+XF6TDn8SwQqWapnIdQE26S8wS8+E111qZ7w73dpABEBAAGJ
ASIEGAECAAwFAkRk6CQFGwwAAAAACgkQqtxqKuxZ2A/+7wf+MxfbgC2+jdpWWlTy
dpWTclxQG8PoiDDHZs9X9opJ/38XZ09rQR5gvRM5F82Fv1Qi5CwA9xrLWRDOHWKC
w27QvD+05JI2Fsqrvo4DBsNFTTg+xT9uQ/rERnIGDvjQmcmDRJ7NnOYCvM9WfjLB
VGU9QyK0ZvywHx1IYKodiYx/k7oITcW5yQILOgU1F1EHG1VqcBC1Bs+vpdoTD1CJ
Dx5N4rvBjgSbrHsuUBzF/XWHI40ZwF2X4dm+RYD9bQjXaPiWHsCLmAYVpHrKLIGo
6KfYiCRjC0tArW99IJPHbB874vfdXMQ/UOoTAEBnyd+k2uHJNnMKcPa5rqkzYVgT
FDUwXg==
```

If importing a private key, enter the key's passphrase.

Passphrase:

3 Paste the key of the Verified Directory Key into the **Import Key Block** box.

4 Enter in the private key **Passphrase**.

5 Click the **Import** button.

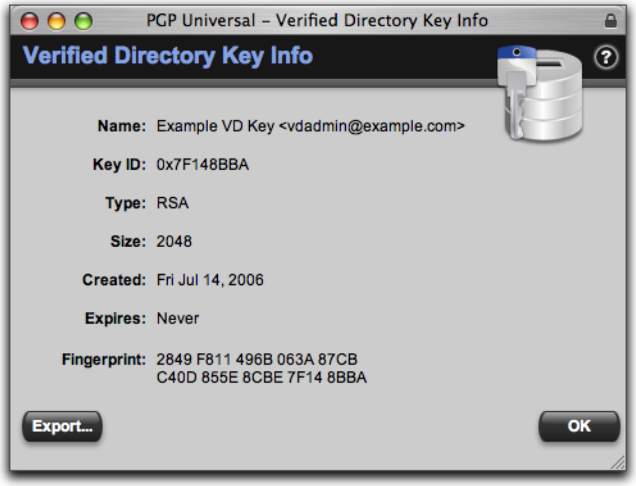
The **Add Verified Directory Key** dialog disappears. The **Verified Directory Key** you added appears in the **Verified Directory Key** row.

Inspecting the Verified Directory Key

To inspect the properties of the Verified Directory Key:

1 Click the name of the **Verified Directory Key**.

The **Verified Directory Key Info** dialog appears.


PGP Universal – Verified Directory Key Info
Verified Directory Key Info
?
Export...
OK

Name: Example VD Key <vdadmin@example.com>

Key ID: 0x7F148BBA

Type: RSA

Size: 2048

Created: Fri Jul 14, 2006

Expires: Never

Fingerprint: 2849 F811 496B 063A 87CB
C40D 855E 8CBE 7F14 8BBA

2 Inspect the properties of the Verified Directory Key.

3 To export the Verified Directory Key, click **Export**.

4 To export just the public key portion of the Verified Directory Key, select **Export Public Key**.

5 To export the public and private key portions of the key, select **Export Keypair** and enter a passphrase that will be used to protect the private key once it is exported.

6 Click the **OK** button.

Deleting the Verified Directory Key

To delete the Verified Directory Key:

1 Click the delete icon in the Action column of the Verified Directory Key.

A confirmation dialog appears.

2 Click the **OK** button.

13 Managing Trusted Keys and Certificates

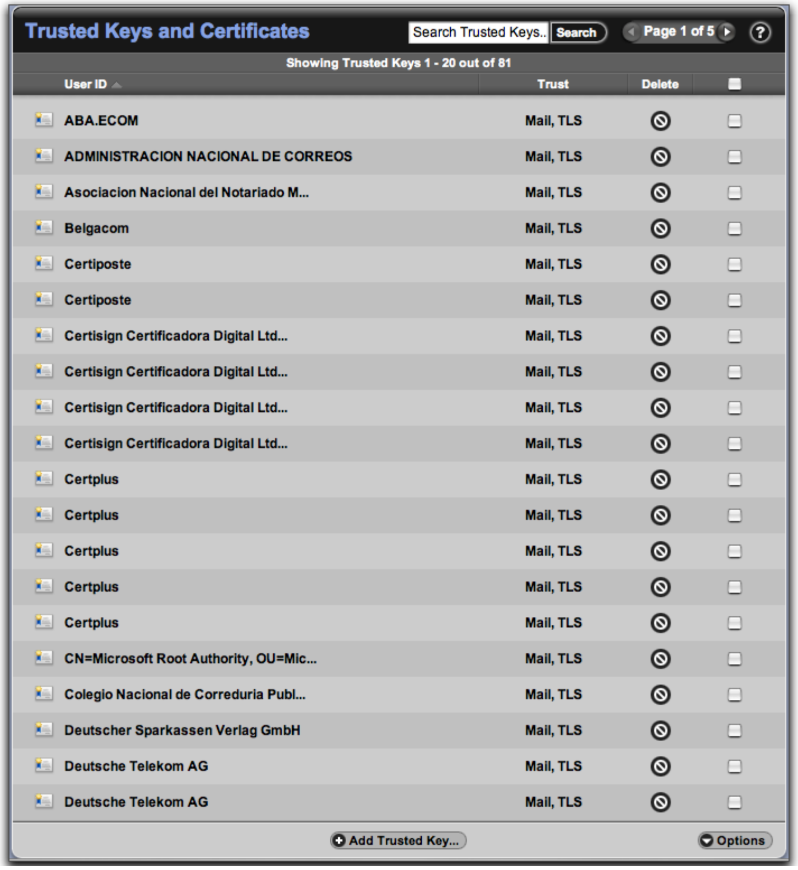
This chapter describes how trusted keys and certificates are used with your PGP Universal Server. You can find the list of trust keys at Organization>Trusted Keys.

Topics in this chapter include:

- "Overview"
- "Adding a Trusted Key or Certificate" on page 99
- "Inspecting and Changing Trusted Key Properties" on page 101
- "Deleting Trusted Keys and Certificates" on page 102
- "Searching for Trusted Keys and Certificates" on page 102

Overview

The Trusted Keys and Certificates card lists keys and certificates that are not part of the SMSA created by PGP Universal Server but which nevertheless you do trust.



Showing Trusted Keys 1 - 20 out of 81

User ID	Trust	Delete	□
ABA.ECOM	Mail, TLS	⊘	□
ADMINISTRACION NACIONAL DE CORREOS	Mail, TLS	⊘	□
Asociacion Nacional del Notariado M...	Mail, TLS	⊘	□
Belgacom	Mail, TLS	⊘	□
Certiposte	Mail, TLS	⊘	□
Certiposte	Mail, TLS	⊘	□
Certisign Certificadora Digital Ltd...	Mail, TLS	⊘	□
Certisign Certificadora Digital Ltd...	Mail, TLS	⊘	□
Certisign Certificadora Digital Ltd...	Mail, TLS	⊘	□
Certisign Certificadora Digital Ltd...	Mail, TLS	⊘	□
Certplus	Mail, TLS	⊘	□
Certplus	Mail, TLS	⊘	□
Certplus	Mail, TLS	⊘	□
Certplus	Mail, TLS	⊘	□
Certplus	Mail, TLS	⊘	□
CN=Microsoft Root Authority, OU=Mic...	Mail, TLS	⊘	□
Colegio Nacional de Correduria Publ...	Mail, TLS	⊘	□
Deutscher Sparkassen Verlag GmbH	Mail, TLS	⊘	□
Deutsche Telekom AG	Mail, TLS	⊘	□
Deutsche Telekom AG	Mail, TLS	⊘	□

Trusted Keys

In those cases where your PGP Universal Server cannot find a public key for a particular user on any of the keyservers you have defined as trusted, it will also search the default directories. If it finds a key in one of the default directories, it will trust (and therefore be able to use) that key only if it has been signed by one of the keys in the trusted keys list.

For example, if your company's law firm uses a PGP Corporate Signing Key (CSK), you could add this key as a trusted key. Then, if someone in your firm wants to send a message to someone at the law firm and the PGP Universal Server finds that person's key, signed by the law firm's CSK, in a default directory, then that key could be used by the server to securely send the message to the recipient at the law firm.

Trusted Certificates

PGP Universal Server can use S/MIME only if it has the root certificates from the CAs available to verify the client certificates. These CAs can be in your company or they can be an outside-managed CA, such as VeriSign.

To enable S/MIME support, the certificate of the issuing Root CA, and all other certificates in the chain between the Root CA and the Organization Certificate, are on the list of trusted keys and certificates on the Trusted Keys and Certificates card.

PGP Universal Server comes with information on many public CAs already installed on the Trusted Keys and Certificates card. Only in-house CAs or new public CAs that issue user certificates need to be manually imported. You can inspect, export (save on your machine), or delete the root certificates at any time.

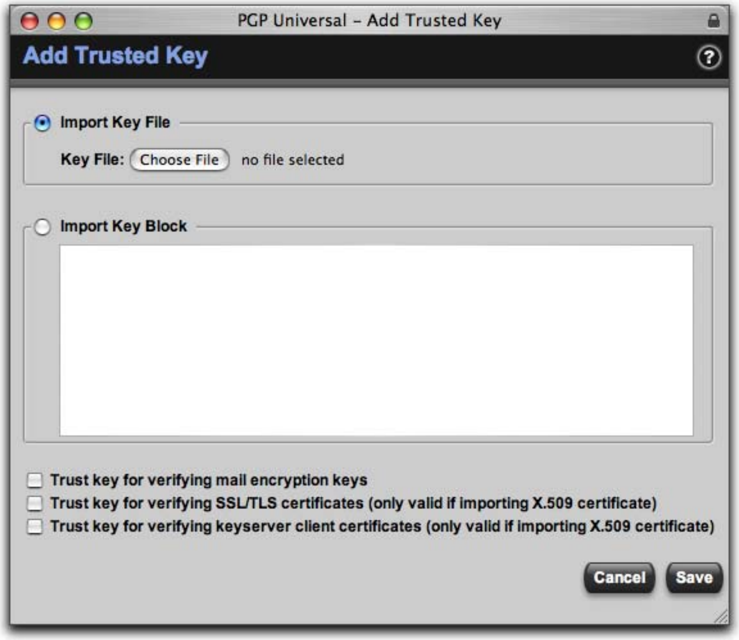
Trusted Certificates can be in any of the following formats: .cer, .crt, .pem and .p7b.

Adding a Trusted Key or Certificate

To add a trusted key or certificate:

1 On the **Trusted Keys and Certificates** card, click **Add Trusted Key**.

The **Add Trusted Key** dialog appears.



● Import Key File

Key File: no file selected

○ Import Key Block

□ Trust key for verifying mail encryption keys
□ Trust key for verifying SSL/TLS certificates (only valid if importing X.509 certificate)
□ Trust key for verifying keyserver client certificates (only valid if importing X.509 certificate)

2 To import a trusted key saved in a file, click **Choose File** in the Import Key File section, and choose the file on your system that contains the trusted key or certificate you want to add.

3 To import a key in key block format, paste the key block of the trusted key or certificate into the **Import Key Block** box (you will need to copy the text of the trusted key or certificate first to paste it).

4 If desired, put a check mark next to:

– **Trust key for verifying mail encryption keys**. Enable this option if you want to trust the key or certificate being added for the purpose of verifying signatures on keys from default keyservers.

– **Trust key for verifying SSL/TLS certificates (only valid if importing X.509 certificate)**. Enable this option if you want the X.509 certificate being added to be trusted for the purpose of verifying SSL/TLS certificates presented from remote SMTP/POP/IMAP mail servers.

– **Trust key for verifying keyserver client certificates (only valid if importing X.509 certificate)**. Enable this option if you want the X.509 certificate being added to be trusted for the purpose of verifying keyserver client authentication certificates.

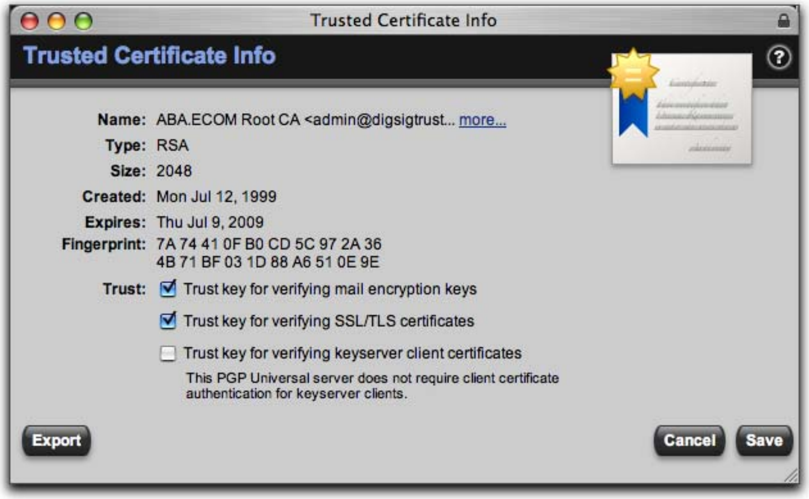
5 Click **Save**.

Inspecting and Changing Trusted Key Properties

To inspect or change the properties of a trusted key or certificate:

1 Click on the User ID (the name) of the trusted key or certificate whose properties you want to inspect in the list of trusted keys and certificates.

The **Trusted Key Info** dialog appears.



Name: ABA.ECOM Root CA <admin@digsigtrust... more...
Type: RSA
Size: 2048
Created: Mon Jul 12, 1999
Expires: Thu Jul 9, 2009
Fingerprint: 7A 74 41 0F B0 CD 5C 97 2A 36
4B 71 BF 03 1D 88 A6 51 0E 9E
Trust: ☑ Trust key for verifying mail encryption keys
☑ Trust key for verifying SSL/TLS certificates
□ Trust key for verifying keyserver client certificates
This PGP Universal server does not require client certificate authentication for keyserver clients.

2 Inspect the properties of the trusted key or certificate you selected. You may need to click **more** to see all the certificate data, which will appear in a pop-up dialog.

3 To export the trusted key, click **Export** and save the file to the desired location.

4 To change the properties of the trusted key or certificate, put a check mark next to:

– **Trust key for verifying mail encryption keys**. Enable this option if you want to trust the key or certificate being added for the purpose of verifying signatures on keys from default keyservers.

– **Trust key for verifying SSL/TLS certificates**. Enable this option if you want the X.509 certificate being added to be trusted for the purpose of verifying SSL/TLS certificates presented from remote SMTP/POP/IMAP mail servers.

– **Trust key for verifying keyserver client certificates**. Enable this option if you want the X.509 certificate being added to be trusted for the purpose of verifying keyserver client authentication certificates.

5 Click **Save**.

Deleting Trusted Keys and Certificates

To delete a trusted key or certificate:

1 Click the delete icon in the row of the trusted key or certificate you wish to delete.

A confirmation dialog appears.

2 Click **OK**.

The trusted key or certificate you specified is removed from the list.

Searching for Trusted Keys and Certificates

To find keys and certificates using search, enter the criteria for which you want to search, and click **Search**. A list of keys and certificates that fit the criteria you specified appears.

14 Recovering Encrypted Data in an Enterprise Environment

PGP Desktop together with PGP Universal Server securely encrypts data and email.

When enterprise-critical data is encrypted, the ability to recover data is necessary.

- How can data be recovered if an employee loses an encryption key, or forgets the key passphrase?
- How can data be recovered if it was encrypted for an employee, and the employee is unable or unwilling to perform the decryption?

When the original encryption key is not available, there are three techniques available to ensure that the enterprise can still access protected data:

- Key reconstruction.
- Recovery of the encryption key material.
- Decryption of the encrypted data using an special data recovery key, known as an Additional Decryption Key (ADK).

PGP Desktop, in conjunction with PGP Universal Server, supports four different key modes. Key modes affect which solutions are available for key reconstruction or recovery. The ADK is suitable for use with all key modes.

Choose the most appropriate solution for your enterprise data security needs.

- "Using Key Reconstruction" on page 104
- "Recovering Encryption Key Material without Key Reconstruction" on page 105
- "Using an Additional Decryption Key for Data Recovery" on page 107

Using Key Reconstruction

Enabling key reconstruction ensures that users can reconstruct their PGP keys. Refer to Chapter 28, "Configuring PGP Desktop Installations" for information on how to enable key reconstruction.

If you enable this option, when the user generates their key, a window appears requiring the user to enter five questions and five corresponding answers. Answers must contain at least six characters, which helps prevent attacks against the key reconstruction material.

Key reconstruction is useful if the user loses their key material, or forgets their key passphrase. To use key reconstruction, the user selects "Reconstruct Key" from the PGP Desktop Keys menu. The user will then be prompted to answer the key reconstruction questions; if they answer three of the five questions correctly, their key will be reconstructed and they can enter a new passphrase for the key.

Key reconstruction is not suitable for enterprise data recovery, since only the user knows the answers to the reconstruction questions.

Key reconstruction is only applicable for CKM, GKM, and SCKM keys. Refer to Chapter 26, “Setting Internal User Policy” for more information on key modes.

Recovering Encryption Key Material without Key Reconstruction

In some circumstances, key material can be recovered from PGP Universal Server without utilizing key reconstruction. It is sometimes possible to continue to use the key normally, or it may be necessary to generate a new key to be used going forward.

PGP Desktop, in conjunction with PGP Universal Server, supports four different key modes. The key mode affects how key recovery is performed.

Refer to Chapter 26, “Setting Internal User Policy” for more information on key modes.

Encryption Key Recovery of CKM Keys

CKM keys are created and managed by users. CKM keys are fully compatible with key reconstruction, but the encryption key material cannot be recovered in any other way. If reconstruction is not available, and the key material is lost or the passphrase is forgotten, the user will need to generate a new CKM key, and begin using that key. Any data recovery must then be accomplished with a data recovery key; refer to “Using an Additional Decryption Key for Data Recovery” on page 107.

Encryption Key Recovery of GKM Keys

Because the PGP Universal Server stores a copy of a GKM key, a user can download a new copy whenever needed. If the user loses their key (due, for example, to a hard disk failure or theft of the computer), they can download the backed-up copy of their key from PGP Universal Server, and continue to use it as before.

The GKM key stored by PGP Universal Server is encrypted using the user's passphrase. If the user has forgotten the passphrase, or is not available to provide the passphrase, it is not possible to recover the encryption key. Any data recovery must be accomplished with a data recovery key; refer to “Using an Additional Decryption Key for Data Recovery” on page 107.

Encryption Key Recovery of SCKM Keys

SCKM keys are generated and managed by users. However, the PGP Universal Server stores a passphraseless, unencrypted copy of the encryption key.

If a user has forgotten their passphrase or has lost their SCKM key material, the user will need to generate and use a new SCKM key.

Because PGP Universal Server keeps a copy of the old SCKM encryption key, you can use this key to decrypt data and email.

User Recovery of the Encryption Key for Email Decryption

When a user attempts to decrypt an email message encrypted to an old SCKM key, PGP Desktop automatically downloads a copy of this key and stores it locally. This process is transparent to the user, but does require that the user have connectivity to PGP Universal Server; the key is not stored permanently by the client.

This method of key recovery is only suitable for decrypting old email. Data cannot be decrypted with the key downloaded from PGP Universal Server.

User Recovery of the Encryption Key for Data Decryption

If a PGP Desktop user needs to recover data encrypted to their old SCKM key, or needs to decrypt email while disconnected from the PGP Universal Server, they must have a local copy of the old SCKM key in their keyring.

The encryption key can be recovered by the PGP Universal Server administrator, by following the following steps:

1. Export the old SCKM key from PGP Universal Server. Since the user has generated a new SCKM key, the old key should be considered revoked.
2. Import the old key into PGP Desktop.
3. Remove the signing subkey.
4. Change the key passphrase, and provide a strong passphrase.
5. Send to the user an email message containing the key.
6. Send the passphrase to the user. You can send the passphrase in an email message, because the email should be encrypted to the user's new SCKM key.
7. The user imports the key into their keyring, and changes the passphrase.

At this point the user will have a copy of the encryption key locally, and can use it off-line to decrypt both email and data.

Enterprise Recovery of the Encryption Key for Email or Data Decryption

If an enterprise needs to decrypt email or data encrypted for a user, they can recover the encryption key using a procedure similar to the one described in "User Recovery of the Encryption Key for Data Decryption" on page 106. Instead of sending the key to the user, the administrator uses the key with the administrator's own installation of PGP Desktop.

Encryption Key Recovery of SKM Keys

SKM keys are always stored on PGP Universal Server, and have no passphrase.

The PGP Universal Server administrator can export any user's SKM key and use it to decrypt messages encrypted for that user. SKM users do not need a key recovery process, because their keys are provided automatically by PGP Universal Server as needed for decrypting email.

SKM keys cannot be used for data encryption. Encryption key recovery of SKM keys is only required when email must be decrypted.

Since SKM keys are stored on the PGP Universal Server, they are only usable when a user has network connectivity to the PGP Universal Server.

Using an Additional Decryption Key for Data Recovery

The ADK (Additional Decryption Key) is only available in PGP Universal Server managed environments. The ADK provides a solution for enterprise data recovery that works with any user key mode. An ADK can be used to decrypt encrypted data and messages if an end user is unable or unwilling to do so.

An ADK is a normal PGP key created in PGP Desktop and uploaded to the PGP Universal Server. The ADK can be a split key, which requires multiple administrators to come together to reconstitute the key and use it for decryption. Refer to the *PGP Desktop User's Guide* for more information on creating keys.

When configured for use in a PGP Universal Server managed environment, all email is encrypted to the ADK as well as the email recipient's keys. The ADK is added as an authorized recipient when a PGP Zip file is created. When a PGP NetShare folder is created, the ADK is added as an authorized user key. In this manner, PGP-encrypted email messages and data encrypted by a user can be decrypted by an administrator in possession of the ADK.

Because the ADK is created the same way as any other key, the holder of the ADK can use it for email and data decryption, using the same method as for any other key in their possession. The holder of the ADK can decrypt any PGP-encrypted message, decrypt PGP Zip files, and access PGP NetShare protected files.

Refer to Chapter 12, "Managing Organization Keys" for more information on how to add an Additional Decryption Key.

SECTION 5

Managing Mail Processing

This section describes how to set up and manage mail processing.

You can control how your PGP Universal Server handles the email traffic in your environment: where it comes into the PGP Universal Server, how the server knows where the traffic came from, and where it's going, so that it can be processed correctly.

You can also set up mail policy to specify how email is processed, including encryption and decryption, on both PGP Universal Server and PGP Desktop.

15 Setting Mail Policy

This chapter describes mail policy, which determines how a PGP Universal Server handles email messages.

Policies are enforced on the PGP Universal Server with PGP Gateway Email, and at the desktop level with PGP Desktop Email. Even if your PGP Universal Server is not proxying and encrypting email in the mailstream, it is important to create secure mail policy, because PGP Desktop Email receives and enforces policy information from PGP Universal Server.

PGP Whole Disk Encryption and PGP NetShare are not affected by mail policy settings. If your PGP Universal Server is only managing these features, mail policy is not required.

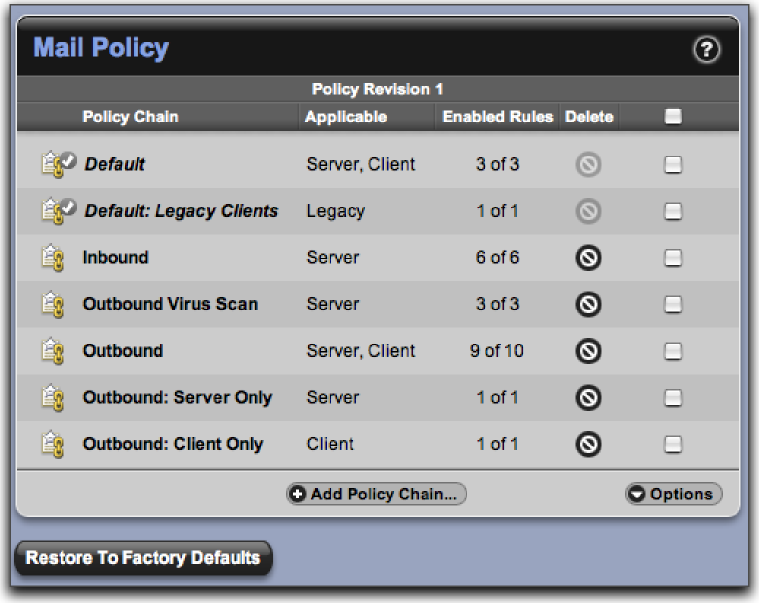
PGP Universal Web Messenger functionality is not available for use with a non-mailstream license.

Topics in this chapter include:

- "Overview"
- "Migrating Settings from Version 2.0.x" on page 113
- "Understanding the Pre-Installed Policy Chains" on page 113
- "Mail Policy Outside the Mailflow" on page 114
- "Building Valid Chains and Rules" on page 115
- "Using the Rule Interface" on page 118
- "Managing Policy Chains" on page 121
- "Managing Rules" on page 125
- "Adding Key Searches" on page 127
- "Choosing Condition Statements, Conditions, and Actions" on page 127
- "Working with Common Access Cards" on page 138

Overview

The PGP Universal Server processes email messages based on the policies you establish. Mail policy applies to inbound and outbound email for both PGP Universal Server traffic and email processed by PGP client software. Mail policy consists of multiple policy chains, comprised of sequential mail processing rules, which appear on the Mail Policy card.



Mail Policy

Policy Revision 1

Policy Chain	Applicable	Enabled Rules	Delete	□
Default	Server, Client	3 of 3	⊘	□
Default: Legacy Clients	Legacy	1 of 1	⊘	□
Inbound	Server	6 of 6	⊘	□
Outbound Virus Scan	Server	3 of 3	⊘	□
Outbound	Server, Client	9 of 10	⊘	□
Outbound: Server Only	Server	1 of 1	⊘	□
Outbound: Client Only	Client	1 of 1	⊘	□

The Mail Policy card lets you change the settings of the default mail policy chains, and add and edit policy chains and rules. It allows you detailed granular control of all aspects of mail processing.

If your PGP Universal Server is in gateway placement and your users do not have PGP client software installed, then mail policy will be applied only to messages sent to recipients outside the managed domain. Messages sent from internal users to internal users will not pass through the PGP Universal Server, so the policy will not be applied.

If your mail policy requires Smart Trailer and/or PGP Universal Web Messenger service, you must enable PGP Universal Web Messenger service. See Chapter 30, “Configuring PGP Universal Web Messenger” for more information on configuring PGP Universal Web Messenger.

Refer to Chapter 16, “Applying Key Not Found Settings to External Users” for information on how mail policy settings appear to external users, and how external users interact with Smart Trailer and PGP Universal Web Messenger.

If you upgrade from PGP Universal Server 2.0.x, your policy settings will be automatically replicated in the new mail policy. Refer to “Migrating Settings from Version 2.0.x” on page 113 to understand how your previous policy settings are replicated.

How Policy Chains Work

Mail policy refers to the entire set of chains and rules as a whole. Individual policy chains process different kinds of email; for example, inbound or outbound mail. Each rule in a policy chain is one step in processing a message.

- **Policy chains** determine how messages are processed. Chains are made up of sequences of rules. A message may pass through more than one policy chain during processing.
- **Rules** consists of sets of conditions and actions. Messages pass through the rules in a chain in order until the message comes to a rule that applies. If the conditions for the rule are met by a message, the rule takes effect. If the conditions of a rule are not met by a message, the message is passed to the next rule in the chain.
- **Conditions** are the set of requirements a message must meet to trigger a rule. If a message meets the conditions, the associated actions are performed on the message. See "Conditions" on page 129 for a complete list of possible conditions.
- **Groups** are sets of one or more conditions, linked together by statements about the Conditions. For example, rule can have a group of conditions that are all required to be true for the rule to be triggered. See "Condition Statements" on page 127 for a complete list of possible condition statements.
- **Condition statements** link together conditions into groups, and specify how conditions should be matched. For example, if you have more than one condition in a rule, you can specify that the rule is triggered if all of the conditions are matched, or you can specify that the rule is triggered if only one of the conditions is matched.
- **Actions** are processes performed on messages when rule conditions apply. Actions applied to a message may include encryption, virus scanning, or simply passing the message along to another policy chain. See "Actions" on page 132 for a complete list of possible actions.

Mail Policy and Dictionaries

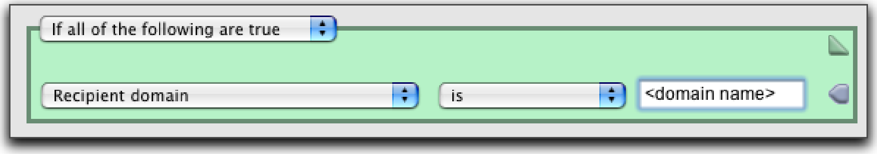
Dictionaries are lists of terms to be matched. Dictionaries work with mail policy to allow you to define content lists that can trigger rules or fulfill the conditions of a rule to trigger actions. For example, dictionaries can contain addresses you want excluded from processing, key words like "confidential," or user names for internal users whose messages need special handling.

A policy rule can have a dictionary associated with it as part of a condition. If a message meets the condition, PGP Universal Server processes the message according the rule's actions. For example, one of the default Outbound rules is called Excluded Signed. The condition for that rule is "If any of the following are true: Recipient address is in dictionary *Excluded Addresses: Sign*." This means the rule applies to any message in which the recipient address matches a term in the dictionary. If that condition is met, the action for the rule is triggered. The action is to sign and send the message with no further processing.

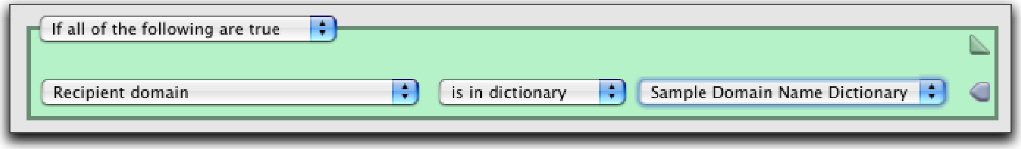
To learn which conditions can be used with dictionaries, refer to "Choosing Condition Statements, Conditions, and Actions" on page 127.

Consider whether the use of a dictionary in your rule is appropriate. There are several different ways to create a rule condition that contains matchable terms. Sometimes you will want to add a single matchable term or pattern directly in the condition itself. Sometimes you will need to use a dictionary instead. If you want your condition to look for matches to multiple terms, it is more appropriate to create a dictionary.

For example, you need to create a rule that applies only to email going to specific recipient domains. If you want the rule to apply only to email to one specific domain, you create the condition as follows:


If all of the following are true
Recipient domain is <domain name>

If you want the rule to apply to email going to many different recipient domains, use a dictionary. From the Policy>Dictionaries card, create a dictionary listing all of the domain names as matchable literal terms. When you create the rule on the policy chain, you can then select that dictionary from a drop-down list. The condition would be:


If all of the following are true
Recipient domain is in dictionary Sample Domain Name Dictionary

Refer to Chapter 17, "Using Dictionaries with Policy" to learn how to create dictionaries.

Mail Policy and Key Searches

External domains sometimes have publicly accessible keyservers containing users' public keys (in a PGP keyserver or an X.509 directory).

Mail policy contains rules that require a message be signed or encrypted to a recipient's key. The PGP Universal Server will always look in its own databases for keys in the Internal Users, External Users, and Key Cache lists. If the PGP Universal Server does not have a copy of a particular key, the policy may then specify searching external sources for the key.

Refer to Chapter 18, "Keyservers, SMTP Servers, and Mail Policy" for more information about how keyserver searches work with mail policy. See "Adding Key Searches" on page 127 to learn how to add searchable keyservers to rules.

Mail Policy and Cached Keys

Public keys for remote users are automatically cached on the PGP Universal Server on the System>Key Cache card. Whenever the PGP Universal Server can harvest a key from the mailflow, the key is stored in the key cache. As long as the key is in the key cache, it can be used to encrypt future email, without requiring a key search.

Whenever email processing requires a remote user key, the PGP Universal Server can automatically search for remote user keys in the cache for any keyserver that you have added to the rule. If you add a keyserver to a rule's Key Search tab, all cached keys from that server are available. If you delete a keyserver from a rule, the rule can no longer use the cached keys from that keyserver to encrypt mail.

Refer to Chapter 19, "Managing Keys in the Key Cache" for more information on cached keys. Refer to Chapter 18, "Keyservers, SMTP Servers, and Mail Policy" for more information on keyservers.

Migrating Settings from Version 2.0.x

If you upgrade from PGP Universal Server 2.0.x, your proxy and external domain policy settings will be automatically replicated in the new mail policy. This section explains the changes in mail policy in PGP Universal Server.

The new mail policy provides many more ways of processing email than the previous version. In the previous version, you created a policy for each external domain. Now mail policy applies to all email traffic to and from all domains, although you can apply special handling to messages to or from certain domains or subdomains.

There is no longer an implicit managed domain policy. Now, all mail policy is clearly and explicitly described and controlled.

You can apply mail policy to email based on many criteria through the creation of rules. Previously, you could only apply policy based on domain name. Now you can match on header, subject, sensitivity, or sender email ID, as well as many other options.

You can process email in many ways. The old external domain policy only permitted you to specify that email be encrypted and signed or sent clear. Now you can specify that email should be bounced, dropped, or scanned for viruses, for example.

Refer to the *PGP Universal Server Upgrade Guide* to learn how to reproduce the old settings manually.

Understanding the Pre-Installed Policy Chains

This section describes the pre-installed policy chains for a new, non-migrated, PGP Universal Server installation. The pre-installed policy chains provide the PGP Universal Server and PGP Desktop with rules for processing email. You can edit any of these policy chains, but you should make sure that you understand each of the processing functions the chains provide before you change them. This section provides an overview of each pre-installed chain, but you should examine the chains as installed on the PGP Universal Server for more details.

- **Default**: This is the starting point for the mail policy. This chain specifies how to evaluate all messages and route them to the next appropriate policy chain for processing. All messages start processing here, and are routed to the *Inbound*, *Outbound*, or *Outbound Virus Scan* chains. Because this is the root policy chain for the entire mail policy, it cannot be deleted. The rules in this chain apply to messages processed by both PGP Universal Server and PGP Desktop.

- **Default: Legacy Client**: This policy chain provides mail policy support for 9.0.x legacy client software. This policy chain cannot be deleted. Refer to "Supporting Legacy Client Software" on page 408 for more information.
- **Inbound**: This policy chain describes how to process inbound messages to users inside the managed domains. The primary function of this policy chain is to decrypt messages, then drop virus-infected messages and deliver clean messages to the user. This is the final chain in processing inbound email. Messages are routed to this chain by the *Default* chain. The rules in this chain apply to messages processed by the PGP Universal Server.
- **Outbound Virus Scan**: This policy chain specifies how to scan email for viruses, then bounce infected email or pass clean messages to the *Outbound* chain. Messages are routed to this chain by the *Default* chain. The rules in this chain apply only to messages processed by the PGP Universal Server.
- **Outbound**: This policy chain contains processing rules for email to external users, excluded addresses, and PGP Universal Web Messenger users. The policy chain also requires the encryption of sensitive email. Any email that is not processed according to these rules is passed along to the *Outbound: Server Only* or *Outbound: Client Only* chains for further processing. The rules in this chain apply to messages processed by both PGP Universal Server and PGP Desktop.
- **Outbound: Server Only**: If the email has not yet been processed and sent, then the final rule in this list completes processing and sends the email. The rules in this chain apply only to messages processed by the PGP Universal Server.
- **Outbound: Client Only**: If the email has not yet been processed and sent, then the final rule in this list completes processing and sends the email. The rules in this chain apply to messages processed by PGP Desktop.

Mail Policy Outside the Mailflow

If your PGP Universal Server is outside the mailflow on your network, mail policy cannot be enforced at the network level. However, you can enforce mail policy on client PGP software. PGP Desktop installations bound to your PGP Universal Server will receive client policy information from that server. Any policy chain marked as applicable to client software is enforced by the installed client application.

Refer to "Creating PGP Desktop Installers" on page 244 for more information on creating PGP Desktop installations bound to your PGP Universal Server.

Building Valid Chains and Rules

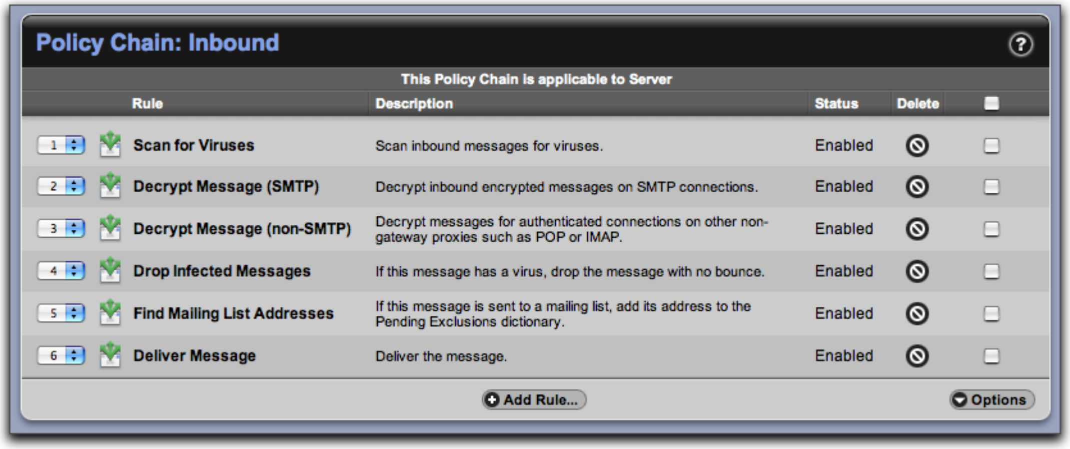
Carefully plan and diagram the entire set of chains and rules before you begin creating mail policy on the PGP Universal Server. Once you have created your mail policy, test it before you implement it in your network. The PGP Universal Server will not prevent you from creating chains that contradict each other or invalid rules. There are many things to think about when creating policy chains and rules.

- When you create a policy chain, organize the policy chains and rules in the correct order.
- Make sure you understand how to use condition settings, conditions, and actions to create valid rules.
- Ensure every email type that needs special processing is covered by a rule that applies; for example, confidential email or email to specific recipients. Refer to "Conditions" on page 128 for a list of possible rule conditions.
- Do not allow email to drop through the end of your policy chains. Make sure that for every message that passes through mail policy, there is a rule with an action that finishes processing by sending, delivering, bouncing, or dropping the email. Refer to "Actions" on page 132 for a list of actions that finish processing.

Using Valid Processing Order

Within a chain, some rules process email and then pass the email along to other actions or rules for further processing; for example, *Scan for viruses*. Other rules end email processing; for example, *Deliver Message*. When constructing a rule or chain of rules, make sure that actions that finish email processing come after the actions that allow continued processing.

The sample policy chain below is an example of invalid processing order. The *Scan for Viruses* rule is before the *Decrypt Message* rules, so that virus scanning is done on encrypted email. This means that PGP Universal Server cannot detect infected messages.



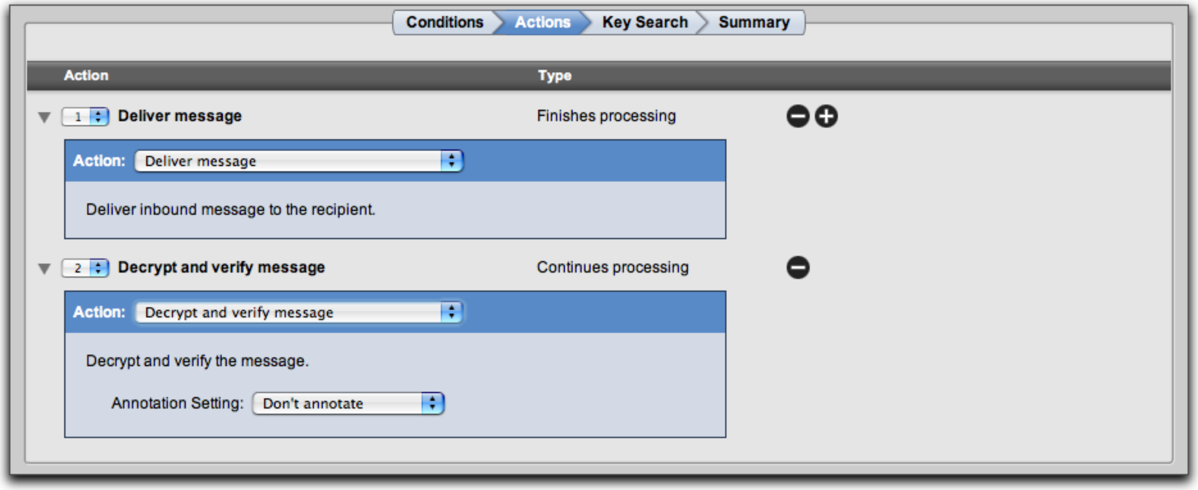
Policy Chain: Inbound

This Policy Chain is applicable to Server

	Rule	Description	Status	Delete	□
1	Scan for Viruses	Scan inbound messages for viruses.	Enabled	⊘	□
2	Decrypt Message (SMTP)	Decrypt inbound encrypted messages on SMTP connections.	Enabled	⊘	□
3	Decrypt Message (non-SMTP)	Decrypt messages for authenticated connections on other non-gateway proxies such as POP or IMAP.	Enabled	⊘	□
4	Drop Infected Messages	If this message has a virus, drop the message with no bounce.	Enabled	⊘	□
5	Find Mailing List Addresses	If this message is sent to a mailing list, add its address to the Pending Exclusions dictionary.	Enabled	⊘	□
6	Deliver Message	Deliver the message.	Enabled	⊘	□

Within a rule, processing order is important to actions as well. Make sure that actions that finish processing come after actions that continue processing.

In the example below, *Deliver message* is before *Decrypt and verify message*, so messages would be sent out without being decrypted.



1 Deliver message — Finishes processing

Action: Deliver message

Deliver inbound message to the recipient.

2 Decrypt and verify message — Continues processing

Action: Decrypt and verify message

Decrypt and verify the message.

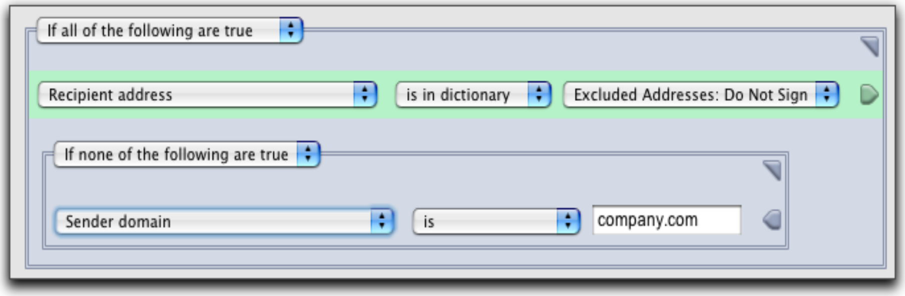
Annotation Setting: Don't annotate

Creating Valid Groups

It is important to pay attention to how your condition settings work, especially if you have nested groups.

In the example below, for the condition to be matched and the rule triggered, there are two things that must be true. The first condition setting states everything it applies to must be true. The first condition setting applies to a condition statement about the recipient address and to a nested group, both of which must be true. The second condition setting states everything it applies to must not be true. The second condition setting applies to a condition statement about the sender domain, which must not be true.

In other words, it must be true that the recipient address is in the *Excluded Addresses: Do Not Sign* dictionary, and it must be true that the *Sender Domain* is not company.com.



If all of the following are true

Recipient address — is in dictionary — Excluded Addresses: Do Not Sign

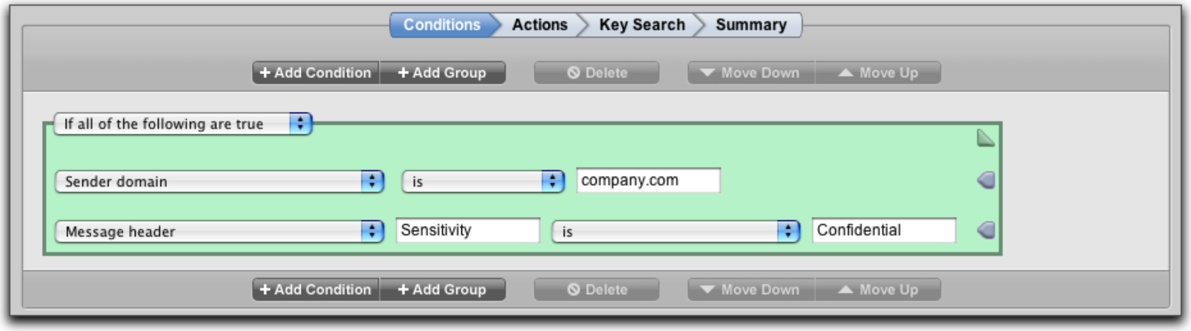
If none of the following are true

Sender domain — is — company.com

Creating a Valid Rule

The following example shows how to create a valid rule. This sample rule applies to any email with a Sensitivity header sent to anyone in a specific domain.

The condition setting requires that all conditions be true to trigger the action. The first condition that must be true is that the email must be from senders in the company.com domain.The second condition that must be true is that the message header called *Sensitivity* must be the key word *Confidential*.

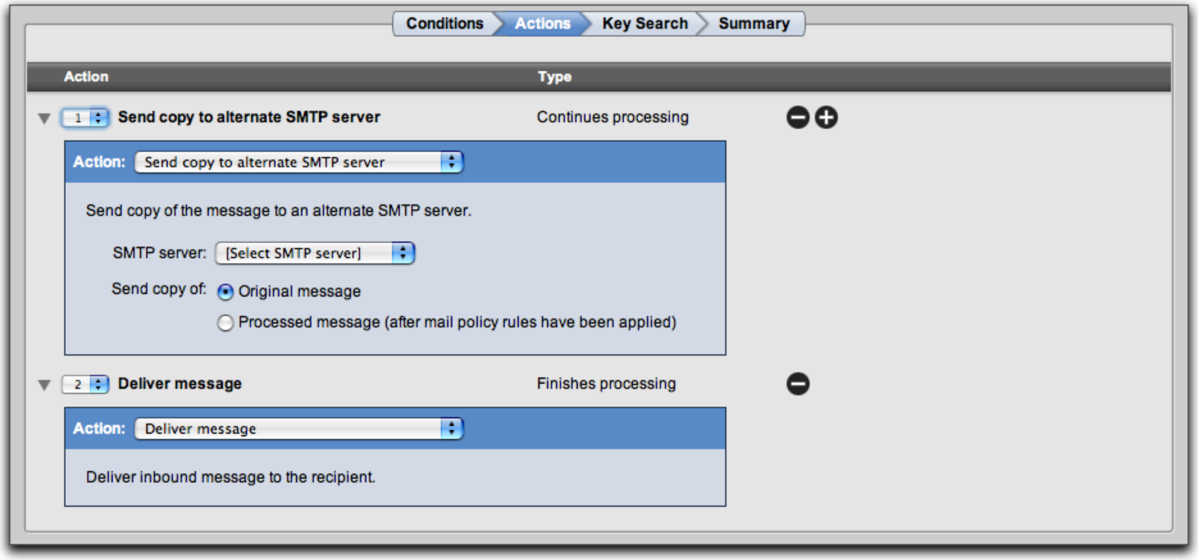


If all of the following are true

Sender domain | is | company.com

Message header | Sensitivity | is | Confidential

The rule action first sends a copy of the message to an SMTP server for archiving. The second action delivers the message. Notice that the action that finishes processing is last. If the action *Deliver message* comes first, the rule *Send copy to alternate SMTP server* cannot be performed.



Action	Type
1 Send copy to alternate SMTP server	Continues processing
2 Deliver message	Finishes processing

Action: Send copy to alternate SMTP server

Send copy of the message to an alternate SMTP server.

SMTP server: [Select SMTP server]

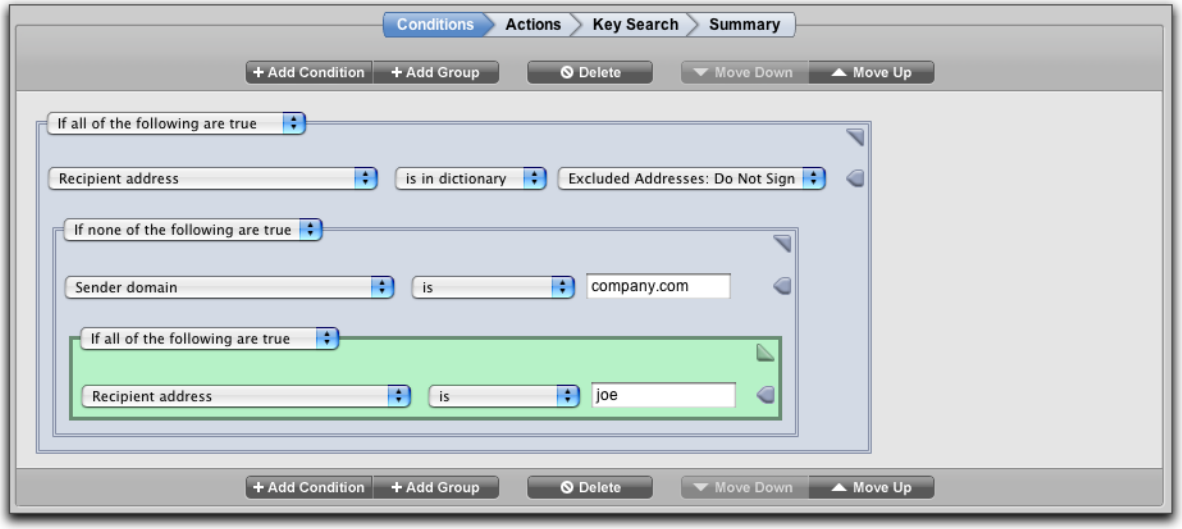
Send copy of: ● Original message
○ Processed message (after mail policy rules have been applied)

Action: Deliver message

Deliver inbound message to the recipient.

Using the Rule Interface

The rule interface has a set of arrows and buttons to help you arrange conditions and actions. When you add or edit a rule, the rule interface will display the **Conditions** card first.



If all of the following are true
Recipient address | is in dictionary | Excluded Addresses: Do Not Sign
If none of the following are true
Sender domain | is | company.com
If all of the following are true
Recipient address | is | joe

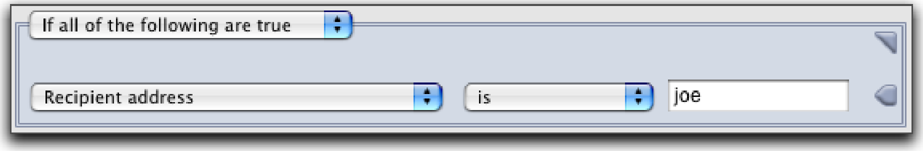
1. Once you have finished creating conditions, click the **Actions** arrow button to open the **Actions** card and add actions to the rule. See "The Actions Card" on page 120.
2. Next, click the **Key Search** arrow button to add searchable keyservers to the rule, if necessary. See "Adding Key Searches" on page 127 for more information on key searches.
3. To see a summary of the entire rule, click the **Summary** arrow button.

The Conditions Card

This section describes how to use the interface to create, add, or delete groups and conditions for your rules. Refer to "Building Valid Chains and Rules" on page 115 for information on how to build valid, well-constructed, logic rules for your mail policy.

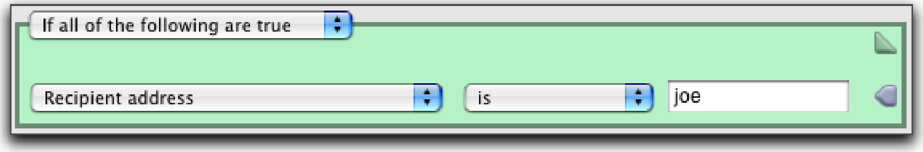
Selecting Groups

This is what an unselected group looks like. Notice that the group box is blue and the triangle in the upper right corner points away from the condition.



If all of the following are true
Recipient address | is | joe

You cannot add conditions to a group until you select the group. To select the group, click the triangle in the upper right corner. The selected group will turn green and the triangle will point toward the condition. You can now delete the group or add more conditions or groups.


If all of the following are true

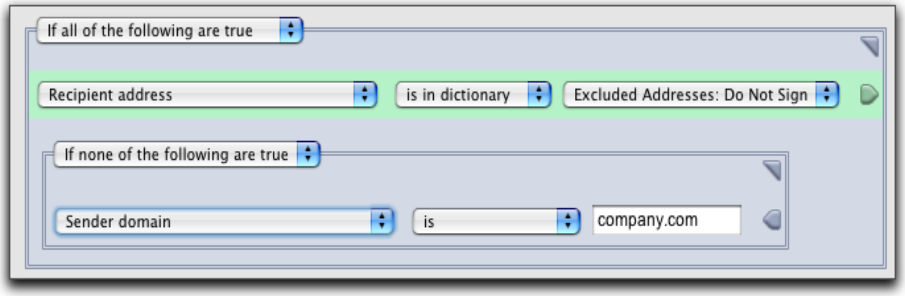
Recipient address | is | joe

Adding Groups or Conditions

To add a condition or group to the selected group, click the **Add Condition** or **Add Group** button.

If you click the **Add Group** button, another group will appear nested inside the group you originally selected. In the example below, for the condition to be matched and the rule triggered, the recipient address must be in the *Excluded Addresses: Do Not Sign* dictionary, and the *Sender Domain* must not be company.com.

You can nest up to 10 levels of groups or conditions.


If all of the following are true

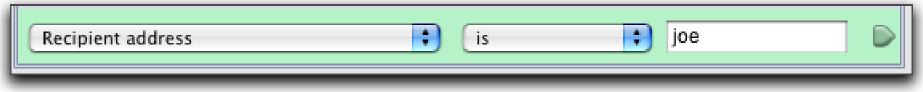
Recipient address | is in dictionary | Excluded Addresses: Do Not Sign

If none of the following are true

Sender domain | is | company.com

Selecting Conditions

To select a condition, click the arrow at the end of the condition. When the condition is selected, the arrow will point away from the condition and the condition background will be green. You cannot delete a condition until you select it.


Recipient address | is | joe

Deleting Groups or Conditions

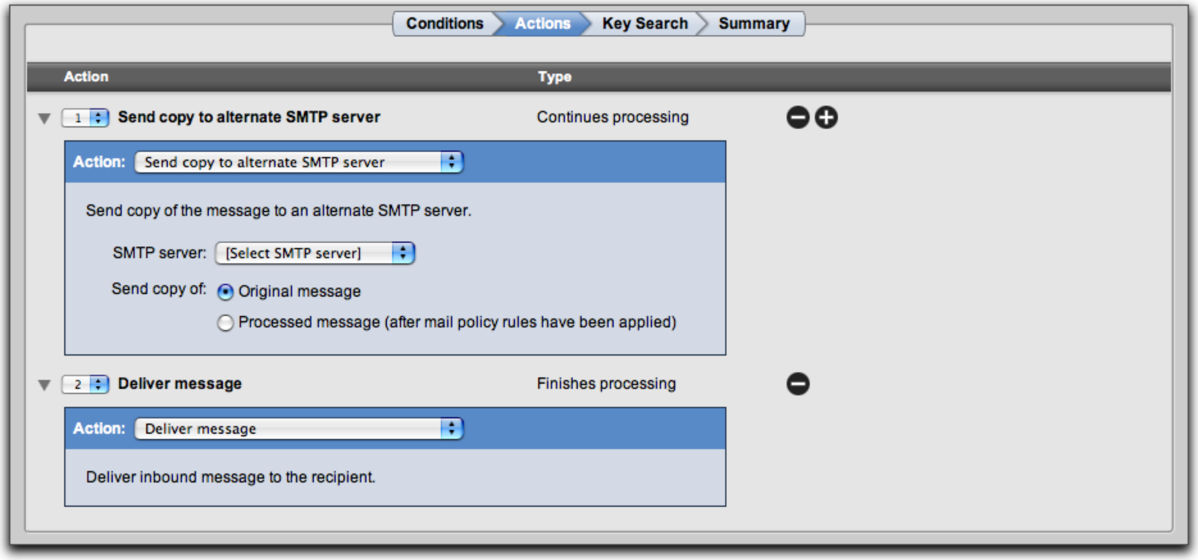
To delete a group or condition, select that group or condition and click the **Delete** button. There must be at least one condition in a rule. If there is only one condition in a rule, you cannot delete it.

Reordering Groups or Conditions

You can also change the order of conditions and groups. To change order, select the condition or group and click the Move Up or Move Down button.

The Actions Card

This section describes how to use the interface to add, delete, and reorder rule actions.



Action	Type
1 Send copy to alternate SMTP server	Continues processing
2 Deliver message	Finishes processing

Action: Send copy to alternate SMTP server

Send copy of the message to an alternate SMTP server.

SMTP server: [Select SMTP server]

Send copy of: ● Original message
○ Processed message (after mail policy rules have been applied)

Action: Deliver message

Deliver inbound message to the recipient.

Adding or Deleting Actions

To add or delete an action in a rule, click the Add or Delete icons to the right of the action.

Reordering Actions

The order in which actions appear is the rule is important. Actions that finish processing must come at the end of a list of actions in a rule. For example, in a list of actions, the *Send copy to alternate SMTP server* action must come before the *Deliver message* action in a list.

To change the order of actions in a rule, renumber the action you want to move. All actions will automatically reorder.

Managing Policy Chains

Use these procedures to edit policy chain settings, add, delete, export, import, and print policy chains.

Mail Policy Best Practices

Managing mail policy through the web interface is the recommended method.

It is possible to export mail policy as an XML file, edit chains and rules directly in XML, and then import the edited file back into the PGP Universal Server. However, there is a higher risk of error using this method. You may want to edit mail policy directly in XML if you have a large number of changes to make at once, for example if you are migrating PGP Universal Server 2.0.6 proxy settings from multiple upgraded clustered Secondaries. Contact PGP Support (www.pgp.com/support) for help if you intend to edit mail policy in XML.

Restoring Mail Policy to Default Settings

You can reset the entire Mail Policy card. This deletes all the changes you have made to the mail policy and restores all the mail policy settings that were originally installed on the server.

To reset the mail policy, click **Restore the Factory Defaults**.

Editing Policy Chain Settings

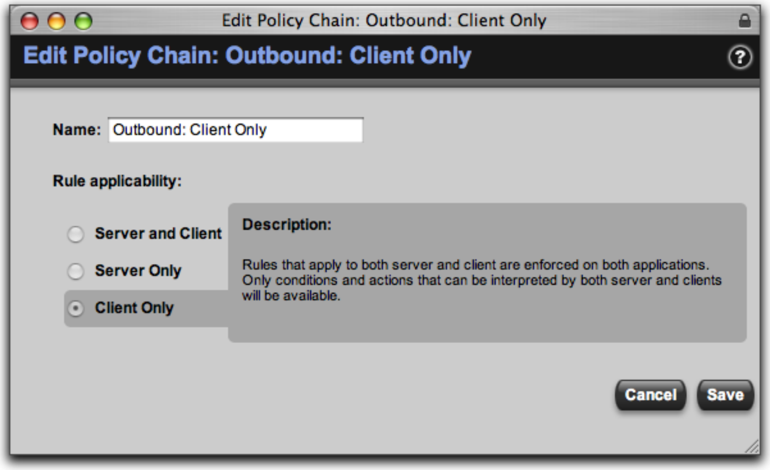
To edit the settings for a policy chain:

1 Click the name of the chain you want to edit.

The **Policy Chain** card appears.

2 Click **Edit Policy Chain Settings**.

The **Edit Policy Chain** dialog appears.



Edit Policy Chain: Outbound: Client Only

Name: Outbound: Client Only

Rule applicability:

○ Server and Client
○ Server Only
● Client Only

Description:

Rules that apply to both server and client are enforced on both applications. Only conditions and actions that can be interpreted by both server and clients will be available.

3 Type a new name for the policy chain, if necessary.

4 Choose which applications, PGP Universal Server and PGP Desktop client, to which you want the rules in the chain to apply. You can choose to apply the rules to both server and client, to server only, or to client only.

Rules that apply to the server only are enforced on the PGP Universal Server. Rules that apply to the client only are enforced on the client. Rules that apply to both server and client are enforced on both applications.

Different conditions and actions will be available in the rules depending on whether the rules apply to PGP Universal Server, PGP Desktop, or both.

5 Click **Save**.

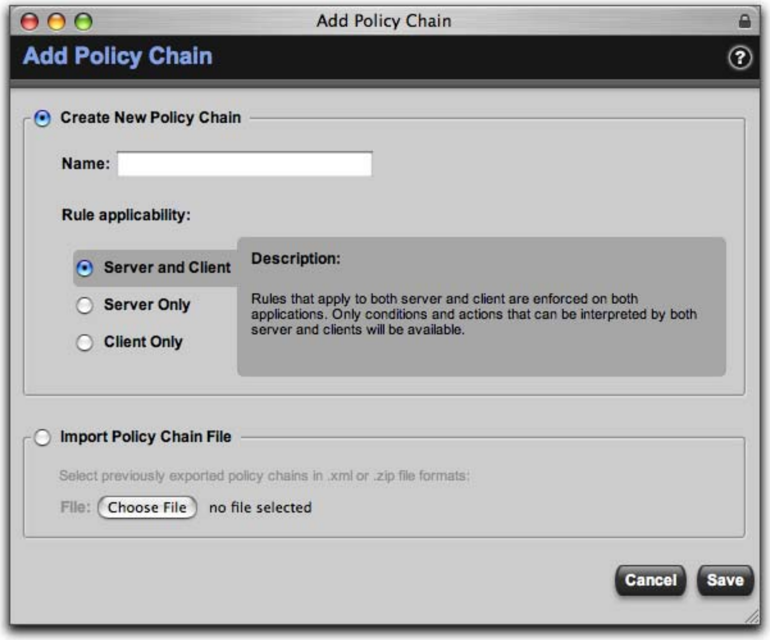
Adding Policy Chains

To create a new policy chain:

1 Do one of the following:

- Click the **Add Policy Chain** button.
- From the **Options** list, select **Import Policy Chains**.

The **Add Policy Chain** dialog appears.



Add Policy Chain

Add Policy Chain

● Create New Policy Chain

Name:

Rule applicability:

● Server and Client

○ Server Only

○ Client Only

Description:

Rules that apply to both server and client are enforced on both applications. Only conditions and actions that can be interpreted by both server and clients will be available.

○ Import Policy Chain File

Select previously exported policy chains in .xml or .zip file formats:

File: Choose File no file selected

2 To create a new chain, select **Create New Policy Chain**.

3 Type in the name for the new chain.

4 Choose which applications, PGP Universal Server and PGP Desktop client, to which you want the rules in the chain to apply. You can choose to apply the rules to both Server and Client, to Server only, or to Client only.

Rules that apply to the server only are enforced on the PGP Universal Server. Rules that apply to the client only are enforced on the client. Rules that apply to both server and client are enforced on both applications.

Different conditions and actions will be available in the rules depending on whether the rules apply to PGP Universal Server, PGP Desktop, or both.

5 Click **Save**.

You can also import a new policy chain from a file. Import policy chain files in XML format, or in a ZIP file containing multiple XML files.

1 Click the **Add Policy Chain** button, or select **Import Policy Chains** from the **Options** list.

The **Add Policy Chain** dialog appears.

2 Select **Import Policy Chain File**, and click **Choose File**.

3 Browse to select the file you want to import.

4 Click **Import**.

If the policy you want to import has the same name as a policy already in your chain, the Import Policy Chain Conflict dialog appears.

5 Choose whether to Ignore or Replace:

- Choose **Ignore** to skip importing policies with duplicate names.
- Choose **Replace** to overwrite the existing policies with names the same as the chains you are importing.

Deleting Policy Chains

⚠ The Default and Default: Legacy Clients policies cannot be deleted, but you can delete or edit the rules within. The Default chains provide a necessary starting point in the mail policy for all message processing. If you delete or change the rules in the Default chains, it can make your mail policy invalid and prevent your messages from being processed.

To delete policy chains:

1 Do one of the following:

■ To delete one policy chain:

a Click the Delete icon of the policy chain you want to delete.

A confirmation dialog appears.

b Click **OK**.

The policy chain is removed from the mail policy list.

■ To delete multiple policy chains:

a Click the checkbox at the far right end of the row of each of the policy chain you want to delete.

b Select **Delete Selected** from the Options menu at the bottom right corner, or **Delete All** to remove all policy chains.

A confirmation dialog appears.

c Click **OK**.

The policy chains are removed from the mail policy list.

Exporting Policy Chains

To export a policy chain:

1 Click the checkbox at the far end of the row for each chain you want to export.

2 From the **Options** list, select **Export Selected**.

3 To export all dictionaries associated with the rules in the chain, click the **Include all associated dictionaries** checkbox.

4 Click **Export**.

The policy chain you chose is exported to your desktop as an XML file. If you exported more than one policy chain, the XML files are inside a ZIP file.

Printing Policy Chains

To create a printable version of your policy chain, including all rules:

1. Click the checkbox at the far end of the row for each chain you want to print.
2. From the **Options** list, select **Print View for Selected**. To print the entire mail policy, select **Print View for All**.

   A printable version of the mail policy appears.
3. Click the **Print** link at the top of the page.

Managing Rules

Use these procedures to add, delete, enable, and disable rules within policy chains.

Adding Rules to Policy Chains

To add a rule:

1. Select the Policy Chain to which you want to add a rule.

   The **Policy Chain** card appears.
2. Click **Add Rule**.

   The **Add Rule** card appears.
3. Type in a name and description for the rule. The description should provide an explanation for what the rule does.
4. Add conditions, actions, and keyserver locations, as needed.

   For information on how to use the rule interface, refer to "Using the Rule Interface" on page 118. For information on how to design a valid rule, see "How Policy Chains Work" on page 111.

Deleting Rules from Policy Chains

To delete a rule:

Do one of the following.

- To delete a specified rule:

  a. Select the policy chain from which you want to delete a rule.

The **Policy Chain** card appears.

b Click the Delete icon of the rule you want to delete.

A confirmation dialog appears.

c Click **OK**.

The rule is removed from the policy chain.

- To delete multiple rules:

a Click the checkbox at the far right end of the row of each of the rule you want to delete.

b From the **Options** list, select **Delete Selected**, or **Delete All** to remove all rules.

A confirmation dialog appears.

c Click **OK**.

The rules are removed from the policy chain.

Enabling and Disabling Rules

An enabled rule is a rule that is turned on and being used to process email on the policy chain. A disabled rule is not deleted, but is not currently in use to process email through the policy chain.

! If you disable a rule in the policy chain, it could cause email to be processed incorrectly. Depending on how you have designed your policy chain, disabling rules may cause email to be sent unintentionally unencrypted, or to fall through the policy chain and not be sent at all.

To enable or disable rules:

1 Click the checkbox at the far right end of the row of each of the rule you want to enable or disable.

2 Select **Toggle Status for Selected** from the **Options** menu at the bottom right corner, or **Toggle Status for All** to enable or disable all rules.

A confirmation dialog appears.

3 Click **OK**.

The rules enabled or disabled.

Changing the Processing Order of the Rules

To change the order in which rules are processed, renumber the rule you want to move. All the rules will reorder automatically.

Adding Key Searches

The PGP Universal Server will always look in its own databases for keys. If the PGP Universal Server does not have a copy of a particular key, a rule may then require searching external sources for the key.

To enable external key searches for a rule:

1. Click the **Key Search** arrow button.
2. Click the checkbox to activate **Search for keys in additional locations**.
3. Select a keyserver from the drop-down.
4. To add more keyservers to the rule, click the Add icon next to the server name.
5. If you have added more than one specified directory in the policy, you can choose the order in which the added directories are searched for keys. Renumber a directory to give it a higher search priority.

You can also add searchable keyservers to the PGP Universal Server list from this card.

To add a new searchable keyserver to the rule:

1. Select **Add new keyserver** from the drop-down.

   The **Add Keyserver** dialog appears.

2. Enter the information for the keyserver you want to add. See "Adding or Editing a Keyserver" on page 159 for more information on this dialog.

   The keyserver information you add will also appear on the Policy>Servers>Keyservers card.

Choosing Condition Statements, Conditions, and Actions

Condition Statements

Condition statements link conditions together into groups, and specify how conditions should be matched. For example, if you have more than one condition in a rule, you can specify that the rule is triggered if all of the conditions are matched, or you can specify that the rule is triggered if just one of the conditions is matched.

Table 6-1. Condition Statements

Statement	Description
If all of the following are true	Every condition and group nested under this statement must be true.
If any of the following are true	Any of the conditions and groups nested under this statement can be true for the statement to be true, but at least one must be true.

Table 6-1. Condition Statements

Statement	Description
If none of the following are true	None of the conditions and groups nested under this statement can be true. Use this statement to exclude certain email from being processed by the rule.
The condition is always true	There are no conditions allowed under this statement. This statement ensures that this rule action will be performed on every email processed by the rule.

Conditions

Conditions are the set of requirements a message must meet to trigger a rule.

Some conditions require matches to terms found in the email headers or body. Terms can be numbers, words, regular expressions, or in dictionaries or user policies. The condition modifier indicates how the term should be matched.

Table 6-2. Condition Modifiers

Modifier	Description
Is	The term can only match against the exact characters specified in the condition. There is one and only one possible match. Not case-sensitive.
Matches pattern	The term in the email must match against a regular expression. Refer to the online help for more information on using regular expressions. Not case-sensitive.
Contains	The term must match against the exact characters specified in the condition, but the characters specified can occur anywhere within the term. Not case-sensitive.
Begins with	The term must match against the exact characters specified in the condition, and the characters specified must occur at the beginning of the term. Not case-sensitive.
Ends with	The term must match against the exact characters specified in the condition, and the characters specified must occur at the end of the term. Not case-sensitive.
Is in dictionary	The term must match against the content of a specified dictionary. Not case-sensitive.
Is a subdomain of	The email domain matches if it is a subdomain of the specified domain. Not case-sensitive.
Is greater than	The term matches if it is greater than the amount specified.
Is less than	The term matches if it is less than the amount specified.
Fewer than	The term matches if it is fewer than the number specified.
Greater than	The term matches if it is greater than the number specified.

Not all conditions are available for all rules. Which conditions can be used in a rule depends on whether the rule's policy chain applies to the PGP Universal Server or the PGP Desktop client.

Table 6-3. Conditions

Condition	Modifiers	Matches	Details
Recipient address	is, contains, begins with, ends with, matches pattern, is in dictionary	email address, partial email address, regular expression, dictionary name	—
Recipient domain	is, contains, begins with, ends with, matches pattern, is in dictionary, is a subdomain of	domain name, partial domain name, regular expression, dictionary name	—
Recipient user group	is	user policies, dictionary names	When you choose to apply this condition to a specific user policy, select the policy you want from the dropdown menu. The dropdown menu will not specify whether a listed user policy is internal or external. If there is more than one policy with the same name, it will only list the policy name once. For example, you have two Default user policies. You may need to create another condition specifying whether you want to apply the rule to internal or external users. If you have multiple user policies with similar names, be sure you are selecting the correct policy.
Recipient address is mailing list	—	user policies	Used with the "Expand mailing list and restart processing Action" on page 137.
Recipient key mode	—	SKM, CKM, GKM, SCKM	—
External user recipient delivery preference	—	PGP Universal Web Messenger, Smart Trailer, PGP Desktop/ PGP Universal Satellite	For external recipients only.
Sender address	is, contains, begins with, ends with, matches pattern, is in dictionary	exact or partial email address, regular expression, dictionary name	—
Sender domain	is, contains, begins with, ends with, matches pattern, is in dictionary, is a subdomain of	exact or partial domain, regular expression, dictionary name	—

Table 6-3. Conditions

Condition	Modifiers	Matches	Details
Sender user group	is, is in dictionary	user policies, dictionary name	When you choose to apply this condition to a specific user policy, select the policy you want from the dropdown menu. The dropdown menu will not specify whether a listed user policy is internal or external. If there is more than one policy with the same name, it will only list the policy name once. For example, you have two Default user policies. You may need to create another condition specifying whether you want to apply the rule to internal or external users. If you have multiple user policies with similar names, be sure you are selecting the correct policy.
Sender key mode	—	SKM, CKM, GKM, SCKM	—
Message header	is, contains, begins with, ends with, matches pattern	message header type (e.g., To, From); exact or partial content of message header, or regular expression	Matches on the content of a message header. You can use regular expressions with the *matches pattern* modifier to express the content of the message header.
Message subject	is, contains, begins with, ends with, matches pattern	exact or partial content of message subject, or regular expression	Matches on the content of the message subject. For example, **[Important]**, **[AAA]**, or **[Confidential]**. You can use regular expressions with the *matches pattern* modifier.
Message body	is, contains, begins with, ends with, matches pattern	exact or partial content of message body, or regular expression	Matches on the content of the message body. You can use regular expressions with the *matches pattern* modifier.
Message size	is, is greater than, is less than	size in KB	—
Any part of the message is encrypted	—	to any key, to key ID, to ADK, to key in dictionary	This condition is available only for server-applicable rules. The key entered in the condition must match the key or subkey used for message encryption. This would be either the encryption key (for v4 keys) or the topkey (for v3 keys). If you enter a v4 topkey into the condition, it will not match the encryption subkey found in the message.

Table 6-3. Conditions

Condition	Modifiers	Matches	Details
All of the message is encrypted	—	to any key, to key ID, to ADK, to key in dictionary	This condition is available for server-applicable rules. It is also applicable to client-applicable rules for SMTP, POP, and IMAP only. It is not applicable to Lotus Notes and MAPI. The key entered in the condition must match the key or subkey used for message encryption. This would be either the encryption key (for v4 keys) or the topkey (for v3 keys). If you enter a v4 topkey into the condition, it will not match the encryption subkey found in the message.
Any part of the message is signed	—	—	This condition is available only for server-applicable rules.
Message contained virus	—	—	Matches if the message was previously processed by a rule that screens for viruses, and the message was marked as containing a virus.
Message has an attachment whose name	is, contains, begins with, ends with, matches pattern	exact or partial content of message attachment name, or regular expression	This action interacts with and is related to the File Blocking feature. Refer to Chapter 21, “Blocking Files” for more information.
Message has an attachment whose type	is, contains, begins with, ends with, matches pattern	exact or partial content of message type name, or regular expression	This action interacts with and is related to the File Blocking feature. Refer to Chapter 21, “Blocking Files” for more information.
Message is from mailing list	—	—	This condition is available only for server-applicable rules.
Mailing list user count is	fewer than, greater than	number of members in list	Default value is 30 users. “Expand mailing list and restart processing Action” on page 137.
Application	—	is internal PGP Desktop/PGP Universal Satellite, is external PGP Desktop/PGP Universal Satellite, is PGP Universal Server, is RIM Blackberry	—
Service type	—	is SMTP Inbound, is SMTP Outbound, is POP, is IMAP, is Microsoft Outlook (MAPI), is Lotus Notes, is PGP Universal Web Messenger	—

Table 6-3. Conditions

Condition	Modifiers	Matches	Details
Connected user has authenticated	—	—	If the PGP Universal Server is in gateway placement, authentication from internal users is not possible because the user is authenicating to the mail server, not directly to the PGP Universal Server.
IP address of local connector	is, contains, begins with, ends with, matches pattern, is in dictionary	exact or partial IP address, regular expression, dictionary name	—
Port of local connector	is, is greater than, is less than	port number	—

Actions

Actions are processes performed on messages when rule conditions apply. Some actions process email and then pass the email along to other actions or rules for further processing; for example, *Scan for viruses*. Other actions end email processing; for example, *Drop message*. When constructing a rule or chain of rules, make sure that actions that finish email processing come after the actions that allow continued processing.

Not all actions are available for all rules.Which actions can be used in a rule depends on whether the rule's policy chain applies to the PGP Universal Server or the PGP Desktop client.

Table 6-4. Actions

Action	Type	Options	Result
Send (encrypted/signed)	Finishes processing	See "Send (encrypted/ signed) Action" on page 134 for information on how to configure this action.	Sends the email encrypted to specified key(s).
Send via Web Messenger	Finishes processing	—	Recipient receives a message (not the original email message) that directs them to a website where they have options for accessing the original message securely. This option is not available for managed domains or non-mailstream installations. This action is available only for server-applicable rules.
Send clear (unencrypted and unsigned)	Finishes processing	—	Sends the email unencrypted and unsigned.

Table 6-4. Actions

Action	Type	Options	Result
Send copy to alternate SMTP server	Continues processing	Select or add an SMTP server. Choose to send original or mail policy-processed message.	Sends a copy of the email (encrypted or unencrypted) to an SMTP server for archiving purposes. Refer "SMTP Servers" on page 161 to for more information on SMTP servers. This action is available only for server-applicable rules.
Deliver message	Finishes processing	—	Delivers inbound email to recipient.
Decrypt and verify message	Finishes processing	See "Decrypt and verify message Action" on page 136 for information on how to configure this action.	Decrypts and verifies email and annotates email with information about verification results.
Bounce message	Finishes processing	—	Returns email to the sender.
Drop message	Finishes processing	—	Drops email. Inbound IMAP and POP mail cannot be dropped. Instead, users will receive the email with the message text replaced by the information in the Blocked Message Content template. Refer to Chapter 25, "Customizing System Message Templates" for information about the message template. This action is available only for server-applicable rules.

Table 6-4. Actions

Action	Type	Options	Result
Scan for viruses	Continues processing	If a virus is found: clean the message of infected attachments, or do not clean but note that the email has a virus and pass on for further processing.	Cleans and forwards on the email to the next rule. If you choose to note the virus and pass the email along for further processing, the email will be marked as infected and moved to the next rule or chain. Make sure to create another rule to clean, bounce, or drop the infected message. This action requires a PGP license that supports virus scanning, as well as a Symantec AntiVirus license. Without those licenses, any rule with this action will not be enforced. This action also interacts with the AntiVirus feature elsewhere in the PGP Universal Server interface. Refer to Chapter 20, "Scanning Email for Viruses" for more information.
Add to dictionary	Continues processing	Add sender, recipient, or mailing list address to chosen dictionary.	Adds data found in email to a selected dictionary. This action is available only for server-applicable rules.
Expand mailing list and restart processing	Continues processing	—	See "Expand mailing list and restart processing Action" on page 137 for information on this action.
Go to chain	Continues processing	Select a policy chain to which to pass the email.	Sends message on to any other chain in the mail policy for further processing.

Details on Actions

Send (encrypted/signed) Action

This action allows you to specify what key(s) to use to encrypt the email, and what happens if a suitable key is not found.

Not all Key Not Found options are possible for all rules. In client-based rules, do not select PGP Universal Web Messenger or Smart Trailer as an action in response to a Key Not Found condition. If you choose these options in a client-based rule, email will instead be sent in the clear: unencrypted and unsigned.

If the sender or recipient uses signing and encryption subkeys, the encryption behavior for this action may be effected. If your policy requires messages be encrypted and signed, all necessary keys must be available. If the recipient's encryption subkey is not available, the message will not be sent. If the policy requires the email be encrypted and signed to the sender's key, and the sender's encryption key is not available, the message will not be sent. However, if the policy requires the email be encrypted and signed to the sender's key, and the sender's signing key is not available, the message will still be sent, encrypted and unsigned.

Refer to Chapter 16, "Applying Key Not Found Settings to External Users" for more information about how external users receive email when no suitable key is found, and how those users interact with Smart Trailer and PGP Universal Web Messenger.

To create the Send (encrypted/signed) action:

1. In the Action section of a rule, select **Send (encrypted/signed)** from the drop-down.
2. Click **Recipient's Key** to encrypt the email to the recipient's key.
3. Choose whether to require a verified key. A verified key is a valid key.
4. Choose whether to require an end-to-end key. An end-to-end key is a key in sole possession of the individual recipient. A CKM or GKM key is an end-to-end key, an SKM key is not. An SCKM key is end-to-end for signing only, but not for encryption.
5. Specify what to do when a suitable key or certificate is not found for the recipient from the drop-down menu:
   - **Bounce:** The email message will be returned to the sender if a key for the recipient cannot be found.
   - **Send clear (signed):** The email will be sent to the recipient unencrypted but signed if a suitable encryption key cannot be found.
   - **Send clear (unsigned):** The email will be sent to the recipient unencrypted and unsigned if a suitable encryption key cannot be found.
   - **Smart Trailer:** The email will be sent to the recipient unencrypted with a trailer that explains how to get mail from the sender in a secure manner in the future. Not available for client policy or non-mailstream installations.
   - **Web Messenger:** The recipient will be sent a message (but not the original email message) that directs them to a website where they have options for accessing the original message securely. Not available for client policy or non-mailstream installations.
6. Click **Sender's Key** to encrypt the email to the sender's key. This can help in retrieving the email message.
7. If you have an Additional Decryption Key uploaded, all outbound email will be encrypted to it. This setting cannot be disabled.
8. Click **Other Keys/Certificates** to encrypt the message to any other key or certificate. You can add or remove more keys by clicking the Add or Delete icons. Only add keys and certificates that can be used for encryption.

- Select **Key ID** and enter the key ID of the key you want to encrypt to.
- Select **Import file** and click the **Import** button to import a key to encrypt to.

9 Click the **Sign** checkbox if you want the email to be signed.

10 From the **Preferred encoding format** drop-down, choose your preferred format for signed messages.

The preferred encoding format is what was called preferred signing format in PGP Universal Server 2.0.x.

The preferred encoding format is important when email is sent signed but not encrypted. Because the email format cannot be set automatically based on the type of key the email is encrypted to when the recipient's key is not available, it is up to the PGP Universal Server administrator to decide which format the users at each domain can handle.

Make your selection for **Preferred encoding format** based on the following:

- **Automatic** enables PGP Universal Server to choose the most appropriate encoding format, taking into account the original format of the message, as well as the preferred-encoding packet of the keys or certificates to which the email is being encrypted.
- **PGP Partitioned** is a mail encoding format that works well with non-MIME mail clients, such as Microsoft Outlook.
- The sender has only a PGP key. In this case, they can use only **PGP/MIME** as a signing format. If you select **S/MIME**, the selection will revert to **PGP/MIME**. Keys generated by PGP Universal Server have preferred encoding set to **PGP/MIME**.
- The sender has only an X.509 certificate. In this case, they can use only **S/MIME** as a signing format. If you select **PGP/MIME**, the selection will revert to **S/MIME**.
- The sender has both a PGP key and an X.509 certificate. In this case, you need to make a choice between **PGP/MIME** and **S/MIME** based on the situation of the recipients and their ability to decrypt messages: If the recipients can read PGP key signatures, choose **PGP/MIME**; if they can read X.509 certificate signatures, choose **S/MIME**. You may need to make this choice based on your best guess of what type of encryption system used by recipients.

Decrypt and verify message Action

This action decrypts and verifies email and annotates email with information about verification results.

To create the Decrypt and verify message action:

1 In the **Action** section of a rule, select **Decrypt and verify message** from the drop-down.

2 From the **Annotation Setting** drop-down, select how you want the email to be annotated.

- **Don't annotate:** Leaves the email as it was sent and does not include information on verification.
- **Annotate failures only:** Annotates the email only if verification failed.
- **Annotate detailed info:** Provides full annotation for all email and all attachments.
- **Smart annotation:** If everything in a message is signed by the same individual, the message has a single annotation. If the message has multiple signatures, then the email receives detailed annotation information.

Expand mailing list and restart processing Action

This action takes any Active Directory-based mailing list in the recipient message header and expands it, replacing the mailing list address in the header with all the mailing list member email addresses. The action then returns the email to the Default policy chain and reruns mail policy on the message, processing it with the expanded addresses.

In the factory-set mail policy, the rule containing this action is on the Outbound chain and is called *Expand mailing list*.

This functionality is important if not all members of a mailing list should have email processed in the same way. For example, you have an Active Directory mailing list called execs@example.com. The mailing list has 3 members, two of whom are executives and one of whom is an administration assistant. Your mail policy specifies that all email received by executives must be encrypted, but email received by the administration assistant should not be encrypted.

If the mailing list is not expanded, the executives will receive mailing-list email unencrypted. The *Expand mailing list* rule means that mail policy is applied to the individual members of a list, not to the list as a whole.

The action is triggered by matching the condition *Recipient address is mailing list*. It is important to limit the size of the mailing list to which you apply the action by also using the condition *Mailing list user count is fewer than <n>*. The default limit for the condition is 30 users, although you can edit the value. Limiting the rule to smaller lists is important because the more recipients addressed in the email, the longer it will take to process and send the message.

If it is necessary to encrypt email to a very large mailing list, use the following procedure:

1. Create a new key and distribute it to all the members of the specific mailing list to which you want to send encrypted email.
2. Create a rule on the Outbound policy chain, and place it before the *Expand Mailing Lists* rule.
3. In the new rule, create the condition

   If all of the following are true:

   Recipient address is mailing list

   so that it is matched by email addressed to the mailing list.

4 In the rule, create a *Send (encrypted/signed)* action.

5 Select **Other Keys/Certificates**, and import the mailing list key for encryption.

Working with Common Access Cards

Common Access Cards (CAC) are a type of smartcard used by the Department of Defense and compatible with PGP Desktop. CACs contain multiple X.509 certificates; one is used to encrypt messages and another is used for signing.

Because PGP Universal Server normally works with only one primary key per user, you must take extra steps to make it possible for your internal PGP Desktop users to use CACs.

To ensure that CACs work with the PGP Universal Server, make sure that the server can access the directory containing the CAC user certificates. You must add the CAC Directory to the **Key Search** screen of every rule in mail policy that specifies a key search.

To access the CAC user certificates:

1 For every rule in mail policy that requires a key search, click **Key Search** to add the user certificate directory to the rule. See "Adding Key Searches" on page 127 for information on adding a keyserver search to a rule.

2 Since the directory contains X.509 certificates, choose directory type X.509 Directory LDAP or LDAPS.

3 All the certificates on the CACs have been signed by some root Certificate Authority. Add the root signing certificate to the Trusted Keys list. See Chapter 13, "Managing Trusted Keys and Certificates" for more information.

16 Applying Key Not Found Settings to External Users

This chapter describes your options for dealing with users who are outside of the Self-Managing Security Architecture (SMSA) each PGP Universal Server creates and maintains. This chapter explains how Key Not Found mail policy settings appear to external users, and how external users interact with Smart Trailer and PGP Universal Web Messenger. See Chapter 15, "Setting Mail Policy" for more information about working with these settings in mail policy.

This feature is an important part of creating mail policy, and is used by PGP Universal Gateway Email and PGP Desktop Email.

Topics in this chapter include:

Overview

Your PGP Universal Server automatically creates and maintains an SMSA by monitoring authenticated users and their email traffic.

However, there will always be email users who are outside the SMSA but to whom you still want to send protected email: for example, the law firm your company uses; email to and from the attorneys includes sensitive information and should probably be encrypted.

Policy options for users outside the SMSA are established on the Mail Policy screen of the administrative interface. These options are controlled through the Key Not Found settings of the *Send (encrypted/signed)* action. See "Details on Actions" on page 134 for more information.

You have a number of policy options you can establish for mail sent to recipients currently outside the SMSA (that is, users for whom the PGP Universal Server cannot find a trusted key). You can:

- bounce the message back to the sender
- send the message unencrypted and signed, or unencrypted and unsigned
- add a "Smart Trailer"
- offer PGP Universal Web Messenger through "Smart Trailer" text (only if PGP Universal Server is in the mailstream)

All of these options are described below.

Bounce the Message

The message is returned to the sender, undelivered, because it could not be sent encrypted. This is the high-security approach; it *requires* encryption to a trusted key or the message is not sent.

If there was more than one recipient, and some messages could be sent encrypted but some could not, only the messages that could *not* be sent encrypted are bounced.

The bounced message will appear to be from an account called “pgpuniversal-admin@manageddomain” (**pgpuniversal-admin@example.com**, for example). Unless you create it, this account does not actually exist on the mail server. You may want to create this account on the mail server if you anticipate that your users may respond to the bounce message (to ask *why* the message bounced, for example).

Send Unencrypted

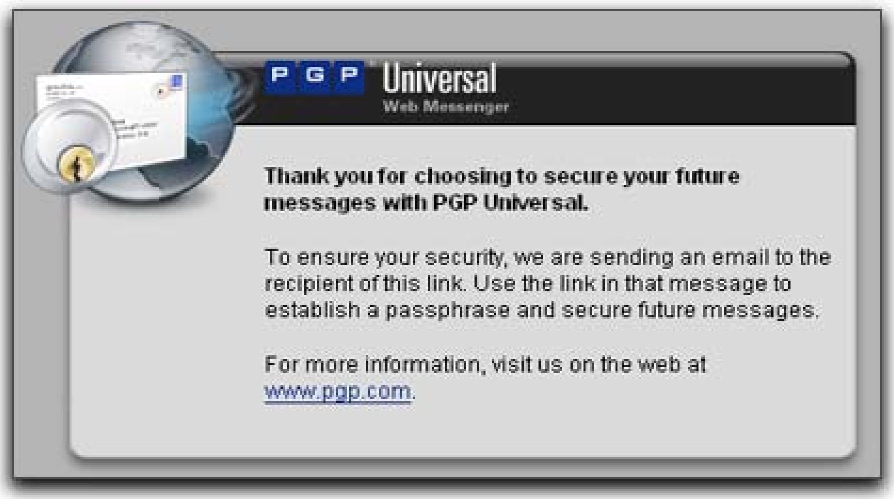
The message is sent to the recipient unencrypted. This is a low-security option. You can specify that the email be unsigned, or signed by the sender’s key.

Smart Trailer

The message is sent *unencrypted* with a “Smart Trailer” added. The Smart Trailer is text that explains that the message could have been encrypted if the recipient were a member of the SMSA.

The Smart Trailer also includes a link to a location on the PGP Universal Server where recipients can set a passphrase and choose how they would like to receive future messages from senders in the same domain. In other words, it gives them ways to become part of the SMSA.

When the recipient follows the link, a Security Confirmation screen appears.

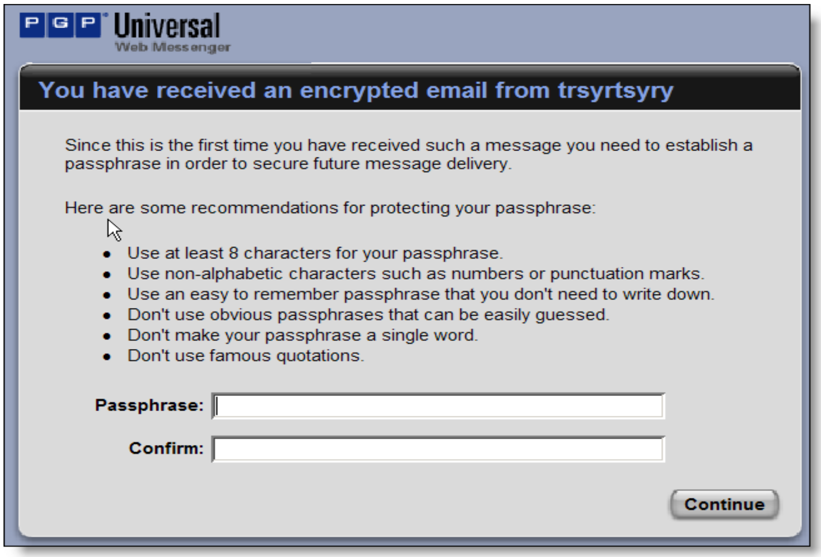


Thank you for choosing to secure your future messages with PGP Universal.

To ensure your security, we are sending an email to the recipient of this link. Use the link in that message to establish a passphrase and secure future messages.

For more information, visit us on the web at www.pgp.com.

The user will then receive another email with a new link. When the user follows the link, the Passphrase screen appears.



You have received an encrypted email from trsyrtsyry

Since this is the first time you have received such a message you need to establish a passphrase in order to secure future message delivery.

Here are some recommendations for protecting your passphrase:

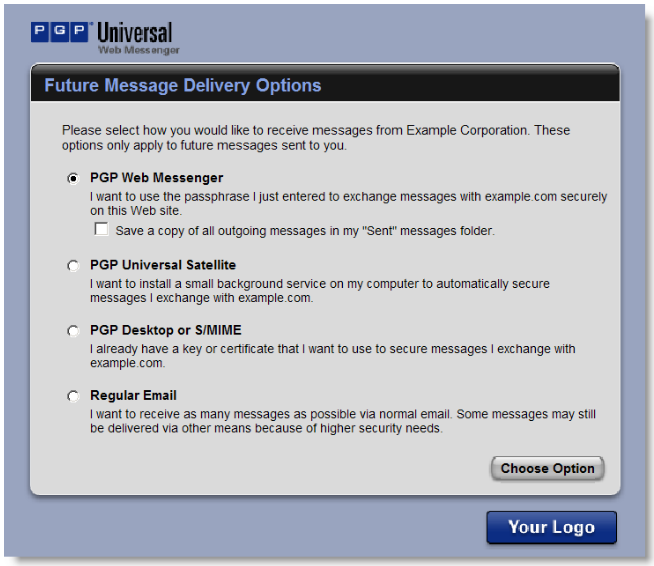
- Use at least 8 characters for your passphrase.
- Use non-alphabetic characters such as numbers or punctuation marks.
- Use an easy to remember passphrase that you don't need to write down.
- Don't use obvious passphrases that can be easily guessed.
- Don't make your passphrase a single word.
- Don't use famous quotations.

Passphrase:

Confirm:

The user enters a passphrase that allow them to securely retrieve all future messages. Then the user clicks **Continue**.

The Future Message Delivery Options screen appears.



Future Message Delivery Options

Please select how you would like to receive messages from Example Corporation. These options only apply to future messages sent to you.

● **PGP Web Messenger**
I want to use the passphrase I just entered to exchange messages with example.com securely on this Web site.
□ Save a copy of all outgoing messages in my "Sent" messages folder.

○ **PGP Universal Satellite**
I want to install a small background service on my computer to automatically secure messages I exchange with example.com.

○ **PGP Desktop or S/MIME**
I already have a key or certificate that I want to use to secure messages I exchange with example.com.

○ **Regular Email**
I want to receive as many messages as possible via normal email. Some messages may still be delivered via other means because of higher security needs.

The options on the Future Message Delivery Options screen depend on the applicable mail policy. Possible choices are:

- **PGP Universal Web Messenger:** The recipient gets access to a Web browser-based email reader called PGP Universal Web Messenger mail. This is available only if PGP Universal Server is in the mailstream.

  If the recipient chooses this option, they can also choose to have all of the outgoing messages they compose in PGP Universal Web Messenger saved to a "Sent Mail" folder.

- **PGP Universal Satellite:** The recipient downloads PGP Universal Satellite, becoming a part of the SMSA. If the recipient selects this option, they will be prompted to download PGP Universal Satellite. Refer to Chapter 36, "PGP Universal Satellite" for more information.

  If downloading PGP Universal Satellite is prohibited by policy, this option does not appear.

- **PGP Desktop or S/MIME:** If recipients are already PGP Desktop users or have X.509 certificates for S/MIME environments, they can provide their keys or certificates; future email messages to them will be encrypted with the key or certificate they provide, making them part of the SMSA.

  If they select this option, they will be prompted to provide the public portion of their key or certificate in a file (.asc format for PGP keys, .pem or .crt formats for X.509 certificates, .p7b or .p7c formats for PKCS #7, or .p12 or .pfx formats for PKCS #12 certificates) or they can copy and paste their PGP key.

  Users providing a PKCS#12 certificate that has a passphrase need to enter that passphrase in the **Optional Passphrase** field.

  Future email messages from the same domain will be encrypted using their key or certificate.

  External users who choose this option and provide their key can opt later to switch to receiving mail through PGP Universal Web Messenger. Refer to "Changing User Delivery Method Preference" on page 144 for more details.

  After providing their PGP Desktop public key or S/MIME certificate, a screen appears describing additional steps needed to use the PGP Desktop key or certificate to decrypt, verify, and encrypt messages:

  – **If a PGP Desktop public key was provided**, then they need to add this PGP Universal Server as a keyserver in PGP Desktop and download and import to their PGP Desktop keyring the Organization Key of the domain they are sending messages to and receiving messages from.

  – **If an S/MIME certificate was provided**, then they need to download the Organization Certificate and install it into their email client (Outlook or Outlook Express, for example) as a trusted root certificate.

- **Regular Email:** The recipient can choose to receive all future email messages unencrypted from senders in the same domain.

  If a user selects Regular Mail, it does not necessarily mean that the user will receive unencrypted email. This option only allows users to express their preference to receive regular mail when possible. The Key Not Found policy can override this choice. For example, if the Key Not Found setting for a *Send (encrypted/signed)* action is PGP Universal Web Messenger, email to a recipient without suitable keys will be delivered through PGP Universal Web Messenger, despite the user's delivery preference.

PGP Universal Web Messenger

PGP Universal Web Messenger mail gives recipients a way to securely read the message that was sent to them and several ways to become part of the SMSA. This is available only if PGP Universal Server is in the mailstream.

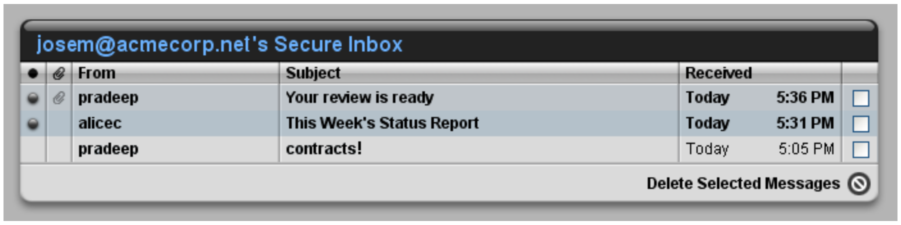
For PGP Universal Web Messenger mail to work, the PGP Universal Server must be accessible from outside the network. One way to do this is to put the server in a DMZ. The PGP Universal Web Messenger port must be accessible from outside your network for external users to access the PGP Universal Web Messenger interface and the synchronization port for PGP Universal Satellite.

Instead of sending the original message to the recipient, PGP Universal Web Messenger leaves the message on the PGP Universal Server and sends the recipient a different message.

Email messages sent to PGP Universal Web Messenger users must be smaller than 15MB. Attachments to email replies created in PGP Universal Web Messenger are limited to approximately 15MB per attachment. Also, users will not be able to send or receive any message that would put them over their message storage Quota.

The PGP Universal Server stores both mail received and mail sent by PGP Universal Web Messenger users. The user’s Quota is the amount of memory allotted for PGP Universal Web Messenger mail storage. You can specify how big the Quota is for each external user. See “External User Settings” on page 293 for more information.

Subsequent email messages from the same domain will contain a link to that message in PGP Universal Web Messenger mail. Following the link will bring up the message. The Inbox icon at the top of the message screen provides access to their secure inbox.



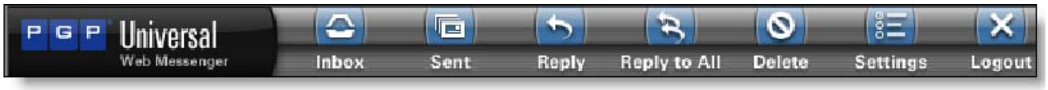
josem@acmecorp.net's Secure Inbox

●		From	Subject	Received		
●		pradeep	Your review is ready	Today	5:36 PM	□
●		alicec	This Week's Status Report	Today	5:31 PM	□
		pradeep	contracts!	Today	5:05 PM	□

Delete Selected Messages

The Inbox can be accessed at any time; the PGP Universal Web Messenger mail user simply points their Web browser to the URL provided in the first PGP Universal Web Messenger email and then enters their passphrase when prompted.

Icons at the top of each message let users access their inbox, reply to the message, delete the message, compose new messages, access their settings (they can change their delivery options or their passphrase), and log out.



PGP Universal Web Messenger allows its users to send reply email to any user in your managed domains, as well as to anyone outside the managed domains but originally carbon-copied in the message, but users cannot add new external recipients to the reply.

Changing Policy Settings

Changing your mail policy may change how current PGP Universal Web Messenger users receive future messages. See Chapter 15, "Setting Mail Policy" for more information.

If your mail policy is currently set to allow PGP Universal Web Messenger accounts, changing that setting affects PGP Universal Web Messenger users differently depending on how you change the setting.

- **Change your policy to Smart Trailer without PGP Universal Web Messenger.** Current PGP Universal Web Messenger users will be able to remain so. They will still be able to read all their old messages in PGP Universal Web Messenger and all their new messages will also be PGP Universal Web Messenger, in spite of the policy change. As long as the user has even one PGP Universal Web Messenger message, the user will still see the PGP Universal Web Messenger option the first time they log in, even if they don't log in for the first time until after the policy changes. Users who do not already have any PGP Universal Web Messenger messages will be treated according to policy, and will not be offered PGP Universal Web Messenger as an option.
- **Change your policy from PGP Universal Web Messenger to Bounce or Don't encrypt.** Treatment of all new messages will follow that policy. Current PGP Universal Web Messenger users will still be able to view their old messages, but no new ones will be added to any user's account.

Changing User Delivery Method Preference

External PGP Desktop users who choose to provide their key can opt later to switch to receiving mail through PGP Universal Web Messenger.

1. The user must log into PGP Universal Web Messenger using their email address and passphrase.
2. On the Secure Message Settings screen, the user should change how to receive future email by selecting **Regular Mail**.
3. The user should log out.

   The next time an internal user sends email to this external user, the external user will receive another PGP Universal Web Messenger invitation.
4. The user should click the link in the email and log into PGP Universal Web Messenger using their email and passphrase.
5. On the Secure Message Settings screen, the user should select PGP Universal Web Messenger.

All future email from internal users will be delivered to this external user through PGP Universal Web Messenger.

17 Using Dictionaries with Policy

This chapter describes dictionaries, which are lists of matchable terms that allow the PGP Universal Server to process messages according to mail policy rules. The Dictionaries card is under the Policy tab.

This feature is available with PGP Universal Gateway Email and PGP Desktop Email.

Topics in this chapter include:

Overview

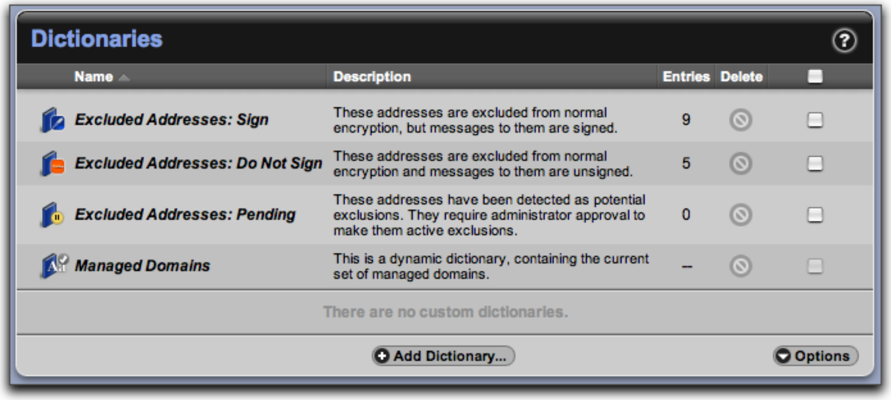
Dictionaries are lists of terms to be matched. Dictionaries work with mail policy to allow you to define content lists that can trigger rules or fulfill the conditions of a rule to trigger actions. For example, Dictionaries can contain addresses you want excluded from processing, key words like "confidential," or user names for internal users whose messages need special handling.

A policy rule can have a dictionary associated with it as a condition. If a message meets the condition, the PGP Universal Server processes the message according the rule's action. For example, one of the default Outbound rules is called Excluded Signed. The condition for that rule is "If any of the following are true: Recipient address is in dictionary *Excluded Addresses: Sign*." This means the rule applies to any message in which the recipient address matches a term in the dictionary. If that condition is met, the action for the rule is triggered. The action is to sign and send the message with no further processing.

Refer to Chapter 15, "Setting Mail Policy" for more information on mail policy conditions and actions.

Dictionaries are also used to match external users to the correct external user policy. Create a dictionary containing a list of external user names, then create an external user policy with a membership made up of users with names in that dictionary. See Chapter 29, "Setting External User Policy" for information about dictionaries and external user policy.

The Dictionaries card lets you add and edit Dictionaries. There are 4 default dictionaries, and you can also create your own.



Dictionaries

Name	Description	Entries	Delete	□
Excluded Addresses: Sign	These addresses are excluded from normal encryption, but messages to them are signed.	9	⊘	□
Excluded Addresses: Do Not Sign	These addresses are excluded from normal encryption and messages to them are unsigned.	5	⊘	□
Excluded Addresses: Pending	These addresses have been detected as potential exclusions. They require administrator approval to make them active exclusions.	0	⊘	□
Managed Domains	This is a dynamic dictionary, containing the current set of managed domains.	–	⊘	□

There are no custom dictionaries.

There are two types of dictionaries:

- **Static** dictionaries are editable lists of literal or pattern strings. All except one of the dictionaries are static.
- **Dynamic** dictionaries are not editable but are maintained by the PGP Universal Server. Information in the dictionary comes from data elsewhere on the PGP Universal Server rather than added directly to the dictionary by hand. There is one dynamic dictionary, the Managed Domains dictionary.

There are two types of entries in a dictionary:

- **Literals** are dictionary entries that can only match against the exact characters in the entry. There is one and only one possible match. For example, if the dictionary entry is "jsmith@example.com", then a message matches the entry only if it contains "jsmith@example.com". Similar strings, for example, "smith@example.com", will not match.
- **Patterns** are dictionary entries that match against characters in messages that satisfy the pattern. For example, the pattern "j.*@example.com" requires a match for the letter "j", then any number of other characters, then the sequence "@example.com", it will match "jsmith@example.com" and "jgreen@example.com". Use regular expression syntax to create patterns. For more information on using regular expressions in building mail policy, refer to the PGP Universal Server online help.

Default Dictionaries

There are four default dictionaries that exist on the server as installed. You cannot delete these dictionaries.

- **Excluded Addresses: Sign**: The addresses in this dictionary do not receive normally encrypted messages; messages to these addresses are signed. These addresses are generally mailing lists. Refer to "Editing Default Dictionaries" on page 150 for how to edit this dictionary.

  The list of "sign" default excluded addresses includes:

  - **.*-announce@.***
  - **.*-bugs@.***
  - **.*-devel@.***
  - **.*-digest@.***
  - **.*-docs@.***
  - **.*-help@.***
  - **.*-list@.***
  - **.*-news@.***
  - **.*-users@.***

  This dictionary corresponds to the default Outbound rule *Excluded Signed*. The rule applies to any message in which the recipient address matches a term in this dictionary. If that condition is met, the action for the rule is triggered. The action is send the message signed but not encrypted.

- **Excluded Addresses: Do Not Sign**: The addresses in this dictionary receive unsigned and unencrypted email. These addresses are generally mailing lists. Refer to "Editing Default Dictionaries" on page 150 for how to edit this dictionary.

  PGP Universal Server includes default exclusion rules that handle email addresses common to mailing lists. You do not need to add these to the Excluded Email Addresses list.

  The list of "do not sign" default excluded addresses includes:

  - **.*-bounces@.***
  - **.*-report@.***
  - **.*-request@.***
  - **.*-subscribe@.***
  - **.*-unsubscribe@.***

  This dictionary corresponds to the default Outbound rule Excluded Unsigned. The rule applies to any message in which the recipient address matches a term in this dictionary. If that condition is met, the action for the rule is triggered. The action is to send the message unsigned and not encrypted.

- **Excluded Addresses: Pending**: If your PGP Universal Server proxies email, possible excluded addresses will be detected and added to this dictionary automatically. You can approve addresses on this list to add them to either Excluded Addresses: Sign or Excluded Addresses: Do Not Sign. Refer to "Editing Default Dictionaries" on page 150 for how to approve a pending excluded address.

  While in Learn Mode, the PGP Universal Server will automatically detect and add to the Excluded Email Addresses dictionary those mailing lists that use standards-based header identification.

When Learn Mode is turned off, the PGP Universal Server will still automatically detect mailing lists, but it will add them to the **Excluded Addresses: Pending** dictionary. The PGP Universal Server administrator must approve the mailing lists before messages to it will be excluded.

The PGP Universal Server detects mailing lists per RFC 2919, "List-Id: A Structured Field and Namespace for the Identification of Mailing Lists," as well as by using default exclusion rules.

If you are using the Directory Synchronization feature, mailing lists found in the directory will be automatically added without requiring approval when using directories that support proper identification of mailing lists, such as Active Directory with Exchange Server.

If a mailing list is not in the **Excluded Addresses: Pending** dictionary, it could be because the list wasn't detected or because the mailing list does not use standards-based header identification.

If a mailing list is not automatically detected and added to the **Excluded Addresses: Pending** dictionary, you can easily add it directly to either of the Excluded Addresses dictionaries manually. Refer to "Editing Default Dictionaries" on page 150.

- **Managed Domains**: You cannot edit this dictionary from the Dictionaries card. If you want to add or delete a managed domain, use the Organization>Managed Domains tab. Refer to Chapter 11, "Managed Domains" for more information on adding Managed Domains.

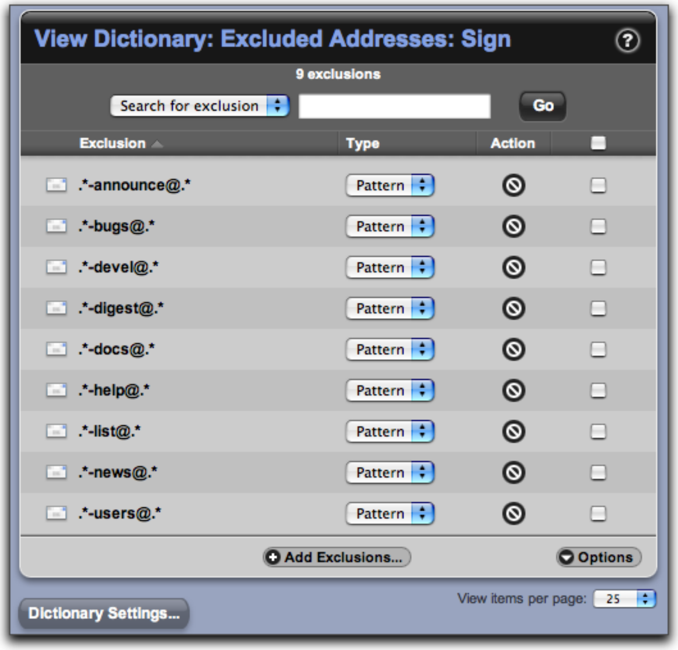
  The dynamic managed domains dictionary automatically includes subdomains. To exclude or include specific subdomains in a rule, create a dictionary listing those domains and reference it in the rule's conditions.

Editing Default Dictionaries

Editing Excluded Addresses Dictionaries

1 From the Policy>Dictionaries tab, click Excluded Addresses: Sign or Excluded Addresses: Do Not Sign.

  The View Dictionary card appears.



9 exclusions

Exclusion	Type	Action	□
.*-announce@.*	Pattern	⊘	□
.*-bugs@.*	Pattern	⊘	□
.*-devel@.*	Pattern	⊘	□
.*-digest@.*	Pattern	⊘	□
.*-docs@.*	Pattern	⊘	□
.*-help@.*	Pattern	⊘	□
.*-list@.*	Pattern	⊘	□
.*-news@.*	Pattern	⊘	□
.*-users@.*	Pattern	⊘	□

2 To delete terms from the dictionary, click the icon in the Delete column of the term you wish to delete, or click checkboxes to select multiple exclusions, and choose **Delete Selected** from the Options drop-down list.

A confirmation dialog appears.

3 Click **OK**.

4 To add to the contents of the dictionary, click **Add Exclusions**.

The Edit Dictionary dialog appears.

5 Select from the drop-down whether you are adding plain text terms, an XML file, or a ZIP file.

6 Type in or paste a list of terms, each separated on its own line, or choose **Import File** and select a file to import.

7 Specify whether the terms are Patterns or Literals.

8 Choose whether to append the new terms to the current contents of the dictionary or to replace the existing terms with the new terms.

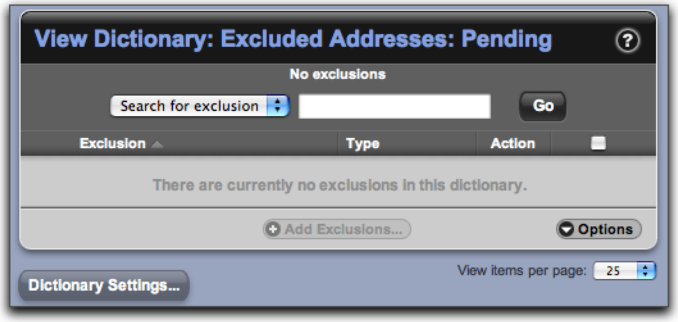
9 Click **Import**.

Approving Pending Excluded Addresses

When you approve a pending excluded address, it moves to the Excluded Addresses: Sign dictionary

1 From the Policy>Dictionaries tab, click the Excluded Addresses: Pending dictionary.

The View Dictionary card appears.



2 To approve excluded addresses, click the checkboxes of the addresses you wish to approve, and choose **Approve Selected** from the **Options** drop-down list.

A confirmation dialog appears.

3 Click **OK**.

User-Defined Dictionaries

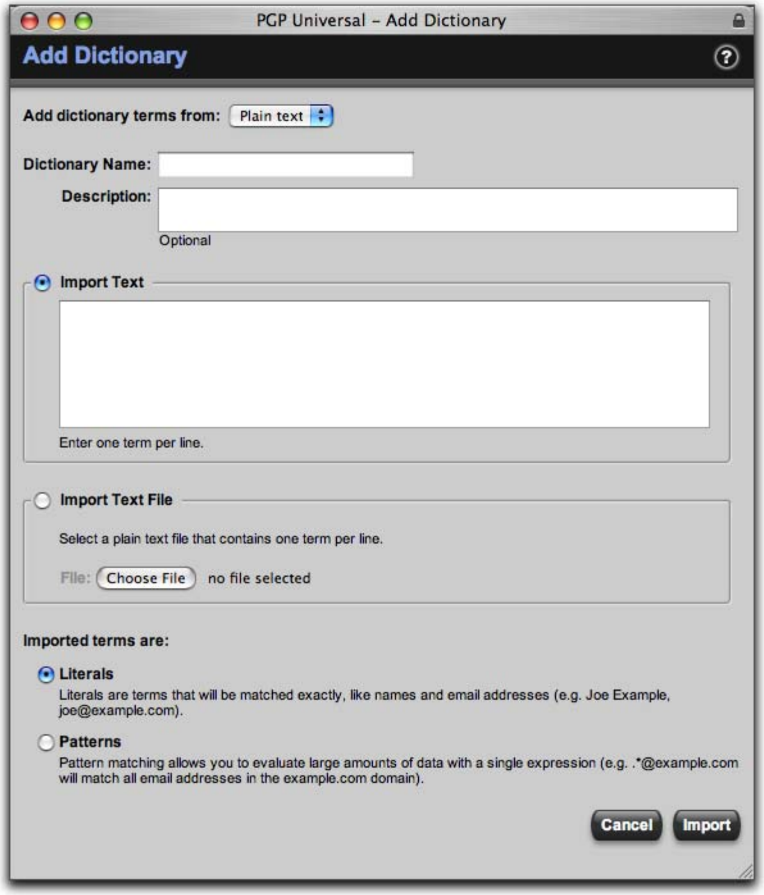
You can add dictionaries to use with specific policy rules.

Adding a User-Defined Dictionary

To add a user-defined dictionary:

1 At the bottom of the Dictionaries card, click **Add Dictionary**.

The Add Dictionary dialog appears.



PGP Universal – Add Dictionary

Add Dictionary

Add dictionary terms from: Plain text

Dictionary Name:

Description:

Optional

● Import Text

Enter one term per line.

○ Import Text File

Select a plain text file that contains one term per line.

File: Choose File no file selected

Imported terms are:

● Literals

Literals are terms that will be matched exactly, like names and email addresses (e.g. Joe Example, joe@example.com).

○ Patterns

Pattern matching allows you to evaluate large amounts of data with a single expression (e.g. .*@example.com will match all email addresses in the example.com domain).

2 Select from the drop-down whether you are adding plain text terms, an XML file, or a ZIP file.

3 Add a Dictionary Name and Description. For example, you can add a dictionary named Managers and the description might be "Messages from these users must always be encrypted and signed."

4 Type in or paste a list of terms, each separated on its own line, or choose **Import Text File** and select a file to import.

5 Specify whether the terms are Patterns or Literals.

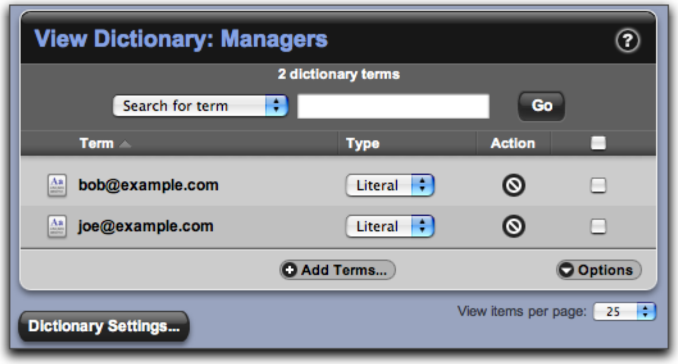
6 Click **Import**.

Editing a User-Defined Dictionary

To edit a user-defined dictionary:

1 Click the name of the domain in the Name column.

The View Dictionary card appears.



View Dictionary: Managers

2 dictionary terms

Term	Type	Action	□
bob@example.com	Literal	⊘	□
joe@example.com	Literal	⊘	□

View items per page: 25

2 To remove terms from the dictionary, click the icon in the Delete column of the term you wish to delete.

A confirmation dialog appears.

3 Click **OK**.

4 Click **Add Terms** to add to the contents of the dictionary.

The Edit Dictionary dialog appears.

5 Select from the drop-down whether you are adding plain text terms, and XML file, or a ZIP file.

6 Type in or paste a list of terms, each separated on its own line, or choose **Import Text File** and select a file to import.

7 Specify whether the terms are Patterns or Literals.

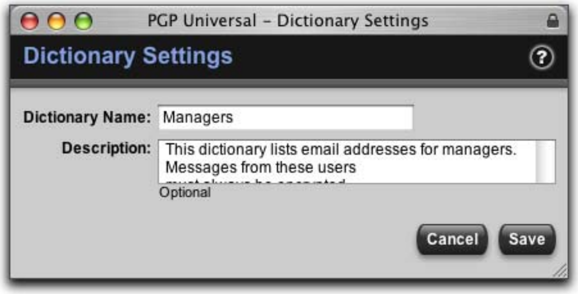
8 Choose whether to append the new terms to the current contents of the dictionary or to replace the existing terms with the new terms.

9 Click **Import**.

10 Click the **Dictionary Settings** button to change the name or description of the dictionary.

> If you change the name of a dictionary, any rule that refers to the original dictionary name will become invalid.

The Dictionary Settings dialog appears.



PGP Universal – Dictionary Settings

Dictionary Settings

Dictionary Name: Managers

Description: This dictionary lists email addresses for managers. Messages from these users

Optional

11 Choose the appropriate setting, then click **Save**.

Deleting a Dictionary

Use this procedure to delete dictionaries. You cannot delete the default dictionaries.

> If you do not want a rule to use a particular dictionary, you can simply remove it from that rule's conditions. If you delete a dictionary from the Dictionaries card, it will no longer be available for any rule in your mail policy and can make your rules invalid.

To delete a dictionary:

1 Click the icon in the Delete column of the dictionary you wish to delete.

A confirmation dialog appears.

2 Click **OK**.

The dictionary you specified is deleted.

Exporting a Dictionary

To export a dictionary:

1 Click the checkbox at the far end of the row for each dictionary you want to export.

2 From the **Options** drop-down list, select **Export Selected**.

The dictionary you chose is exported to your desktop as an XML file. If you exported more than one dictionary, the XML files are inside a ZIP file called dictionaries.zip.

Searching the Dictionaries

You can search dictionaries in 2 different ways.

- **Search for exclusion/term** allows you to find a term in the dictionary. This substring search returns entries that exactly match the characters you enter into the search box. For example, if you have dictionary entries "jsmith@example.com" (literal) and "j.*@example.com" (pattern), and you search for "@example", both entries would be returned.

- **Evaluate expression** allows you to determine whether any term in the dictionary matches a certain string. You can use this as a trial of the dictionary as it would act in a rule condition. Enter in a test string that you know should match a dictionary entry to see if the string would trigger the action in the rule. The results of the evaluation are the matches for the test string. For example, if you have dictionary entries "jsmith@example.com" (literal) and "j.*@example.com" (pattern), and you evaluate the expression "jsmith", neither entry is returned. If you evaluate "jsmith@example.com", both entries are returned. If you evaluate the expression "jgreen@example.com", only the pattern "j.*@example.com" is returned.

1. From the Policy>Dictionaries card, click the name of the dictionary you want to search.

2. Select **Search for exclusion/Search for term** or **Evaluate expression** from the drop-down list.

3. Enter the term you want to find or evaluate.

4. Click **Go**.

   A list of terms that fit the criteria you specified appears.

To clear the search, click the cancel button to the right of the search field.

18 Keyservers, SMTP Servers, and Mail Policy

This chapter describes the Servers card, which allows you to add keyserver and SMTP server information to the PGP Universal Server. Policy rules can then refer to those servers to enforce your mail policy.

This feature is available with PGP Universal Gateway Email and PGP Desktop Email.

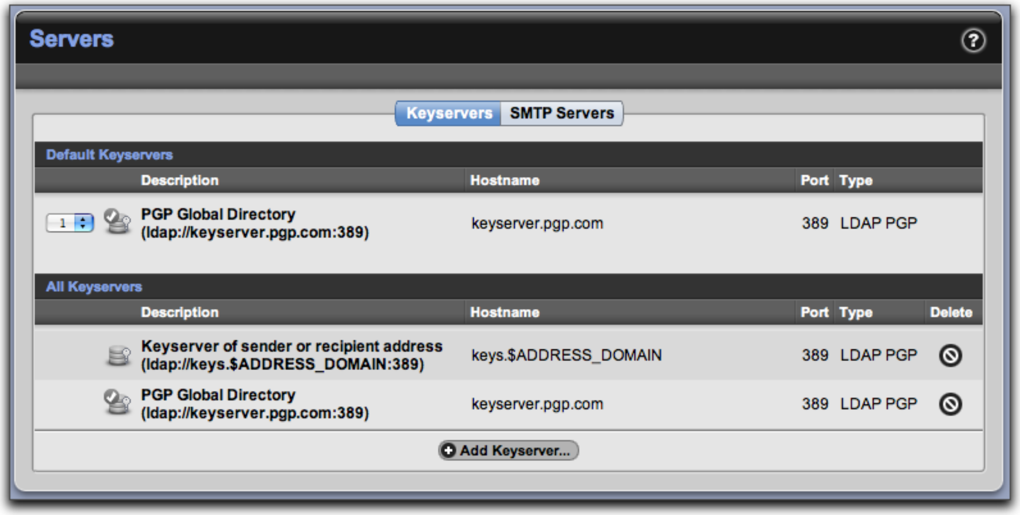
Topics in this chapter include:

Overview

This tab allows you to add and manage information about servers outside your network. There are two tabs on this screen, Keyservers and SMTP Servers. Policy rules can specify the keyservers listed on this tab for recipient key searches, as required by mail policy. The SMTP servers you add to this tab are used by policy rules to archive messages, as required by mail policy.

Keyservers

Mail policy contains rules that require a message be signed or encrypted to a recipient's key. The PGP Universal Server will always look in its own databases for keys in the Internal Users, External Users, and Key Cache lists. If the PGP Universal Server does not have a copy of a particular key, the policy may then specify searching external sources for the key. The Keyservers tab of the Servers card allows you to add and edit information for those external keyservers.



Default Keyservers

	Description	Hostname	Port	Type
1	PGP Global Directory (ldap://keyserver.pgp.com:389)	keyserver.pgp.com	389	LDAP PGP

All Keyservers

Description	Hostname	Port	Type	Delete
Keyserver of sender or recipient address (ldap://keys.$ADDRESS_DOMAIN:389)	keys.$ADDRESS_DOMAIN	389	LDAP PGP	⊘
PGP Global Directory (ldap://keyserver.pgp.com:389)	keyserver.pgp.com	389	LDAP PGP	⊘

Refer to Chapter 15, "Setting Mail Policy" for information on how to use keyservers with policy rules.

The keyservers on the Keyservers tab are divided into two groups:

- All keyservers available to be searched for recipient keys are listed under All Keyservers. You can use the Policy>Mail Policy card to select which keyservers a mail policy rule searches.
- Keyservers in the default set are referred to when legacy client software verifies signatures. If PGP Desktop or PGP Universal Satellite requests a key, the PGP Universal Server will search the default keyservers for the correct key, based on the key ID in the email. Legacy client software includes PGP Desktop 9.0.x and PGP Universal Satellite 2.0.x.

You can specify the order in which default keyservers are searched by numbering the keyservers in the order you want them searched.

The PGP Universal Server has one pre-selected Default Keyserver, the PGP Global Directory at ldap://keyserver.pgp.com:389. The PGP Global Directory is a free, publicly available keyserver hosted by PGP Corporation that lets PGP users find the public keys of other PGP users with whom they want to exchange secure messages. It provides quick and easy access to the universe of PGP keys. If your policy requires it, you can keep the PGP Global Directory from being searched for keys by removing it from the policy rules' Key Lookup lists. Refer to Chapter 15, "Setting Mail Policy" for more information on Key Lookup.

The PGP Universal Server has one other preinstalled keyserver. This keyserver's hostname appears on the Keyservers tab as *keys.$ADDRESS_DOMAIN*. If you add this keyserver to the Key Search tab for a rule, PGP Universal Server will search for a keyserver at the domain given in the recipient's email. For example, if the rule states that a message sent to jsmith@company.com must be encrypted, and the recipient's key is not already stored on the PGP Universal Server, the PGP Universal Server can search for the key in a keyserver called keys.company.com. Keys found in this type of keyserver will be used for encrypting messages.

You can add more searchable keyservers to the Keyservers card. Keyservers can be PGP keyservers or X.509 directories.

You can also add new locations to search for keys directly from a mail policy rule's Key Lookup tab. Servers entered this way will be automatically added to the list on the Policy>Servers card.

PGP Universal Server does not support HTTP keyservers. Key queries to HTTP keyservers will be unsuccessful.

Adding or Editing a Keyserver

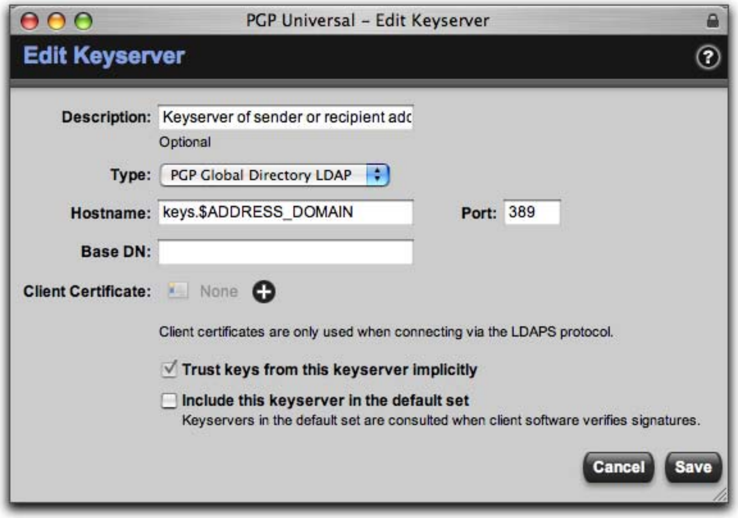
If you know of a keyserver or directory outside your own network that may contain keys belonging to people receiving mail from inside your network, you can add that keyserver to the list of searchable keyservers. The PGP Universal Server will search the specified keyserver for recipient keys or certificates, if mail policy rules containing that keyserver apply to the message being sent.

The following procedure covers both adding and editing keyservers.

To add or edit a keyserver:

1 Click **Add Keyserver** on the Keyservers tab of the Servers card, or click the name of the keyserver you want to edit.

The Add (or Edit) Keyserver dialog appears.



PGP Universal – Edit Keyserver

Edit Keyserver

Description: Keyserver of sender or recipient adc
Optional

Type: PGP Global Directory LDAP

Hostname: keys.$ADDRESS_DOMAIN Port: 389

Base DN:

Client Certificate: None

Client certificates are only used when connecting via the LDAPS protocol.

☑ Trust keys from this keyserver implicitly

□ Include this keyserver in the default set
Keyservers in the default set are consulted when client software verifies signatures.

2 If you choose, you can enter a description of the keyserver into the Description field. The description will appear in the Key Lookup area of rules in your mail policy, to help you choose keyservers for each mail policy rule.

3 Select the keyserver type and method of access from the Type drop-down list:

– **PGP Keyserver LDAP:** Select this option to connect to a PGP Keyserver via LDAP. The default port is 389.

- **PGP Keyserver LDAPS:** Select this option to connect to a PGP Keyserver via LDAPS. The default port is 636.
- **X.509 Directory LDAP:** Select this option to connect to an LDAP directory to search for X.509 certificates. The default port is 389.
- **X.509 Directory LDAPS:** Select this option to connect to an LDAPS directory to search for X.509 certificates. The default port is 636.
- **PGP Global Directory LDAP:** Select this option to connect to the PGP Global Directory via LDAP. The default port is 389. The host is ldap://keyserver.pgp.com.
- **PGP Global Directory LDAPS:** Select this option to connect to the PGP Global Directory via LDAPS. The default port is 636. The host is ldaps://keyserver.pgp.com.

4. Enter a hostname or IP address in the **Hostname** field.
5. If you want to change the default port, enter the desired port number in the **Port** field.
6. Enter a base distinguished name (base DN) in the **Base DN** field, if appropriate.
7. If you selected a X.509 Directory LDAP or PGP Global Directory LDAP, you can specify a client certificate to be used to authenticate when the PGP Universal Server queries the directory. Click the **Add** icon next to **Client Certificate** to import a certificate or generate a CSR or self-signed certificate using the New Keyserver Client Certificate dialog.

   a. To add an existing certificate, click **Import**, select the certificate file or paste in the certificate block, and enter an optional passphrase.

   b. To generate a self-signed certificate or CSR, enter the appropriate information into the New Keyserver Client Certificate dialog and click either **Generate Self-signed** or **Generate CSR**.
8. Select **Trust keys from this keyserver implicitly** to automatically trust all keys from this keyserver.
9. Select **Include this keyserver in the default set** to add the keyserver to the default set for client software signature verification requests.
10. On the Add Keyserver dialog, click **Save**.

    The Servers card reappears.

Deleting a Keyserver

If you do not want a rule to search a particular keyserver, you can simply remove it from that rule's Key Lookup. If you delete a keyserver from the Servers card, it will no longer be available for any rule in your mail policy and can make your rules invalid.

To delete a keyserver:

1 Click the **Delete** icon to the right of the name of the keyserver you want to delete.

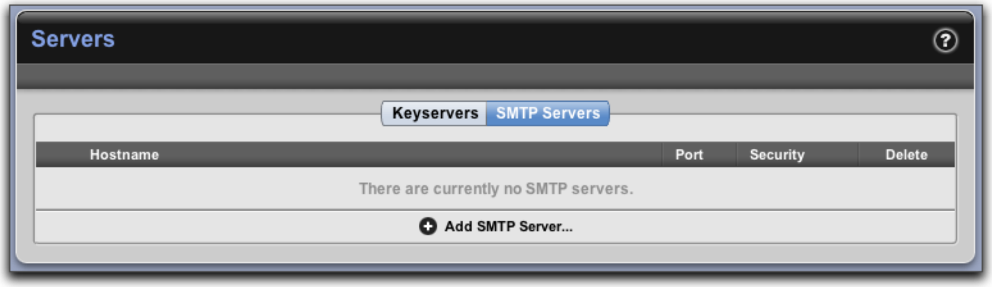
   A confirmation dialog appears.

2 Click **OK**.

   The keyserver you specified is deleted.

SMTP Servers

The SMTP servers you add to this tab are used by policy rules to archive messages, as required by mail policy. When you create a rule with the action *Send copy to alternate SMTP server*, the PGP Universal Server sends a copy of the message to the SMTP server specified in the rule. See Chapter 15, "Setting Mail Policy" for more information on SMTP servers work with policy rules.



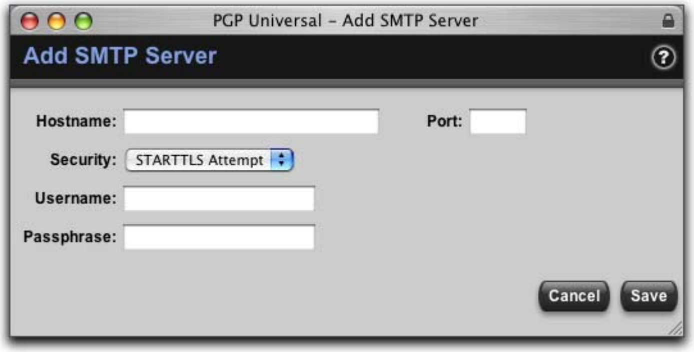
Hostname	Port	Security	Delete
There are currently no SMTP servers.			

Adding or Editing an SMTP Server

To add or edit an SMTP server:

1 Click the SMTP Servers tab on the Servers card.

2 Click **Add SMTP Server** or click the hostname of the SMTP Server you want to edit. The Add SMTP Server dialog appears.



Hostname:

Port:

Security: STARTTLS Attempt

Username:

Passphrase:

3 Enter a hostname or IP address in the **Hostname** field.

4 If you want to change the default port, enter the desired port number in the **Port** field.

5 Select the security type from the **Security** drop-down:

- **STARTTLS Attempt**: Allows the security of the connection to be upgraded to TLS via negotiation when communications begin. The SMTP server must support STARTTLS for the upgrade to occur.
- **STARTTLS Disable**: STARTTLS will not be allowed for this connection.
- **STARTTLS Require**: Requires that the connection be secured by TLS. Only select this option if you are confident that the SMTP server supports upgrading the security to STARTTLS.
- **SSL**: Uses SSL to protect the connection between the SMTP server and the PGP Universal Server.

6 Enter a username into the **Username** field if you chose a secure SMTP connection.

7 Enter a passphrase into the **Passphrase** field for the secure SMTP connection.

8 On the Add SMTP Server dialog, click **Save**.

The Servers card reappears.

Deleting an SMTP Server

> ! If you do not want a rule to archive messages to an SMTP server, you can simply remove the server from the rule. If you delete an SMTP server from the Servers card, it will no longer be available for any rule in your mail policy and can make your rules invalid.

To delete an SMTP server:

1 Click the **Delete** icon to the right of the name of the SMTP server you want to delete.

A confirmation dialog appears.

2 Click **OK**.

The SMTP server you specified is deleted.

19 Managing Keys in the Key Cache

This chapter describes the key cache, which stores public keys on the PGP Universal Server.

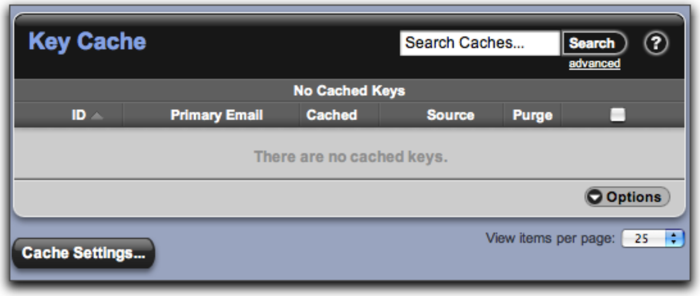
This feature is available with PGP Universal Gateway Email and PGP Desktop Email.

Topics in this chapter include:

- "Overview"
- "Changing Cached Key Timeout" on page 164
- "Searching the Key Cache" on page 165

Overview

Public keys for remote users are automatically cached on the PGP Universal Server on the System>Key Cache card. Whenever the PGP Universal Server can harvest a key from the mailflow or finds a recipient key on an external keyserver, the key is stored in the key cache. As long as the key is in the key cache, it can be used to encrypt future email, without requiring a key search.



ID	Primary Email	Cached	Source	Purge	□

There are no cached keys.

Keys stay in the cache for a time period you specify. After the specified time period, the keys are purged.

If you have clustered PGP Universal Servers, there will be duplicate keys in the cache, because keys cached from the mailflow are replicated across the cluster and the same key may already be cached on more than one cluster member. PGP Universal Server does not share keys found on external keyservers between cluster members.

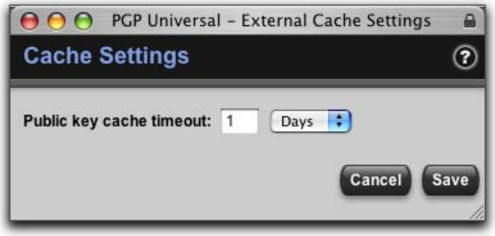
Bound PGP Desktop installations harvest S/MIME certificates from messages and send those certificates, and all certificates in the chain, to the PGP Universal Server key cache.

Changing Cached Key Timeout

To change the cache settings:

1 On the System>Key Cache card, click the **Cache Settings** button.

The Cache Settings dialog appears.



PGP Universal – External Cache Settings

Cache Settings

Public key cache timeout: 1 Days

2 Enter the desired number in the **Public key cache timeout** field and then select **Hours** or **Days**, as appropriate.

3 Click **Save** to save changes to the scheduled cache timeout period.

The Key Cache card reappears.

Purging Keys from the Cache

Purging the cache is useful, for instance, if you are aware that a given key has been updated and you want to force the PGP Universal Server to retrieve the latest copy before the cache expires.

1 To purge a single key manually, click the purge icon next to the key you want removed.

2 To purge multiple public keys and certificates currently in the cache, click the checkbox at the far right end of the row of each of the keys you want to purge.

3 Select **Purge Selected** from the Options menu or select **Purge All** to purge all the keys in the cache.

A confirmation dialog appears.

4 Click **OK**.

Trusting Cached Keys

1 To mark as trusted the public keys and certificates currently in the cache, click the checkbox at the far right end of the row of each of the keys you trust.

2 Select **Trust Selected** from the Options menu.

3 The newly trusted key is added to the list of external users on the Users>External Users card.

Viewing Cached Keys

You can view information about each key in the cache, and either purge the key or mark it trusted.

1 From the System>Key Cache card, click the ID of the key you want.

  The Key Information dialog appears. The dialog shows the Key ID, the User ID, when the key was created, when the key expires, when the key was cached, on which keyserver the key was found, and when the key will be purged, as well as a list of email addresses associated with that key.

2 Click the **Trust Key** button to trust this key. The key is added to the list of external users.

3 Click the **Purge Key Now** button to purge this key from the cache.

4 Click **OK** to save changes and close the dialog.

Searching the Key Cache

To find a cached key using a simple search, enter the criteria for which you want to search, and click the **Search** button. A list of users that fit the criteria you specified appears.

To search using advanced criteria:

1 On the Key Cache card, click **advanced**.

  The User Search dialog appears.

2 Specify your criteria:

  – In the drop-down list on the left, select search criteria from: **Key ID**, **Primary Email**, **Key Cached**, or **Source**.

  – In the middle drop-down list, select how to limit the search, for example: **contains**, **does not contain**, **is on**, **is before**, et cetera.

  – In the text box on the right, enter or select the criteria you want to search for.

  – If you want to use more search criteria, click the plus sign icon and enter the appropriate criteria. Returned results will match all the search criteria you enter.

3 Click **Search**.

  A list of keys that fit the criteria you specified appears.

To clear the search, click the cancel button to the left of the search field.

20 Scanning Email for Viruses

The AntiVirus feature lets you integrate enterprise-quality virus scanning from Symantec into your PGP Universal Server environment. When licensed and enabled, virus scanning is always active, even if the PGP Universal Server is in Learn Mode.

Virus scanning is a PGP Universal Server–only feature, not applicable for PGP Desktop users. The AntiVirus features are available with PGP Universal Gateway Email only.

> You must be using a PGP Universal Server license that includes the Symantec AntiVirus™ Scan Engine, or the AntiVirus tab does not appear in the administrative interface.

Topics in this chapter include:

AntiVirus Scanning and Mail Policy

In previous versions of PGP Universal Server, virus scanning was controlled though settings on the proxy interface. PGP Universal Server virus scanning is controlled through a combination of mail policy and the AntiVirus screen. As installed, the virus scanning action is set in the Outbound Virus Scan and the Inbound policy chains. When infected messages are found, PGP Universal Server can either remove infected attachments from the message, or note that the message is infected and pass it along for further processing. For more information on mail policy, refer to Chapter 15, "Setting Mail Policy".

The AntiVirus feature's Scanning Options dialog allows you to specify what types of attachments you want scanned, and whether you want PGP Universal Server to obey or override mail policy in handling infected attachments. For more information, refer to "Scanning Options" on page 171.

Messages and their attachments are scanned according to mail policy. In the default installation mail policy, messages are scanned at the following times:

- **SMTP outbound mail:** Before encryption.
- **SMTP inbound mail:** After decryption.
- **PGP Universal Web Messenger mail:** Mail from internal users, before the message is saved in the database. Replies from external users, on arrival.
- **POP and IMAP:** After the message is decrypted and before it is picked up.

If you are using the IMAP protocol with a PGP Universal Server that is internally placed, the AntiVirus feature will only be scanning encrypted messages for server-managed key users, which is unlikely to discover any viruses, except in cases where the virus is sent by another internal user. A second PGP Universal Server should be installed in gateway placement so that both cleartext and encrypted messages are scanned for viruses. If your PGP Universal Server is in gateway placement, or you are using the POP protocol, the unencrypted messages are virus–scanned.

PGP Universal Satellite messages are also scanned for viruses, but because most PGP Universal Satellite messages traversing a PGP Universal Server are already encrypted, it is unlikely any viruses will be found. The server will not decrypt an already encrypted message that is passing through it so that it can scan the message for viruses.

Viruses may be found in those cases where PGP Universal Satellite messages that are traversing a PGP Universal Server are not encrypted (if the recipient is a PGP Universal Web Messenger user, or if the policy specifies signed but non-encrypted mail, for example).

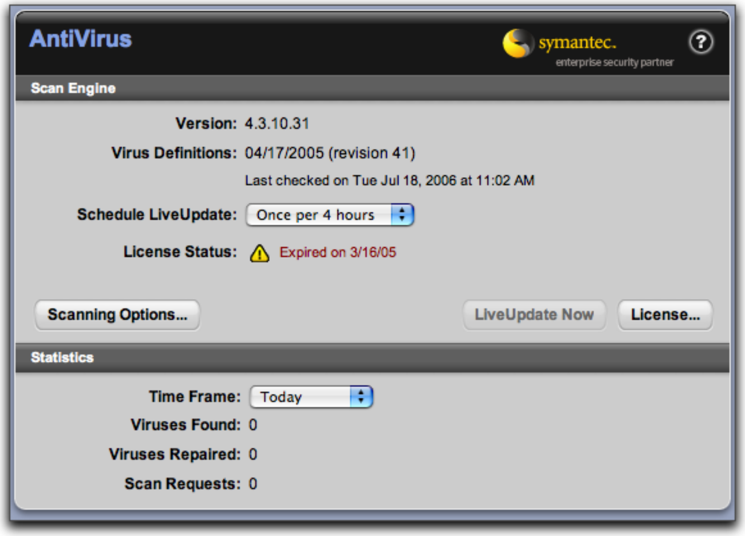
Because the PGP Universal Satellite software has no virus-scanning capabilities, PGP Corporation strongly recommends desktop-based virus scanning for PGP Universal Satellite users.

When the Symantec AntiVirus feature is licensed on a PGP Universal Server, virus scanning is automatically enabled on all configured services through replication of mail policy settings. When you license the AntiVirus feature on the Primary PGP Universal Server in a cluster, the Secondary servers in the cluster are automatically licensed for Symantec AntiVirus.

Global AntiVirus settings (including license information, scanning options, and File Blocking options) are synchronized between the cluster members.

The AntiVirus Card

The AntiVirus card displays information about the AntiVirus feature for this PGP Universal Server.



AntiVirus

Scan Engine

Version: 4.3.10.31

Virus Definitions: 04/17/2005 (revision 41)

Last checked on Tue Jul 18, 2006 at 11:02 AM

Schedule LiveUpdate: Once per 4 hours

License Status: ⚠ Expired on 3/16/05

Statistics

Time Frame: Today

Viruses Found: 0

Viruses Repaired: 0

Scan Requests: 0

(If a PGP Universal Server has a license that includes AntiVirus support, but the Symantec license is not installed, a License button appears on the AntiVirus card and the other features are disabled.)

The Scan Engine section of the AntiVirus card includes:

- **Version:** Displays the version of the Symantec scan engine being used.
- **Virus Definitions:** Displays the version of the virus definitions being used, when LiveUpdate was last checked for updates, and if a LiveUpdate is in progress.
- **Schedule LiveUpdate:** Lets you select the LiveUpdate frequency. Options are Off; Once per hour; Once per 2, 3, 4, 6, 8, 12 hours; or Once per day. The default setting is Once per 4 hours.
- **License Status:** Shows for how long the license will be valid.
- **Scanning Options button:** Click to bring up the AntiVirus Scanning Options dialog, which is described in "Scanning Options" on page 171.
- **LiveUpdate Now button:** Click to have the LiveUpdate feature check for updates to the Symantec virus definitions.

  LiveUpdate Now functionality operates independently for members of a cluster; if you want to check for updates for all PGP Universal Servers in a cluster, you must click the LiveUpdate Now button in the administrative interface of each PGP Universal Server in the cluster.
- **License button:** Click to enter the AntiVirus license (if you haven't already) by bringing up the Enter AntiVirus License dialog, which is described in "AntiVirus Licensing" on page 170.

The Statistics section of the AntiVirus card allows you to view information about viruses scanned and found, including:

- **Time frame:** Specify the time frame for the other statistics. Options are Today, This week, This month, This year, and All statistics. The default is Today.
- **Viruses found:** The total number of viruses found in the files scanned in the specified time frame.
- **Viruses repaired:** The total number of viruses that were cleaned in the specified time frame.
- **Scan requests:** The total number of requests for virus scans in the specified time frame.

Statistics shown are for this PGP Universal Server.

AntiVirus Licensing

Using the AntiVirus feature on a PGP Universal Server requires two licenses: one from PGP Corporation to activate the PGP Universal Server and the Symantec AntiVirus™ Scan Engine feature (this license is different from the standard PGP Universal Server license, which does not activate the AntiVirus feature) and one from Symantec to activate virus scanning and LiveUpdate.

If a PGP Universal Server is part of a cluster, only the Primary server in the cluster needs to license the AntiVirus feature; the license is then synchronized with the Secondary servers in the cluster.

To license AntiVirus on a PGP Universal Server:

1. Obtain a PGP Universal Server license from PGP Corporation that includes Symantec AntiVirus support (the standard PGP Universal Server license does not include AntiVirus support).

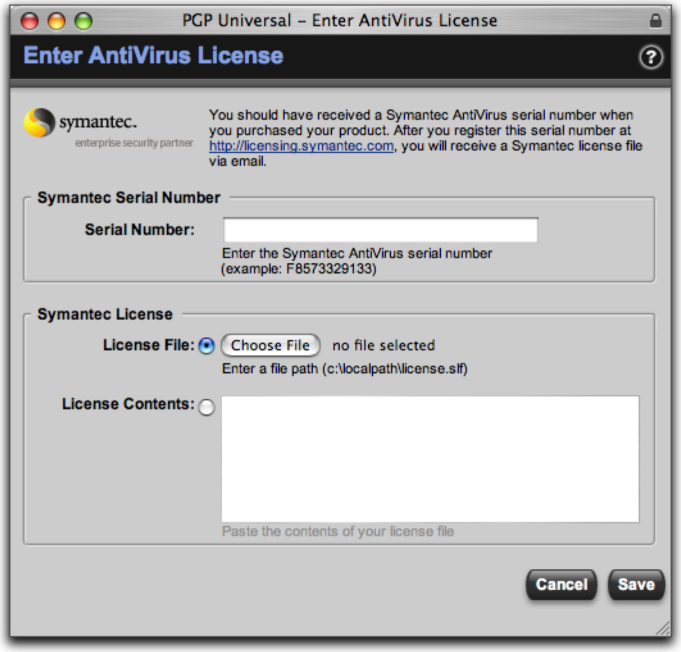
   Included with the PGP Universal Server license will be a Symantec serial number.

2. Using a Web browser, navigate to **http://licensing.symantec.com**.
3. Enter the Symantec serial number you received from PGP Corporation and complete the required information.

   A Symantec AntiVirus license file that includes perpetual scanning and 1 year of LiveUpdates will be emailed to you.

4. On the PGP Universal Server you are licensing for AntiVirus, access the administrative interface.
5. On the AntiVirus card, click the **License** button.

   The Enter AntiVirus License dialog appears.



PGP Universal – Enter AntiVirus License
Enter AntiVirus License
symantec.
enterprise security partner
Choose File
Cancel
Save

You should have received a Symantec AntiVirus serial number when you purchased your product. After you register this serial number at http://licensing.symantec.com, you will receive a Symantec license file via email.

Symantec Serial Number

Serial Number:

Enter the Symantec AntiVirus serial number (example: F8573329133)

Symantec License

License File: ● no file selected

Enter a file path (c:\localpath\license.slf)

License Contents: ○

Paste the contents of your license file

6 In the Symantec Serial Number section, enter the Symantec serial number you received from PGP Corporation when you got the PGP Universal Server license that includes AntiVirus support.

7 In the Symantec License section, click **Choose File** next to **License File** and navigate to the AntiVirus license file you received from Symantec, or copy the contents of the AntiVirus license file and paste it into the **License Contents** field.

8 Click the **License** button.

The AntiVirus License Status dialog reappears, showing the updated AntiVirus license status of the PGP Universal Server.

A confirmation message tells you that virus scanning is now enabled on all currently configured services.

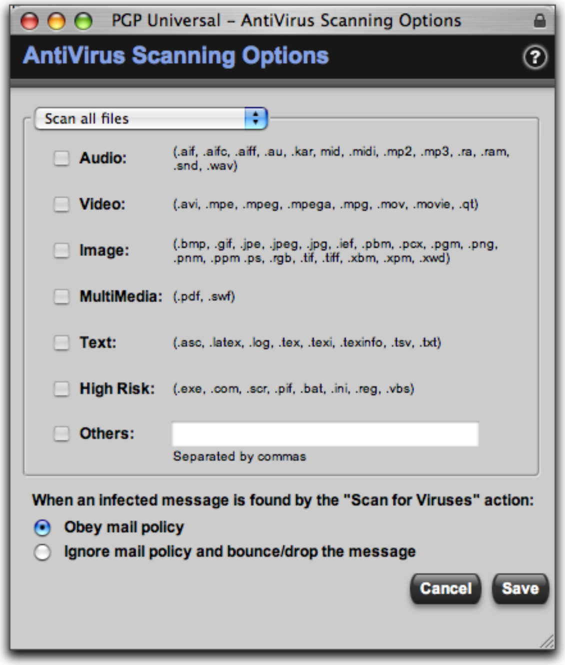
Scanning Options

The AntiVirus feature gives you control over what file types will be scanned on the AntiVirus Scanning Options dialog.

To specify what file types you want scanned:

1 On the AntiVirus card, click the **Scanning Options** button.

The AntiVirus Scanning Options dialog appears.


PGP Universal – AntiVirus Scanning Options
AntiVirus Scanning Options
?

Scan all files

□ **Audio:** (.aif, .aifc, .aiff, .au, .kar, mid, .midi, .mp2, .mp3, .ra, .ram, .snd, .wav)

□ **Video:** (.avi, .mpe, .mpeg, .mpega, .mpg, .mov, .movie, .qt)

□ **Image:** (.bmp, .gif, .jpe, .jpeg, .jpg, .ief, .pbm, .pcx, .pgm, .png, .pnm, .ppm .ps, .rgb, .tif, .tiff, .xbm, .xpm, .xwd)

□ **MultiMedia:** (.pdf, .swf)

□ **Text:** (.asc, .latex, .log, .tex, .texi, .texinfo, .tsv, .txt)

□ **High Risk:** (.exe, .com, .scr, .pif, .bat, .ini, .reg, .vbs)

□ **Others:**

Separated by commas

When an infected message is found by the "Scan for Viruses" action:

● **Obey mail policy**

○ **Ignore mail policy and bounce/drop the message**

2 Specify what file types you want scanned:

- **Scan all files:** All file types will be scanned.
- **Scan only these file types**: Only those file types selected on the Anti- Virus Scanning Options dialog will be scanned. Make sure you specify all of the file types you want scanned. At least one type must be selected.
- **Scan all file types except for:** All file types except those selected on the AntiVirus Scanning Options dialog will be scanned. Make sure to select only those file types you do not want scanned. At least one type must be selected.

3 If there are other file types you want to scan for, put a checkmark next to **Others** and enter the appropriate extensions in the text box.

Make sure to separate entries using commas: for example, ".dll," without the quotes.

You can set the antivirus feature to scan .zip files. However, non-.zip files contained in the .zip file will not be scanned unless you also set the antivirus feature to scan for those files types. For example, for the antivirus feature to scan .doc files inside an attached .zip file, you must enable scanning for both .zip and .doc files.

4 You can choose what to do when an infected attachment is found. In the **When an infected attachment is found by the "Scan for Viruses" action** section, select:

- **Obey mail policy:** When infected attachments are found, PGP Universal Server will obey the Scan for Viruses action in mail policy, and either remove the infected attachment or mark the message as infected and pass it along for further processing.

- **Ignore mail policy and bounce/drop the message:** When infected attachments are found, PGP Universal Server will override the setting in the mail policy Scan for Viruses action. Inbound messages are blocked and senders receive the **Message Bounced — Infected** system message. Outbound messages are bounced back to the sender. No other mail policy processing will be applied to the message.

  Refer to "Handling Infected Attachments" on page 173 for details on how these settings interact with mail policy.

Infected messages from external users are **not** returned to the sender, because this could be used as a virus distribution method.

5 Click **Save**.

Handling Infected Attachments

The AntiVirus feature of PGP Universal Server handles messages with infected attachments based on four factors:

- The mail policy action specified for infected messages.
- The infected attachment setting on the AntiVirus Scanning Options dialog.
- Where the message originated.
- Whether or not the message can be cleaned.

Ignore Mail Policy and Bounce/Drop the Message

This AntiVirus Scanning Options selection overrides mail policy.

When infected attachments are found, PGP Universal Server will override the **Scan for Viruses** action in mail policy and instead will block or bounce messages with infected attachments. Inbound messages are blocked and senders receive the **Message Bounced — Infected** system message. Outbound messages are bounced back to the sender. No other mail policy processing will be applied to the message.

This setting overrides mail policy, even if mail policy specifies that the message should be cleaned of any infected attachments. No attempt is made to clean an infected attachment. How the message is handled depends on where it originated:

- **If the message originated from an external user,** the message and the infected attachment is silently deleted; no notification is sent to the external sender nor to the internal recipient. If the message includes other attachments that are not infected, they will also be deleted.
- **If the message originated from an internal user,** the message and the infected attachment are deleted. If the message includes other attachments that are not infected, they will also be deleted. A separate message, the **Message Bounced — Infected** system message, is sent back to the internal sender of the message,

stating that the message (identified by subject and date) and the infected attachment were deleted. The external recipient of the original message is not notified that the sender attempted to send a message to them.

Obey Mail Policy

This AntiVirus Scanning Options selection enforces mail policy.

The mail policy action **Scan for Viruses** provides two possible treatments for infected messages. The administrator can choose to have PGP Universal Server clean the message of any infected attachments and then pass the message on, or can have PGP Universal Server mark the message as infected and pass it on for further processing, for example dropping the message.

If the action specifies **Clean the message of any infected attachment**, PGP Universal Server attempts to clean the infected attachment. How the message is handled depends on where the message originated and whether or not the attempt to clean the infected attachment was successful.

- If the message originated from an external user:
  - **If the infected attachment can be repaired,** the message and the now virus-free attachment are sent to the internal recipient. Neither the external sender nor the internal recipient are notified that the infected attachment has been repaired.

    If a message includes an infected attachment and one or more uninfected attachments, and the infected attachment cannot be repaired, the infected attachment will be deleted, but the message and the uninfected attachments will be delivered.
  - **If the infected attachment cannot be repaired,** the message and the infected attachment are silently deleted; no notification is sent to the external sender nor the internal recipient.
- If the message originated from an internal user:
  - **If the infected attachment can be repaired,** the message and the now virus-free attachment are sent to the external recipient. Neither the internal sender nor the external recipient are notified that the infected attachment has been repaired.
  - **If the infected attachment cannot be repaired,** the message and the infected attachment are deleted. If the message includes other attachments that are not infected, they will also be deleted. A separate message, not the original, is bounced back to the internal sender of the message, stating that the message (identified by subject and date) and the infected attachment have been deleted. The external recipient of the original message is not notified that the sender attempted to send a message to them.

> If the AntiVirus feature finds one infected file in a Zip file that includes multiple files, and it cannot clean the one infected file, it will delete the infected file from the Zip file and then send the message and the attached Zip file to the recipient. The recipient will not see any notification that the infected file was deleted from the Zip file.

21 Blocking Files

This chapter describes the File Blocking feature.

This feature is available with PGP Universal Gateway Email.

> You must be using a PGP Universal Server license that includes Symantec AntiVirus or the File Blocking tab is not selectable on the administrative interface. If your PGP Universal Server has a license that supports AntiVirus but the Symantec license has not been entered, File Blocking functionality is disabled. Refer to Chapter 9, "Licensing Your Software" for more information.

File Blocking and Mail Policy

The File Blocking Settings card lets you block attachments that match any of the filenames you specify. For example, if a new virus application appears, you can quickly prevent it from entering your network using File Blocking even before the virus definitions are updated. File Blocking is especially useful for blocking message with attachments that are known to be viruses; mydoom.exe, for example.

You can also enable file blocking through mail policy, by creating rules using the conditions **Message has an attachment whose name** or **Message has an attachment whose type**, and then choosing to bounce or drop matching messages. Refer to Chapter 15, "Setting Mail Policy" for more information on these mail policy conditions.

The File Blocking feature requires a Symantec AntiVirus license, but the mail policy file blocking function does not. The File Blocking feature can simply remove an attachment, while mail policy can only drop or bounce email.

File Blocking interacts with the mail policy engine by being invoked when the **Scan For Viruses** action is performed. PGP Universal Server scans for both File Blocking and AntiVirus at the same time, and blocks any matching files at that time.

> File Blocking settings can override mail policy. If you set mail policy to scan and continue processing infected messages, but File Blocking is set to reject any message with a specified filename, infected messages that also contain a matching attachment will always be blocked and will not be passed on.

If you create a mail policy rule to search for and drop any message with a specific attachment, but the File Blocking feature is set to delete the attachment and send the message, mail policy rule processing order determines which action occurs. If **Scan for Viruses** appears in the policy chain before the rule that searches for attachments, the attachment and message are handled as the File Blocking feature specifies. The mail policy attachment rule will never be matched. If your mail policy attachment rule comes before **Scan for Viruses** in the policy chain, then mail policy determines how the message is processed and matching messages are dropped.

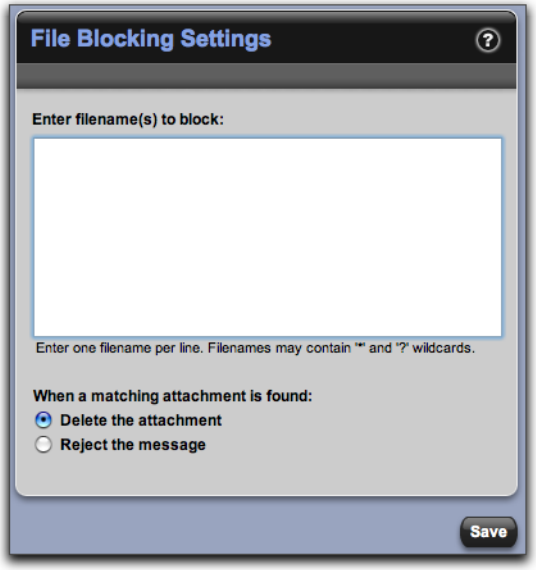
If an attachment is deleted because it matches a listed filename, neither the sender or the recipient is notified.

Adding a Filename to be Blocked

To add a filename to be blocked:

1 In the administrative interface, select **Mail** and then click on the **File Blocking** tab.

The File Blocking Settings card appears.



File Blocking Settings

Enter filename(s) to block:

Enter one filename per line. Filenames may contain '*' and '?' wildcards.

When a matching attachment is found:

● Delete the attachment

○ Reject the message

2 Click in the box under **Enter filename(s) to block** and enter a filename that you want blocked.

3 Press **Enter** when you have finished entering the filename.

Enter one filename per line. Wildcards are allowed. Wildcard * represents a string, and ? represents a single character. For example, ***.bat** or **?.bat**.

4 In the **When a matching attachment is found** section, select:

- **Delete the attachment:** Deletes just the attachment; the underlying message will be delivered to the recipient. There will be no notification that the attachment was deleted.
- **Reject the message:** Both the attachment and the message will be deleted.

5 Click **Save**.

22 Configuring Mail Proxies

This chapter describes the mail proxies that a PGP Universal Server uses to determine how to handle incoming and outgoing mail traffic.

This feature is available with PGP Universal Gateway Email.

> You must be using a PGP Universal Gateway Email license or you will not be able to use the Mail Proxies feature on the administrative interface. If your license has not been entered, server-side mail proxy functionality is disabled. You will not be able to add or edit proxies. If you upgraded from a previous version of PGP Universal Server and your new license does not include Gateway Email, your mail is no longer being proxied.

Topics include:

- "Overview"
- "PGP Universal Server and Mail Proxies" on page 179
- "Changes in Proxy Settings from PGP Universal Server 2.0 to 2.5 and Later" on page 183
- "Mail Proxies Card" on page 183
- "Creating New or Editing Existing Proxies" on page 184
- "Mail Processing Settings" on page 193

Overview

Mail proxies control how your PGP Universal Server handles the email traffic in your environment: where it comes into the PGP Universal Server, how the server knows where the traffic came from, and where it's going, so that it can be processed correctly.

PGP Universal Server accepts up to 30 proxy connections per second.

The Mail Proxies card lets you create new POP, IMAP, and SMTP proxies, and edit existing proxies to match your security requirements. You also have control over Learn Mode.

PGP Universal Server and Mail Proxies

A PGP Universal Server provides security for email messaging by inserting itself into the flow of email traffic in your network, intercepting, or proxying, that traffic, and processing it (encrypt, sign, decrypt, verify) based on the applicable policies.

Chapter 15, "Setting Mail Policy" discussed how email is processed and protected by PGP Universal Server. This chapter focuses on correctly setting up how your PGP Universal Server proxies email traffic in your network. A PGP Universal Server cannot protect your email messages unless proxying is set up correctly.

Proxying means "to act on behalf of." And that's what a PGP Universal Server does: it intercepts email traffic before it gets to the intended destination, accepting the traffic on behalf of the intended destination for a brief period while it processes it (based on applicable mail policy) and then forwarding it onto the intended destination when it is done. Connections are proxied in real time, meaning PGP Universal Server does not typically take possession of messages for any longer than necessary to apply policies.

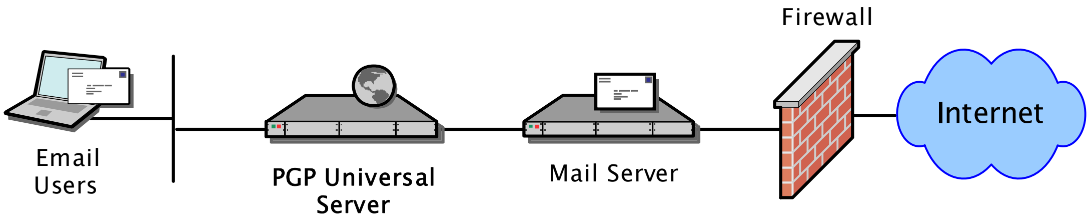
Let's look at a real-life example of using PGP Universal Server in an *internal placement*. Suppose your mail server supports the POP protocol, which your email users use to retrieve their email messages from the mail server. Before you installed a PGP Universal Server in an internal placement, your email users retrieved their email, using POP, by connecting directly from their email client to your mail server. Now that you have installed a PGP Universal Server in an internal placement, when your email users want to retrieve their email using POP, they should connect from their mail client directly to the PGP Universal Server. The PGP Universal Server then creates its own connection directly to your mail server, and proxies the POP request between the two connections. While doing this, the PGP Universal Server processes the mail according to policy.

When you run the Setup Assistant for a PGP Universal Server, you tell the Setup Assistant whether you want an *internal placement* or a *gateway placement*. The Setup Assistant combines this information with the information you provide about your network and your mail server, and the Setup Assistant configures your mail proxies for you.

Mail Proxies in an Internal Placement

For an *internal placement*, the Setup Assistant creates three mail proxies: one POP and one IMAP (the protocols used to retrieve messages from a mail server) and one SMTP (a protocol for sending mail messages). Because the POP and IMAP proxies are used for the same purpose (retrieving mail), they'll be referred to as POP/IMAP from here on out.

Here's a simplified look at the configuration we're talking about.



The POP/IMAP proxy listens for incoming mail traffic on ports 110 and 143, respectively, on a virtual interface configured on the PGP Universal Server; this interface/port combination is called the *local connector*. The connection between the user trying to retrieve their email and the local connector can optionally be secured and/or restricted by the connecting IP address, if desired. At least one local connector is required for a mail proxy; however, you can have as many as you want, as long as they use different interface/port combinations.

The POP/IMAP proxy also has a *proxy peer*—the device to which the PGP Universal Server sends the email traffic after it has processed it. The proxy peer for the POP/IMAP proxy is the mail server from which the email users are retrieving their email messages.

The initial SMTP proxy created by the Setup Assistant is an *Outbound* type (SMTP proxies can be *Outbound* only, *Inbound* only, or *Unified*, which combines the settings for Inbound and Outbound into a single proxy); Outbound means the email traffic originates from the local network (and often heads out to the Internet).

The Outbound SMTP proxy also has one or more local connectors, the interface/port combination on which the PGP Universal Server listens for and accepts email traffic. As with the POP/IMAP proxy, the local connectors can optionally use secured connections and/or restrict access by IP address.

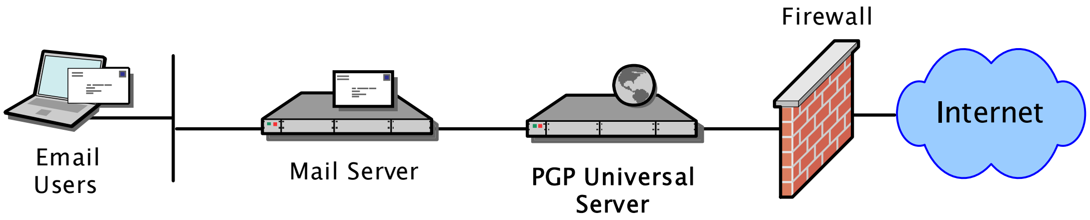
The Outbound SMTP proxy also has a proxy peer, the device to which outbound email traffic is sent after processing by the PGP Universal Server. By default, this is the mail server that outgoing mail messages would have been sent to if the PGP Universal Server had not been inserted into the flow of email traffic; it is called the *recipient mail server*.

To summarize, when you use the Setup Assistant to configure a PGP Universal Server in an *internal placement* (between your email users and their local mail server), the Setup Assistant configures the PGP Universal Server with a POP proxy and an IMAP proxy to process email messages the local email users are retrieving and an Outbound SMTP proxy for messages the local email users are sending.

Mail Proxies in a Gateway Placement

When you use the Setup Assistant to configure a PGP Universal Server in a *gateway placement* (the PGP Universal Server is between your network's outward-facing mail server and the Internet), the Setup Assistant creates the proxies differently. In the case of a gateway placement, the Setup Assistant creates a single, *Unified* SMTP proxy.

Here's a simplified view of the network we're talking about now.



The default *local connector*, the interface/port combination on which PGP Universal Server listens for email traffic, is interface 1 and port 25. To enhance security, you could add a second local connector that uses port 465 (SMTPS) with SSL security, for example. And you can also restrict access by IP address, as is possible for any local connector. Whichever combinations of local connectors you use, these local connectors are where email traffic will be coming in, whether inbound from the Internet or outbound from your network's outward-facing mail server.

Because this is the *Unified* SMTP proxy, and thus handles both incoming mail traffic from the Internet and outgoing mail traffic from your network’s outward-facing mail server, the Unified SMTP proxy has **two** *proxy peers*, two destinations to which email traffic will be sent. Which one is used depends on where each connection is coming from.

To deal with two destinations, the proxy peer for the Unified SMTP proxy has two sections: *Outbound* Mail and *Inbound* Mail. The Outbound Mail section handles mail traffic coming from your outward-facing mail server on its way out onto the Internet and then to its destination. The Inbound Mail section handles mail traffic coming in from the Internet on its way to your outward-facing mail server.

The *Outbound* Mail section lists *Designated Source IPs*. If the PGP Universal Server receives a connection from an IP address on this Designated Source IPs list, it knows that the email traffic is from your outward-facing mail server(s) on its way to the Internet and processes it accordingly.

The O*utbound* Mail section of the Unified SMTP proxy also lets you choose between sending outgoing email traffic that has been processed by the PGP Universal Server directly to the recipient mail server (the default) or to a different device (a SMTP relay) that you specify by hostname and port. You can also specify security settings for the connection to this device.

The *Inbound* Mail section of the Unified SMTP proxy handles email traffic coming in from the Internet. Because it is listening on the same local connector as the Outbound Mail section, how does the Inbound Mail section know what is inbound mail traffic and what isn’t? The **opposite** way the Outbound section does: any connection from an IP address that *doesn’t* appear in the *Designated Source IPs* list is considered Inbound mail from the Internet and is processed accordingly.

The *Inbound* Mail section of the Unified SMTP proxy includes one mailserver field; this is where you specify the connection details for your outward-facing mail server. The PGP Universal Server then sends inbound mail traffic there as it proxies it. You specify the host, port, and type of security for the connection.

In virtually all cases, one of the IP addresses in the *Designated Source IPs* listed in the *Outbound* Mail section should be the IP address of the mailserver host configured in the *Inbound* Mail section. In both cases, this is your network’s outward-facing mail server. Typical organizations that have only one mail server will only have one entry on the *Designated Source IPs* list, and this entry will also be the same mail server the *Inbound* mail traffic is going to. This is how the Setup Assistant initially configures the Unified SMTP proxy (note these will both refer to the same mail server; one referenced by IP address, the other by hostname).

To summarize, when you use the Setup Assistant to configure a PGP Universal Server in g*ateway placement* (between the outward-facing mail server and the Internet), the Setup Assistant creates and configures one *Unified* SMTP proxy that proxies both inbound and outbound mail traffic between your mail server and the Internet.

Changes in Proxy Settings from PGP Universal Server 2.0 to 2.5 and Later

Some of the settings that in previous versions of PGP Universal Server were controlled through the Mail Proxies card are now managed on the Mail Policy card. You can now manage the following settings through mail policy rules:

- Enable AntiVirus Checking
- Decrypt Upon Receipt
- Apply Mail Policy for Authenticated Connections
- Always Encrypt Internal Mail

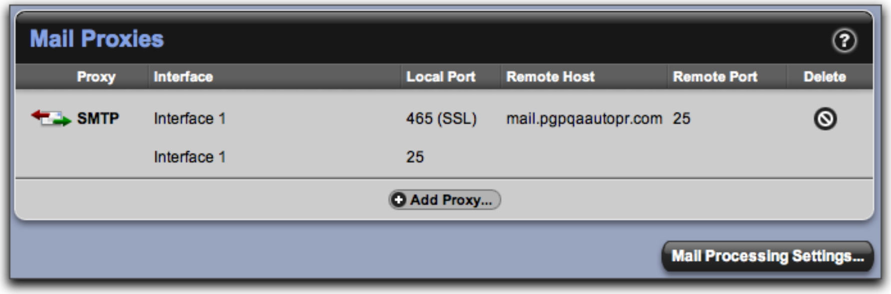
When you migrate from PGP Universal Server 2.0 to version 2.5 and later, your previous settings are also automatically migrated. Policy rules will reflect your previous choices. However, if you had multiple SMTP proxies, or if you have clustered PGP Universal Servers, you will need to recreate some of your settings manually.

To learn more about how your previous settings are now reflected in mail policy, or to learn how to recreate your settings if necessary, refer to the *PGP Universal Server Upgrade Guide*. Refer to Chapter 15, "Setting Mail Policy" for more information on mail policy.

Mail Proxies Card

The Mail Proxies card:

- Displays the proxies that are configured on this PGP Universal Server, lets you manage existing proxies, and lets you create new ones.
- Lets you control the mail processing settings.



Mail Proxies

Proxy	Interface	Local Port	Remote Host	Remote Port	Delete
SMTP	Interface 1	465 (SSL)	mail.pgpqaautopr.com	25	⊘
	Interface 1	25			

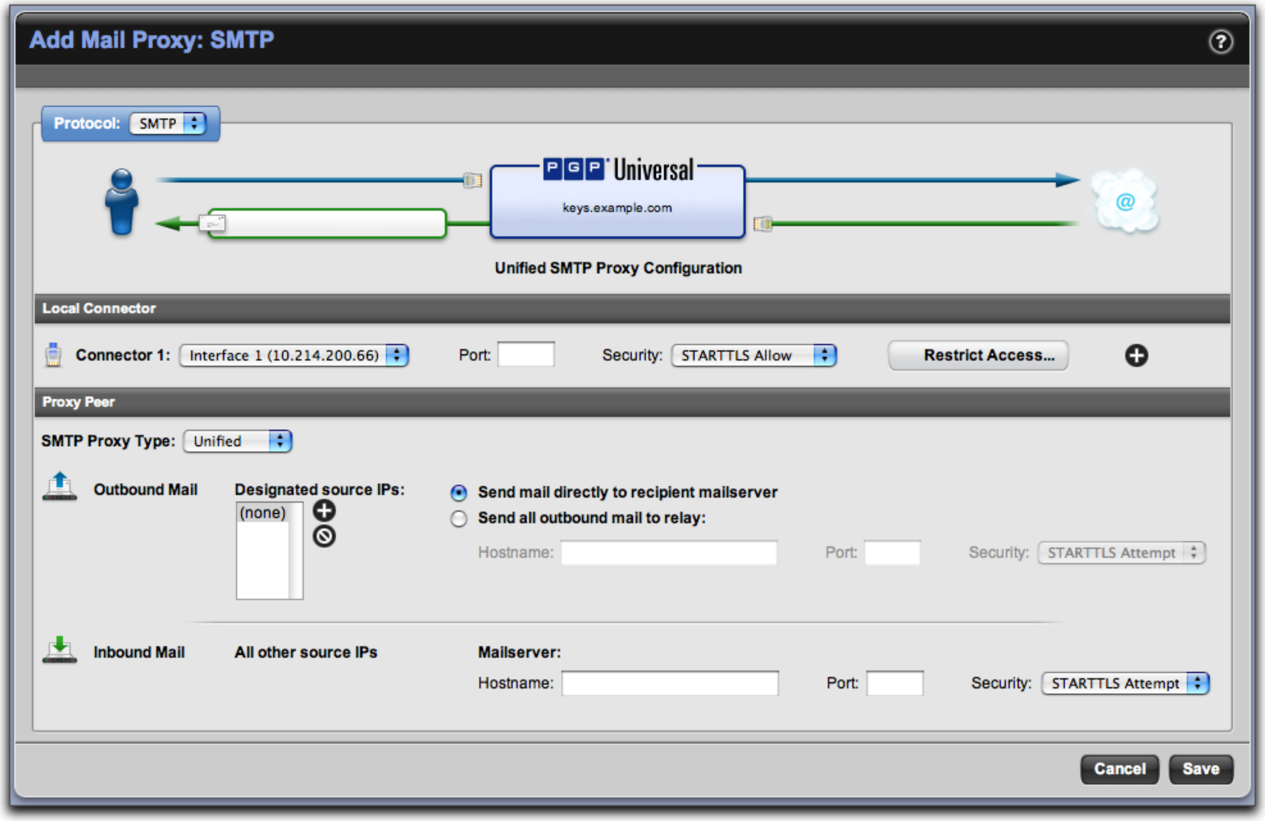
The Mail Proxies card lists the proxies currently configured on a PGP Universal Server. It shows the protocol of the proxy, the assigned interface, the local port, and the remote host and port; it also lets you delete proxies.

Depending on your environment, the proxies created for a PGP Universal Server using the Setup Assistant may be adequate. On the other hand, you may need to add or edit a proxy. You use the Mail Proxies card to do these things.

Creating New or Editing Existing Proxies

You can add or edit three types of proxies:

- **POP**. The POP protocol is available only for internal placements. The POP protocol is used by email clients to retrieve email messages from a mail server.
- **IMAP**. The IMAP protocol is also available only for internal placements. The IMAP protocol is also used by email clients to retrieve email messages from a mail server.
- **SMTP**. The SMTP protocol is available for internal or gateway placements. With an internal placement, you can only create or edit an Outbound SMTP proxy. With an external placement, you can create or edit an Outbound, Inbound, or Unified SMTP Proxy.



Add Mail Proxy: SMTP

Protocol: SMTP

Unified SMTP Proxy Configuration

Local Connector

Connector 1: Interface 1 (10.214.200.66) Port: Security: STARTTLS Allow

Proxy Peer

SMTP Proxy Type: Unified

Outbound Mail

Designated source IPs: (none)

● Send mail directly to recipient mailserver

○ Send all outbound mail to relay:

Hostname: Port: Security: STARTTLS Attempt

Inbound Mail

All other source IPs

Mailserver:

Hostname: Port: Security: STARTTLS Attempt

Creating or Editing a POP/IMAP Proxy

The POP and IMAP proxies support email traffic where your internal email users are retrieving their messages from their local mail server. Because the PGP Universal Server is sitting between the email users and their mail servers, a POP and/or IMAP proxy must exist to proxy that traffic.

POP and IMAP proxies are only needed if your PGP Universal Server is placed internally, between your email users and their local mail server. They are not needed if your PGP Universal Server is in a gateway placement.

Because the POP and IMAP proxies are virtually identical, the following procedure applies to both. Differences will be noted in the text.

To create or edit a POP/IMAP proxy:

1. If you are editing an existing POP or IMAP proxy, click on the name of the proxy you want to edit in the Proxy column on the Mail Proxies card.

   The Edit Mail Proxy screen appears.

2. Or, if you are creating a new POP or IMAP proxy, click **Add Proxy** on the Mail Proxies card and select POP or IMAP, as appropriate, from the **Protocol** drop-down list.

   The Add Mail Proxy: POP or IMAP screen appears.

3. In the **Connector 1** field, in the Local Connector section, select the interface for the local connector for this proxy from the drop-down list.

   The interfaces available are those configured on the Network Settings card (System>Network). If you want more interfaces to be available for your proxies, you need to configure them on the Network Settings card. See Chapter 44, "Setting Network Interfaces" for more information.

4. In the **Port** field, select the appropriate port.

   The default for POP is 110; the default for IMAP is 143. The default for POPS (secure POP) is 995; the default for IMAPS (secure IMAP) is 993.

   The port number automatically changes based on your selection from the **Security** drop-down list.

5. In the **Security** drop-down list, select from:

   – **STARTTLS Allow**. Allows the security of the connection to be upgraded to TLS via negotiation when communications begin. The email client must support STARTTLS for the upgrade to occur.

   – **STARTTLS Disable**. STARTTLS will not be allowed for this connection.

   – **STARTTLS Require**. Requires that the connection be secured by TLS. Only select this option if you are confident that all of the email clients connecting to this local connector support upgrading the security to STARTTLS.

   – **SSL**. Uses SSL to protect the connection between the email client and the PGP Universal Server.

6. Click the **Restrict Access** button if you would like to enhance the security of this local connector by restricting access by IP address.

On the Access Control for Connector dialog, put a check in the **Enable Access Control for Connector** checkbox, then specify:

- In the **Hostname/IP** field, enter a hostname or IP address, then click **Add**. What you enter here will go onto the list in the **Block or Allow** field below. If you enter a hostname like **example.com**, the name will be resolved to an IP address.
- In the **IP Range** fields, enter starting and ending IP addresses for an IP address range, then click **Add**. What you enter here will go onto the list in the **Block or Allow** field below.
- In the **Block or Allow** field, select **Block these addresses** or **Allow only these addresses**, as appropriate, for the IP addresses or ranges in the box below.

To remove an IP address or range from the box, select it then click **Remove**.

Click **Save** when you have configured the appropriate access control restrictions.

The Access Control for Connector dialog disappears.

7. In the **Mailserver** field, in the Proxy Peer section, enter the mail server from which the email clients are attempting to retrieve their messages.

   This is the mail server from which the email clients would be retrieving their messages directly if the PGP Universal Server were not between them in the flow of email traffic.

8. In the **Port** field, select the appropriate port.

   The default for POP is 110; the default for IMAP is 143. The default for POPS (secure POP) is 995; the default for IMAPS (secure IMAP) is 993.

   The port number automatically changes based on your selection from the **Security** drop-down list.

9. In the **Security** drop-down list, select between:

   - **STARTTLS Attempt**. Allows the security of the connection to be upgraded to TLS via negotiation when communications begin. The mail server must support STARTTLS for the upgrade to occur.
   - **STARTTLS Disable**. STARTTLS will not be allowed for this connection.
   - **STARTTLS Require**. Requires that the connection be secured by TLS. Only select this option if you are confident that the mail server connecting to this local connector supports upgrading the security to STARTTLS.
   - **SSL**. Uses SSL to protect the connection between the PGP Universal Server and the mail server.

10. Click **Save**.

Creating or Editing an Outbound SMTP Proxy

An Outbound SMTP proxy can be configured for either an internal placement of your PGP Universal Server or a gateway placement.

In the case of an internal placement, the Outbound SMTP proxy proxies messages being sent by your internal email users to the local mail server for delivery to the intended recipient.

In the case of an external placement, the Outbound SMTP proxy proxies messages being sent by your outward-facing mail server to the Internet on the way to the intended recipient.

To create or edit an Outbound SMTP proxy:

1 If you are editing an existing Outbound SMTP proxy, click on the name of the proxy you want to edit in the Proxy column on the Mail Proxies card.

The Edit Mail Proxy screen appears.

2 If you are creating a new Outbound SMTP proxy, click **Add Proxy** on the Mail Proxies card, select **SMTP** from the **Protocol** drop-down list, then select **Outbound** from the SMTP Proxy Type in the Proxy Peer section.

The Add Mail Proxy: SMTP screen appears.

3 In the **Connector 1** field, in the Local Connector section, select the interface for the local connector for this proxy from the drop-down list.

The interfaces available are those configured on the Network Settings card (System>Network). If you want more interfaces to be available for your proxies, you need to configure them on the Network Settings card.

4 In the **Port** field, select the appropriate port.

The default port for SMTP is 25. The default for SMTPS (secure SMTP) is 465.

The port number automatically changes based on your selection from the **Security** drop-down list.

5 In the **Security** drop-down list, select between:

– **SSL**. Uses SSL to protect the connection between the email client and the PGP Universal Server.

– **STARTTLS Allow**. Allows the security of the connection to be upgraded to TLS via negotiation when communications begin. The email client must support STARTTLS for the upgrade to occur.

– **STARTTLS Disable**. STARTTLS will not be allowed for this connection.

– **STARTTLS Require**. Requires that the connection be secured by TLS. Only select this option if you are confident that all of the email clients connecting to this local connector support upgrading the security to STARTTLS.

6 Click the **Restrict Access** button if you would like to enhance the security of this local connector by restricting access by IP address.

On the Access Control for Connector dialog, put a check in the **Enable Access Control for Connector** checkbox, then specify:

- In the **Hostname/IP** field, enter a hostname or IP address, then click **Add**. What you enter here will go onto the list in the **Block or Allow** field below. If you enter a hostname like **example.com**, the name will be resolved to an IP address.
- In the **IP Range** fields, enter starting and ending IP addresses for an IP address range, then click **Add**. What you enter here will go onto the list in the **Block or Allow** field below.
- In the **Block or Allow** field, select **Block these addresses** or **Allow only these addresses**, as appropriate, for the IP addresses or ranges in the box below.

To remove an IP address or range from the box, select it then click **Remove**.

Click **Save** when you have configured the appropriate access control restrictions.

The Access Control for Connector dialog disappears.

7. In the Proxy Peer section, choose between:

    - **Send mail directly to recipient mailserver**. When selected, the outgoing email messages coming from your internal email users will be sent to the recipient mail server after processing by the PGP Universal Server per the appropriate policies.
    - **Proxy mail to SMTP server**. When selected, the outgoing email messages from your internal email users will be sent to the device you specify after processing by the PGP Universal Server per the appropriate policies.

8. If you selected **Proxy mail to SMTP server**, in the **Hostname** field, enter the hostname or IP address of the device you want outgoing email messages to be sent to after processing by the PGP Universal Server.

    In the **Port** field, select the appropriate port. The default port for SMTP is 25. The default for SMTPS (secure SMTP) is 465. The port number automatically changes based on your selection from the **Security** drop-down list.

    In the **Security** drop-down list, select between **SSL**, **STARTTLS Attempt**, **STARTTLS Disable**, and **STARTTLS Require**. These are the same options available for the Security drop-down list in the Local Connector section.

9. Click **Save**.

Creating or Editing an Inbound SMTP Proxy

The Inbound SMTP proxy processes mail traffic coming into your network from the Internet. An Inbound SMTP proxy can be configured only for a PGP Universal Server in a gateway placement.

To create or edit an Inbound SMTP proxy:

1. If you are editing an existing Inbound SMTP proxy, click on the name of the proxy you want to edit in the Proxy column on the Mail Proxies card.

    The Edit Mail Proxy screen appears.

2 If you are creating a new Inbound SMTP proxy, click **Add Proxy** on the Mail Proxies card, select **SMTP** from the **Protocol** drop-down list, then select **Inbound** from the SMTP Proxy Type in the Proxy Peer section.

The Add Mail Proxy: SMTP screen appears.

3 In the **Connector 1** field, in the Local Connector section, select the interface for the local connector for this proxy from the drop-down list.

The interfaces available are those configured on the Network Settings card (System>Network). If you want more interfaces to be available for your proxies, you need to configure them on the Network Settings card.

4 In the **Port** field, select the appropriate port.

The default port for SMTP is 25; the default for SMTPS (secure SMTP) is 465.

The port number automatically changes based on your selection from the **Security** drop-down list.

5 In the **Security** drop-down list, select between:

- **STARTTLS Allow**. Allows the security of the connection to be upgraded to TLS via negotiation when communications begin. The external MTA must support STARTTLS for the upgrade to occur.
- **STARTTLS Disable**. STARTTLS will not be allowed for this connection.
- **STARTTLS Require**. Requires that the connection be secured by TLS. Only select this option if you are confident that all of the other devices connecting to this local connector support upgrading the security to STARTTLS.
- **SSL**. Uses SSL to protect the connection between the external MTA sending and the PGP Universal Server.

6 Click the **Restrict Access** button if you would like to enhance the security of this local connector by restricting access by IP address.

On the Access Control for Connector dialog, put a check in the **Enable Access Control for Connector** checkbox, then specify:

- In the **Hostname/IP** field, enter a hostname or IP address, then click **Add**. What you enter here will go onto the list in the **Block or Allow** field below. If you enter a hostname like **example.com**, the name will be resolved to an IP address.
- In the **IP Range** fields, enter starting and ending IP addresses for an IP address range, then click **Add**. What you enter here will go onto the list in the **Block or Allow** field below.
- In the **Block or Allow** field, select **Block these addresses** or **Allow only these addresses**, as appropriate, for the IP addresses or ranges in the box below.

To remove an IP address or range from the box, select it then click **Remove**.

Click **Save** when you have configured the appropriate access control restrictions.

The Access Control for Connector dialog disappears.

7 In the **Mailserver** field, in the Proxy Peer section, in the **Hostname** field, enter the hostname or IP address of the device you want incoming email messages to be sent to after processing by the PGP Universal Server.

Under most circumstances, this should be your outward-facing mail server.

In the **Port** field, select the appropriate port. The default port for SMTP is 25; the default for SMTPS (secure SMTP) is 465. The port number automatically changes based on your selection from the **Security** drop-down list.

In the **Security** drop-down list, select between **SSL**, **STARTTLS Attempt**, **STARTTLS Disable**, and **STARTTLS Require**. These are the same options available for the Security drop-down list in the Local Connector section.

8 Click **Save**.

Creating or Editing a Unified SMTP Proxy

The Unified SMTP proxy is a single proxy that includes the properties of both the Inbound SMTP proxy and the Outbound SMTP proxy. In fact, you could individually configure one Inbound and one Outbound SMTP proxy and achieve the same result as with the Unified SMTP proxy.

The Unified SMTP proxy can only be configured for a PGP Universal Server in gateway placement.

With the Unified SMTP proxy, all mail traffic arrives on the same local connectors. This means that you don’t need a second IP address for your PGP Universal Server, which you would need if you created separate Inbound and Outbound SMTP proxies.

It also means you need to configure the Unified SMTP proxy so that it can distinguish between inbound and outbound mail traffic, because all mail traffic is arriving on the same local connectors.

You do this by creating a Designated Source IPs list, a list of IP addresses which by definition are sending outbound mail traffic to the PGP Universal Server. Traffic from all other IP addresses are, by definition, inbound from the Internet.

Put a different way, on the Unified SMTP proxy you put the IP addresses of your trusted internal mail servers on the Designated Source IPs list, because these are the only devices that should be sending outbound email traffic to the PGP Universal Server in gateway placement.

The PGP Universal Server checks the source IP addresses of all incoming mail traffic on its local connectors and decides the traffic fits one of these two categories:

- The mail traffic is coming from an IP address *on* the Designated Source IPs list. This traffic is thus outbound traffic coming from an internal mail server, and is processed as such. Messages will be encrypted and/or signed, per the applicable policy, but not decrypted or verified.
- The mail traffic is coming from an IP address *not* on the Designated Source IPs list. This traffic is thus inbound traffic coming from the Internet, and is processed as such. Messages will be decrypted and verified, but not encrypted or signed.

To create or edit a Unified SMTP proxy:

1 If you are editing an existing Unified SMTP proxy, click on the name of the proxy you want to edit in the Proxy column on the Mail Proxies card.

The Edit Mail Proxy screen appears.

2 If you are creating a new Unified SMTP proxy, click **Add Proxy** on the Mail Proxies card, select **SMTP** from the **Protocol** drop-down list, then select **Unified** from the SMTP Proxy Type in the Proxy Peer section.

The Add Mail Proxy: SMTP screen appears.

3 In the **Connector 1** field, in the Local Connector section, select the interface for the local connector for this proxy from the drop-down list.

The interfaces available are those configured on the Network Settings card (System>Network). If you want more interfaces to be available for your proxies, you need to configure them on the Network Settings card.

4 In the **Port** field, select the appropriate port.

The default port for SMTP is 25; the default for SMTPS (secure SMTP) is 465.

The port number automatically changes based on your selection from the **Security** drop-down list.

5 In the **Security** drop-down list, select between:

– **STARTTLS Allow**. Allows the security of the connection to be upgraded to TLS via negotiation when communications begin. The external MTA must support STARTTLS for the upgrade to occur. The default port is 25.

– **STARTTLS Disable**. STARTTLS will not be allowed for this connection. The default port is 25.

– **STARTTLS Require**. Requires that the connection be secured by TLS. Only select this option if you are confident that all of the devices connecting to this local connector support upgrading the security to STARTTLS. The default port is 25.

– **SSL**. Uses SSL to protect the connection between the external MTA and the PGP Universal Server. The default port is 465.

6 Click the **Restrict Access** button if you would like to enhance the security of this local connector by restricting access by IP address.

On the Access Control for Connector dialog, put a check in the **Enable Access Control for Connector** checkbox, then specify:

– In the **Hostname/IP** field, enter a hostname or IP address, then click **Add**. What you enter here will go onto the list in the **Block or Allow** field below. If you enter a hostname like **example.com**, the name will be resolved to an IP address.

– In the **IP Range** fields, enter starting and ending IP addresses for an IP address range, then click **Add**. What you enter here will go onto the list in the **Block or Allow** field below.

- In the **Block or Allow** field, select **Block these addresses** or **Allow only these addresses**, as appropriate, for the IP addresses or ranges in the box below.

To remove an IP address or range from the box, select it then click **Remove**.

Click **Save** when you have configured the appropriate access control restrictions.

The Access Control for Connector dialog disappears.

7 In the **Designated Source IPs** list, add the internal mail server(s) that will be sending mail traffic to the PGP Universal Server that is outbound for the Internet.

To add the IP address of a mail server, click the plus sign icon, enter the IP address, then click **Save**.

The Unified SMTP proxy considers all mail traffic coming from IP addresses on this list to be outbound for the Internet, and processes it accordingly.

8 Choose between:

- **Send mail directly to recipient mailserver**. When selected, the outgoing email messages coming from your internal email users will be sent to the recipient mail server after processing by the PGP Universal Server per the appropriate policies.
- **Send all outbound mail to relay**. When selected, the outgoing email messages from your internal email users will be sent to the device you specify after processing by the PGP Universal Server per the appropriate policies.

9 If you selected **Send all outbound mail to relay**, in the **Hostname** field, enter the hostname or IP address of the device you want outgoing email messages to be sent to after processing by the PGP Universal Server.

In the **Port** field, select the appropriate port. The default port for SMTP is 25. The default for secure SMTP is 465. The port number automatically changes based on your selection from the **Security** drop-down list.

In the **Security** drop-down list, select between **SSL**, **STARTTLS Attempt**, **STARTTLS Disable**, and **STARTTLS Require**. These are the same options available for the Security drop-down list in the Local Connector section.

10 In the **Mailserver** field, for **Hostname**, enter the hostname or IP address of the device you want incoming email messages to be sent to after processing by the PGP Universal Server.

Under most circumstances, this should be your outward-facing mail server.

In the **Port** field, select the appropriate port. The default port for SMTP is 25; the default for SMTPS (secure SMTP) is 465. The port number automatically changes based on your selection from the **Security** drop-down list.

In the **Security** drop-down list, select between **SSL**, **STARTTLS Attempt**, **STARTTLS Disable**, and **STARTTLS Require**. These are the same options available for the Security drop-down list in the Local Connector section.

11 Click **Save**.

Mail Processing Settings

The Mail Processing Settings dialog gives you control over Learn Mode. When you finish configuring a PGP Universal Server using the Setup Assistant, it begins operation in Learn Mode, where the PGP Universal Server proxies traffic normally but does not encrypt or sign any messages. Learn Mode gives the PGP Universal Server a chance to build its SMSA, so that when Learn Mode is turned off, the PGP Universal Server knows the environment and can immediately begin securing messages.

In previous versions of PGP Universal Server, this dialog also controlled whether internal messages were always encrypted. This function is now controlled through mail policy. Refer to the *PGP Universal Server Upgrade Guide* for more information.

To control mail processing settings:

1. On the Mail Proxies card, click **Mail Processing Settings**.

   The Mail Processing Settings dialog appears.

2. To have this PGP Universal Server operate in Learn Mode, put a check in the **Operate in Learn Mode** checkbox; to take the server out of Learn Mode, clear the checkbox.

3. Click **Save**.

   The Mail Processing Settings dialog disappears.

23 Email in the Mail Queue

This chapter describes the Mail Queue feature.

You can configure Mail Queue options from the Mail>Mail Queue card.

This feature is available with PGP Universal Gateway Email.

Overview

The Mail Queue card lists email messages that are waiting to be sent by the PGP Universal Server. The list is often empty, even on medium-load servers.

When there are messages in the list, the following information is shown about each queued message: the email address of the sender, the email address of the recipient, the reason the message is in the queue, when the server received the message, and its size.

If the reason is too long to display in full, it will be truncated. Click on or roll your cursor over the shortened reason to see the complete text.

There are several reasons why an email message would appear on the list:

- While looking for a key for the recipient of a message, a keyserver did not respond. Only keyserver failures for $ADDRESS_DOMAIN keyservers do not cause a message to be queued.
- A problem with the network or the recipient mail server is preventing the PGP Universal Server from sending messages (a network outage could be the root problem here). While the PGP Universal Server waits for the mail server to respond, it queues up outgoing messages.
- The message recipient’s email address does not exist. If the message is not immediately deliverable, the PGP Universal Server will place it in the Mail Queue and keep trying to send it. The message will time out and disappear from the queue after 4 days (96 hours).

You can wait for the messages to be sent or you can delete them from the queue.

ⓘ If a message is addressed to multiple recipients, and the keys for some of the recipients cannot be found immediately, PGP Universal Server will break the message into multiple messages and only queue the messages for those recipients whose key(s) could not be found.

Deleting Messages from the Mail Queue

When there are messages in the list, the Mail Queue card lists each one on its own row. You can delete one, some, or all messages from the list:

- To delete individual email messages from the queue, click on the icon in the Delete column of the message you wish to delete. The message is deleted.
- To delete some of the email messages from the queue, click the checkboxes for the messages you want to delete, then select **Delete Selected** from the Options menu.
- To delete all email messages in the queue at one time, select **Delete All** from the Options menu. The messages are deleted.

PGP Universal Server does not notify the sender of a deleted message of the deletion.

For information about what messages have been handled by the PGP Universal Server, refer to Chapter 41, "System Logs".

24 Specifying Mail Routes

This chapter describes how to use mail routes with your PGP Universal Server.

Mail routes apply to all email processed by PGP Universal Gateway Email. For PGP Desktop Email, mail routes apply only to messages generated by PGP Universal Server and sent to internal users.

> Creating static Mail Routes is an advanced feature that should only be used by customers who have a specific reason to override the default mail routing behavior of a PGP Universal Server. Incorrect configuration could cause mail loops or other delivery problems.

Topics include:

- "Overview"
- "Managing Mail Routes" on page 198

Overview

Mail routing is used to establish static mail routes that will override the DNS MX-record lookup normally used when determining where to route mail. In certain instances, this can provide a more efficient route, bypassing the "loop" through DMZ and the firewall.

For example, if you set static routes, email for internal users can be forwarded from the PGP Universal Server directly to the internal mail server. Mail traffic for certain destinations could also be routed over leased lines instead of the Internet.

Typically, PGP Universal Server proxies SMTP connections to specific hosts defined by the PGP administrator. These proxied connections do not involve mail routing, and thus are not affected by any configured static mail routes. However, in certain instances, PGP Universal Server will transmit messages directly — in these instances, any configured static mail routes will apply.

Examples of such instances are:

- When messages are being retransmitted from the mail queue.
- For PGP Universal Server–generated messages: Daily Status Email, PGP Universal Web Messenger notifications, bounce notifications, and so on.
- When the outbound SMTP proxy is configured to "Send mail directly to recipient mailserver."

When no static mail routes are configured, the Mail Routes card displays the text "Your mail is being routed normally."

The PGP Universal Server can automatically create or adjust static mail routes when you add or remove managed domains or when you change the server's placement within your network. For example, if the PGP Universal Server is externally placed, the Setup Assistant automatically adds a mail route based on the managed domain and mail server information you enter. You should make sure that the mail route is correct, because it is not always possible for the PGP Universal Server to determine the correct rules for your network.

Managing Mail Routes

You can add a new mail route, change route priority, edit an existing mail route, or delete a mail route. You can only create one mail route per domain.

Adding a Mail Route

To add a static mail route:

1. Click **Add Mail Route**.

   The Add New Mail Route dialog appears.

2. In the **Domain Name** field, enter the domain name of the email that is to be statically routed.

   For example, if you want all email bound for example.com to be routed to a device other than the MX-listed mailservers for example.com, you would enter "example.com" here.

3. In the **Hostname/IP** field, enter the hostname or IP address of the device to which mail should be routed.

   For example, "mail.example.com" or "10.1.1.30."

   There is no requirement that the device you enter in the Hostname/IP field be a device in the domain you specified in the Domain Name field.

4. Click **Save**.

   The new static mail route is added.

Editing a Mail Route

To edit a static mail route:

1. Click on the static route you want to edit.

   The Edit Mail Route dialog appears.

2. Enter the desired changes for the domain name and the IP address of the host.

3. Click **OK**.

   The information about the host is changed.

Deleting a Mail Route

To delete a static mail route:

1 Click the icon in the Delete column of the static route you want to delete.

A confirmation dialog box appears.

2 Click **OK**.

The static route you specified is removed from the list.

25 Customizing System Message Templates

This chapter describes message templates, which allow you to modify the content of predefined messages sent out by your PGP Universal Server in various circumstances. For example, you can edit the content of messages sent out when email bounces, or when notifying PGP Universal Web Messenger users of new email.

These messages are available for PGP Universal Gateway Email and PGP Desktop Email.

Topics include:

- "Overview"
- "Editing a Message Template" on page 202

Overview

Message templates let you modify the contents of the predefined messages sent out by the PGP Universal Server in various circumstances; the wording of the Smart Trailer, for example.

Each message template can be customized so you can add any content that may be important for your specific situation.

Most message templates include one or more template variables. These variables always begin with a $, such as $URL. These variables convert directly into RFC 822 headers with appropriate text when the message is sent. Some variables are optional, others are required. Be very careful when editing templates; the PGP Universal Server will not send messages based on a template with incorrect or 822-unsupported variables.

Changing the format of the template can also cause it to fail. If you change or remove the blank line between the email headers and the message body, a template will no longer be considered by the system to be well-formed, and the template will fail.

The list of permitted variables for each template along with a description of each is provided on the dialog itself. You can also restore a message to the factory default setting, if necessary.

You should always test template changes to confirm that the template is still correctly formatted. You should make sure, for example, that the mail built from the template was successfully received by the proper recipients and that it contained the proper information and/or links. Test the template by forcing the circumstance that causes the edited template to be used. The test message should be sent to an external account that you can access immediately. Then you can quickly see what may have been broken and correct it.

The Message Templates card shows the list of message templates.

The messages template character set is UTF-8. Do not change the character set, or messages based on the templates will be unreadable.

Templates and Message Size

There are two ways email senders are notified if they send messages too large to be received by PGP Universal Web Messenger users.

If the email is smaller than the recipient's quota but would exceed the quota when added to the rest of the email stored for that user, the sender receives a message based on the template **Quota Exceeded for Web Messenger Recipient (Delivered to Sender)**. The original email is not delivered to the PGP Universal Web Messenger user.

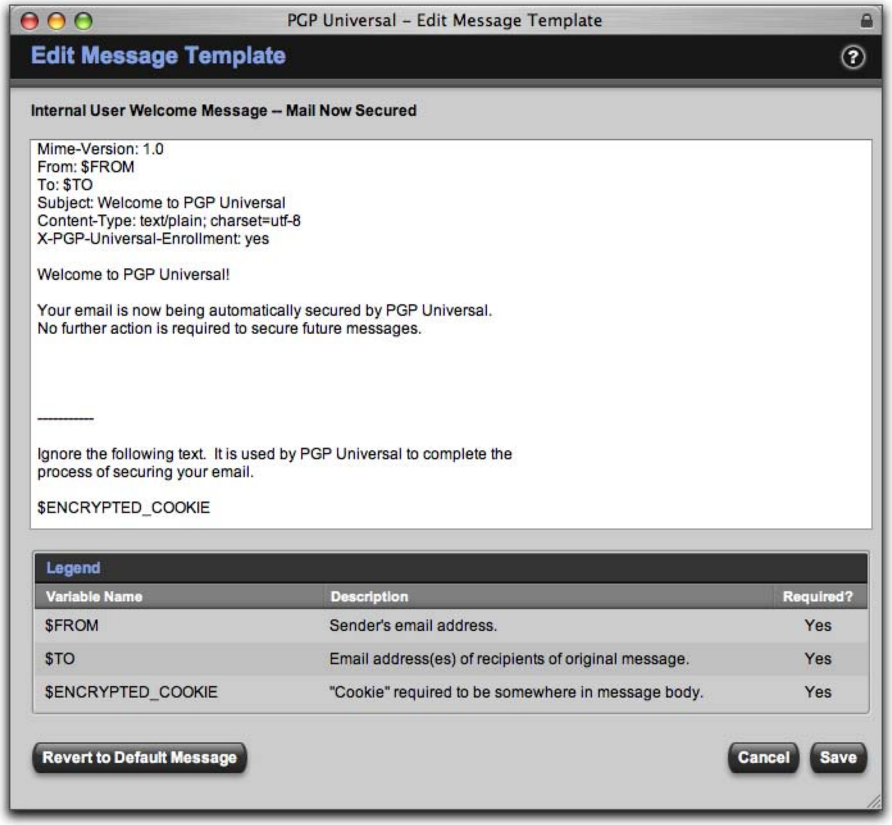
If the email is larger than the recipient's quota, or if the message is larger than 50MB total, the sender receives a message based on the template **Message Bounced - Message Too Large**. The original email is not delivered to the PGP Universal Web Messenger user.

Editing a Message Template

To edit a message template:

1. Click on the description of the template you wish to edit.

   The appropriate Edit Message Template dialog appears.


PGP Universal – Edit Message Template
Edit Message Template
Revert to Default Message
Cancel
Save

Internal User Welcome Message -- Mail Now Secured

```
Mime-Version: 1.0
From: $FROM
To: $TO
Subject: Welcome to PGP Universal
Content-Type: text/plain; charset=utf-8
X-PGP-Universal-Enrollment: yes

Welcome to PGP Universal!

Your email is now being automatically secured by PGP Universal.
No further action is required to secure future messages.




-----------

Ignore the following text.  It is used by PGP Universal to complete the
process of securing your email.

$ENCRYPTED_COOKIE
```

Legend

Variable Name	Description	Required?
$FROM	Sender's email address.	Yes
$TO	Email address(es) of recipients of original message.	Yes
$ENCRYPTED_COOKIE	"Cookie" required to be somewhere in message body.	Yes

2 Make the desired changes to the template.

3 To revert to the default content (both text and variables) of a message template, click **Revert to Default Message**.

4 Click **Save**.

SECTION 6

Managing Users

This section describes how to set up policy for internal users, to create and manage PGP Desktop and PGP Universal Satellite client installations. You can also create policy to specify key settings and PGP Universal Web Messenger settings and PGP Universal Satellite installations for external users. This section will also explain how to manage individual user accounts. You can also find information on how to control the PGP Verified Directory, PGP Universal Web Messenger, and Keyserver services.

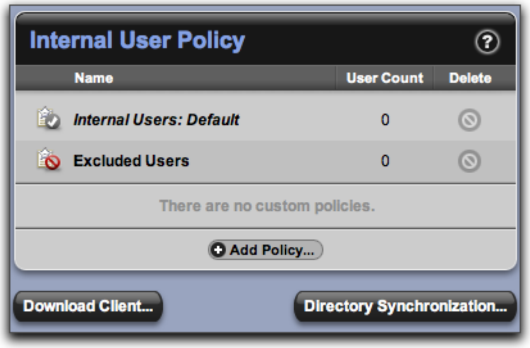
26 Setting Internal User Policy

This chapter describes the Internal User Policy card, which allows you to create and manage PGP Desktop and PGP Universal Satellite client installations for internal users. Topics include:

This feature is applicable to all PGP encryption solutions. You create PGP Universal Satellite clients for PGP Gateway Email. This feature also allows you to create and manage PGP Desktop Email, PGP Whole Disk Encryption, and PGP NetShare client installations, depending on what your license permits. Refer to Chapter 28, "Configuring PGP Desktop Installations" for more information.

Overview

The Internal User Policy card allows you to manage PGP Desktop and PGP Universal Satellite clients by creating customized installers which communicate with PGP Universal Server for their policies.



Internal User Policy

Name	User Count	Delete
Internal Users: Default	0	⊘
Excluded Users	0	⊘

There are no custom policies.

PGP Universal Server lets you group internal users and apply policies to the groups. The correct policy settings will be applied to new users automatically, as the users interact with PGP Universal Server for the first time. If you update the policies later, user installations associated with the changed policies will be updated automatically.

You can define different policies for different groups of users, so that each group gets settings appropriate for their environment. You can then create a customized installer for that user group, which will automatically apply the correct policy.

After you distribute the installer to the appropriate users, you can change a policy's settings. Users will automatically see those changes the next time they interact with PGP Universal Server.

There are two ways to manage which users get assigned to what user policies. You can bind the policy to the installer and distribute the installer. You will not be able to change which policy each user is bound to without having the user reinstall their client software.

If LDAP directory synchronization is enabled, then you can assign policies to internal users based on their directory attributes, and switch which policy they are bound to by changing their LDAP attributes, or changing the LDAP attributes of the user group. Then the next time the user interacts with the server, they receive new settings based on which policy they are now bound to.

There are two default internal user policies:

- Internal Users: Default. This user policy lets you control the key settings for new internal (managed domain) users and the default options for downloadable PGP Desktop installers. The key settings apply to both PGP Universal Satellite and PGP Desktop users. The key settings and the PGP Desktop options established here are used by default when new internal users are created or downloadable PGP Desktop or PGP Universal Satellite installers are created.

  You cannot delete this user policy, but you can change settings at any time.

  You can also create custom internal user polices that will be applied to specific groups of users instead of the Internal Users: Default settings.

- Excluded Users. These are users from within managed domains, who you do not want treated as internal users. In other words, their messaging will not be protected by the PGP Universal Server. You can exclude users through policy if the Directory Synchronization feature is enabled. You specify which users are excluded using LDAP attributes. You cannot delete this user group, but you can change settings at any time.

The Internal User Policy card shows the default user policies and those user policies you configure.

Managing Internal User Policies

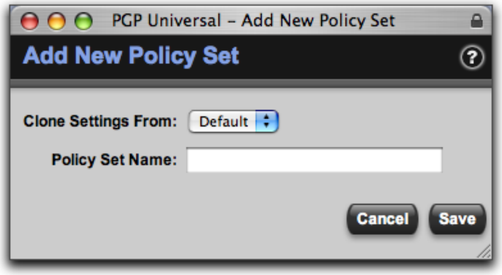
Adding a New Internal User Policy

You can only create new internal user policies. The Excluded Users policy is editable, but you cannot delete nor override it with user policies you create.

To create a new internal user policy:

1. On the Internal User Policy card, click **Add Policy**.

   The Add New Policy Set dialog appears.



Clone Settings From: Default

Policy Set Name:

2 In the **Clone Settings From** drop-down list, select the existing policy with the settings you would like to use as a starting point for a new policy.

If this is the first new user policy to be created, the drop-down list will only have one entry, Default, the internal users default policy.

3 In the **Policy Set Name** field, enter a name for the policy you are creating. Try to choose a name that shows this is an internal user policy; for example, Internal: Executives.

4 Click **Save**.

5 Edit the new policy settings as appropriate.

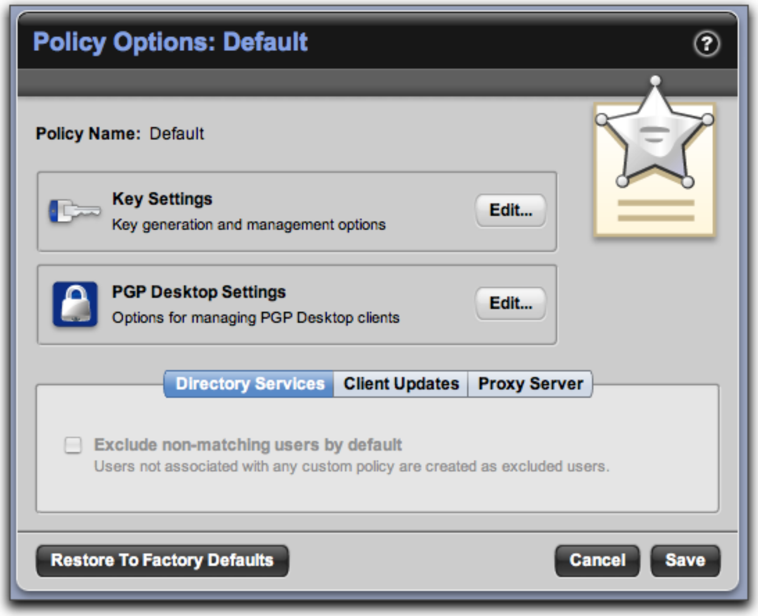
Editing Internal User Policies

The internal user policies let you control the settings that are applied to internal users. These include the key settings and the PGP Desktop settings for deployments of PGP Desktop.

To edit any internal user policy:

1 On the Internal User Policy card, select the policy you want to edit.

The Policy Options card appears.



Policy Name: Default

Key Settings
Key generation and management options

PGP Desktop Settings
Options for managing PGP Desktop clients

☐ **Exclude non-matching users by default**
Users not associated with any custom policy are created as excluded users.

2 Click **Restore to Factory Defaults** if you want all settings returned to their default settings.

3 The **Directory Services** section of the Policy Options card is different depending on whether you are editing the Internal Users: Default policy or a policy you created.

- If you are editing the Internal Users: Default policy, select **Exclude non-matching users by default** if you want your user polices to be able to include some users from your LDAP directory using Directory Synchronization but exclude others. Checking this box means that if none of the custom user policies you configure apply to a user, that user will be automatically treated as an excluded user. If you do not check this box, and if none of the custom user policies apply to a user, then the default internal user policy applies.
- If you are editing a user-created policy, you can assign policies to internal users based on their directory attributes, if LDAP directory synchronization is enabled. Refer to "Matching Attributes" on page 231 for more information.

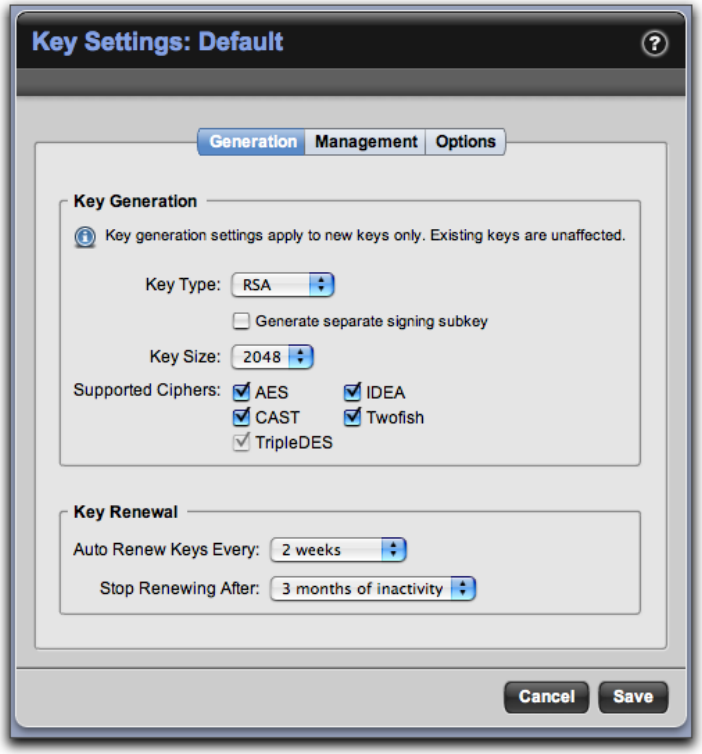
4 Click **Client Updates** and select **Notify users of software updates and automatically download** if you want PGP client software to automatically search for and download updates.

Uncheck this option to prevent automatic download of new PGP client software.

5 Click **Proxy Server** and select **Use an HTTPS Proxy Server for PGP client communications** if the client must connect through a proxy server. Type in the hostname and port for the HTTPS proxy server.

6 Click the **Edit** button for **Key Settings** to establish key settings. These settings apply to keys generated for use with any of the PGP encryption products, including PGP Universal Satellite.

The Key Settings card appears.



Key Generation

Key generation settings apply to new keys only. Existing keys are unaffected.

Key Type: RSA

□ Generate separate signing subkey

Key Size: 2048

Supported Ciphers: ☑ AES ☑ IDEA ☑ CAST ☑ Twofish ☑ TripleDES

Key Renewal

Auto Renew Keys Every: 2 weeks

Stop Renewing After: 3 months of inactivity

7 From the **Generation** card, in the **Type** drop-down list, select **RSA** or **DH/DSS**. The default is RSA.

> DH/DSS key types are incompatible with S/MIME. Users with DH/DSS keys will not have a certificate with which they can sign their messages to S/MIME users, even when there is an Organization Certificate present.

8 Specify whether you want to generate a separate signing subkey for the user. Separate signing subkeys are not available to SKM users. Refer to "Key Mode" on page 313 for more information on signing subkeys.

9 In the **Key Size** drop-down list, select the size of the keys to be created. Available options are: 1024, 1536, 2048, 3072, and 4096.

10 In the **Supported Ciphers** section, remove the check mark from any cipher type you do not want created keys to support or that do not meet your security requirements. TripleDES is the default cipher, used if none of the other ciphers are chosen or available, and cannot be unchecked.

11 In the **Auto-Renew Keys Every** drop-down list, select an auto-renewal time frame.

> You can only set key renewal policy for server-managed keys. If you select **Client Key Mode (CKM)** in step 13 below, and the user chooses to generate and self-manage keys, key renewal policy will not apply.

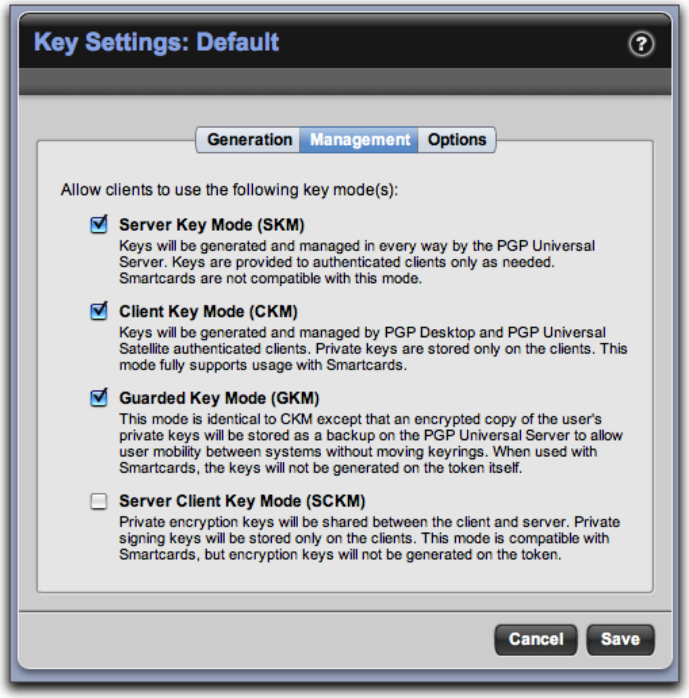
Internal keys will automatically be renewed in the time frame you specify unless they have exceeded the inactivity threshold in **Stop Renewing After**. Select **Never renew** if you want your internal keys never to renew; this means the keys will never expire, regardless of inactivity.

12 In the **Stop Renewing After** drop-down list, specify a period of inactivity after which a key will *not* be automatically renewed.

Select **Never stop renewing** if you want keys of internal users to be continually renewed. The question you should ask yourself here is how long a period of inactivity for a given user should be before you reasonably conclude that the user account is no longer in use.

It is generally a good idea to set the auto-renewal time to be fairly short. This helps ensure that the SMSA manages itself without you needing to delete a user manually in the event someone leaves your organization.

13 Click **Management** to select the user key mode.



Allow clients to use the following key mode(s):

☑ **Server Key Mode (SKM)**
Keys will be generated and managed in every way by the PGP Universal Server. Keys are provided to authenticated clients only as needed. Smartcards are not compatible with this mode.

☑ **Client Key Mode (CKM)**
Keys will be generated and managed by PGP Desktop and PGP Universal Satellite authenticated clients. Private keys are stored only on the clients. This mode fully supports usage with Smartcards.

☑ **Guarded Key Mode (GKM)**
This mode is identical to CKM except that an encrypted copy of the user's private keys will be stored as a backup on the PGP Universal Server to allow user mobility between systems without moving keyrings. When used with Smartcards, the keys will not be generated on the token itself.

□ **Server Client Key Mode (SCKM)**
Private encryption keys will be shared between the client and server. Private signing keys will be stored only on the clients. This mode is compatible with Smartcards, but encryption keys will not be generated on the token.

14 Select among:

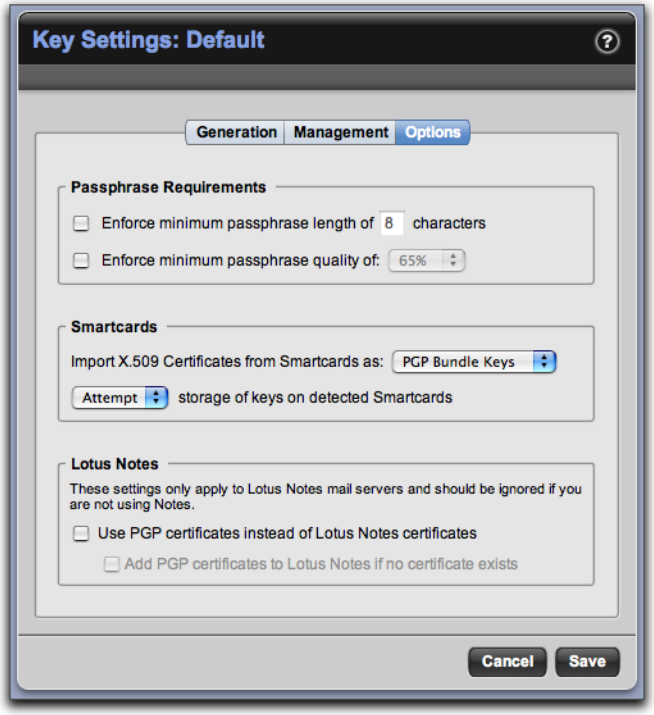
- **Server Key Mode (SKM)**. Select this option if you want the PGP Universal Server to generate and manage user keys.
- **Client Key Mode (CKM)**. Select this option if you want your users to be able to generate and manage their own keys.
- **Guarded Key Mode (GKM)**. Select this option if you want your users to be able to generate and manage their own keys, and you also want encrypted copies of users' private keys stored on the PGP Universal Server.

- **Server Client Key Mode (SCKM)**. Select this option if you want private encryption keys shared between clients and the PGP Universal Server, and private signing keys stored only on clients.

  To disable key generation for this internal user group, do not select any key mode.

  Refer to "Choosing a Key Mode For Key Management" on page 217 for information on how to choose the appropriate key mode. Refer to "Key Mode" on page 313 for general information on key modes.

15 Click **Options** to select key generation options.



Passphrase Requirements

☐ Enforce minimum passphrase length of 8 characters

☐ Enforce minimum passphrase quality of: 65%

Smartcards

Import X.509 Certificates from Smartcards as: PGP Bundle Keys

Attempt storage of keys on detected Smartcards

Lotus Notes

These settings only apply to Lotus Notes mail servers and should be ignored if you are not using Notes.

☐ Use PGP certificates instead of Lotus Notes certificates

☐ Add PGP certificates to Lotus Notes if no certificate exists

16 Select **Enforce minimum passphrase length of X characters** if you want to require a minimum number of characters in passphrases for new keys. The default is 8 characters.

17 Select **Enforce minimum passphrase quality of X%** if you want to require a minimum passphrase quality level for new keys.

These passphrase requirements apply to both key and PGP Whole Disk Encryption passphrases.

18 Select into which format you want to import X.509 certificates from smartcards:

- **PGP Bundle Keys**. Bundles user X.509 signing and encryption certificates into a single identity. This is the recommended option.

- **PGP Wrapper Keys**. This allows user X.509 signing and encryption certificates to be imported as separate identities. This option is not recommended because it only functions in an exclusively S/MIME environment.
- **User selectable**. Allows users to choose how to import their smartcard X.509 certificates.

19 Select **Require or Attempt storage of keys on detected Smartcards** if you want to store user keys on any detected smartcard.

20 If you are using a Lotus Notes mail server, you can choose to select **Use PGP certificates instead of Lotus Notes certificates**.

A PGP X.509 certificate becomes the user's active certificate in Lotus Notes, but only if the user is already using a non-PGP X.509 certificate. The Lotus Notes certificate is suppressed.

Lotus Notes users without PGP client software will be able to find PGP X.509 certificates in the Domino Directory and use them to encrypt mail.

If someone using both PGP Desktop and Lotus Notes turns off PGP Desktop Email proxying, the user can still decrypt incoming mail and sign outgoing mail.

The Lotus Notes full-text indexer can index PGP-encrypted content; MIME-formatted mail becomes searchable, but Lotus Notes Rich Text mail does not.

21 Select whether you want to **Add PGP certificates to Lotus Notes if no certificate exists**.

The PGP certificate is inserted into the Lotus Notes certificate directory, whether the user has another certificate or not.

For more details about the interaction between PGP Certificates and Lotus Notes, refer to "X.509 Certificate Management in Lotus Notes Environments" on page 221.

22 Click **Save**.

The Policy Options: Default card reappears.

23 Click the **Edit** button for **PGP Desktop Settings**.

The PGP Desktop: Default card appears. Make the changes you want to make.

Refer to Chapter 28, "Configuring PGP Desktop Installations" for complete information about this card and how to manage PGP Desktop deployments.

24 Click **Save**.

The Policy Options: Default card reappears.

Editing the Excluded Users Policy

The Excluded Users policy lets you tell your PGP Universal Server to exclude certain users from being added as internal users. The Directory Synchronization feature must be enabled to make the exclusion policy work. See Chapter 27, "Using Directory Synchronization to Manage Users" for more information.

You can edit the settings of the Excluded Users policy, but you cannot delete the policy.

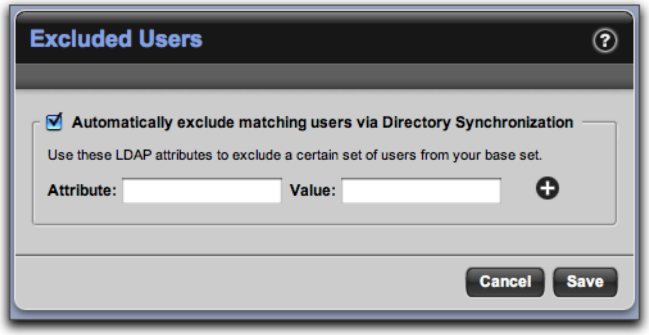
If some of your users are excluded users, and you later disable Directory Synchronization, those users will become internal users governed by the Internal Users: Default policy.

You can also exclude internal users by adding their email addresses to either of the default exclusions dictionaries. If a user's email address appears on the Excluded Addresses: Sign or the Excluded Addresses: Do Not Sign dictionaries, that user will not be added as an internal user. This is true even if none of the mail policy rules use the default exclusions dictionaries. Excluding users this way does not require Directory Synchronization. Refer to Chapter 17, "Using Dictionaries with Policy" for more information on dictionaries.

To edit the Excluded Users policy:

1 On the Internal User Policy card, click **Excluded Users**.

The Excluded Users card appears.


Excluded Users

☑ Automatically exclude matching users via Directory Synchronization

Use these LDAP attributes to exclude a certain set of users from your base set.

Attribute: Value:

2 Select **Automatically exclude matching users via Directory Synchronization**.

3 In the **Attribute** field, enter the attribute on which you want to match.

4 In the **Value** field, enter a value appropriate to the attribute on which you want to match, if desired.

5 If you would like to add more attribute/value pairs, click the plus sign icon. In the new row that appears, enter the appropriate values.

6 Click **Save**.

Deleting Internal User Policies

The Internal Users: Default and Excluded Users policies cannot be deleted.

If you delete an internal user policy and you have the Directory Synchronization feature disabled, all the users with that policy will be moved to the Internal Users: Default policy. If Directory Synchronization is enabled and you delete an internal user policy, users will be moved to another appropriate user policy. If there is no policy that matches a user, that user will be covered by the Internal Users: Default policy.

To delete a user-created internal user policy, click the Delete icon for the policy you want to remove.

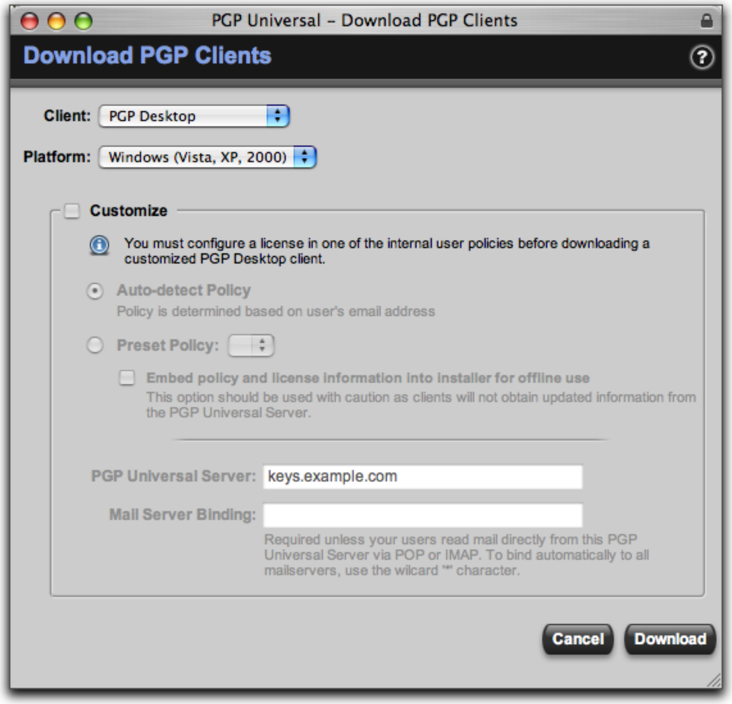
Downloading Client Software

The Download PGP Clients card lets you download Windows and Mac OS X installers of PGP Desktop and PGP Universal Satellite. You can create a customized version of the software installer to make it specific to the user environment. Each customized installer is associated with an internal user policy. You must have a license for PGP Desktop Email, PGP Whole Disk Encryption, or PGP NetShare to create customized PGP Desktop installers.

To download a PGP Desktop or PGP Universal Satellite installer:

1 On the Internal User Policy card, click **Download Client**.

The Download PGP Clients card appears.



PGP Universal – Download PGP Clients

Download PGP Clients

Client: PGP Desktop

Platform: Windows (Vista, XP, 2000)

□ Customize

You must configure a license in one of the internal user policies before downloading a customized PGP Desktop client.

● Auto-detect Policy
Policy is determined based on user's email address

○ Preset Policy:

□ Embed policy and license information into installer for offline use
This option should be used with caution as clients will not obtain updated information from the PGP Universal Server.

PGP Universal Server: keys.example.com

Mail Server Binding:

Required unless your users read mail directly from this PGP Universal Server via POP or IMAP. To bind automatically to all mailservers, use the wilcard "*" character.

2 In the Client drop-down list, select **PGP Desktop** or **PGP Universal Satellite**.

3 In the Platform drop-down list, select **Windows (Vista, XP, 2000)** or **MacOS X**.

4 If you want to customize the installers you are creating, put a check in the **Customize** checkbox and continue with this procedure. You must have a license for PGP Desktop Email, PGP Whole Disk Encryption, or PGP NetShare to create customized PGP Desktop installers.

If you don’t want the installers customized, click **Download**.

5 Select **Auto-detect Policy** or **Preset Policy** (this option is only available when creating a PGP Desktop installer; to create a PGP Universal Satellite installer, continue on to step 7):

- With **Auto-detect Policy**, PGP Desktop will periodically interact with the PGP Universal Server that created it to determine what policy it should implement. This option requires Directory Synchronization to be enabled. The user’s policy is based on the user’s email address and their attributes in the LDAP directory. If no policy matches, or if you have not created any new user policies, the default internal users policy will be implemented. Refer to Chapter 28, “Configuring PGP Desktop Installations” for more information on setting policy for PGP Desktop.

- With **Preset Policy**, the application implements the policy you select from the drop-down list. If you select an internal user policy that you have created, and that policy later is deleted, the application reverts to implementing the default internal users policy.

  If you select Preset Policy, be sure to choose the desired policy from the drop-down list.

6 If you chose to create a preset policy, you can also select to embed policy and license information into the installer for offline use. Offline use means no connection between PGP Desktop and PGP Universal Server. Policy information normally downloaded during installation is instead embedded in the installer itself. You can install the client even with no connect between PGP Desktop and PGP Universal Server. The client will not receive any updated policy information from the PGP Universal Server, even if the policy is updated on the server side, while offline. When the client is online, it will receive policy information normally.

7 In the **PGP Universal Server** field, enter the PGP Universal Server you want the application to interact with.

The PGP Universal Server you are using to create the installer is listed by default.

8 In the **Mail Server Binding** field, enter the name of the mail server you want bound to that PGP Universal Server. You can use wildcards. You must enter this information unless your users read mail directly from this PGP Universal Server via POP or IMAP. Customized client installations will not work without mail server binding.

Refer to “Binding” on page 317 for more information.

If you are creating a binding for an internal MAPI email client, you **must** use the WINS name of the Exchange Server.

If you are creating a binding for an internal Lotus Notes email client, you **must** use the fully qualified domain name of the Domino server.

9 Click **Download**.

The installer is downloaded to your system.

Directory Synchronization

The Directory Synchronization feature has two parts. These features let you synchronize your PGP Universal Server with an LDAP directory (such as Microsoft Active Directory) so that internal users can be created from the users in the directory.

- **The Directory Synchronization card**. This card, which you access via the Internal User Policy card, lets you enable the Directory Synchronization feature (a prerequisite to using it with your internal user policies) and establish its settings.
- **Excluding and matching users**. Once the Directory Synchronization feature is enabled, it can be used in other places, for example in specifying excluded users, and in matching users to specific policies.

Refer to Chapter 27, "Using Directory Synchronization to Manage Users" for more information about using the Directory Synchronization feature in concert with your user policies.

Choosing a Key Mode For Key Management

When you create PGP Universal Satellite and PGP Desktop installers, you can choose whether you want internal and external users to be able to manage their own keys, or whether keys should be managed by the PGP Universal Server.

	PGP NetShare Support	**PGP Universal Gateway Email Functions**			**End-to-end Email Processing Functions**			**Keys Managed By Server**
		Encrypt	Decrypt	Sign	Encrypt	Decrypt	Sign	
Client Key Mode (CKM)	Yes	No	No	No	Yes	Yes	Yes	No
Guarded Key Mode (GKM)	Yes	No	No	No	Yes	Yes	Yes	Private keys stored passphrase-protected
Server Key Mode (SKM)	No	Yes	Yes	Yes	Yes	No	Yes	Yes
Server Client Key Mode (SCKM)	Yes	Yes	Yes	No	Yes	Yes	Yes	Public and private encryption subkeys stored on client and PGP Universal Server, private signing subkeys stored only on client

- **Server Key Mode (SKM)**—The PGP Universal Server will generate and manage user keys.
  - Users cannot manage their own keys.
  - PGP Universal Server administrators have access to private keys.
  - If a user has a PGP client installation, the user's keys are downloaded to the client at each use.
  - SKM can also be used without client installations; if there is no client installation, you must use SKM.
  - Users with SKM keys will not be able to read email offline.

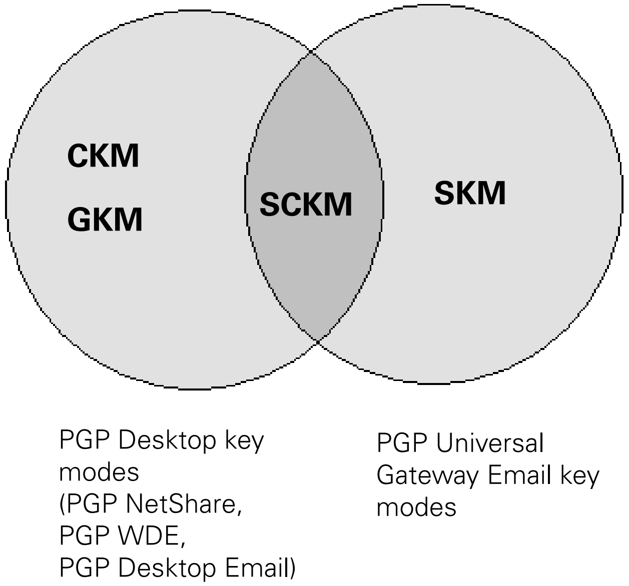
  - PGP NetShare does not support SKM.
  - In PGP Universal Gateway Email environments, existing users with SKM key mode keys who install PGP Desktop for the first time will be prompted automatically to re-enroll and create a CKM, GKM, or SCKM key.

- **Client Key Mode (CKM)**—Users use PGP client software to generate and manage their own keys.
  - PGP Universal Server administrators do not have access to private keys.
  - CKM user email is secure on the mail server.
  - CKM users are responsible for backing up their keys; if they lose their private keys, there is no way to retrieve them.
  - Users who want to be able to read their email offline and unconnected to PGP Universal Server must use CKM.
  - PGP NetShare supports CKM; it requires that users control their own keys.
  - PGP Universal Gateway Email does not support CKM.
- **Guarded Key Mode (GKM)**—Users will be able to generate and manage their own keys, and store their passphrase-protected private keys on the server.
  - GKM is similar to CKM, except that PGP Universal Server stores protected copies of private keys.
  - PGP NetShare supports GKM; it requires that users control their own keys.
  - PGP Universal Gateway Email does not support GKM.
- **Server Client Key Mode (SCKM)**—Keys are generated on the client. Private encryption subkeys will be stored on both the client and PGP Universal Server, and private signing subkeys will be stored only on the client.
  - SCKM allows for separate signing and encryption subkeys, comparable to X.509 signing and encryption keys.
  - The public and private encryption subkey is on the server, but by default encryption is not performed on the server.
  - The public-only signing subkey is on the server. PGP Universal Server cannot sign email for the user.
  - Mail processing must take place on the client side in order to use the SCKM signing subkey. If you want to use PGP Universal Gateway Email with SCKM keys, you must be using PGP Universal Server 2.5 or later. PGP Universal Gateway Email allows email encryption and decryption with SCKM keys, but email will not be signed.
  - SCKM is compatible with smartcards, but encryption keys will not be generated on the token. Copy the keys onto the token after generation.

- If an SCKM user resets their key, the entire SCKM key is revoked, including all subkeys, and remains on the PGP Universal Server as a non-primary key for the user. This non-primary key can still be used for decryption, and will remain on the PGP Universal Server until manually removed by the administrator.
- SCKM is not supported by legacy PGP Desktop installations before version 9.0.
- PGP NetShare supports SCKM; it requires that users control their own keys.

Which key management option you choose depends on what your users need and which PGP client application they use. Server Key Mode is generally appropriate for PGP Universal Satellite users. Client Key Mode is more appropriate for PGP Desktop users. If your security policy requires that a user's signing key is only in the possession of the user, but the user's encryption key must be archived, SCKM is the correct choice.

Figure 7-1. Recommended Key Mode Compatibility Per PGP Product


CKM
GKM
SCKM
SKM
PGP Desktop key modes (PGP NetShare, PGP WDE, PGP Desktop Email)
PGP Universal Gateway Email key modes

If you want to use both PGP Desktop and PGP Universal Gateway Email, your users will need SCKM keys.

If your users only require support for messaging, PGP Universal Satellite and SKM are sufficient. Both public and private keys are stored on the PGP Universal Server, and the private key is only temporarily sent to the client application for message signing and decryption. SKM is not as secure as CKM because the private keys are not under individual management. Separate signing subkeys are not available to SKM users.

PGP Desktop has more features than PGP Universal Satellite, and those features require client-controlled keys. For example, to use the PGP Whole Disk Encryption option with a hardware token in PGP Desktop, users must be able to generate and manage the key stored on the Whole Disk token. If you want a PGP Virtual Disk to be created automatically at installation, that also requires CKM. PGP Netshare is also unavailable to SKM users.

Refer to "Editing Internal User Policies" on page 208 for more information on key management settings. Refer to "Key Mode" on page 313 for general information on key modes and how they affect PGP Universal Satellite.

Disabling Key Generation

You can choose to disable key generation for a user group. This option enables you to control the creation and distribution of keys to users. If you disable key generation, you must manually create keys for all users in that user group.

For example, you can create keys with an attached Additional Decryption Key. Then, if your security policy requires the user keys be stored on client computers rather than on a central server, you can distribute these customized keys to PGP Desktop users.

From the Key Settings>Management card, uncheck all the key mode options to disable key generation.

Adding PGP Desktop Solutions to Existing PGP Universal Gateway Email Environments

PGP NetShare requires users' keys to use CKM, GKM, or SCKM mode. In PGP Universal Gateway Email environments, existing users with SKM key mode keys who install PGP Desktop for the first time will be prompted automatically to re-enroll and create a CKM, GKM, or SCKM key.

Enrolling will revoke the user's SKM key and replace it with the key the user generates using the wizard. Users can continue to decrypt with the revoked SKM keys, but all new messages will be encrypted to the new key and must be decrypted at the client.

Changing Key Modes

If you allow PGP Desktop users to change their options and allow user-initiated key generation, users will be able to switch key modes.

If the user's policy has changed to permit user-managed keys, then the user will automatically be prompted to create a new key, and no further action is necessary. However, if the user's policy has always permitted user key management, and the user would like to switch key modes now, the user should follow this procedure.

To change key mode:

1 Open PGP Desktop and select the PGP Messaging service whose key mode you want to determine.

The account properties and security policies for the selected service appear.

2 Click **Key Mode**.

The PGP Universal Key Mode screen appears, describing your current key management mode.

3 Click **Reset Key**.

The PGP Key Setup Assistant appears.

4 Read the text, then click **Next**.

The Key Management Selection screen appears.

5 Select the desired key mode.

Depending on how your PGP Universal administrator configured your copy of PGP Desktop, some key modes may not be available.

6 Click **Next**.

The Key Source Selection screen appears.

7 Choose one of the following:

– **New Key**. You will be prompted to create a new PGP key, which will be used to protect your messaging.

– **PGP Desktop Key**. You will be prompted to specify an existing PGP key to use to protect your messaging.

– **Import Key**. You will be prompted to import a PGP key, which will be used to protect your messaging.

8 Make the desired selection, then click **Next**.

9 If you selected **New Key**:

a Enter a passphrase for the key, then click **Next**.

b When the key is generated, click **Next**.

c Click **Finish**.

10 If you selected **PGP Desktop Key**:

a Select the key from the local keyring that you want to use, then click **Next**.

b Click **Finish**.

11 If you selected **Import Key**:

a Locate the file that holds the PGP key you want to import (it must contain a private key), then click **Next**.

b Click **Finish**.

X.509 Certificate Management in Lotus Notes Environments

This section applies only if you have ***both*** a PGP Universal Server enterprise encryption platform managing PGP Desktop clients and a Lotus Notes/Domino environment.

You can populate your Lotus Notes Domino X.509 certificate store with X.509 certificates created by and managed by your PGP Universal Server through the PGP Universal Encryption Platform. This includes deploying the private portion of the certificate into the user's Lotus Notes ID file and the public portion into the organization’s Domino Directory.

This feature is disabled by default.

This feature allows you to take advantage of the management capabilities of your PGP Universal Server and to maintain cryptographic compatibility in places where PGP Universal cannot otherwise play a role.

For example:

- If a user or administrator selects “encrypt incoming mail” on the user’s Domino person document, any mail encrypted by the server can be decrypted by PGP Desktop when the user opens the message. All of the secure-messaging features provided by PGP Desktop can be used, including notifications and logging.
- The Lotus Notes full-text indexer can index PGP-encrypted content; MIME-formatted mail becomes searchable, but Lotus Notes Rich Text mail does not.
- External or internal users who are not using PGP client software (PGP Desktop or PGP Universal Satellite) can still find the PGP-generated X.509 certificates deployed by Lotus Notes-based PGP Desktop users and send S/MIME-encrypted mail to those users. The PGP-managed X.509 certificates proliferate into the Notes/Domino X.509 certificate stores so that all Notes/Domino services may make native use of them.

> Further integration with the Lotus Domino X.509 environment, including participation in the Domino Certificate Authority (CA) server process, is not included in this feature. Certificates deployed by PGP Desktop will not be included in the Domino Issued Certificate List (ICL) or its internal Certificate Revocation List (CRL).

Trusting Certificates Created by PGP Universal

To populate your Domino Directory with X.509 certificates created by PGP Universal, you must configure the Domino Directory to trust the X.509 certificates, then establish how the PGP Universal X.509 certificates are pushed to the Lotus Notes/Domino environment.

> By taking the following steps, you are extending explicit trust of X.509 certificates that are created and managed by PGP Universal into your Lotus Notes/Domino environment.

To configure the Domino Directory to trust the X.509 certificates:

- Export the root public and passphrase-protected private X.509 Organization Certificate from the PGP Universal Server to a PKCS12 file.
- Import the PKCS12 file into the Domino Directory.
- Configure the Domino Directory to trust the X.509 certificates.
- Establish how PGP Universal X.509 certificates are pushed to the Lotus Notes/ Domino environment.

To export the root X.509 Organization Certificate from the PGP Universal Server to a PKCS12 file.

1 On the PGP Universal Server, from **Organization>Organization Keys**, open the Organization Certificate.

2 Click **Export**.

3 From the Export Certificate dialog, select **Export Keypair**.

4 Enter a passphrase.

5 Click **Export** to export the root public and passphrase-protected private X.509 certificate from the PGP Universal Server to a PKCS12 file.

To import the PKCS12 file into your Domino Directory:

1 On the Domino Directory **Administration Client**, select **Configuration**.

2 Open the **Certificates** part of the directory tree.

3 From the Certificates part of the directory tree, select **Certificates**.

4 From the Action menu, select **Import Internet Certificates**.

The Specify File dialog appears.

5 Browse to select the PKCS12 certificate, then click **Open**.

6 Enter the certificate passphrase in the Enter Password dialog.

The Import Internet Certificate dialog appears.

7 Click **Accept All**. The certificate is imported.

To configure the Domino Directory to cross-certify (trust) the X.509 certificates:

1 On the Domino Directory **Administration Client**, select **Configuration**.

2 Open the **Certificates** part of the directory tree.

3 From the Certificates part of the directory tree, select **Certificates**.

4 From **Internet Certificates**, find and double-click the imported certificate.

The certificate opens.

5 From the **Actions** menu, select **Create Cross Certificate**.

The Create Cross Certificate dialog appears.

6 Select the certificate and click **OK**.

7 From the Issue Cross Certificate dialog, click **Server** and select the server where the certificate should be stored, then click **OK**.

8 Click **Certifier**, choose the appropriate Notes/Domino certifying ID file (or use the Domino CA Process if it is in use), and click **OK**.

9 Choose the subject name and expiration date for the certificate.

10 Click **Cross Certify**. The imported root certificate is cross-certified (trusted).

To establish how PGP Universal X.509 certificates should be pushed to the Lotus Notes/ Domino environment:

1. On the PGP Universal Server, from **Policy>Internal User Policy**, select the internal user policy you want to modify.
2. Click the **Edit** button for **Key Settings**.
3. Click **Options** and choose the correct Lotus Notes settings. For information on how to select the appropriate settings, refer to "Setting the Lotus Notes Key Settings in PGP Universal" on page 224.

Setting the Lotus Notes Key Settings in PGP Universal

There are two options in PGP Universal that control how PGP Universal X.509 certificates are used in the Lotus Notes/Domino environment.

These options are:

- **Use PGP certificates instead of Lotus Notes certificates**. This option adds the users' PGP X.509 certificate into the Lotus Notes/Domino credential store if and only if the user has an active X.509 certificate not generated by PGP Universal. Lotus Notes users do not receive an X.509 certificate by default; instead, the user or administrator must provide one.

  Once enabled, the PGP X.509 certificate becomes the users' active certificate in Lotus Notes; the Lotus Notes certificate is suppressed. Lotus Notes users without PGP client software will be able to find PGP X.509 certificates in the Domino Directory and use them to encrypt mail.

  This setting allows the organization to eliminate certificate confusion by making the PGP-generated certificate primary and any other certificates secondary. The setting prevents message verification failure, which occurs when a recipient without PGP Desktop client software opens an S/MIME message signed by a sender who does use PGP Desktop. The sender's signing certificate is generated by PGP Desktop, but the recipient directory lookup in the Domino Directory fails to find a match.

- **Add PGP certificates to Lotus Notes if no certificate exists**. If you enable this setting in addition to the **Use PGP certificates instead of Lotus Notes certificates** setting, this setting inserts the PGP X.509 certificates into the Lotus Notes certificate directory, overlaying and overriding any X.509 certificates already there. Every Lotus Notes-based PGP Desktop client automatically inserts its PGP X.509 certificate into the Lotus Notes/Domino environment.

Technical Deployment Information

Before you use PGP-generated certificates with your Domino server, you must prepare your email environment. To prevent an inconsistent state, there are steps you must take before any change to the Lotus Notes/Domino certificate store is committed.

The steps are:

1 Make sure the user has Author or Editor access to her “person document” in the Domino Directory on her home server. This enables PGP Desktop and certificate settings to be shared.

   – If the Domino directory template has been installed unmodified, give users Author access.

   – If the Domino directory template has been installed with modifications, Author access may not be sufficient. If Author access does not allow PGP Desktop and certificates settings to be shared, give users Editor access.

2 If the public certificate to be deployed is not found in the person document, add the certificate and mark it as the default encryption certificate.

3 If the public certificate is not found in the user’s Notes ID file (keyring), add the associated private key and the certificate to the ID file, marking it as the default signing certificate for Internet mail.

Furthermore, PGP Desktop will maintain any certificates deployed, updating them when they expire, for instance, and PGP Universal issues replacements. No certificates are ever deleted from the Lotus Notes/Domino certificate store by PGP Desktop, as legacy certificates must be preserved in order to decrypt or verify content previously encrypted to or signed by those certificates.

27 Using Directory Synchronization to Manage Users

This chapter describes the Directory Synchronization feature, which lets you synchronize an LDAP directory with your PGP Universal Server. Directory Synchronization allows you to assign different user polices to specific internal user groups.

With Directory Synchronization for a PGP Universal Server, internal users for that PGP Universal Server can come only from the directory you specify when you enable Directory Synchronization. If users are in the directory, they will be added to the system as internal users. If users are *not* in that directory, their disks, messaging, or files will *not* be protected by the PGP Universal Server.

PGP Universal Server supports LDAPv2, and LDAPS. You can use any of a number of directories with PGP Universal Server, although directories that more closely conform to the OpenLDAP or X.500 standards will work best.

Topics in this chapter include:

Overview

Enabling Directory Synchronization lets you do multiple things:

- Include users from the specified directory as internal users for the PGP Universal Server.
- Exclude specified users from the directory from being internal users.
- Include only specified users from the directory, allowing them to be added to the PGP Universal Server as internal users, and excluding users that don't match the criteria.
- Match certain users from the specified directory with an internal user policy you create.
- When you enable Directory Synchronization, your PGP Universal Server will use the LDAP directory to assist it with creating and enrolling internal users.

Synchronization occurs when the local user (a user in a managed domain) sends or receives an email message. When a local user sends or receives a message, the PGP Universal Server checks to see if the sender is known to it. If not, it will check the LDAP directory (assuming Directory Synchronization is enabled) to see if the user is present. Changes made to an LDAP directory may take up to 10 minutes to take effect in PGP Universal Server.

If the user is found in the LDAP directory (or the portion of it you specify), the PGP Universal Server adds that person as an internal user. You also have options to narrow the scope of the searching to certain parts of the directory (see "Base DN and Bind DN" on page 233) or to users with certain attributes (see "Matching Attributes" on page 231).

When users are added to PGP Universal Server from a directory via Directory Synchronization, their names, email addresses, and existing X.509 certificates (used to secure S/MIME email messages) will be imported. If certificates are not found, PGP Universal Server will generate PGP keys (and certificates, if configured for certificates) for these users.

To import an X.509 certificate (RSA only) found on an LDAP directory, that certificate must have been issued by a trusted certificate. To ensure this happens, be sure the certificate of the issuing Root CA, and all other certificates in the chain between the Root CA and the X.509 certificate, are on the list of trusted keys and certificates on the Trusted Keys and Certificates card (Policy>Trusted Keys) and is trusted for verifying mail encryption keys. If it is not, import the certificate of the issuing Root CA that issued the user certificate to the list as soon as you enable Directory Synchronization. Refer to Chapter 13, "Managing Trusted Keys and Certificates" for instructions.

Certificates that include an email address that is ***not*** in a domain being managed by the PGP Universal Server will **not** be added to the internal user account that is created. Expired, revoked, weak certificates (less than 1024-bit encryption), and certificates with greater than 4096-bit encryption will not be imported via Directory Synchronization.

When Directory Synchronization is enabled, for a user to be correctly added to PGP Universal Server, the "mail" attribute must be present in the directory and they must match the information PGP Universal Server has about them. The "uid" attribute must also be present, unless the directory is a Microsoft Active Directory, which requires the "sAMAccountName" attribute. For example, if PGP Universal Server discovers a user with a login name of "ming" and an email address of "mingp@example.com," that user must have attributes "uid=ming" and "mail=mingp@example.com" in the directory. If these attributes do not match or are empty, the user will not be added correctly. Refer to "Directory Attributes" on page 238 for a list of attributes.

The X.509 certificates stored in LDAP directories contain only public keys, so these users will be imported into PGP Universal Server as Client Key Mode (CKM) users, which means that the PGP Universal Server does **not** have the private key for these users.

You can only synchronize one LDAP directory with one PGP Universal Server. You may, however, use a different LDAP directory for each PGP Universal Server in a cluster. In such a scenario, the LDAP directories should mirror each other.

Enabling Directory Synchronization

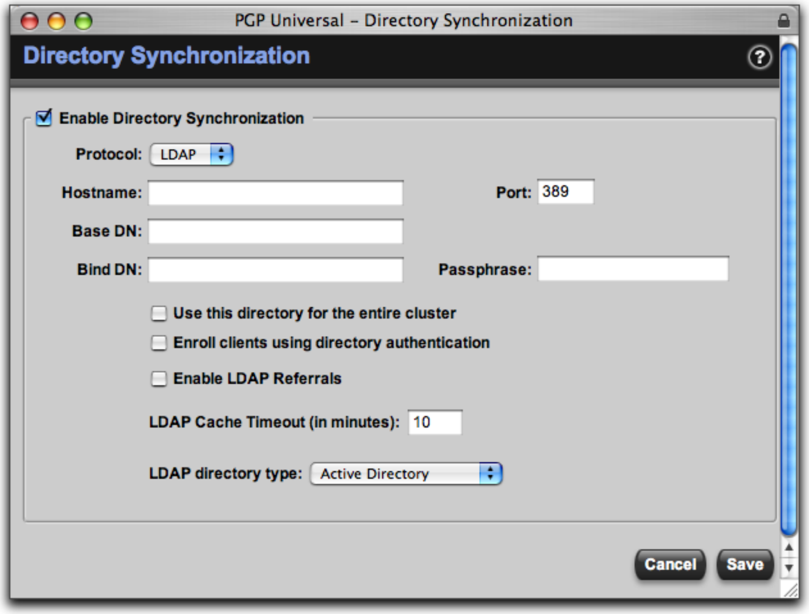
To enable Directory Synchronization:

1 Go to Policy>Internal User Policy in the administrative interface.

The Internal User Policy card appears.

2 Click **Directory Synchronization**.

The Directory Synchronization card appears.



PGP Universal – Directory Synchronization

Directory Synchronization

☑ Enable Directory Synchronization

Protocol: LDAP

Hostname:

Port: 389

Base DN:

Bind DN:

Passphrase:

□ Use this directory for the entire cluster

□ Enroll clients using directory authentication

□ Enable LDAP Referrals

LDAP Cache Timeout (in minutes): 10

LDAP directory type: Active Directory

3 Select the **Enable Directory Synchronization** checkbox.

4 Pull down the Protocol drop-down menu and select **LDAP** or **LDAPS**.

5 Enter the fully qualified domain name or IP address of the LDAP directory server in the **Hostname** field.

6 Keep the default value of 389 for LDAP or 636 for LDAPS, or enter a preferred value in the **Port** field.

7 If desired, enter a value in the **Base DN** field; this narrows the search for users and certificates to that portion of the directory. This is an optional field. Refer to "Base DN and Bind DN" on page 233 for more information about the Base DN and Bind DN fields.

8 Enter an appropriate value in the **Bind DN** field. This value will be used to initially bind (or log in) to the directory server. Binding determines the permission level granted for the duration of a connection.

If you are using the Bind DN field, enter the passphrase used for authentication in the **Passphrase** field.

9 If you are working on the Primary server in a cluster, put a checkmark next to **Use this directory for the entire cluster** if this is the only directory server you want searched for users, and you want all of the PGP Universal Servers in the cluster to access this same directory.

Additionally, if you enable this setting, all Directory Synchronization settings will be automatically copied to the Secondary servers in the cluster. You do not need to enable Directory Synchronization on Secondary servers.

If this setting is not enabled, you must manually connect to each Secondary server in the cluster and configure the Directory Synchronization settings on each of them.

This checkbox is only available on the Primary server in a cluster.

10 Select **Enroll clients using directory authentication** if you want PGP Desktop user enrollment authentication through Directory Synchronization instead of through email. If you do not choose this enrollment option, users will be enrolled through email.

User enrollment through LDAP allows you to deploy standalone PGP Whole Disk Encryption to users without requiring email processing.

Refer to "Understanding User Enrollment Methods" on page 234 for more information on user enrollment.

11 Select **Enable LDAP Referrals** to allow PGP Universal Server to query referred LDAP directories for user information.

The LDAP directory you choose for Directory Synchronization can respond to PGP Universal Server queries with a referral or reference to another LDAP directory. If you allow PGP Universal Server to query referred LDAP directories, the search can take a long time. If you do not allow referred queries, PGP Universal Server will disable users not found in the named directory, even if user information is available in the referred directory.

12 Set the **LDAP Cache Timeout (in minutes)**. The default is 10 minutes.

The LDAP cache contains timestamps that record when the PGP Universal Server last queried user information. The user information itself is stored in the PGP Universal Server database, not in the cache. The time stamp in the cache prevents another search on the user within the cache timeout limit, to keep LDAP queries from overloading the system.

13 Select your **LDAP directory type**. Choose **Active Directory** or **OpenLDAP (RFC 1274)**. Active Directory is the default setting.

Microsoft Active Directory uses the sAMAccountName attribute for user information where OpenLDAP-based directories use the attribute uid for user information. PGP Universal Server queries user information using only the necessary attributes, providing faster results when querying user information.

Users upgrading to PGP Universal Server 2.5.2 and later from the previous version will need to set this manually after upgrade.

14 Click **Save**.

Excluding Users

If you have users in the LDAP directory you specified to use for Directory Synchronization whose messaging you do *not* want to protect, you can tell your PGP Universal Server that these users should not be added as valid internal users. Users in the directory who do not meet the exclusion criteria are eligible to be added as internal users to the PGP Universal Server.

If you have not enabled Directory Synchronization, you will not be able to exclude users.

You can exclude users based on specific attributes, or you can exclude all users to whom no custom policy applies.

To exclude users with no custom policy:

1 Go to Policy>Internal User Policy in the administrative interface.

The Internal User Policy card appears.

2 Click Internal Users: Default in the list of internal user policies.

3 Select **Exclude non-matching users by default**. Checking this box means that if none of the custom user policies you configure apply to a user, that user will be automatically treated as an excluded user. If you do not check this box, if none of the custom user policies apply to a user, then the default internal user policy applies.

4 Click **Save**.

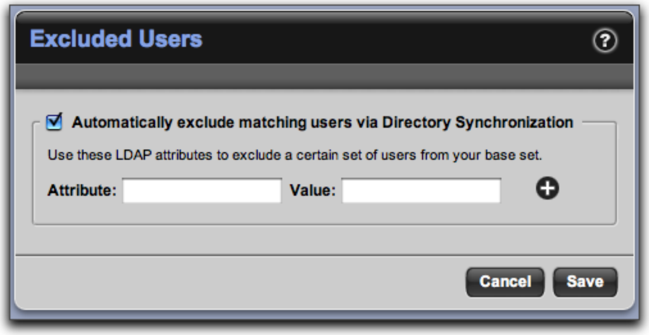
To exclude users by attribute:

1 Go to Policy>Internal User Policy in the administrative interface.

The Internal User Policy card appears.

2 Click **Excluded Users** in the list of internal user policies.

The Excluded Users card appears.



☑ Automatically exclude matching users via Directory Synchronization

Use these LDAP attributes to exclude a certain set of users from your base set.

3 Put a check in the **Automatically exclude matching users via Directory Synchronization** checkbox.

4 In the **Attribute** field, enter the attribute on which you want to match. For example, you can add attributes such as O for organization, OU for organizational unit, M for email address, L for locality, or C for country.

5 In the **Value** field, enter a value appropriate to the attribute on which you want to match, if desired.

6 If you would like to add more attribute/value pairs, click the plus sign icon. In the new row that appears, enter the appropriate values.

7 Click **Save**.

Including Only Some Users

The Directory Synchronization feature also makes it possible to include only those users in the directory that match criteria you specify and exclude all other users.

To do this, Directory Synchronization must be enabled; refer to "Enabling Directory Synchronization" on page 228 for instructions.

Then you must configure the default internal user policy to support excluding some users. This allows customized user group policies to be applied to users instead of the default policy.

Finally you must create a new internal user group policy that matches users based on the attribute and value pair you specify. All those users in the directory that match the criteria in the new policy will be included as internal users on the PGP Universal Server; all others will be excluded. The custom settings of the new policy will be applied to these users. See to Chapter 26, "Setting Internal User Policy" learn how to create and edit internal user policies.

Matching Attributes

There are two reasons to match users from your LDAP directory (Directory Synchronization must be enabled) so that the settings from an internal user policy can be applied to them:

- You want specific key settings to apply only these users.
- You want to deploy PGP Desktop to these users with specific settings.

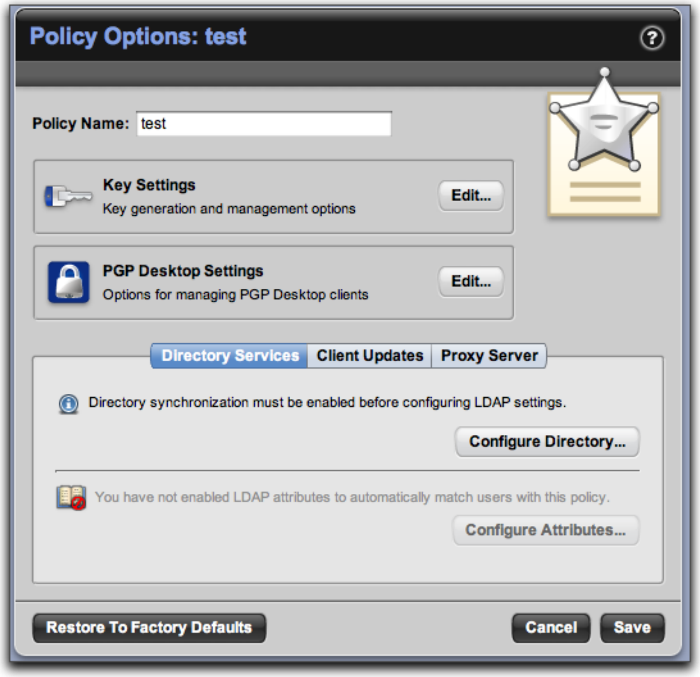
To specify users for an internal user policy:

1 On the Internal User Policy card, create a new internal user policy.

Refer to Chapter 26, "Setting Internal User Policy" for more information.

2 On the Internal User Policy card, click on the name of the new internal user policy.

The Policy Options card for the selected internal user policy appears.



Policy Options: test

Policy Name: test

Key Settings
Key generation and management options

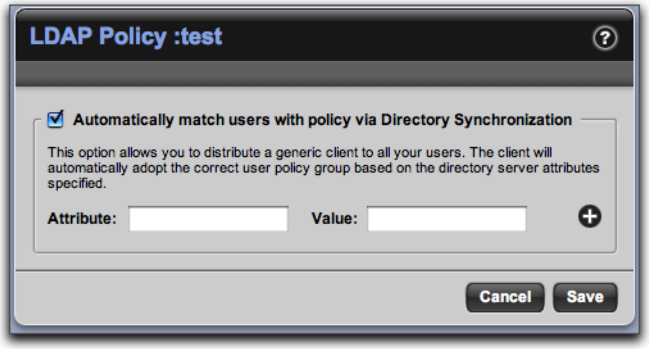
PGP Desktop Settings
Options for managing PGP Desktop clients

Directory synchronization must be enabled before configuring LDAP settings.

You have not enabled LDAP attributes to automatically match users with this policy.

3 Click **Configure Attributes**.

The LDAP Policy for the selected user group policy appears.



LDAP Policy :test

☑ Automatically match users with policy via Directory Synchronization

This option allows you to distribute a generic client to all your users. The client will automatically adopt the correct user policy group based on the directory server attributes specified.

Attribute: Value:

4 Put a check in the **Automatically match users with policy via Directory Synchronization** checkbox.

5 In the **Attribute** field, enter the attribute on which you want to match.

6 In the **Value** field, enter a value appropriate to the attribute on which you want to match, if desired.

Only one policy can apply to each user. Make sure to set attributes so that each user only matches one set of attributes.

7 If you would like to add more attribute/value pairs, click the plus sign icon. In the new row that appears, enter the appropriate values.

If you specify more than one attribute/value pair, directory user data only needs to match one pair for the policy to apply.

8 Click **Save**.

The Policy Options card reappears.

Base DN and Bind DN

When you have to set criteria for the Directory Synchronization feature, you will need to decide whether to use Base DN or Bind DN based on the access permissions of the users in the LDAP directory.

Base DN

The Base Distinguished Name (DN) is where directory lookups occur by default and where all user details will be placed in your directory tree. If you enter a Base DN value, you will narrow the search for users and certificates to that specific portion of the directory. While an LDAP directory may have multiple Base DNs on one server, the PGP Universal Server can only refer to one Base DN.

Base DN entries usually look as follows in an Active Directory environment:

CN=users,DC=<yourcompany_name>,DC=<yourcompany_domain>

(CN=users, DC=acmecorp, DC=net, for example)

PGP Universal Server can automatically determine the Base DN to use if your LDAP directory supports the RFC 2252 namingContexts attribute. If it does not support this attribute, you will need to manually enter the Base DN to search.

Bind DN

The Bind Distinguished Name (DN) will be used to initially bind (or log on) to the directory server.

The Bind DN entry creates a user in the directory. This user represents the PGP Universal Server, allowing PGP Universal Server to log in to the directory and retrieve information.

Bind DN entries usually look as follows in an Active Directory environment:

CN=LDAP user,CN=users,DC=<yourcompany_name>,
DC=<yourcompany_domain>

(CN=LDAP user,CN=users,DC=acmecorp, DC=net, for example)

Supply a passphrase for the created user to enable PGP Universal Server to access the directory.

Following is a sample Directory Synchronization configuration for an Exchange Server for a fictitious company called Acme Corporation:

Host: mail.acmecorp.net

Bind DN: CN=LDAP Search, CN=Users, DC=acmecorp, DC=net

Base DN: Leave blank

Here the "LDAP Search" user is a fake user created explicitly for this purpose, to allow the PGP Universal Server access to the directory, with its passphrase listed in the next field. To properly authenticate to the Active Directory Server, create a new user in that directory to allow PGP Universal Server access.

Understanding User Enrollment Methods

Enrollment is the process of binding a machine with PGP client software installed to a PGP Universal Server. After a client is bound it receives feature policy information from the PGP Universal Server; for example, encryption keys, email policy, PGP NetShare, or PGP Whole Disk Encryption administration.

There are 2 ways to enroll client software:

- **Email enrollment**. This is the default method; if you do not select **Enroll clients using directory authentication** when you enable Directory Synchronization, users will enroll through email.

  This method is available to all client installations, including PGP Whole Disk Encryption-only installations, as long as there is an email account on the installed computer. Email enrollment is possible even if the PGP Universal Server does not perform email encryption or is out of the mailflow. Email enrollment only requires that the PGP Universal Server be able to send an SMTP message to the client's mail server.

  Refer to "Email Enrollment" on page 235 to learn how to enroll clients through email.

- **LDAP directory enrollment**. If you select **Enroll clients using directory authentication** when you enable Directory Synchronization, you allow clients to enroll with LDAP.

  LDAP enrollment requires certain attributes in the directory in order to bind the client to the PGP universal Server. Refer to "Directory Attributes" on page 238 for more information on necessary attributes.

  Refer to "Directory Enrollment" on page 237 to learn how to enroll clients using directory synchronization.

Before Creating a Client Installer

Perform the following tasks before you create a client installer. These tasks apply to both email and LDAP enrollment.

1. Make sure that port 443 is open between the client machine and the PGP Universal Server. Clients use this port to retrieve policy information and encryption keys from the PGP Universal Server. Enrollment fails if port 443 is unavailable.

2. If the client must connect through a proxy server, from the applicable internal user policy, click **Proxy Server**, select **Use an HTTPS Proxy Server for PGP client communications**, and type in the hostname and port for the HTTPS proxy server.

3 Enter a valid PGP Desktop license. From Policy>Internal User Policy, choose the policy for which you want to enter a license. Refer to Chapter 28, "Configuring PGP Desktop Installations"for more information on how to enter a license for your client software.

4 Ensure that the domain you use for email appears as a managed domain on the Organization>Managed Domains page. This is necessary even if you are not using PGP Universal Server or PGP Desktop Email to process email. If your email domain does not appear on the Managed Domains page, add the domain. Refer to Chapter 11, "Managed Domains" for more information on managed domains.

5 Make sure you have DNS properly configured. Properly configured DNS settings (including root servers and appropriate reverse lookup records) are required in all cases to support PGP Universal Server. Make sure both host and pointer records are correct. IP addresses must be resolvable to hostnames, as well as hostnames resolvable to IP addresses.

6 If you are reinstalling PGP Desktop from a previous failed attempt, delete the folder under `C:\Documents` and `Settings\<username>\Application Data\PGP Corporation`. This deletes the preferences file and allows you to start with new settings.

Email Enrollment

This method is available to all client installations, including PGP NetShare-only and PGP Whole Disk Encryption-only installations, as long as there is an email account on the installed computer. Email enrollment is possible even if the PGP Universal Server does not perform email encryption or is out of the mailflow. Email enrollment only requires that the PGP Universal Server be able to send an SMTP message to the mail server.

If your email protocol cannot be proxied, then you cannot use email enrollment, but must choose LDAP enrollment instead. POP, IMAP, Lotus Notes, and MAPI protocols can all be proxied. Novell GroupWise cannot be proxied and does not allow email enrollment.

If you do not select **Enroll clients using directory authentication** when you enable Directory Synchronization, clients will enroll through email.

There are 2 parts to the client installation and enrollment process:

- On the PGP Universal Server, you create a client installer. Tasks include: adding mail routes, checking port and SMTP settings, enabling Directory Synchronization, creating user policies, and customizing and downloading the client installer.
- On the client machine, you install the client software. Tasks include: uploading the installer file, installing the client software, and following the enrollment wizard.

To create an client installer for email enrollment:

1 From Mail>Mail Routes on your PGP Universal Server, create a mail route that sends mail for your domain to the hostname of your mailserver. Refer to Chapter 24, "Specifying Mail Routes" for more information on adding mail routes.

2 Make sure port 25 is open between your PGP Universal Server and your mail server.

3 Make sure your mail server accepts SMTP. Some mail servers, for example Domino servers, may not be set to accept SMTP by default.

4 If you want to use directory synchronization to assign users to user policies, enable Directory Synchronization. From Policy>Internal User Policy, select **Directory Synchronization**. Do not select **Enroll clients using directory authentication**. Refer to "Enabling Directory Synchronization" on page 228 for more information.

5 From Policy>Internal User Policy, create internal user policies. Refer to Chapter 26, "Setting Internal User Policy" and Chapter 28, "Configuring PGP Desktop Installations" for more information.

6 Create a client installer. From Policy>Internal User Policy, select **Download Client**.

7 Click **Customize**, and add the settings you want for the installer.

Make sure to add your mail server name to the **Mail Server Binding** field. You can use wildcards. Mail Server Binding is necessary for email enrollment because it tells the client where to send enrollment email. This setting is also particularly important when PGP Universal Server is proxying email, because it specifies the mail server for which policies are being locally enforced. When the client machine sends email using the specified mail server, policy from the PGP Universal Server will be enforced.

Refer to "Downloading Client Software" on page 215 for more information on creating a client installer.

8 Click **Download** to download the installer.

If your Microsoft Internet Explorer security settings do not allow downloads, to override the security setting, click **Download** while you press and hold the CTRL button on your keyboard.

To install and enroll a client through email enrollment:

1 Upload the installer file to the client machine.

2 Install PGP Desktop by double-clicking the installer file.

3 Follow the on-screen instructions to install.

4 Restart the client machine when instructed.

The PGP Desktop Setup Assistant appears. Follow the instructions to enroll.

5 Enter the user's email address.

6 Run the email client application and check for new email.

7 The user should receive an enrollment email from the PGP Universal Server. You may need to open the email to use the enrollment cookie embedded in the email.

> If the user does not receive an enrollment email, make sure you followed the process correctly. In particular, make sure the email domain matches a managed domain, and make sure the correct ports are open.

8 From the Enrollment Assistant, continue with enrollment by following the instructions.

Directory Enrollment

If you select **Enroll clients using directory authentication** when you enable Directory Synchronization, you allow clients to enroll with LDAP. If you do not select this setting, clients will enroll through email.

To use LDAP enrollment your directory schema must contain certain attributes. Refer to “Directory Attributes” on page 238 for information on attributes.

There are 2 parts to the client installation and enrollment process:

- On the PGP Universal Server, you create a client installer. Tasks include: enabling Directory Synchronization, creating user policies, and customizing and downloading the client installer.
- On the client machine, you install the client software. Tasks include: uploading the installer file, installing the client software, and following the enrollment wizard.

To create an client installer for directory enrollment:

1 Enable Directory Synchronization on the PGP Universal Server. From Policy>Internal User Policy, select **Directory Synchronization**.

2 Select the **Enable Directory Synchronization** checkbox and enter all necessary information. For more information, refer to “Enabling Directory Synchronization” on page 228.

3 Select **Enroll clients using directory authentication**.

4 Click **Save**.

5 From Policy>Internal User Policy, create internal user policies. Refer to Chapter 26, “Setting Internal User Policy” and Chapter 28, “Configuring PGP Desktop Installations” for more information.

6 Create a client installer. From Policy>Internal User Policy, select **Download Client**.

7 Click **Customize**, and add the settings you want for the installer.

Make sure to add your mail server name to the **Mail Server Binding** field. You can use wildcards. This setting is particularly important when PGP Universal Server is proxying email, because it specifies the mail server for which policies are being locally enforced. When the client machine sends email using the specified mail server, policy from the PGP Universal Server will be enforced.

Refer to “Downloading Client Software” on page 215 for more information on creating a client installer.

8 Click **Download** to download the installer.

If your Microsoft Internet Explorer security settings do not allow downloads, to override the security setting, click **Download** while you press and hold the CTRL button on your keyboard.

To install and enroll a client through directory enrollment:

1. Upload the installer file to the client machine.
2. Install PGP Desktop by double-clicking the installer file.
3. Follow the on-screen instructions to install.
4. Restart the client machine when instructed.

   The PGP Desktop Setup Assistant appears. Follow the instructions to enroll.
5. Enter your network login username and password when prompted.
6. Click **Next**, and continue with enrollment.

ⓘ If enrollment fails, make sure you followed the process correctly. In particular, make sure that the attributes, especially the email address, are present in the directory and are populated with data.

Directory Attributes

Below is a list of required and optional attributes your LDAP directory must have for LDAP enrollment.

Because you specify what type of LDAP directory you use, PGP Universal Server queries user information using only the necessary attributes, providing faster results when querying user information.

ⓘ Microsoft Windows 2000/2003 Active Directory with Exchange Server has all required attributes. Other Directory Server and Email Server combinations might not have the necessary attributes.

Required attributes:

- **uid** or **sAMAccountName**. These attributes are interchangeable. Microsoft Active Directory uses sAMAccountName. All other LDAP directories use uid.
- **DN**. This attribute will exist if the user exists in the directory.
- **mail** or **proxyAddresses**. These attributes are interchangeable. Every user must have an email address for the attribute `mail`.
- **cn**. This attribute matches what PGP Universal Server refers to as Display Name.

Each user must have a password defined in the directory. This security feature prevents enrollment unless the user can authenticate with a username and password.

Optional attributes:

- **userCertificate**. This attribute allows PGP Universal Server to find user X.509 S/MIME public certificates.
- Attributes used to assign users to Internal User Policies. Refer to "Matching Attributes" on page 231 for more information.

Serving PGP Admin 8 Preferences

You can import and store Administrative Preferences from PGP Admin 8.x clients in an LDAP directory associated with your new PGP Universal Server. This allows you to retain preferences for PGP Desktop 8.x users, and still replace the old PGP Keyserver.

PGP Admin preferences do not affect PGP Desktop 9.x clients. The preferences are only stored for the benefit of users running previous versions of PGP Desktop.

You can use LDAP or LDAPS. If you choose LDAPS, make sure you have enabled LDAPS keyserver service on the new PGP Universal Server.

Read-only and Service Control Only PGP Universal Server administrators do not have write access to the LDAP servers, so they will not be able to import PGP Admin preferences.

1. Install and set up your new PGP Universal Server.
2. Open PGP Admin on your PGP administrative machine.
3. From **Administrative Options>Updates**, change the previous LDAP Server URL (for example, ldap://<oldkeyservername>) to the LDAP server URL you are using with your PGP Universal Server.

   The LDAP server URL format must be ldap://<newservername>/o=Prefs or ldaps://<newservername>/o=Prefs.

   The bind DN must be cn=<username>,o=Prefs.

   The username is the username of the PGP Universal Server administrator, and the passphrase is that user's PGP Universal Server passphrase. An example of the new LDAP server URL format would be ldap://keys.example.com,o=Prefs, which replaces ldap://oldkeyserver.example.com.
4. Click **OK**. The PGP Admin screen appears.
5. Click **Update Server Configuration**. The login screen for your new LDAP server appears. Log in with the username and passphrase specified in step 3.

   The current PGP Admin settings file is uploaded to the new LDAP server.

PGP Desktop 8 clients will download the preferences from the old server at ldap://<oldkeyserver>. Those preferences contain the new LDAP URL.

When your PGP Desktop 8 clients next poll for preference updates, they will download them from the new LDAP URL at ldap://<newservername>/o=Prefs.

Once your users have all started receiving preferences from the new PGP Universal Server, you can remove your old PGP Keyserver from service.

28 Configuring PGP Desktop Installations

This chapter describes the ability of PGP Universal Server to manage deployments of the PGP Desktop product line, which includes PGP Desktop Email, PGP Whole Disk Encryption, and PGP NetShare.

Topics include:

PGP Desktop Licensing

While all possible PGP Desktop Email, PGP Whole Disk Encryption, and PGP NetShare settings are visible, your license determines which settings are applied to client installations. Refer to Chapter 28, "Configuring PGP Desktop Installations" for information on creating client installations.

The following features are available depending on what PGP Desktop license you purchased:

	PGP Desktop Email 9.6	**PGP Whole Disk Encryption 9.6**	**PGP NetShare 9.6**	**PGP Desktop Professional 9.6**	**PGP Desktop Storage 9.6**	**PGP Desktop Enterprise 9.6**
PGP Desktop Email	Yes	No	No	Yes	No	Yes
PGP Whole Disk Encryption	No	Yes	No	Yes	Yes	Yes
PGP NetShare	No	No	Yes	No	Yes	Yes
PGP Virtual Disk	Yes	Yes	Yes	Yes	Yes	Yes
PGP Keys	Yes	Yes	Yes	Yes	Yes	Yes
PGP Shred	Yes	Yes	Yes	Yes	Yes	Yes
PGP ZIP	Yes	Yes	Yes	Yes	Yes	Yes

PGP Whole Disk Encryption Administration

PGP Whole Disk Encryption 9.6 offers a Single Sign-On feature. It synchronizes the PGP Whole Disk Encryption authentication process with the one required by Microsoft Windows when a user boots a computer. Once a disk or boot partition is encrypted, the next time the user starts the system, the PGP Whole Disk Encryption BootGuard screen appears immediately upon startup. Logging in at this point also logs the user into the Windows session. The users does not have to log in twice.

The Single Sign-On feature is enabled through the **Encrypt disks to existing Windows password (Single Sign-On)** checkbox on the File and Disk screen of the PGP Desktop Settings for any internal user policy.

If you select the checkbox, users with this policy are forced to choose the Single Sign-On feature when they initially protect a boot partition or an entire disk using PGP Whole Disk Encryption.

How Does Single Sign-On Work?

Microsoft Windows has a few methods available by which other companies can customize the Windows login experience. One method is the Graphical Identification and Authentication (GINA) dynamic-link library (DLL), the pluggable part of WinLogon, which third parties may replace to customize login functionality or the login user interface. GINA can be used to create, for example, biometric login methods, or smartcard logins.

PGP Whole Disk Encryption's Single Sign-On feature does not use GINA, as there are certain compatibility issues with GINA. For example, it is possible to have multiple, conflicting GINAs on the same system. Instead, Single Sign-On utilizes another method, the Windows Automatic Login feature. PGP WDE uses your configured authentication info to create, dynamically, specific registry entries when you attempt to log in. Note that your Windows password is never stored in the registry, nor in any form on the disk—neither encrypted, nor as cleartext.

Implementation details differ between the various versions of Microsoft Windows, but user interaction with the feature is the same, regardless of Windows platform.

Note that Single-Sign On is not compatible with other GINAs. You may encounter some issues if you attempt to use Single-Sign On in conjunction with another GINA.

Multiple Users and Single Sign-On

You can configure multiple users on one system for Single Sign-On—up to 28. PGP Corporation, however, recommends limiting the number of Single Sign-On users to the fewest possible persons who must share the system. While technically feasible to do so, a large number of users sharing a single, encrypted computer is not a secure solution, and PGP Corporation discourages this practice.

Note that the Single Sign-On feature is passphrase-only; you cannot utilize Single Sign-On with users' keys, nor is the feature compatible with smartcards or tokens.

Local Users

If a computer is not a part of a domain, PGP Whole Disk Encryption automatically disables certain User Access features, including "Use Welcome Screen" and "Fast User Switching" (which relies on the welcome screen), such that it then makes the CTRL+ALT+DEL available.

These features are automatically disabled when computers are part of a domain.

Enabling Single Sign-On

- Your license must include PGP Whole Disk Encryption.
- The internal user policy setting **Encrypt disks to existing Windows password (Single Sign-On)** for PGP Whole Disk Encryption must be selected.
- The user must have PGP Whole Disk Encryption installed.
- You must ensure that the Microsoft Windows Password Complexity setting (Password must meet complexity requirements) is enabled. If you are administering this feature for systems on a domain, ensure this setting is enabled on the Domain Controller. This setting is used by the Single Sign-On feature to synchronize password changes; if not set, Windows password changes will not be synchronized with PGP Single Sign-On.

To enable the Password Complexity feature on the user's Windows desktop:

1. From the **Start** menu, select **Settings > Control Panel > Administrative Tools**.
2. Double-click **Local Security Policy**.
3. Double-click **Account Policies**.
4. Double-click **Password Policy**.
5. Enable **Password must meet complexity requirements**.

Once you have enabled this feature, you can set up Single Sign-On.

To set up the Single Sign-On feature through the user's PGP Whole Disk Encryption installation:

1. Click the PGP Virtual Disk control box, then select **Encrypt Whole Disk**.
2. Select the disk or partition that you would like to encrypt, and choose the PGP Whole Disk Encryption options that you would like, if any.
3. In the User Access section, select **New Passphrase User**.
4. Select **Use Windows Password**, and then click **Next**.
5. Type your Windows login password, and then click **Finish**.

   PGP Whole Disk Encryption verifies that your name is correct across the domain, and that the Windows password is correct. PGP Whole Disk Encryption also checks your password to make sure that it contains only allowable characters. If your password does contain any such characters, you are not allowed to continue.

6 Click **Encrypt**, and then click **OK**.

Changing the User's Passphrase

For PGP Whole Disk Encryption Single Sign-On to work properly, the user must change the password for Single-Sign On using the Change Password… feature in the Windows Security dialog box, which you access by pressing CTRL+ALT+DEL.

To change the user passphrase:

1. Press CTRL+ALT+DEL.
2. Type the old password.
3. Type and confirm the new password.
4. Click OK.

Single Sign-On automatically and transparently synchronizes with this new password. The user can use the new password immediately, in the next login attempt.

If you change the password in any other manner—via Domain Controller, the Windows Control Panel, via the system administrator, or from another system, the next login attempt on the PGP BootGuard screen will fail. The user must then supply the old Windows password. Successful login on the PGP BootGuard screen using the old Windows password then brings up the Windows Login username/password screen. The user must then log in successfully using the new Windows password, at which time PGP WDE will synchronize with the new password.

If the user cannot synchronize the password, check to ensure that the Password Complexity setting is enabled for the system as described in the section "Enabling Single Sign-On" on page 242.

Supported Characters and Keysets

PGP WDE Single Sign-On supports alphanumeric, punctuation characters, spaces, and standard meta-characters. TABs and control characters are not supported.

The following characters are supported:

abcdefghijklmnopqrstuvwxyz

ABCDEFGHIJKLMNOPQRSTUVWXYZ

0123456789

` ! @ # $ % ^ & * ( ) _ + = { } : ; [ ] ' " < > , . ? / -

PGP Desktop Installer Policies

The ability to manage PGP Desktop deployments falls under the Internal User Policy section of the PGP Universal Server administrative interface (this functionality was previously in a separate application called PGP Admin).

You can create PGP Desktop installers for your internal users with one of three available policy settings:

- **No policy settings**. In this scenario, you create a PGP Desktop installer with no policy settings, which means that you, the PGP administrator, have no way to control how your users use PGP Desktop on their systems.
- **Auto-detect policy**. In this scenario, which is only available if you have an LDAP directory and have enabled the Directory Synchronization feature, PGP Desktop will coordinate with the PGP Universal Server and link to the correct user policy. Policy settings for your PGP Desktop users are determined by the email address of the user and their attributes in your LDAP directory. Based on these attributes, the appropriate user policy is applied. If you later create a new user policy and the user's attributes match the group to which the policy applies, the policy for the PGP Desktop user will be switched to the more appropriate policy. If you have not created any custom user policies, the default internal users policy will be applied.
- **Preset policy**. In this scenario, you select a user policy to apply to the installer you are creating. All of the users who get this installer are bound to the selected policy. If you change the settings of the policy later, those settings that are not implemented at installation (such as creating a PGP Virtual Disk volume) will be modified for the PGP Desktop users who are bound to this policy. If you have not created any custom user policies, the default internal users policy will be the only user policy you can apply to the installer.

You must have a PGP Desktop license to create customized PGP Desktop installers. You can use the same license for all your policies, but unless you clone your user settings from a policy that already has license information entered, you will need to enter the license information into each policy individually.

Changes you make to download policies will be automatically updated. If you make changes to the Key Setup section of a policy, those changes will only affect new users. Existing user keys will not change.

You cannot upgrade or install a PGP Desktop 9.6 bound client to PGP Universal Server 2.0.x. You must upgrade your PGP Universal Server to version 2.6 to support PGP Desktop 9.6 bound clients. PGP Universal Server versions 2.5 and later do support 9.0.x clients.

Creating PGP Desktop Installers

Creating PGP Desktop installers for your users is slightly different depending on the policy settings you want to use. All three procedures include configuring settings on the PGP Desktop card; refer to "Configuring PGP Desktop Settings" on page 248 for details.

Creating an Installer with No Policy Settings

To create a PGP Desktop installer with no associated policy:

1. On the Internal User Policy card, click **Download Client**.

   The Download PGP Clients card appears.

2. In the **Client** field, select **PGP Desktop**.

3. In the **Platform** field, select **Windows (Vista, XP, 2000)** or **MacOS X**, as appropriate.

4. Make sure the **Customize** checkbox is *unchecked*. If it is checked, uncheck it.

5. Click **Download**.

   The PGP Desktop installer is created and downloaded to your system.

6. Distribute the PGP Desktop installer to your users and have them install it on their systems.

Creating an Installer with Auto-Detect Policy

This option requires you to have an LDAP directory and to enable the Directory Synchronization feature.

To create a PGP Desktop installer with auto-detect policy:

1. Create the custom user policies you want to be linked to your PGP Desktop users.

   If you don't create any custom user policies, then your PGP Desktop users will automatically be linked to the Internal Users: Default policy. You can, however, create custom user policies in the future that may be linked to your PGP Desktop users, depending on the settings in the custom policies.

2. Configure the settings on the PGP Desktop screen appropriately for these custom user policies.

   Refer to "Configuring PGP Desktop Settings" on page 248 for specific instructions.

3. Click **Save**.

   The Policy Options card for the custom policy appears.

4. Click **Save**.

   The Internal User Policy card appears.

5. On the Internal User Policy card, click **Download Client**.

   The Download PGP Clients card appears.

6. In the **Client** field, select **PGP Desktop**.

7. In the **Platform** field, select **Windows (Vista, XP, 2000)** or **Mac OS X**, as appropriate.

8 Make sure the **Customize** checkbox is *checked*. If it is unchecked, select it.

9 Select **Auto-detect Policy**.

10 In the **PGP Universal Server** field, enter the PGP Universal Server you want the application to interact with.

The PGP Universal Server you are using to create the installer is listed by default.

11 In the **Mail Server Binding** field, enter the name of the mail server you want bound to that PGP Universal Server. You must enter this information unless your users read mail directly from this PGP Universal Server via POP or IMAP. Customized client installations will not work without mail server binding.

You can use the * wildcard character to bind automatically to any mail server. Mail policy will be enforced for any mail server to which the client connects. You can use the wildcard as follows: *, *.example.com, and example.*.com.

Refer to “Binding” on page 317 for more information.

If you are creating a binding for an internal MAPI email client, you **must** use the WINS name of the Exchange Server.

If you are creating a binding for an internal Lotus Notes email client, you **must** use the fully qualified domain name of the Domino server.

12 Click **Download**.

The PGP Desktop installer is created and downloaded to your system.

13 Distribute the PGP Desktop installer to your users and have them install it on their systems.

Once installed, PGP Desktop will coordinate with the PGP Universal Server and link to the most appropriate user policy. This linkage is based on how closely the settings for the particular user in the LDAP directory match the settings of the available user policies.

If a PGP administrator later adds a more appropriate policy, the affected PGP Desktop users will automatically become linked to the new, more appropriate policy.

Creating an Installer with Preset Policy

To create a PGP Desktop installer with preset policy:

1 Create the custom user policy you want to be linked to your PGP Desktop users.

If you don’t create a custom user policy, then the Internal Users: Default policy will be the only policy you can link your PGP Desktop users with.

2 Configure the settings on the PGP Desktop screen appropriately for the custom user policy.

Refer to “Configuring PGP Desktop Settings” on page 248 for specific instructions.

3 Click **Save**.

The Policy Options card for the custom policy appears.

4 Click **Save**.

The Internal User Policy card appears.

5 On the Internal User Policy card, click **Download Client**.

The Download PGP Clients card appears.

6 In the **Client** field, select **PGP Desktop**.

7 In the **Platform** field, select **Windows (Vista, XP, 2000)** or **Mac OS X**, as appropriate.

8 Make sure the **Customize** checkbox is *checked*. If it is unchecked, select it.

9 Select **Preset Policy**, then select the policy you want your PGP Desktop users to be linked to from the drop-down list.

If you haven't created any custom user policies, then the drop-down list will have **Default** as the only entry.

10 You can also select to embed policy and license information into the installer for offline use. Offline use means no connection between PGP Desktop and PGP Universal Server. The client will not receive any updated policy information from the PGP Universal Server, even if the policy is updated on the server side.

11 In the **PGP Universal Server** field, enter the PGP Universal Server you want the application to interact with.

The PGP Universal Server you are using to create the installer is listed by default.

12 In the **Mail Server Binding** field, enter the name of the mail server you want bound to that PGP Universal Server. You must enter this information unless your users read mail directly from this PGP Universal Server via POP or IMAP. Customized client installations will not work without mail server binding.

You can use the * wildcard character to bind automatically to any mail server. Mail policy will be enforced for any mail server to which the client connects. You can use the wildcard as follows: *, *.example.com, and example.*.com.

Refer to "Binding" on page 317 for more information.

If you are creating a binding for an internal MAPI email client, you **must** use the WINS name of the Exchange Server.

If you are creating a binding for an internal Lotus Notes email client, you **must** use the fully qualified domain name of the Domino server.

13 Click **Download**.

The PGP Desktop installer is created and downloaded to your system.

14 Distribute the PGP Desktop installer to your users and have them install it on their systems.

Once installed, PGP Desktop will coordinate with the PGP Universal Server to retrieve the settings from the linked user policy. This linkage cannot be changed once PGP Desktop is installed.

If the linked policy is deleted, the linkage will revert to the Internal Users: Default user policy.

Configuring PGP Desktop Settings

PGP Desktop settings can be established for the default internal user policy as well as any custom internal user policy you create. Each of these can have different sets of PGP Desktop settings.

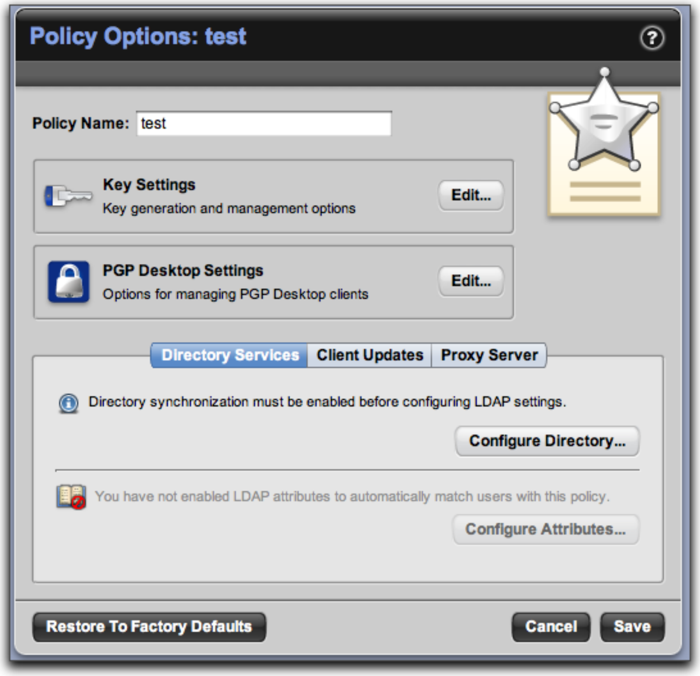
While all possible PGP Desktop, PGP Whole Disk Encryption, and PGP NetShare settings are visible, your license determines which settings are applied to client installations. Refer to "PGP Desktop Licensing" on page 240 to learn which of the settings below apply to your license.

To establish PGP Desktop settings:

1 On the Internal User Policy card, click the name of the Internal Users: Default policy or a custom internal user policy.

The possible PGP Desktop settings are the same for both types of policy.

The Policy Options card appears.



Policy Options: test

Policy Name: test

Key Settings
Key generation and management options

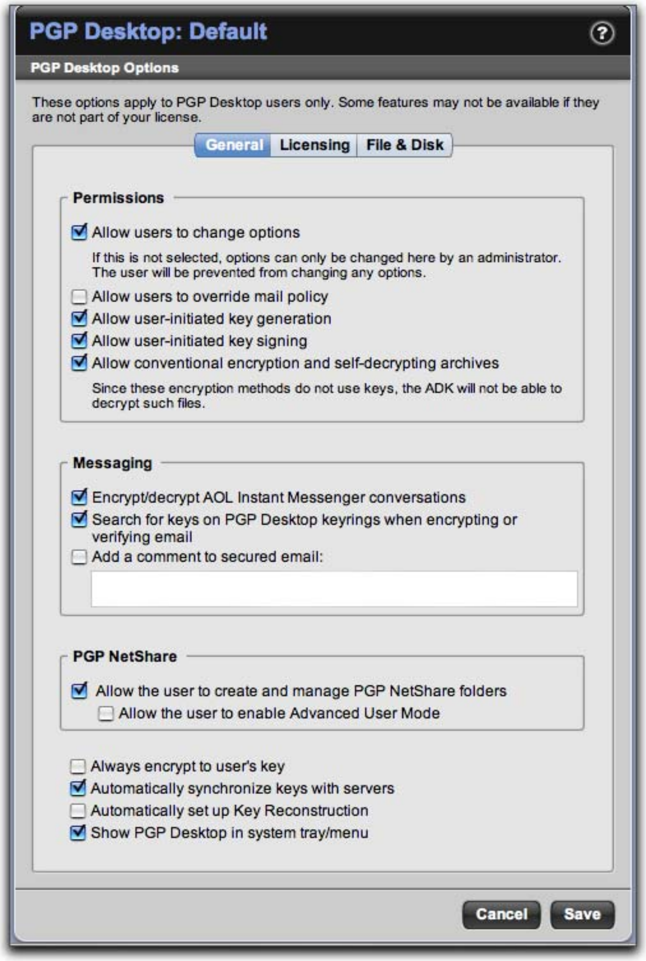
PGP Desktop Settings
Options for managing PGP Desktop clients

Directory synchronization must be enabled before configuring LDAP settings.

You have not enabled LDAP attributes to automatically match users with this policy.

2 Click the **Edit** button for **PGP Desktop Settings**.

The appropriate PGP Desktop card appears, titled with the policy name.



PGP Desktop: Default

PGP Desktop Options

These options apply to PGP Desktop users only. Some features may not be available if they are not part of your license.

Permissions

☑ Allow users to change options

If this is not selected, options can only be changed here by an administrator. The user will be prevented from changing any options.

□ Allow users to override mail policy
☑ Allow user-initiated key generation
☑ Allow user-initiated key signing
☑ Allow conventional encryption and self-decrypting archives

Since these encryption methods do not use keys, the ADK will not be able to decrypt such files.

Messaging

☑ Encrypt/decrypt AOL Instant Messenger conversations
☑ Search for keys on PGP Desktop keyrings when encrypting or verifying email
□ Add a comment to secured email:

PGP NetShare

☑ Allow the user to create and manage PGP NetShare folders
□ Allow the user to enable Advanced User Mode

□ Always encrypt to user's key
☑ Automatically synchronize keys with servers
□ Automatically set up Key Reconstruction
☑ Show PGP Desktop in system tray/menu

3 Check **Allow users to change options** if you want your PGP Desktop users to be able to change the options that you, the PGP administrator, establish.

Uncheck this option to prevent them from making changes. Users will not be able to skip or cancel any part of the customized PGP Desktop installation.

4 Check **Allow users to override mail policy** if you want your PGP Desktop users to be able to take actions that override the mail policy of this PGP Universal Server.

Allowing users to override mail policy means that they can create and apply their own policies to email. However, users will not be able to override mail policy in ways that make messages less secure, as long as PGP Universal Server is in the mail flow. For example, if a user decides not to encrypt messages to external domain sample.com, and the PGP Universal Server mail policy is to encrypt messages to sample.com, then messages will be encrypted in spite of the user's choice. However, if PGP Universal Server is not in the mail flow, this setting does allow users to create policy that could make messages less secure.

Uncheck this option to prevent users from overriding mail policy.

5 Check **Allow user-initiated key generation** if you want your PGP Desktop users to be able to create new keys and subkeys in addition to the key created during installation.

Uncheck this option to prevent them from creating new keys. Be aware that if users are not able to generate keys, they will not be able to make certain changes to their keypairs, such as add and remove Additional Decryption Keys (ADKs), appoint and remove third-party key revokers, or create and use subkeys.

6 Check **Allow user-initiated key signing** if you want your PGP Desktop users to be able to sign keys.

Uncheck this option to prevent them from signing keys. You may need to do this to enforce centralized control over the validity of keys in your organization.

7 Check **Allow conventional encryption and self-decrypting archives** if you want your PGP Desktop users to be able to conventionally encrypt files (using a passphrase instead of a key) or create self-decrypting archives (SDAs).

Conventionally encrypted and self-decrypting files cannot be decrypted by the ADK, which may conflict with your data recovery policy.

Uncheck this option to prevent users from conventionally encrypting files or creating SDAs.

8 Check **Encrypt/Decrypt AOL Instant Messenger conversations** if you want instant messages (IM) between users of AOL Instant Messenger to be protected. IMs will only be protected if both users are running PGP Desktop with this option enabled.

Uncheck this option if you do not want these IM sessions to be protected.

9 Check **Search for keys on PGP Desktop keyrings when encrypting or verifying email** to allow users to import keys into the PGP Desktop keyring so that the client can encrypt or verify messages without needing to refer to the PGP Universal Server for key information. This allows PGP Desktop to operate as if it were not bound to the PGP Universal Server, even if it is bound.

10 Check **Add a comment to secured email** if you want the text you enter in the box to be appended to clear-signed PGP blocks, including exported key files, and encrypted files and text.

Uncheck this option and leave the box empty if you do not want the comment to be appended to these messages.

11 Check **Allow the user to create and manage PGP NetShare folders** if you want users to be able to create and manage PGP NetShare protected folders. When this option is disabled, users can participate in a PGP NetShare Work Group that someone else has created, but cannot create files themselves. PGP NetShare is only available for Windows users. Refer to the *PGP Desktop 9.6 for Windows User’s Guide* for more information on PGP NetShare.

12 Check **Allow user to enable Advanced User mode** if you want PGP NetShare users to protect individual files that are moved out of a Protected Folder.

13 Check **Always encrypt to user's key** if you want every message your PGP Desktop users send to be encrypted to their key. This is in addition to any other user- or system-specified key, for example, the ADK.

Uncheck this option if you do not want messages to be automatically encrypted to the user's key. Users can still manually encrypt their messages to their key.

14 Check **Automatically synchronize keys with servers** if you want PGP Desktop to automatically keep your users' keys synchronized with configured servers.

If you enable this option, user key data synchronizes every 24 hours with the data on the PGP Universal Server. Public keys are retrieved from the PGP Universal Server and merged into the keyring, which keeps userids, signatures, and revocation status current. If a key isn't found on the server, it will automatically be disabled in the keyring, preventing encryption to that key. If a disabled key is found, it will be re-enabled in the keyring.

This option also allows key data to automatically synchronize with the PGP Universal Server every time the user makes changes to their private key, such as adding or removing ADKs, subkeys, userIDs, or changing preferred ciphers or compression algorithms.

Uncheck this option to prevent automatic synchronization of keys.

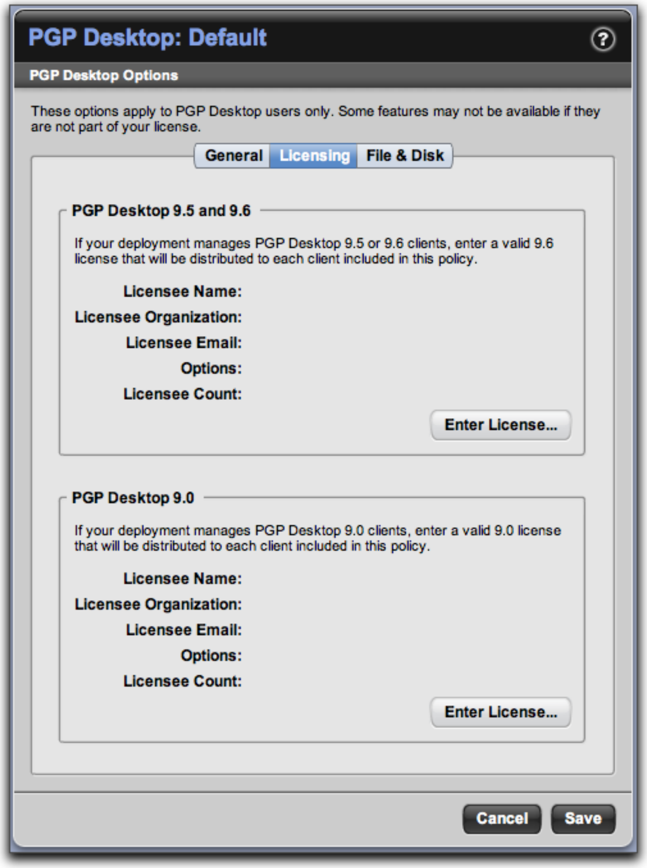
15 Check **Automatically set up Key Reconstruction** if you want key reconstruction to be available when new keys are created. The key reconstruction data is stored on the PGP Universal Server.

Refer to the *PGP Desktop User's Guide* and the *Inside PGP Key Reconstruction* white paper on the PGP Corporation website for information on key reconstruction, and to Chapter 14, "Recovering Encrypted Data in an Enterprise Environment".

16 Check **Show PGP Desktop in system tray/menu** if you want a PGP Desktop padlock icon to display in the system tray of Windows users or the system menu of Mac OS X users when PGP Desktop is active on their systems. The icon provides access to some PGP Desktop features without requiring users to launch the whole application.

Uncheck this option to hide the icon.

17 Click **Licensing** to add or change PGP Desktop 9.0 or 9.6 licenses.



These options apply to PGP Desktop users only. Some features may not be available if they are not part of your license.

PGP Desktop 9.5 and 9.6

If your deployment manages PGP Desktop 9.5 or 9.6 clients, enter a valid 9.6 license that will be distributed to each client included in this policy.

Licensee Name:
Licensee Organization:
Licensee Email:
Options:
Licensee Count:

PGP Desktop 9.0

If your deployment manages PGP Desktop 9.0 clients, enter a valid 9.0 license that will be distributed to each client included in this policy.

Licensee Name:
Licensee Organization:
Licensee Email:
Options:
Licensee Count:

18 Click **Enter License** to enter a PGP Desktop 9.5 or 9.6 license that will be integrated into the installer, or a 9.0 license that will support legacy PGP Desktop 9.0 installations.

The Enter License Information dialog appears.

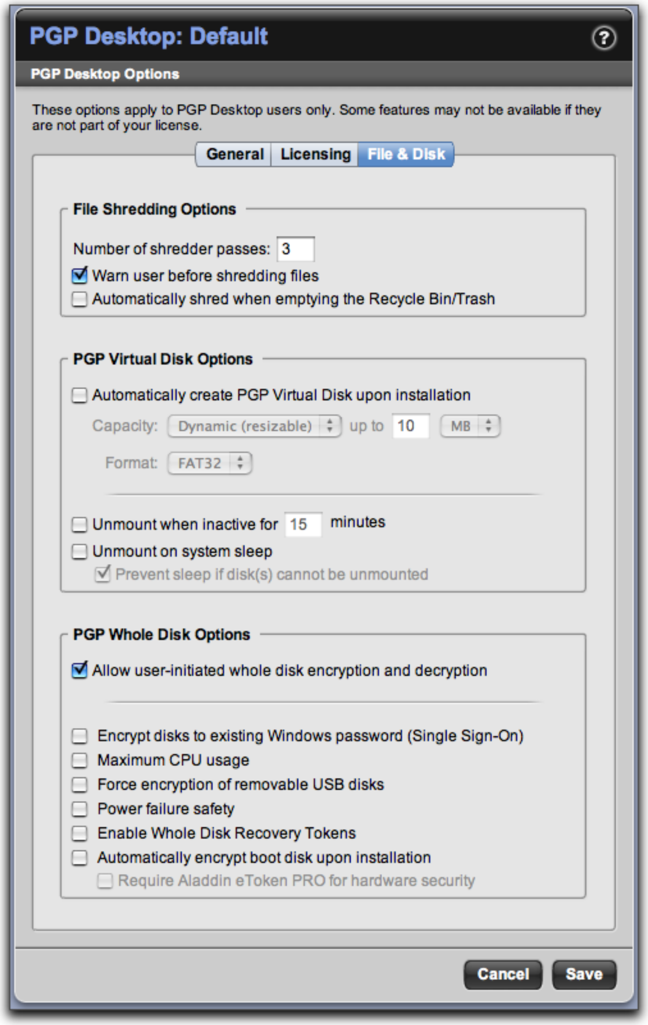
19 Type in the **Licensee Name**, **Licensee Organization**, **Licensee Email**, and the **License Number**, then click **Save**.

20 If your PGP Universal Server does *not* have an active connection to the Internet, for example because it is behind a proxy server, your license authorization will be needed; click **Manual**.

21 Type in the appropriate license information, paste your license authorization information in the **License Authorization** box, and click **Save**.

When the PGP Desktop license number information is added, it will display.

22 Click **File & Disk** to manage file shredding options, as well as PGP Virtual Disk and PGP Whole Disk Encryption options.



These options apply to PGP Desktop users only. Some features may not be available if they are not part of your license.

File Shredding Options

Number of shredder passes: 3

☑ Warn user before shredding files

□ Automatically shred when emptying the Recycle Bin/Trash

PGP Virtual Disk Options

□ Automatically create PGP Virtual Disk upon installation

Capacity: Dynamic (resizable) up to 10 MB

Format: FAT32

□ Unmount when inactive for 15 minutes

□ Unmount on system sleep

☑ Prevent sleep if disk(s) cannot be unmounted

PGP Whole Disk Options

☑ Allow user-initiated whole disk encryption and decryption

□ Encrypt disks to existing Windows password (Single Sign-On)

□ Maximum CPU usage

□ Force encryption of removable USB disks

□ Power failure safety

□ Enable Whole Disk Recovery Tokens

□ Automatically encrypt boot disk upon installation

□ Require Aladdin eToken PRO for hardware security

23 Enter the **Number of shredder passes**. The default is 3. The larger the number, the more secure the shred, but it may take a little longer.

24 Check **Warn user before shredding files** if you want your PGP Desktop users to be warned before files on their system are shredded (securely deleted).

Uncheck this option to suppress this warning.

25 Check **Automatically shred when emptying the Recycle Bin/Trash** if you want files that are deleted from your PGP Desktop users’ system to be shredded instead of just deleted.

Uncheck this option to prevent the files from being shredded.

26 Check **Automatically create PGP Virtual Disk upon installation** if you want a PGP Virtual Disk volume created automatically on your PGP Desktop users’ systems

If you enable this option, specify:

- **Capacity**. Choose a fixed or dynamic (resizable) capacity. A dynamic PGP Virtual Disk automatically resizes to only take up as much space as it needs, up to the limit you set. Resizable PGP Virtual Disks are not compatible with PGP Virtual Disk files created by previous fixed version of PGP Virtual Disk. Define the capacity for the PGP Virtual Disk volume in GB, MB, or TB.

  Minimum and maximum disk sizes for each type of file system are:

  FAT16: no minimum, 2GB maximum

  FAT32: 512MB minimum, 32GB maximum

  NTFS: 10MB minimum, unlimited maximum, although the underlying file system may limit the maximum PGP Virtual Disk size

- **Format**. From the drop-down menu, select which file system to use for the PGP Virtual Disk volume: FAT16, FAT32, or NTFS. These are Windows OS options. If this custom version of PGP Desktop is installed on Mac OS X, then the file system will always be HFS Extended, no matter what choice is selected here.

27 Check **Unmount when inactive for X minutes** if you want your PGP Desktop users’ PGP Virtual Disk volumes to be automatically unmounted after the specified number of minutes of inactivity.

This option could prevent the protected data on a PGP Virtual Disk volume from being available to unauthorized persons if you leave work without unmounting the volume, for example.

Uncheck this option to prevent PGP Virtual Disk volumes from being automatically unmounted because of inactivity.

28 Check **Unmount on system sleep** if you want your PGP Desktop users’ PGP Virtual Disk volumes to automatically unmount if the system goes to sleep. Some systems don’t support sleep mode, so this option would not apply.

Uncheck this option to prevent unmount on sleep.

29 Check **Prevent sleep if disk(s) cannot be unmounted** if you want your PGP Desktop users’ machines not to sleep if, for some reason, a volume cannot be unmounted. Using this option could prevent loss of data.

Uncheck this option to permit sleep even if a volume cannot be unmounted.

30 Check **Allow user-initiated whole disk encryption and decryption** if you want your PGP Desktop users to be able to encrypt the whole disk drive on their system. You PGP Desktop license must support PGP Whole Disk Encryption if you want to use this feature.

Uncheck this option to prevent your users from whole-disk encrypting.

31 Check **Encrypt disks to existing Windows password (Single Sign-On)** to force users to log into PGP Whole Disk at the same time they log into their computer. Refer to “PGP Whole Disk Encryption Administration” on page 241 for more information.

32 Check **Maximum CPU Usage** to make encrypting PGP Whole Disk faster by using more CPU.

33 Check **Force encryption of removable USB disks** to encrypt any portable drive attached to the client computer. If the user attaches a portable drive to the client system, the user is prompted to either accept encryption of the drive or unmount the drive. This prevents protected data from being copied onto an unprotected drive. This feature is only available for Microsoft Windows clients.

All removable disks are subject to forced encryption, including both USB and FireWire drives. This feature will also apply to music devices and digital cameras attached to the client computer. These devices will not function while encrypted. Devices that were encrypted by mistake can be decrypted to restore functionality.

There are 3 ways to encrypt the portable drive. By default, PGP Desktop encrypts the drive to the existing credentials if the primary computer disk in encrypted. If the primary computer is not encrypted, PGP Desktop will try to encrypt the portable drive to another private key, if one is available. If there is no other private key, the user will be prompted to create a passphrase user account to use to encrypt the disk.

If a Whole Disk Recovery Token is required for encryption, then if the user attaches a previously unencrypted removable drive to the client computer while the PGP Universal Server cannot be reached, the removable disk cannot be encrypted and will be automatically unmounted. The removable disk cannot be used and the user will see the following error message: "The administrative server is not available for storing the administrative recovery token. Disk encryption cannot continue."

34 Check **Power failure safety** to allow the user's computer to track the progress of PGP Whole Disk encryption so that in case power fails during encryption, the computer can recover the data and restart encryption.

35 Check **Enable Whole Disk Recovery Tokens** if you want to be able to remotely recover a disk that has been whole-disk encrypted.

Uncheck to disable this option. If this option is disabled, and one of your PGP Desktop users whole-disk encrypts a drive, then only that user will be able to access the data on that drive. If the user forgets their passphrase, the data will be lost.

If a Whole Disk Recovery Token is used, a new one is generated and immediately synchronized with the PGP Universal Server.

36 Check **Automatically encrypt boot disk upon installation** if you want your PGP Desktop users to automatically have their boot volume whole disk encrypted when they install PGP Desktop on their system.

Users can pause the encryption of their boot volumes during the encryption process, even indefinitely, but potions of the disk will already have been encrypted. It is also possible for users to decrypt their disks.

Uncheck this option to prevent the boot volume from being automatically encrypted.

37 Check **Require Aladdin eToken Pro for hardware security** if you want to require that your PGP Desktop users who whole disk encrypt their systems to have an Aladdin eToken Pro installed to use the data that has been whole disk encrypted. Users will not be able to complete the installation of PGP Desktop without setting up token use.

This requirement means that someone who simply has access to the whole disk encrypted drive couldn't access the data on it without the eToken. It also means that if the eToken is lost, the encrypted drive is inaccessible.

Keys created on smartcards and tokens are not compatible with PGP Desktop's key reconstruction feature.

Uncheck this option to prevent this requirement.

> ! Before a user can install PGP Desktop with this option enabled, they must already have the Aladdin eToken drivers installed on their computer. You can find the drivers on the Aladdin website at www.aladdin.com.

38 Click **Save**.

The Policy Options card reappears.

29 Setting External User Policy

This chapter describes the external user policy, which to create and manage policy settings for external users.

This feature is available with PGP Universal Gateway Email and PGP Desktop Email, if the PGP Universal Server is within the mailstream.

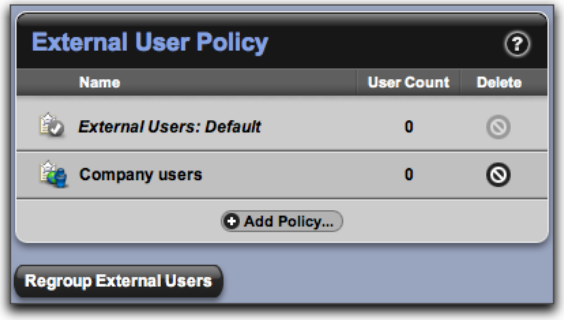
PGP Universal Web Messenger functionality is only available for use with a PGP Universal Gateway Email license.

Topics in this chapter include:

- "Overview"
- "Managing External User Policies" on page 259

Overview

The External User Policy card lets you control the key generation and key management settings for external users, who are not within a managed domain.



Name	User Count	Delete
External Users: Default	0	⊘
Company users	0	⊘

The External User Policy card allows you to add external user policies and specify which users receive those policy settings. You can create an external user policy for users from a specific domain. You can also create lists of users within dictionaries, and then create external user policies associated with those dictionaries. If no other external user policy applies, then PGP Universal Server will apply the default external user policy settings.

The **External Users: Default** policy is the pre-installed default external user policy. You cannot delete this user policy, but you can change settings at any time.

You can specify which external users should receive which policy based on domain and/or dictionary membership. For example, you can choose to apply an external user policy to any user from domain company.com. Or, you can create a dictionary containing a list of specific external user names, then create an external user policy that applies only to users with names in that dictionary. See Chapter 17, "Using Dictionaries with Policy" for information on how to create dictionaries.

Based on external user policy settings, the recipient will be offered ways to join the SMSA; for example, PGP Universal Satellite or PGP Universal Web Messenger. See Chapter 16, "Applying Key Not Found Settings to External Users" for information on how external users interact with Smart Trailer and PGP Universal Web Messenger.

Managing External User Policies

Regrouping External Users

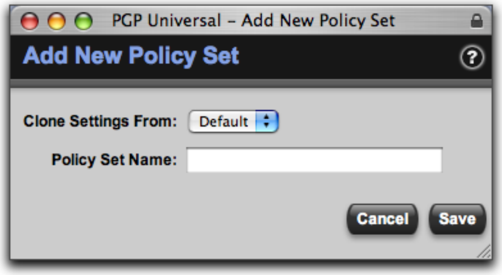
Click the **Regroup External Users** button to examine external user accounts to make sure the correct policy is applied to each user, and correct any misapplied policies. If you have a large number of external users, this process will not be immediate and may take some time to complete.

Adding a New External User Policy

To create a new external user policy:

1 On the External User Policy card, click **Add Policy**.

The Add New Policy Set dialog appears.



PGP Universal – Add New Policy Set

Add New Policy Set

Clone Settings From: Default

Policy Set Name:

2 In the **Clone Settings From** drop-down list, select the existing policy with the settings you would like to use as a starting point for a new policy.

If this is the first new external user policy to be created, the drop-down list will only have one entry, Default, the external users default policy.

3 In the **Policy Set Name** field, enter a name for the policy you are creating. Try to choose a name that shows this is an external user policy; for example, External:Executives.

4 Click **Save**.

5 Edit the new policy settings as appropriate.

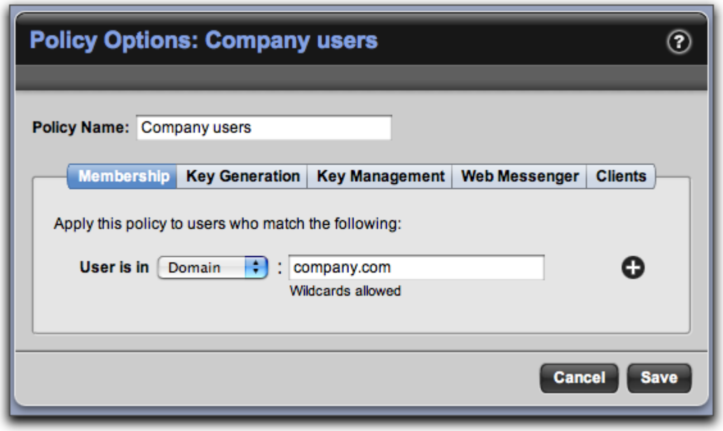
Editing External User Policies

External user policies let you establish the key generation and key management settings applied to external users.

To edit an external user policy:

1 On the External User Policy card, select the external user policy you want to change.

The Policy Options card appears.



Policy Options: Company users

Policy Name: Company users

Apply this policy to users who match the following:

User is in Domain : company.com

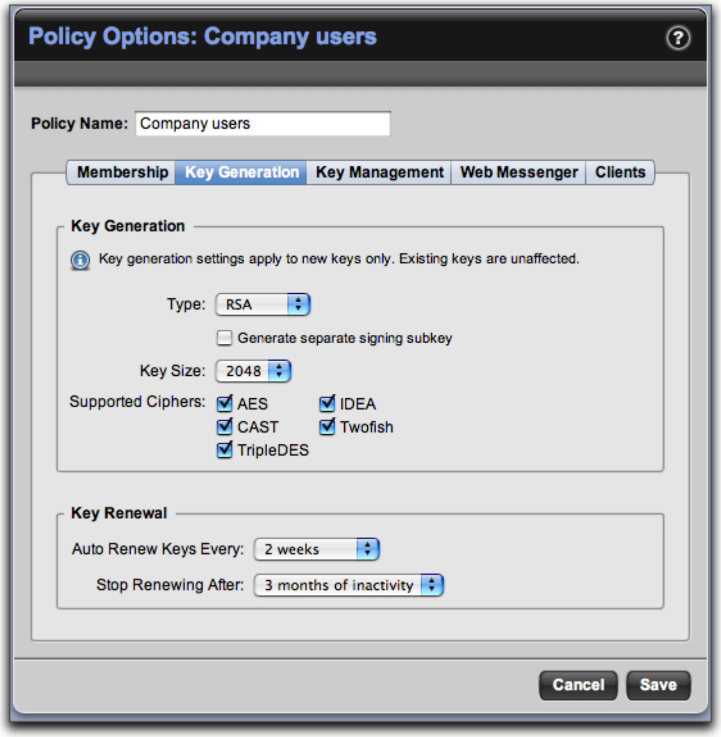
Wildcards allowed

2 Specify to which external users the policy applies. Choose from one of the following:

- Select **Domain** from the dropdown list, and type in an external domain. The policy will be applied to users from that domain.
- Select **Dictionary** from the dropdown list, and select a dictionary. The policy will be applied to users listed in that dictionary.

3 Click the Add icon to apply the user policy to more than one domain or dictionary.

4 Click **Key Generation** to choose key types.



Policy Options: Company users

Policy Name: Company users

Key Generation

Key generation settings apply to new keys only. Existing keys are unaffected.

Type: RSA

□ Generate separate signing subkey

Key Size: 2048

Supported Ciphers: ☑ AES ☑ IDEA ☑ CAST ☑ Twofish ☑ TripleDES

Key Renewal

Auto Renew Keys Every: 2 weeks

Stop Renewing After: 3 months of inactivity

5 From the **Key Generation** card, in the **Type** drop-down list, select **RSA** or **DH/DSS**. The default is RSA.

DH/DSS key types are incompatible with S/MIME. Users with DH/DSS keys will not have a certificate with which they can sign their messages to S/MIME users, even when there is an Organization Certificate present.

6 Specify whether you want to generate a separate signing subkey for the user. Refer to "Key Mode" on page 313 for more information on signing subkeys.

7 In the **Key Size** drop-down list, select the size of the keys to be created. Available options are: 1024, 1536, 2048, 3072, and 4096.

8 In the **Supported Ciphers** section, remove the check mark from any cipher type you do not want created keys to support or that do not meet your security requirements. TripleDES is the default cipher, used if none of the other ciphers are chosen or available, and cannot be unchecked.

9 In the **Auto-Renew Keys Every** drop-down list, select an auto-renewal time frame.

You can only set key renewal policy for server-managed keys. If you select **Client Key Mode (CKM)** in step 12 below, and the user chooses to generate and self-manage keys, key renewal policy will not apply.

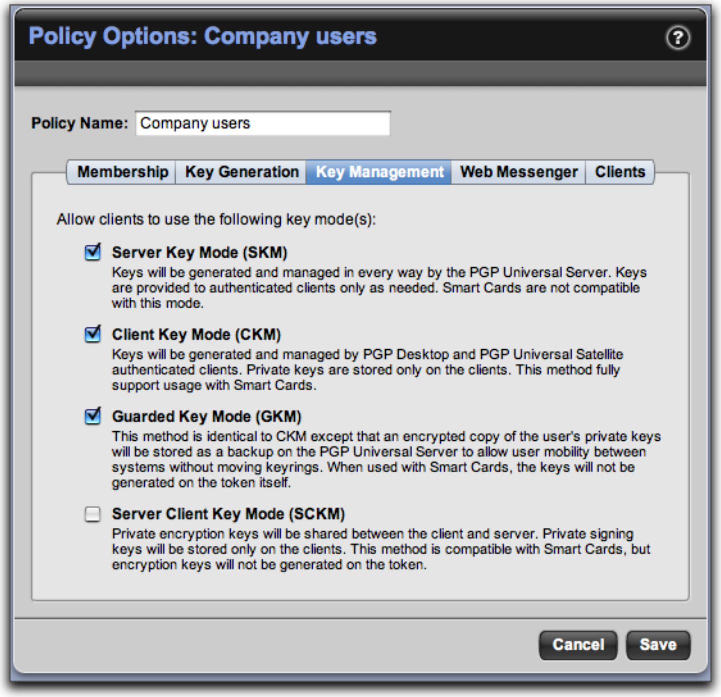
External keys will automatically be renewed in the time frame you specify unless they have exceeded the inactivity threshold in **Stop Renewing After**. Select **Never renew** if you want your external keys never to renew; this means the keys will never expire, regardless of inactivity.

10 In the **Stop Renewing After** drop-down list, specify a period of inactivity after which a key will *not* be automatically renewed.

Select **Never stop renewing** if you want keys of external users to be continually renewed. The question you should ask yourself here is how long a period of inactivity for a given user should be before you reasonably conclude that the user account is no longer in use.

It is generally a good idea to set the auto-renewal time to be fairly short. This helps ensure that the SMSA manages itself without you needing to delete a user manually.

11 Click **Key Management** to select the user key mode.



Policy Name: Company users

Allow clients to use the following key mode(s):

☑ **Server Key Mode (SKM)**
Keys will be generated and managed in every way by the PGP Universal Server. Keys are provided to authenticated clients only as needed. Smart Cards are not compatible with this mode.

☑ **Client Key Mode (CKM)**
Keys will be generated and managed by PGP Desktop and PGP Universal Satellite authenticated clients. Private keys are stored only on the clients. This method fully support usage with Smart Cards.

☑ **Guarded Key Mode (GKM)**
This method is identical to CKM except that an encrypted copy of the user's private keys will be stored as a backup on the PGP Universal Server to allow user mobility between systems without moving keyrings. When used with Smart Cards, the keys will not be generated on the token itself.

☐ **Server Client Key Mode (SCKM)**
Private encryption keys will be shared between the client and server. Private signing keys will be stored only on the clients. This method is compatible with Smart Cards, but encryption keys will not be generated on the token.

12 In the **Key Management** section, select from among:

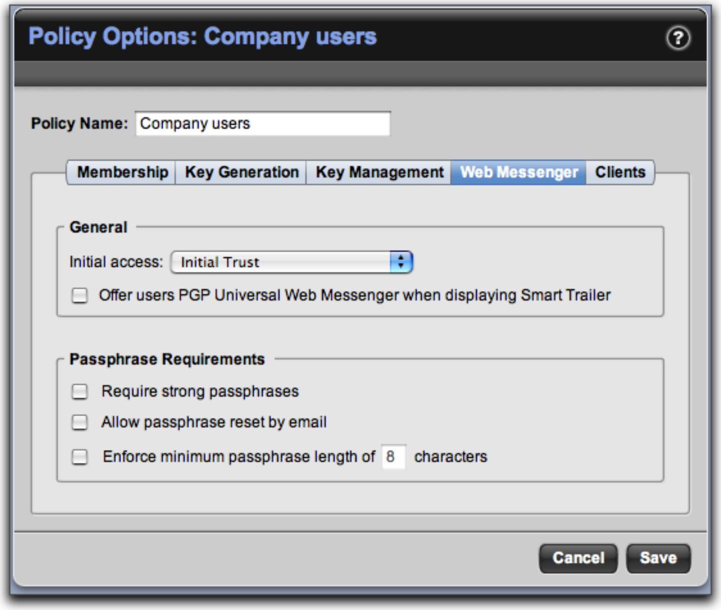
- **Server Key Mode (SKM)**. Select this option if you want the PGP Universal Server to generate and manage user keys.
- **Client Key Mode (CKM)**. Select this option if you want external users to be able to generate and manage their own keys.
- **Guarded Key Mode (GKM).** Select this option if you want external users to be able to generate and manage their own keys, and you also want encrypted copies of users' private keys stored on the PGP Universal Server.

- **Server Client Key Mode (SCKM)**. Select this option if you want private encryption keys shared between clients and the PGP Universal Server, and private signing keys stored only on clients.

  To disable key generation for this external user group, do not select any key mode.

  Refer to “Choosing a Key Mode For Key Management” on page 217 for information on how to choose the appropriate key mode. Refer to “Key Mode” on page 313 for general information on key modes.

13 Click **Web Messenger** to choose Smart Trailer and PGP Universal Web Messenger options.



Policy Options: Company users

Policy Name: Company users

General

Initial access: Initial Trust

□ Offer users PGP Universal Web Messenger when displaying Smart Trailer

Passphrase Requirements

□ Require strong passphrases

□ Allow passphrase reset by email

□ Enforce minimum passphrase length of 8 characters

14 Smart Trailer and PGP Universal Web Messenger users access their accounts for the first time in one of two ways. Select one of these settings from the **Initial Access** drop-down list:

- **Initial Trust**. Users are trusted on first access without providing any other form of authentication.

- **Require Sender Authorization**. Recipients on first access must enter a passphrase to gain access; the passphrase is sent to the sender, and then the sender transmits it to the recipient, usually through a telephone conversation.

15 If you want Smart Trailer to offer the use of PGP Universal Web Messenger to the users covered by this policy, select **Offer users PGP Universal Web Messenger when displaying Smart Trailer**. Not available to managed domains or non-mailstream installations.

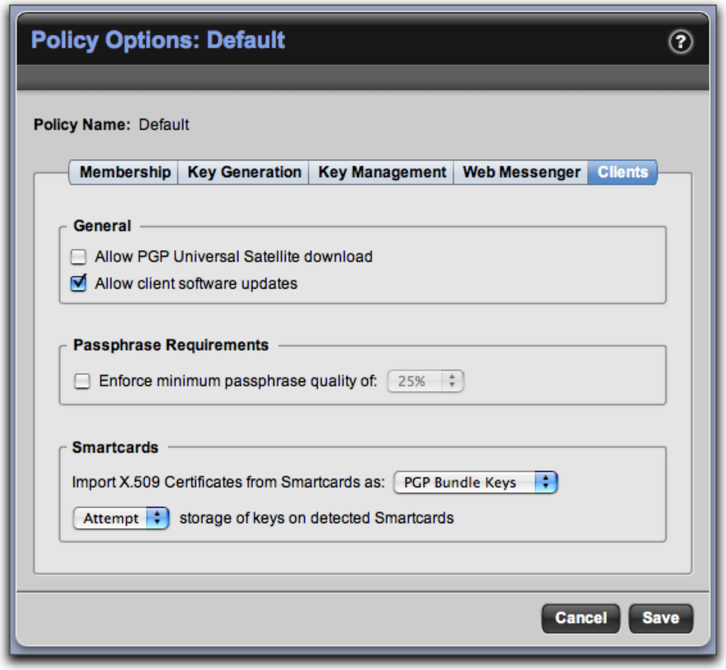
16 Select **Require strong passphrases** for better security.

A strong passphrase requires 8 characters, and consists of at least one of each of the following: a lowercase letter, an uppercase letter, a number, and a punctuation mark. If your users are in an environment where meeting these requirements is not possible, for example if they use the Kanji character set, then you should not require strong passphrases.

17 Select **Allow passphrase reset by email** if you want the users covered by this domain policy to be able to reset their Smart Trailer, PGP Universal Satellite, or PGP Universal Web Messenger passphrases by email.

18 Select **Enforce minimum passphrase length of X characters** if you want to require a minimum number of characters in passphrases. The default is 8 characters.

19 Click **Clients** to manage external user client installations.


Policy Options: Default

Policy Name: Default

General

☐ Allow PGP Universal Satellite download

☑ Allow client software updates

Passphrase Requirements

☐ Enforce minimum passphrase quality of: 25%

Smartcards

Import X.509 Certificates from Smartcards as: PGP Bundle Keys

Attempt storage of keys on detected Smartcards

20 Choose **Allow PGP Universal Satellite download** if you want to offer external users the opportunity to download PGP Universal Satellite.

21 Remove the checkmark from **Allow client software updates** if you do not want the client software to retrieve updates automatically. If you leave this option unchecked and then want to update the software users have, you will need to distribute software update material manually.

22 Select **Enforce minimum passphrase quality of X%** if you want to require a minimum passphrase quality level for new keys.

23 Select into which format you want to import X.509 certificates from smartcards:

- **PGP Bundle Keys**. Bundles user X.509 signing and encryption certificates into a single identity. This is the recommended option.

   - **PGP Wrapper Keys**. This allows user X.509 signing and encryption certificates to be imported as separate identities. This option is not recommended because it only functions in an exclusively S/MIME environment.
   - **User selectable**. Allows users to choose how to import their smartcard X.509 certificates.

24. Select **Require or Attempt storage of keys on detected Smartcards** if you want to store user keys on any detected smartcard.
25. Click **Save**.

Deleting External User Policies

The External User: Default policy cannot be deleted.

To delete a user-created external user policy, click the **Delete** icon for the policy you want to remove.

30 Configuring PGP Universal Web Messenger

This chapter describes how to configure the PGP Universal Web Messenger service.

PGP Universal Web Messenger functionality is available for use with PGP Universal Gateway and PGP Desktop Email, if PGP Universal Server is in the mailstream.

Refer to Chapter 16, "Applying Key Not Found Settings to External Users" for information about using PGP Universal Web Messenger.

Topics in this chapter include:

Overview

The Web Messenger Configuration card lets you enable and configure the PGP Universal Web Messenger service.

The PGP Universal Web Messenger service allows an external user to securely read a message from an internal user *before* the external user has a relationship with the SMSA.

If PGP Universal Web Messenger is available via mail policy for a user and the recipient's key cannot be found, the message is stored on the PGP Universal Server and an unprotected message is sent to the recipient. The unprotected message includes a link that sets up an SSL-protected connection to the original message, waiting on the PGP Universal Server.

When they go to read their messages, recipients are given several options for how future messages from the same PGP Universal Server will be handled:

- Continue to use PGP Universal Web Messenger
- Install PGP Universal Satellite, if the policy permits
- Encrypt messages using an existing PGP Desktop key or an S/MIME certificate that the external user provides

If the PGP Universal Web Messenger service is not enabled, messages processed by policy rules that use PGP Universal Web Messenger as the key not found setting will bounce. You must also enable the PGP Universal Web Messenger service if your policy rules use Smart Trailer, even if you are not also using the PGP Universal Web Messenger service for external users.

If users continue to use PGP Universal Web Messenger to read and send messages, the PGP Universal Server will store both mail received and, if the user chooses, mail sent by the users. The user's Quota is the amount of disk space allotted for PGP Universal Web Messenger mail storage. You can set the size of the Quota. There is also a 50MB limit to the total encoded message size of email sent to PGP Universal Web Messenger users, and a limit of approximately 15MB per uploaded attachment (after encoding) in email replies created in PGP Universal Web Messenger. Users will not be able to send or receive any message that would put them over their message storage Quota or exceed 50MB.

If you protect your PGP Universal Server with an ignition key, PGP Universal Web Messenger messages are stored encrypted. Refer to Chapter 46, "Protecting PGP Universal Server with Ignition Keys" for more information.

PGP Universal Web Messenger supports browser languages English, German, Japanese, French, and Spanish.

High Availability Mode

If you have multiple PGP Universal Servers clustered together, you can choose to store PGP Universal Web Messenger user account information in either of 2 modes.

- Home Server Mode assigns a home PGP Server for each new PGP Universal Web Messenger user account. All account information for an external user exists on a single cluster member.
- High Availability Mode replicates new PGP Universal Web Messenger user accounts on all clustered PGP Universal Servers. All external user account information exists on all members of the cluster. If a cluster member is not functioning, PGP Universal Web Messenger users will still be able to use the service.

Switching account creation modes does not modify existing accounts. Any user account created in High Availability Mode will continue on in that mode, even if High Availability Mode is later turned off. Only users created after you turn the mode off will be affected. If your PGP Universal Server is in Home Server Mode, and you later turn on High Availability Mode, only new user accounts will be replicated across the cluster, and all existing user accounts will remain saved to a single server.

If you have migrated to PGP Universal Server 2.5 or later and choose to enable High Availability Mode, only PGP Universal Web Messengers users created after your migration will be affected. Existing PGP Web Messenger users will not be converted. If you need to convert existing user accounts, contact PGP Support (www.pgp.com/support) for help.

PGP Universal Web Messenger messages are replicated to all members of the cluster, even those not running the service.

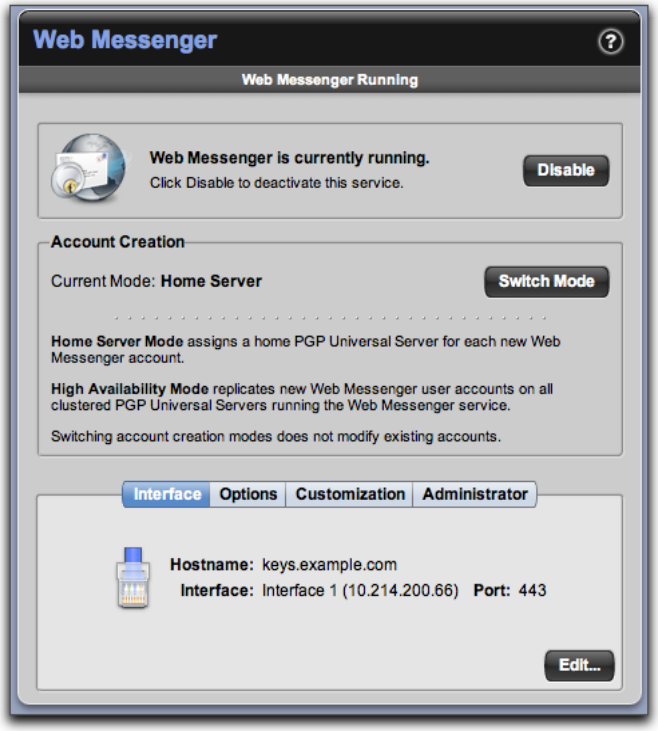
Click the **Switch Mode** button to turn High Availability Mode on or off.

Refer to Chapter 45, "Clustering your PGP Universal Servers" for more information about clusters.

Configuring the PGP Universal Web Messenger Service

To enable the PGP Universal Web Messenger service:

1. On the Services>Web Messenger card, click the **Enable** button to enable the service.



Web Messenger is currently running.
Click Disable to deactivate this service.

Account Creation

Current Mode: **Home Server**

Home Server Mode assigns a home PGP Universal Server for each new Web Messenger account.

High Availability Mode replicates new Web Messenger user accounts on all clustered PGP Universal Servers running the Web Messenger service.

Switching account creation modes does not modify existing accounts.

Hostname: keys.example.com
Interface: Interface 1 (10.214.200.66) **Port:** 443

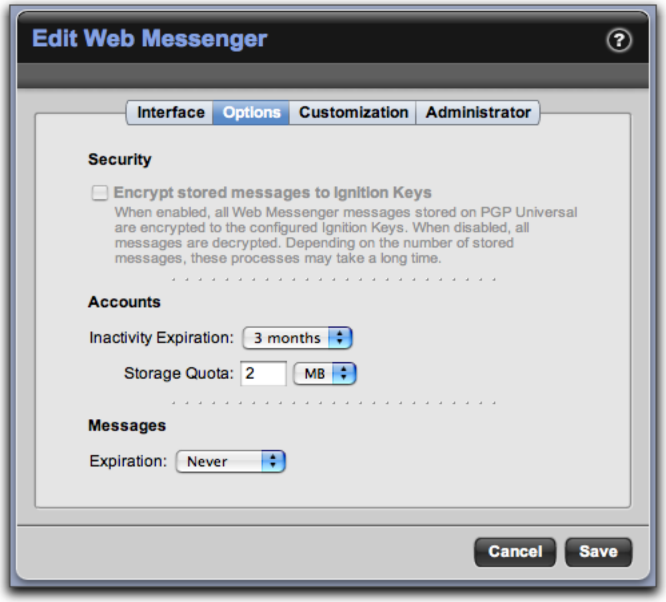
2 To disable the PGP Universal Web Messenger service, click the **Disable** button on the Web Messenger card.

To configure the PGP Universal Web Messenger service:

1 To turn High Availability Mode on or off, click the **Switch Mode** button on the Web Messenger card, then click **OK** on the confirmation dialog.

2 On the Services>Web Messenger card, click the **Edit** button.

The Edit Web Messenger screen appears.



Security

□ Encrypt stored messages to Ignition Keys

When enabled, all Web Messenger messages stored on PGP Universal are encrypted to the configured Ignition Keys. When disabled, all messages are decrypted. Depending on the number of stored messages, these processes may take a long time.

Accounts

Inactivity Expiration: 3 months

Storage Quota: 2 MB

Messages

Expiration: Never

3 Select the **Interface** tab to specify where external users log into the PGP Universal Web Messenger service.

4 In the **Hostname** field, enter a PGP Universal Web Messenger hostname. This is the hostname used in Smart Trailer and PGP Universal Web Messenger links.

If the keyserver is behind a load balancer, this name may be different from the PGP Universal Server's network name. Once you specify a custom value for the PGP Universal Web Messenger's hostname here, it will remain there permanently even if the actual hostname changes later.

5 In the **Interface** field, select the interface on which the PGP Universal Server should listen for PGP Universal Web Messenger traffic.

Because PGP Universal Web Messenger offers a secure environment for reading messages, it only supports traffic over SSL/TLS.

6 In the **Port** field, keep the default or enter an appropriate port number.

7 Select the **Options** tab to create settings for PGP Universal Web Messenger external user accounts.

8 Put a checkmark in the **Encrypt stored messages to Ignition Keys** field to encrypt all stored PGP Universal Web Messenger messages to your Ignition Key(s).This option is not available if you have not created any Ignition Keys. See Chapter 46, "Protecting PGP Universal Server with Ignition Keys" for more information.

If this option is currently enabled and you disable it by deselecting the checkbox, all encrypted stored messages are decrypted.

9 In the **Inactivity Expiration** field, specify how long a PGP Universal Web Messenger account can be inactive before it expires.

When the account inactivity time-out is reached, the account is deleted—including any keys, email, or settings associated with the account.

10 In the **Storage Quota** field, enter the desired per-user storage quota for PGP Universal Web Messenger user accounts in megabytes (MB) or gigabytes (GB).

11 From the **Expiration** menu, select when you want user messages to expire, from 1 week to 5 years, or never. When a message expires, it is deleted from the user’s account.

12 Select the **Customization** tab to add the information you want external users to see when they log into the PGP Universal Web Messenger service.

13 In the **Company Name** field, enter the name of your company, if you want external users to be able to see it.

14 In the **Company Logo** field, select the image to be used for the PGP Universal Web Messenger logo.

Click **Choose File** to select the path to the corporate logo you want to display to external users, if any.

The company logo file should be in a browser–compatible format, such as GIF or JPEG. For the best appearance, PGP Corporation recommends a black-and-white version of your logo with some of the background color in the image for smoothing, and a size of no more than 200 pixels wide and no more than 32 pixels high.

a To view or delete the selected logo file, click **Save**.

The Web Messenger card will appear.

b Select the **Customization** tab.

c Click the **View** icon to see PGP Universal Web Messenger’s interface with the selected logo.

d Click the **Delete** button to delete the currently configured logo.

15 In the **Welcome Banner** field, enter any text you want PGP Universal Web Messenger users to see when they log in.

16 Select the **Administrator** tab to provide text your external users will see if there is a problem when they log into the PGP Universal Web Messenger service. PGP Universal Web Messenger users will see the message if there is a program error.

17 Enter a message to users into the **Contact Message** field. You should include contact information for your organization.

18 Click **Save**.

The PGP Universal Server restarts, which takes a few seconds.

31 Configuring the PGP Verified Directory

This chapter describes how to configure the PGP Verified Directory feature to enable users to submit their keys.

You can configure PGP Verified Directory options from the Services>Verified Directory card.

Topics in this chapter:

Overview

The PGP Verified Directory gives you the option of hosting a Web-accessible keyserver for the public keys of your internal or external users. This feature is optional; you do not have to enable it. You can choose whether to allow your internal users or external users, or both, to submit their keys.

The PGP Verified Directory feature is also part of the replacement for the PGP Keyserver product. It allows users running older PGP client software not directly supported by PGP Universal Server to submit their keys.

The PGP Verified Directory uses next-generation keyserver technology that lets users manage their own keys, including submitting and removing them. These features are not available on keyservers with older keyserver technology.

These advanced features simplify managing user keys and ensure that the keys in the directory can be trusted.

Specifically, the PGP Verified Directory sends verification messages to the email addresses on keys submitted to it. If the key owner responds to the verification message with permission to add the key, then the key is added to the directory. This approach keeps the PGP Verified Directory free of useless keys and protects users' privacy by foiling the upload of bogus keys that use their email addresses.

Published user keys are signed by another key. Keys submitted by internal users are signed by the Organization Key attached to the PGP Universal Server; keys submitted by external users (also called directory users) are signed by the Verified Directory Key.

You must add a Verified Directory Key to the PGP Universal Server before you allow users outside your managed domain to submit keys. See Chapter 12, "Managing Organization Keys" for more information on the Verified Directory Key.

The signature on the submitted key expires on a timetable you set. Every time the key signature expires, the key must be renewed based on the selected vetting method. For example, using the email vetting method, the user receives an email asking them to re-confirm that the email and key still belong to them. If the user responds to the verification email, the posted key is renewed. If the user does not respond, the key is removed from the PGP Verified Directory.

Additionally, the PGP Verified Directory lets the owner of a key remove it from the directory, even if the passphrase has been lost. This prevents the buildup of unusable keys; with older keyserver technology, once a key was posted, it was there forever unless the keyserver administrator manually removed it.

Finally, the PGP Verified Directory lets users search the directory through a web interface for the public keys of persons to whom they want to send secured messages.

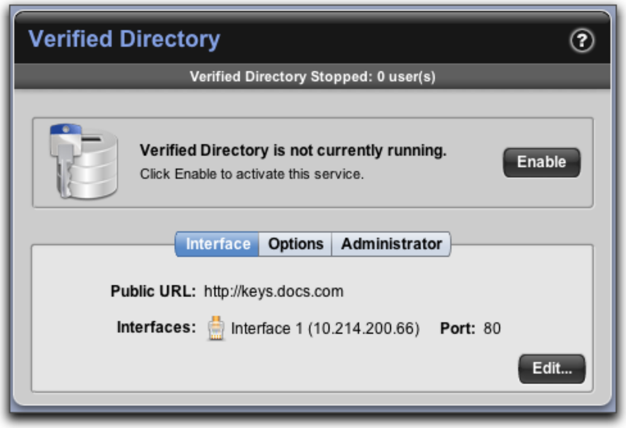
Once the PGP Verified Directory accepts an uploaded key, the verified key material is shared with the keyserver, to be used in encrypting messages.

Enabling the PGP Verified Directory

To enable the PGP Verified Directory feature:

1 On the Services>Verified Directory card, click the **Enable** button to enable the service.

2 To disable the PGP Verified Directory service, click the **Disable** button on the Verified Directory card.



Verified Directory

Verified Directory Stopped: 0 user(s)

Verified Directory is not currently running.
Click Enable to activate this service.

Public URL: http://keys.docs.com

Interfaces: Interface 1 (10.214.200.66) Port: 80

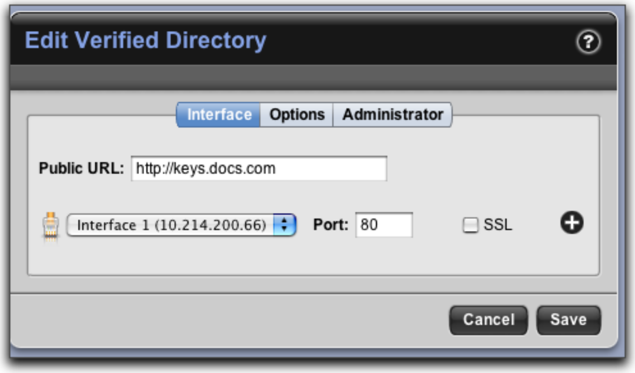
Configuring the PGP Verified Directory

To configure the PGP Verified Directory service:

1 On the Services>Verified Directory card, click the **Edit** button.

The Edit Verified Directory screen appears.

2 Click the **Interface** tab to specify how users access the directory.



Public URL: http://keys.docs.com

Interface 1 (10.214.200.66) Port: 80 □ SSL

3 In the **Public URL** field, enter the PGP Verified Directory's network name. Directory users access the PGP Verified Directory using this URL. The default URL is the hostname of the server, and the default port is port 80. You may want to change the URL, depending on your network configuration. By default, SSL is turned off. If the PGP Verified Directory runs on an interface with SSL, use HTTPS, and not HTTP, for the public URL. If the port you choose is not the default, add the number to the end of the URL; for example, https://<publicURL>:9999.

4 In the **Interface** field, select the appropriate interface for the PGP Verified Directory from the drop-down list.

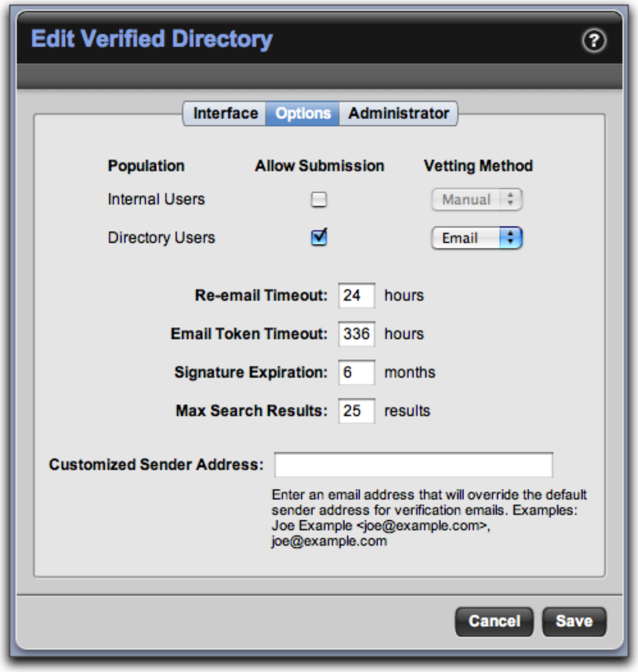
5 In the **Port** field, enter a port number for the PGP Verified Directory to listen on or keep the default setting.

The above two fields establish the interface and port on which the PGP Verified Directory will be established.

6 Put a check in the **SSL** checkbox to require that connections to the PGP Verified Directory be over SSL.

7 Click the plus sign icon to the right of the **Edit** field to add another network interface, and select the appropriate interface, port, and SSL information.

8 Click the **Options** tab to specify key and user interaction settings.



Population	Allow Submission	Vetting Method
Internal Users	□	Manual
Directory Users	☑	Email

Re-email Timeout: 24 hours

Email Token Timeout: 336 hours

Signature Expiration: 6 months

Max Search Results: 25 results

Customized Sender Address:

Enter an email address that will override the default sender address for verification emails. Examples: Joe Example <joe@example.com>, joe@example.com

9 Establish key submission criteria for internal users:

- **Allow Submission**. When checked, users can submit their public keys to the PGP Verified Directory. When unchecked, they can't. You can choose whether internal or directory users can submit their keys. Internal users are inside your managed domain; directory users are users outside your managed domain.
- **Vetting Method**. Choose a method for determining whether or not the owner of a submitted key agrees to it being posted in the PGP Verified Directory.

  Implicit means anyone who submits a key is by default trusted. **Manual** means the PGP administrator will manually approve or disapprove all submitted keys (the default). **Email** means an email message will be sent and must be responded to. See "Approving Pending Keys" on page 282 in the Internal Users chapter for information about manually approving internal user submitted keys. See Chapter 34, "Managing PGP Verified Directory User Accounts" for information on approving submitted external user keys.

10 In the **Re-email Timeout** field, enter a timeout value for resending email. The default is 24 hours. If for some reason a user's key is submitted multiple times, the timeout value specifies how often the user will receive the vetting email in response. The default of 24 hours means that users will only receive the email once every 24 hours.

11 In the **Email Token Timeout** field, enter the timeout value for the expiration of the email token. The default is 336 hours (14 days).

12 In the **Signature Expiration** field, enter the expiration time for the Organization Key's signature. The default is 6 months.

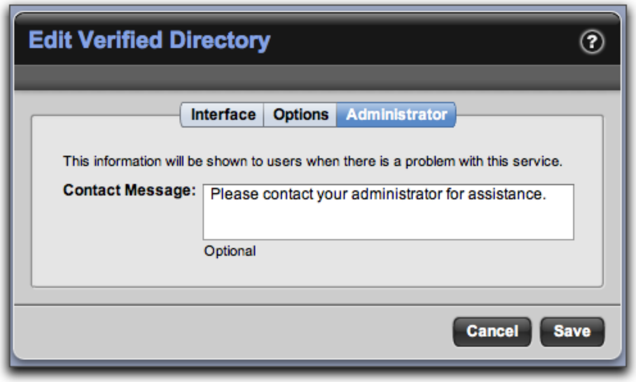
When signature expiration time period is reached, the user's key will automatically be re-verified using the selected vetting method.

13 In the **Max Search Results** field, enter the maximum number of results users receive for a web-based search. The default number of results returned for web-based searches is 25.

14 In the **Customized Sender Address** field, type the email address you want all PGP Verified Directory-generated email to appear to be from. Every email users receive from the PGP Verified Directory will have this address in the email "From" line. The customized sender address prevents your PGP Universal Server's hostname from appearing in the "From" line.

You do not need to create an email account to correspond to the email address you choose, because users should only interact with the PGP Verified Directory through the PGP Verified Directory interface, or through the information you provide in the Administrator Contact Message. However, if you want users to be able to reply to verification email using this address, you can create an email account using this email address. If you do not create an email account, reply email sent to the customized sender address will bounce.

15 Click the **Administrator** tab to create a message to directory users that will appear when there is a problem with the service.



This information will be shown to users when there is a problem with this service.

Contact Message: Please contact your administrator for assistance.

Optional

16 Click **Save**.

The settings you established are saved.

32 Managing Internal User Accounts

This chapter describes the internal users on your PGP Universal Server.

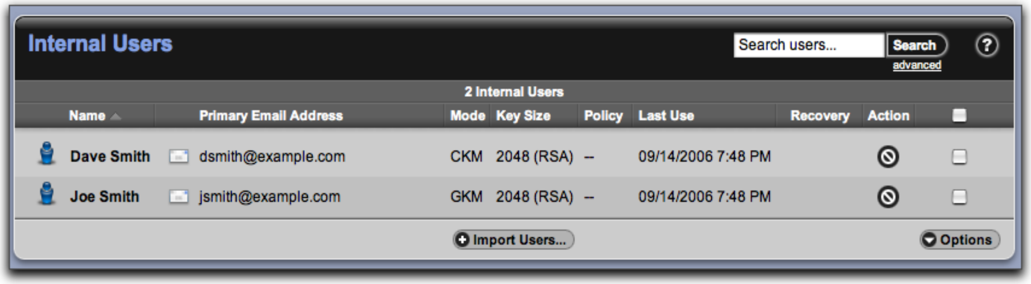
You can view information on internal users from the Users>Internal card.

Topics in this section include:

Overview

Internal users are defined as email users from managed domains. Internal users are created automatically by your PGP Universal Server when those internal users interact with the mail server.

The list on the Internal Users card shows all of the internal users that are part of the SMSA created by the PGP Universal Server. It lists their Name, Primary Email address, key mode and size, the user group policy that applies to them, the last time they sent or received a message, key recovery information, and it lets you delete a user or export their key.



2 Internal Users

Name	Primary Email Address	Mode	Key Size	Policy	Last Use	Recovery	Action	□
Dave Smith	dsmith@example.com	CKM	2048 (RSA)	--	09/14/2006 7:48 PM		⊘	□
Joe Smith	jsmith@example.com	GKM	2048 (RSA)	--	09/14/2006 7:48 PM		⊘	□

Sometimes a user is listed on the Internal Users card with no email address shown. This happens when the user account was created automatically by the PGP Universal Server when the user accessed email over a POP or IMAP connection, but the PGP Universal

Server does not know what email address is associated with that user. As soon as that user sends email over SMTP, the PGP Universal Server will be able to add the rest of the user information to the record.

You can also manually add the keys of PGP Desktop users to the list, search for an internal user, and approve keys submitted by internal users.

When user keys are created, they automatically contain information on the preferred keyserver URL, as specified on the Services>Keyserver page. If the Public URL for the preferred keyserver changes, the information will be updated on the key the next time the Organization Key signature on the user key is renewed.

If you previously used your PGP Keyserver to store keys and key reconstruction blocks for users in your managed domains, you can now import and store that key data on the PGP Universal Server. Refer to the *PGP Universal Server Upgrade Guide* for information on how to create an importable file containing user keys.

Certificate Revocation Lists

A certificate revocation list (CRL) is a list of certificates that have been revoked before their scheduled expiration date. The PGP Universal Server retrieves CRLs for certificates from CRL Distribution Points (DP).

The PGP Universal Server checks the CRL DPs automatically before encrypting a message to a certificate, including certificates for internal and external users, as well as certificates in the cache. The server also checks the CRL DPs before importing any internal or external user certificate. It does not check before importing Trusted Certificates, or before connecting to servers with SSL certificates.

The PGP Universal Server checks the revocation status of just the certificate. It will not check the revocation status of the other certificates in the signing chain.

Once retrieved, certificate revocation status is stored on the parent certificate, so the Trusted Certificate for each user certificate stores the list of all the associated revoked certificates. Once the CRL is stored on the Trusted Certificate, the PGP Universal Server will run future CRL checks based on the "next update" date for that list.

Adding Internal Users Manually

In addition to automatically creating a key for your email users, the PGP Universal Server also lets you manually add internal users. This option is useful for internal users who already have keys, such as existing PGP Desktop users who of course would have their own PGP key, or existing S/MIME users from a previous PKI in your organization.

The PGP Universal Server checks the Certificate Revocation List Distribution Points automatically before importing any internal user certificate. See "Certificate Revocation Lists" on page 279 for more information.

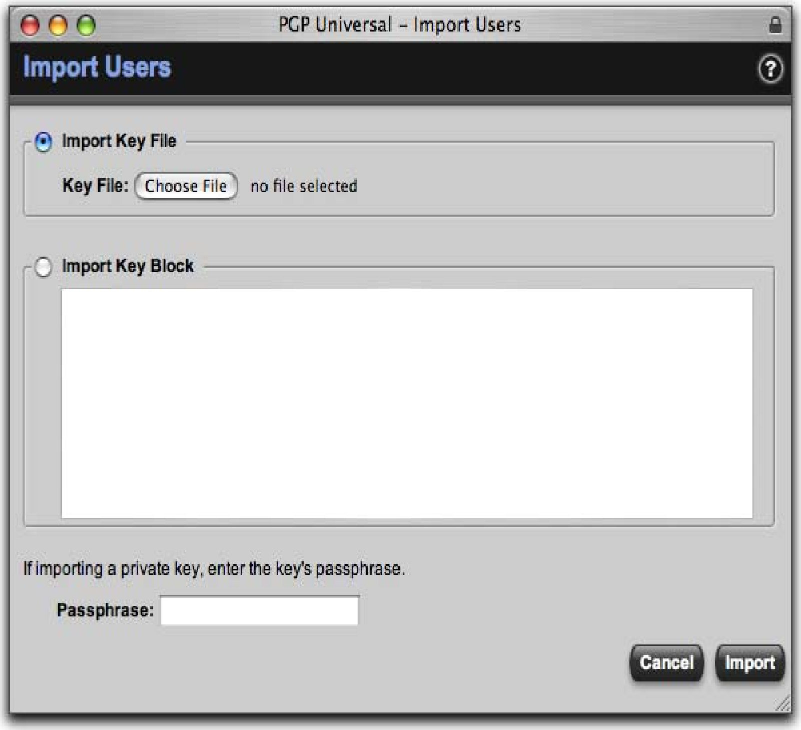
There are some important things to know before you import the key of an internal user:

- You can only import users with email addresses in a domain being managed by the PGP Universal Server.
- You can import more than one key at a time (if appropriate, of course). Paste the keys into the Key Block box one after the other or put them together in one file.
- If users should manage their private keys on their own computers, called Client Key Mode (CKM), then paste in only their public keys.
- If the PGP Universal Server will be managing both the private key and the public key for the user, called Server Key Mode (SKM), paste in a keypair that was created with no passphrase.
- If the user wants to manage their private key on their own computer, but wants to keep a copy of their private key on the server in encrypted format, called Guarded Key Mode (GKM), paste in a keypair that was created with a passphrase.
- If the user wants to store their private encryption key on both their own computer and on the PGP Universal Server, but wants to store their private signing key only on their own computer, called Server Client Key Mode (SCKM), paste in only the user's private encryption key.

To manually add an internal user:

1 Click **Import Users**.

The Import Users dialog appears.


PGP Universal – Import Users

Import Users

● Import Key File

Key File: Choose File no file selected

○ Import Key Block

If importing a private key, enter the key's passphrase.

Passphrase:

2 To import a user who has exported their key to a file, select **Import Key File**, use the **Browse** button to select the key file, type in the passphrase for the key (if appropriate), then click **Import**.

For importing PGP keys, use the ASCII key file format (.asc). For importing X.509 certificates, use PKCS 7, PKCS 12, or PEM files.

3 To import a user using their key block, select **Import Key Block**, copy the key block(s) of the key(s) you want to import, paste them into the **Key Block** box, then click **Import**.

To import the key block of a PGP key, paste the ASCII-armor key block. To import an X.509 certificate, paste the certificate block.

4 If the key or certificate is protected by a passphrase, enter it in the **Passphrase** field.

5 Click **Import**.

The key data is imported.

If you are importing a PGP Keyserver file, all keys belonging to internal users are imported, and all other key information is discarded.

Deleting Internal Users

Deleting a user is a permanent operation. If you delete a user, all private key material will be lost with no way to get it back. Anything encrypted only to those keys will not be recoverable. If there is any chance that user's private key might be needed in the future, it is a much better idea to revoke the user's key instead of deleting the user. See "Revoking the PGP Key of an Internal User" on page 285.

To delete one internal user:

1 Click the Delete icon of the internal user you want to delete.

A confirmation dialog appears.

2 Click **OK**.

The user is removed from the list of internal users.

To delete multiple internal users:

1 Click the checkbox at the far right end of the row of each of the internal users you want to delete.

2 Select **Delete Selected** from the Options menu at the bottom right corner, or **Delete All** to delete all internal users.

A confirmation dialog appears.

3 Click **OK**.

The users are removed from the list of internal users.

Approving Pending Keys

In addition to automatically creating a key for your email users or manually adding internal users, you can allow internal users to submit their own keys through the PGP Verified Directory. Allowing user key submission is useful for internal users who already have keys, such as existing PGP Desktop users who of course would have their own PGP key. If the user already has a PGP key, and the new key is approved, the new key will replace the old key.

PGP Desktop users upload their public keys through the PGP Verified Directory interface at the interface and port you configure on the Verified Directory card.

On the Verified Directory card, you can specify how you want these user-submitted keys approved. If you have set the PGP Verified Directory to require either a confirmation email from the user or to require you, the administrator, to manually approve the key, the user’s PGP key status will be marked pending. See Chapter 31, “Configuring the PGP Verified Directory” for information on the PGP Verified Directory.

To manually approve the key submission:

1 From the Internal Users card, click the plus sign icon to approve the key.

2 Click the minus sign icon to deny the submitted key.

3 Click the delete icon to delete the user.

Searching for Internal Users

To find an internal user using a simple search, enter the criteria for which you want to search, and click the **Search** button. A list of users that fit the criteria you specified appears.

To search using advanced criteria:

1 On the Internal Users card, click **advanced**.

The User Search dialog appears.

2 Specify your criteria:

– In the drop-down list on the left, select search criteria from: **Email Address**, **Key Expiration**, **Last Use**, **Name**, **Policy**, **Status**, **User Type**.

– In the middle drop-down list, select how to limit the search, for example: **contains**, **does not contain**, **is on**, **is before**, et cetera.

– In the text box on the right, enter or select the criteria you want to search for.

– If you want to use more search criteria, click the plus sign icon and enter the appropriate criteria. Returned results will match all the search criteria you enter.

3 Click **Search**.

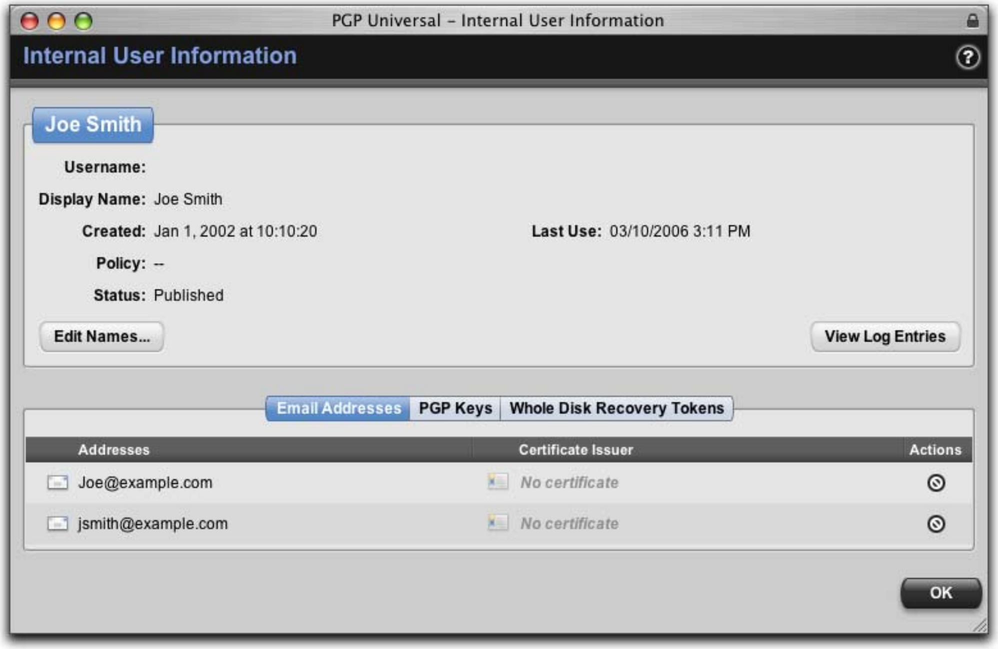
A list of users that fit the criteria you specified appears.

To clear the search, click the cancel button to the left of the search field.

Internal User Settings

To inspect the settings of an internal user, click on the name of the user whose information you want to inspect.

The Internal User Information dialog appears.


PGP Universal – Internal User Information
Internal User Information
Edit Names...
View Log Entries
Email Addresses
PGP Keys
Whole Disk Recovery Tokens
OK

Joe Smith

Username:
Display Name: Joe Smith
Created: Jan 1, 2002 at 10:10:20
Last Use: 03/10/2006 3:11 PM
Policy: --
Status: Published

Addresses	Certificate Issuer	Actions
Joe@example.com	No certificate	⊘
jsmith@example.com	No certificate	⊘

The top section of this dialog displays the Username, Display Name, when the user account was created, Status, Last Use, and what policy applies for the selected internal user.

Status reflects a user’s key status. Key status for CKM and SKM users is always Published because those keys are published to your LDAP directory. If a user submits their keys using the PGP Verified Directory interface, the key status will indicate where the key is in the PGP Verified Directory process. Refer to Chapter 31, “Configuring the PGP Verified Directory” for more information.

The Email Addresses tab lists the email addresses associated with the selected internal user, any certificates attached to their email addresses, and anything you can do in regards to their certificates. If the internal user’s key includes an X.509 certificate, it will also be shown. Refer to “Exporting an Internal User’s X.509 Certificate” on page 284 for instructions how to export the X.509 certificate.

The PGP Keys tab lists the key ID, key mode, key size, creation date, expiration time, status, reconstruction block status, pending keys, and actions you can take for PGP keys associated with the selected internal user. For example, you can delete internal users' key reconstruction blocks uploaded to the PGP Universal Server; refer to "Deleting a PGP Desktop Key Reconstruction Block" on page 287 for instructions.

If the internal user has an associated PGP key, you can export or delete the key. If the user's key is in SKM, you can also revoke it. Pending keys can be exported, but you cannot revoke or delete them.

The Whole Disk Recovery Tokens tab lists any whole disk recovery tokens associated with the internal user, their status, and actions you can take. Refer to "Using Whole Disk Recovery Tokens" on page 287 for instructions how to use a whole disk recovery token.

Changing Internal User Settings

To change the settings of an internal user:

1. Click on the name of the user whose information you want to inspect.

   The Internal User Information dialog appears.

2. To change or add usernames or email addresses associated with a user's key and display name, click **Edit Names**.

   The Edit Names dialog appears.

3. Enter the usernames you want to add. To add another username, click the Add icon next to the username field.

4. Enter the Display Name you want to appear on the Internal Users card. Display names containing the symbol @ are not valid unless the display name is typed within quotation marks; for example, "joe@example.com" is valid.

5. Click **Save**.

6. Click **OK** to save changes.

Exporting an Internal User's X.509 Certificate

To export the X.509 certificate of an internal user:

1. Select the user you want from the Internal Users card.

   The Internal User Information dialog appears.

2. From the Email Addresses tab, click the Export icon to export the certificate.

   If only the public key is attached to the certificate, the text of the certificate will be downloaded to your system.

   If both the public and the private key are attached to the certificate, the Export Certificate dialog appears, allowing you to choose to export only the public key, or both public and private portions of the key.

3 Select **Export Public Key** to export just the public key portion of the certificate.

4 Select **Export Keypair** to export the entire certificate.

5 If you want to protect the exported certificate file with a passphrase, enter it in the **Passphrase** field.

If the X.509 certificate is already protected by a passphrase, you will not be able to export the private portion. You will export only a PEM file containing the public certificate.

6 Click **Export**.

The X.509 certificate is exported.

Revoking the PGP Key of an Internal User

Only keys for which the PGP Universal Server has the private key can be revoked; that is, only the keys of SKM users can be revoked. The Revoke button is disabled for all other keys.

If you revoke an internal user's PGP key, it continues being published via the LDAP server, but appears marked as a revoked key, and it will appear on the Certificate Revocation Lists. Revoking an internal user's S/MIME certificate means it will no longer be published via the LDAP server; however, it will not automatically be sent to the Certificate Revocation Lists.

Once you revoke a key, you cannot un-revoke it.

Revoking a key is a safer operation than deleting a user because the private key material is preserved, which means that decryption continues to work.

To revoke the PGP key of an internal user:

1 Select the user you want from the Internal Users card.

The Internal User Information dialog appears.

2 From the PGP Keys tab, click the Revoke icon next to the key you want to revoke.

A confirmation dialog appears.

3 Click **OK**.

The internal user's key is revoked.

Exporting the PGP Key of an Internal User

If the user's key data is stored in Server Key Mode, you will be able to export both public and private key information. If the private key is stored protected by the user's passphrase, you will not be able to export it unencrypted. If the key data is in Client Key Mode, the private key is not stored on the server and cannot be exported.

To export the PGP key of an internal user:

1. Select the user you want from the Internal Users card.

   The Internal User Information dialog appears.

2. From the PGP Keys tab, click the Export icon in the Options column for the keys you want to export.

   If only the public key is available, the text of the key will be downloaded to your system.

   If both the public and the private key are available, the Export Key dialog appears, allowing you to choose to export only the public key, or both public and private portions of the key.

3. Select **Export Public Key** to export just the public key portion of the keypair.

4. Select **Export Keypair** to export the entire keypair, the public key and the private key portions.

5. If you want to protect the exported key file with a passphrase, enter it in the Passphrase field.

   If a private key already has an attached passphrase, it is already protected and there is no need to enter another passphrase at this time. When you export the keypair, you will receive a file containing an unencrypted public key and an encrypted private key.

6. Click **Export**.

   The key is exported to your system.

Deleting the PGP Key of an Internal User

If you delete a user's key, the private key material will be gone, which means messages will no longer be decryptable.

To delete the PGP key of an internal user:

1. Select the user you want from the Internal Users card.

   The Internal User Information dialog appears.

2. From the PGP Keys tab, click the Delete icon in the Options column of the PGP key you want to delete.

   A confirmation dialog appears.

3. Click **OK**.

   The key of the internal user is deleted.

Deleting a PGP Desktop Key Reconstruction Block

If an internal PGP Desktop user has uploaded a key reconstruction block to the PGP Universal Server, you can delete it. You may want to delete a key reconstruction block if you have already deleted or revoked the associated key and you do not want the key to be recoverable. If you delete the key reconstruction block, it will no longer be stored on the PGP Universal Server, although it is possible that the user may also have a copy. See "Key Reconstruction Blocks" on page 288 for more information.

To delete a key reconstruction block:

1. Select the user you want from the Internal Users card.

   The Internal User Information dialog appears.

2. From the PGP Keys tab, click the Delete icon in the Reconstruction column.

   A confirmation dialog appears.

3. Click **OK**.

   The key reconstruction block is deleted.

Using Whole Disk Recovery Tokens

If the internal user whose settings you are viewing has a whole disk recovery token stored on the PGP Universal Server, it will be listed in the Whole Disk Recovery Tokens section of the Internal User Information dialog.

Otherwise, the text "No tokens were found" appears.

To recover a whole disk:

1. Click the View icon in the Options column.

   The recovery token string appears.

2. Provide this information to the user, who uses it to recover the disk.

   Once the token is used, it is presented as a "broken" or opened token, and a new token is automatically generated by PGP Desktop and synchronized with the PGP Universal Server as soon as the user logs in. The new token will then re-appear as unviewed or valid.

Viewing Internal User Log Entries

You can search for system logs for any internal user directly from the Internal User Information card.

1. Select the user you want from the Internal Users card.

   The Internal User Information dialog appears.

2. Click **View Log Entries** on the Internal User Information dialog.

   The System Logs card appears with search results for the user you chose. Results are from the Mail logs only.

Refer to Chapter 41, “System Logs” for more information on exploring the system logs.

Key Reconstruction Blocks

Key reconstruction blocks allow users to retrieve their private keys if they forget their passphrases.

Key reconstruction blocks contain several user-defined questions and the user's private key, which is encrypted with the answers to those questions.

PGP Universal Server stores these questions and answers so that users can get back their private keys in case they lose their passphrases. For example, if a user writes five questions and answers, they may be asked to answer three (or more) of these questions to reconstruct their private key.

If an internal PGP Desktop user has uploaded a key reconstruction block to the PGP Universal Server, you can delete it. You may want to delete a key reconstruction block if you have already deleted or revoked the associated key and you do not want the key to be recoverable. If you delete the key reconstruction block, it will no longer be stored on the PGP Universal Server, although it is possible that the user may also have a copy.

ℹ Keys created on smartcards and tokens are not compatible with PGP Desktop's key reconstruction feature.

33 Managing External User Accounts

This chapter describes the external users on your PGP Universal Server.

You can view information on external users from the Users>External card.

This feature allows you to store keys belonging to individuals outside your managed domains. If you are only managing PGP NetShare or PGP Whole Disk Encryption installations for internal users, you may not require external user keys.

Topics in this section include:

Overview

External users are defined as email users outside of managed domains but who are part of the SMSA. (Internal users are email users from managed domains.) External users may be running PGP Universal Satellite or PGP Desktop, or they may interact with the PGP Universal Server through PGP Universal Web Messenger.

Importing external users allows your internal users to easily send encrypted messages to them, because external users' public keys are stored locally. This is similar to adding external domains and directories to the PGP Universal Server, except that you are adding information about specific individuals rather than domains. PGP Universal Server stores the key material for external users, rather than having to look for it on an external keyserver directory.

The PGP Universal Server checks the Certificate Revocation List Distribution Points automatically before importing any external user certificate. See "Certificate Revocation Lists" on page 279 for more information.

The External Users card lists all of the external users your PGP Universal Server knows. It lists their Email Address, Name, User Type, Mode, Key Size, Policy, Usage, Last Use, and lets you delete or export the user.

You can also change the default account settings your server uses when it creates a new external user or search for an external user.

If you previously used your PGP Keyserver to store keys and key reconstruction blocks for users outside your managed domains, you can now import and store that key data on the PGP Universal Server. Refer to Appendix 48, "Migrating a PGP Keyserver" for information on how to create an importable file containing user keys.

If you would prefer your external users to manage their own keys stored on the PGP Universal Server, rather than you importing and managing their keys yourself, you can allow them to submit keys to the PGP Verified Directory. Refer to Chapter 34, "Managing PGP Verified Directory User Accounts" for more information.

Importing External Users

If PGP Universal Web Messenger is enabled, you can add external users by sending them email invitations. The email invites the users to establish a passphrase, and to choose how they would like to receive secure email in the future, including the option to submit their public keys.

To manually import one or more external users using their email addresses:

1 On the External Users card, click **Import Users**.

The Add Users dialog appears.

2 In the **Email addresses** field, enter the email addresses of the external users you are adding. Separate email addresses with commas, semi-colons, or on new lines.

3 Click **Save**. The added users will then receive an invitation email.

If you have an external user's public key, you can import it directly into the PGP Universal Server, so that your internal users can immediately begin sending encrypted email to that user. If PGP Universal Web Messenger is not enabled, you can add external users by manually importing user keys. To manually import one or more external users by importing their keys:

1 On the External Users card, click **Import Users**.

The Add Users dialog appears.

2 Click **Import keys**.

On the Import Users dialog, import your external users by choosing their key file or pasting their key block. Enter a passphrase if necessary.

3 Click **Import**.

The key data is imported.

If you are importing a PGP Keyserver file, all keys belonging to external users are imported, and all other key information is discarded.

Deleting External Users

To delete one external user:

1 Click the delete icon in the Delete column of the external user you want to delete.

A confirmation dialog appears.

2 Click **OK**.

The user is removed from the list of external users.

To delete multiple external users:

1 Click the checkbox at the far right end of the row of each of the external users you want to delete.

2 Select **Delete Selected** from the Options menu.

A confirmation dialog appears.

3 Click **OK**.

The users are removed from the list of external users. PGP Universal Web Messenger messages stored for the user will also be deleted.

To delete all external users, select **Delete All** from the Options menu, and click **OK** on the confirmation dialog.

Searching for External Users

To find an external user using a simple search, enter the criteria for which you want to search, and click the **Search** button. A list of users that fit the criteria you specified appears.

To search using advanced criteria:

1 On the **External Users card**, click **advanced**.

The User Search dialog appears.

2 Specify your criteria:

- In the drop-down list on the left, select search criteria from: **Email Address**, **Last Use**, **Name**, or **User Type**.
- In the middle drop-down list, select how to limit the search, for example: **contains**, **does not contain**, **is on**, **is before**, et cetera.
- In the text box on the right, enter or select the criteria you want to search for.
- If you want to use more search criteria, click the plus sign icon and enter the appropriate criteria. Returned results will match all the search criteria you enter.

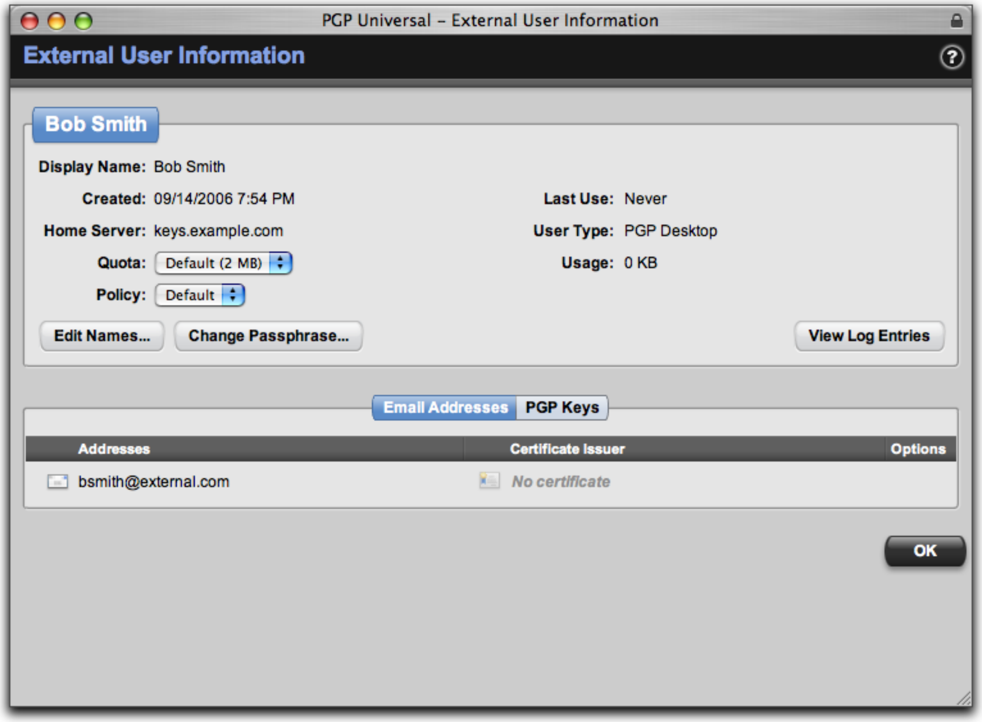
3 Click **Search**.

A list of users that fit the criteria you specified appears.

To clear the search, click the cancel button to the left of the search field.

External User Settings

From the Users>External card, click on the name of the user whose information you want to inspect. The External User Information dialog appears.



PGP Universal – External User Information

External User Information

Bob Smith

Display Name: Bob Smith

Created: 09/14/2006 7:54 PM

Last Use: Never

Home Server: keys.example.com

User Type: PGP Desktop

Quota: Default (2 MB)

Usage: 0 KB

Policy: Default

Addresses	Certificate Issuer	Options
bsmith@external.com	No certificate	

The top section of this dialog shows the Display Name, when the user account was created, which PGP Universal Server is the home server, Last Use, User Type, Quota, Policy, and Usage for the selected external user.

The user's Quota is the amount of storage space allotted for PGP Universal Web Messenger mail storage. Both mail received and mail sent and saved are counted.

The Home Server is where the user's PGP Universal Web Messenger data is stored. If you have clustered PGP Universal Servers, external user PGP Universal Web Messenger data will be stored on only one of the cluster members, unless the user is a High Availability user. Refer to Chapter 30, "Configuring PGP Universal Web Messenger" for more information.

The User Type describes the external user's encryption method, for example, Web Messenger or S/MIME.

Usage refers to how much of the user's Quota has already been used.

The Email Addresses tab lists the email addresses associated with the selected external user, any certificates attached to their email addresses, and the actions you can take in regards to their certificates. If the external user's key includes an X.509 certificate, it will also be shown. Refer to "Exporting an External User's X.509 Certificate" on page 295 for instructions how to export the X.509 certificate.

The PGP Keys tab lists the key ID, key mode, key size, creation date, expiration date, status, and actions you can take for PGP keys associated with the selected external user. If the external user has an associated PGP key, you can export or delete the key. If the user's key is in SKM, you can also revoke it. If the user has a key reconstruction block, you can also delete that.

Changing External User Settings

To change the settings of an external user:

1. Click on the name of the user whose information you want to inspect.

   The External User Information dialog appears.

2. To change the user's Quota, select a value, from 1MB to 1GB, from the Quota drop-down list.

3. To change the user's Policy, select a different policy from the drop-down list. The new policy assignment takes effect immediately.

4. To change the user name displayed the External User list, click **Edit Names**. When the Edit Names dialog appears, enter the display name you want to use and click **Save**. Display names containing the symbol @ are not valid unless the display name is typed within quotation marks; for example, "joe@example.com" is valid.

5. To change the user's passphrase, click **Change Passphrase**. This lets you change the passphrase this external user uses to access PGP Universal Server services. When the Change Passphrase dialog appears, enter and confirm the new passphrase and click **Save**. Passphrases must be at least 6 characters long.

6. Click the Delete icon to delete email addresses from the Email Addresses tab list; at least one email address must be left on the list.

7. Refer to "Exporting an External User's X.509 Certificate" on page 295 for instructions how to export the X.509 certificate from the Email Addresses tab list.

8. Click the PGP Keys tab to manage the user's keys. If the external user has an associated PGP key, you can revoke, export, or delete the key. You can also delete the user's key reconstruction block from this tab.

9. Click **OK** to save changes.

Viewing External User Log Entries

You can search for system logs for any external user directly from the External User Information card.

1. Select the user you want from the External Users card.

The External User Information dialog appears.

2 Click **View Log Entries** on the External User Information dialog.

The System Logs card appears with search results for the user you chose. Results are from the Mail logs only.

Refer to Chapter 41, "System Logs" for more information on exploring the system logs.

Exporting an External User's X.509 Certificate

To export the X.509 certificate of an external user:

1 Select the user you want from the External Users card.

The External User Information dialog appears.

2 Click the Export icon to export the certificate.

If only the public key is attached to the certificate, the text of the certificate will be downloaded to your system.

If both the public and the private key are attached to the certificate, the Export Certificate dialog appears.

3 Select **Export Public Key** to export the public key part of the certificate.

4 Select **Export Keypair** to export the entire certificate.

5 If you want to protect the exported certificate file with a passphrase, enter it in the **Passphrase** field.

If the X.509 certificate is already protected by a passphrase, you will not be able to export the private portion. You will export only a PEM file containing the public certificate.

6 Click **Export**.

The X.509 certificate is exported.

Exporting the PGP Key of an External User

To export the PGP key of an external user:

1 Click the checkbox for the external user whose key you want to export.

1 From the Options menu, select Export Selected.

If only the public key is available, the text of the key will be downloaded to your system.

If both the public and the private key are available, the Export Key dialog appears.

2 Select **Export Public Key** to export just the public key portion of the keypair.

3 Select **Export Keypair** to export the entire keypair, the public key and the private key portions.

4 If you want to protect the exported key file with a passphrase, enter it in the **Passphrase** field.

If a private key already has an attached passphrase, it is already protected and there is no need to enter another passphrase at this time. When you export the keypair, you will receive a file containing an unencrypted public key and an encrypted private key.

5 Click **Export**.

The key is exported.

Deleting the PGP Key of an External User

To delete the PGP key of an external user:

1 Select the user you want from the External Users card.

The External User Information dialog appears.

1 Click **PGP Keys**, then click the Delete icon for the PGP key you want to delete.

A confirmation dialog appears.

2 Click **OK**.

The key of the external user is deleted.

Changing the Passphrase of an External User

To change the passphrase of an external user:

1 On the External User Information dialog, click **Change Passphrase**.

The Change Passphrase dialog appears.

2 In the **New Passphrase** field, enter the new passphrase. The passphrase must be at least 6 characters long.

3 In the **Confirm New Passphrase** field, enter the new passphrase again, exactly as you entered it in the New Passphrase field.

4 Click **Save**.

The passphrase is changed.

34 Managing PGP Verified Directory User Accounts

This chapter describes how to manage the PGP Verified Directory users on your PGP Universal Server.

You can view information on PGP Verified Directory users from the Users>Verified Directory card.

This feature allows you to store keys belonging to individuals outside your managed domains. If you are only managing PGP NetShare or PGP Whole Disk Encryption installations for internal users, you may not require external user keys.

Topics in this section include:

- "Overview"
- "Importing Verified Directory Users" on page 299
- "PGP Verified Directory User Settings" on page 300
- "Deleting PGP Verified Directory Users" on page 302
- "Exporting PGP Verified Directory Users" on page 303
- "Searching for PGP Verified Directory Users" on page 303

Overview

PGP Verified Directory users are users external to your domain who can manage their keys stored on PGP Universal Server through the PGP Verified Directory.

Storing external user keys through the PGP Verified Directory allows directory users to manage their keys themselves through the PGP Verified Directory interface, without requiring them to establish PGP Universal Web Messenger accounts.

> External user keys submitted through the PGP Verified Directory are replicated across a cluster.

You must add a Verified Directory Key to the PGP Universal Server before you import keys or allow users outside your managed domain to submit keys. The Verified Directory Key is the signing key for PGP Verified Directory users outside your managed domain. (Internal PGP Verified Directory user keys are signed by your Organization Key.)

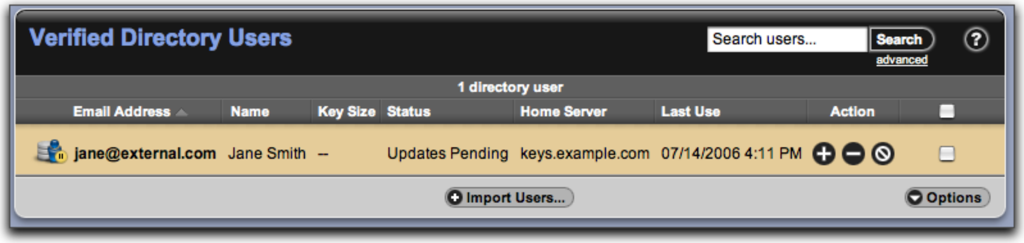
Once you choose the setting to allow external users to submit their keys through the PGP Verified Directory, you must upload a Verified Directory Key. External users will not be able to submit their keys to PGP Verified Directory until you have added the Verified Directory Key.

See Chapter 12, "Managing Organization Keys" for more information on the Verified Directory Key.

Refer to Chapter 31, "Configuring the PGP Verified Directory" to learn how to enable users outside your managed domain to use the PGP Verified Directory.

If you would prefer to manage external user keys, or you would like external users to use PGP Web Messenger, refer to Chapter 33, "Managing External User Accounts" for more information.

You can manage Verified Directory users through the Verified Directory Users card.



Verified Directory Users

1 directory user

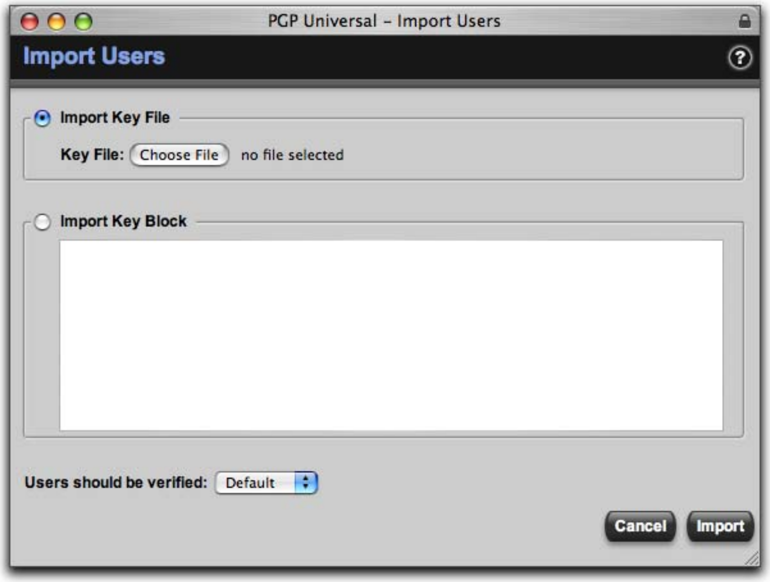
Email Address	Name	Key Size	Status	Home Server	Last Use	Action	□
jane@external.com	Jane Smith	--	Updates Pending	keys.example.com	07/14/2006 4:11 PM		□

Importing Verified Directory Users

While you can allow directory users to submit their own keys through the PGP Verified Directory interface, you can also import their keys manually, and still allow the users to manage their own keys.

1 On the Verified Directory Users card, click **Import Users**.

The Import Users dialog appears.



PGP Universal – Import Users

Import Users

● Import Key File

Key File: Choose File no file selected

○ Import Key Block

Users should be verified: Default

2 On the Import Users dialog, import directory users by choosing their key file or pasting their key block.

3 Choose how the user keys should be verified:

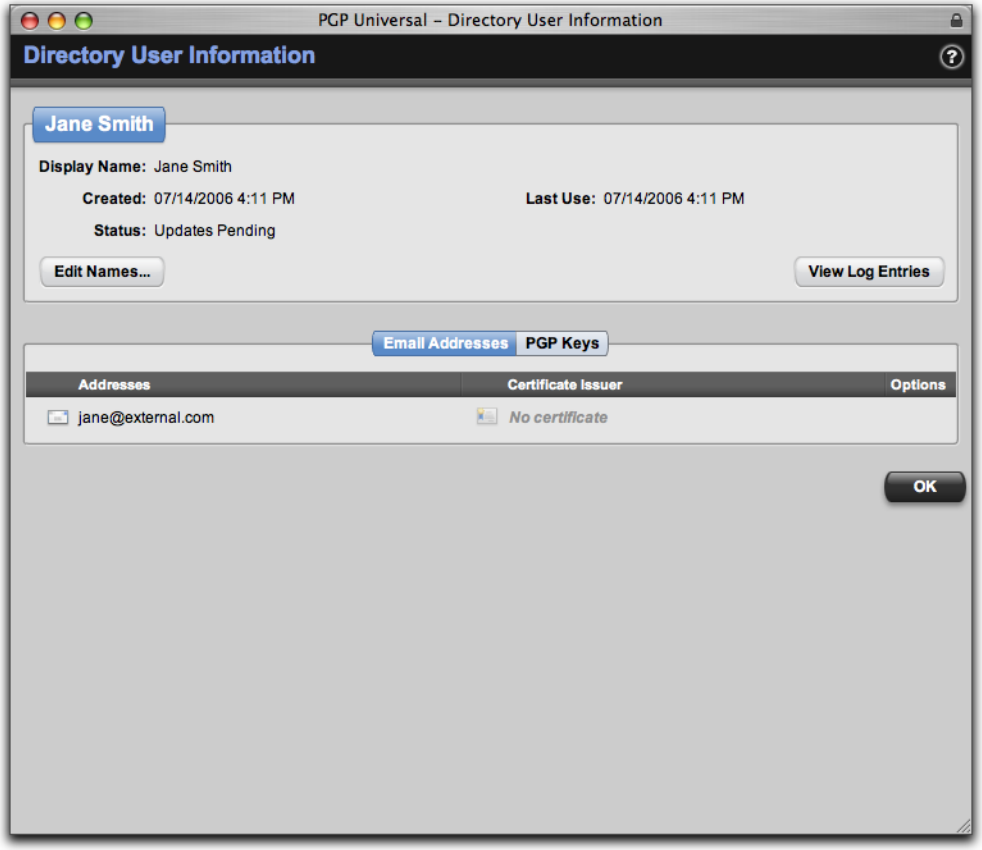
- **Default**. Applies the vetting method you selected on the Verified Directory service card.
- **Implicitly.** The keys are by default trusted.
- **Via Email.** An email message will be sent to the directory users and must be responded to.
- **Manually.** The PGP administrator will manually approve or disapprove the directory user keys.

4 Click **Import**.

The key data is imported.

PGP Verified Directory User Settings

From the Users>Verified Directory card, click on the name of the user whose information you want to inspect. The Directory User Information dialog appears.



PGP Universal – Directory User Information

Directory User Information

Jane Smith

Display Name: Jane Smith

Created: 07/14/2006 4:11 PM

Last Use: 07/14/2006 4:11 PM

Status: Updates Pending

Addresses	Certificate Issuer	Options
jane@external.com	*No certificate*	

The top section of this dialog shows the Display Name, when the user account was created, Last Use, and Status of the user's key. The key status indicates where the key is in the PGP Verified Directory process: Updates Pending, Published, or Delete Pending

The Email Addresses tab lists the email address associated with the selected directory user.

The PGP Keys tab lists the key ID, key mode, key size, creation date, expiration time, status, and actions you can take for PGP keys associated with the selected directory user. You can export or delete the key. Pending keys can be exported, but you cannot delete them.

Changing PGP Verified Directory User Settings

To change the settings of a directory user:

1. Click on the name of the user whose information you want to inspect.

   The Directory User Information dialog appears.

2. To change the user name displayed the Directory User list, click **Edit Names**. When the Edit Names dialog appears, enter the display name you want to use and click **Save**.

3. Click the Delete icon to delete email addresses from the Email Addresses tab list; at least one email address must be left on the list.

4. Click the PGP Keys tab to manage the user's keys. If the directory user has an associated PGP key, you can export or delete the key.

5. Click **OK** to save changes.

Approving Pending Keys

If you have set the PGP Verified Directory to require either a confirmation email from the user or to require you, the administrator, to manually approve the key, the user's PGP key status will be marked pending.

To manually approve the key submission, choose one of the following:

1. To approve a single user key, click the plus sign icon in the Options column to approve the key.

2. Click the minus sign icon to deny the submitted key.

3. Click the delete icon to delete the user.

Or

1. To approve multiple user keys, click the checkbox at the far right end of the row of each of the directory user key you want to approve.

2. Select **Approve Selected** or **Approve All** from the Options menu.

Deleting the PGP Key of a PGP Verified Directory User

To delete the PGP key of a directory user:

1 Select the user you want from the Verified Directory Users card.

The Directory User Information dialog appears.

2 Click **PGP Keys**, then click the Delete icon for the PGP key you want to delete.

A confirmation dialog appears.

3 Click **OK**.

The key of the PGP Verified Directory user is deleted.

Viewing PGP Verified Directory User Log Entries

You can search for system logs for any directory user directly from the Directory User Information card.

1 Select the user you want from the Verified Directory Users card.

The Directory User Information dialog appears.

2 Click **View Log Entries** on the Directory User Information dialog.

The System Logs card appears with search results for the user you chose. Results are from the Mail logs only.

Refer to Chapter 41, “System Logs” for more information on exploring the system logs.

Deleting PGP Verified Directory Users

To delete PGP Verified Directory users, choose one of the following:

1 To delete a single directory user, click the delete icon in the Delete column of the directory user you want to delete.

A confirmation dialog appears.

2 Click **OK**.

The user is removed from the list of directory users.

Or

1 To delete multiple directory users, click the checkbox at the far right end of the row of each of the directory users you want to delete.

2 Select **Delete Selected** from the Options menu.

A confirmation dialog appears.

3 Click **OK**.

The users are removed from the list of directory users.

4 To delete all directory users, select **Delete All** from the Options menu, and click **OK** on the confirmation dialog.

Exporting PGP Verified Directory Users

To export the PGP key of directory users:

1 Click the checkboxes for the users whose keys you want to export.

2 From the Options menu, select Export Selected.

The text of the keys will be downloaded to your system.

Searching for PGP Verified Directory Users

To find a PGP Verified Directory user using a simple search, enter the criteria for which you want to search, and click the **Search** button. A list of users that fit the criteria you specified appears.

To search using advanced criteria:

1 On the Verified Directory Users card, click **advanced**.

The User Search dialog appears.

2 Specify your criteria:

- In the drop-down list on the left, select search criteria from: **Email Address**, **Name**, **Status**.
- In the middle drop-down list, select how to limit the search, for example: **contains**, **does not contain**, **starts with**, et cetera.
- In the text box on the right, enter or select the criteria you want to search for.
- If you want to use more search criteria, click the plus sign icon and enter the appropriate criteria. Returned results will match all the search criteria you enter.

3 Click **Search**.

A list of users that fit the criteria you specified appears.

To clear the search, click the cancel button to the left of the search field.

35 Managing Administrator Accounts

This chapter describes how to create administrators for your PGP Universal Server.

You can configure Administrator options from the Users>Administrators card.

Topics in this section include:

Overview

You can have as many administrators as you want for each PGP Universal Server, and those administrators can be configured in any of five roles, each role having a fixed set of privileges attached to it.

During the Setup Assistant, one administrator must be created. This administrator is automatically created with the highest level of privileges, called SuperUser. Other administrators, created by the first SuperUser administrator, can also be SuperUser administrators or they can have fewer privileges.

Once administrators are configured, they can log in and have access to only those functions they are entitled to based on their role. Administrators who do not have all privileges will be able to see everything in the administrative interface, but those functions they cannot affect will be disabled.

Any administrator can receive a daily status email sent from the PGP Universal Server. You can also have the PGP Universal Server send a status email at any time.

There are six preconfigured administrator roles (from fewest privileges to most privileges):

- **Read-Only Administrator**. Can view all settings and logs.
- **WDRT-only Administrator**. Can view all settings and logs, and can access and read Whole Disk Recovery Tokens.
- **Service Control Only**. Can view all settings and logs, and can start and stop software and hardware services but not configure them.

- **Basic Administrator**. Can view all settings and logs, control and configure services, access and read Whole Disk Recovery Tokens, configure system settings, install updates, restore backups, manage messaging policies, manage users and their public keys, and can vet users.
- **Full Administrator**. Can view all settings and logs, control and configure services, access and read Whole Disk Recovery Tokens, configure system settings, install updates, restore backups, manage messaging policies, manage users and their public keys, vet users, configure clustering, export user private keys, and manage organization, trusted, ignition, and Additional Decryption Keys (ADKs).
- **SuperUser**. Can view all settings and logs, control and configure services, access and read Whole Disk Recovery Tokens, configure system settings, install updates, restore backups, manage messaging policies, manage users and their public keys, vet users, configure clustering, export user private keys, and manage organization, trusted, ignition, and ADKs, access the PGP Universal Server via SSH, and create and manage other administrators.

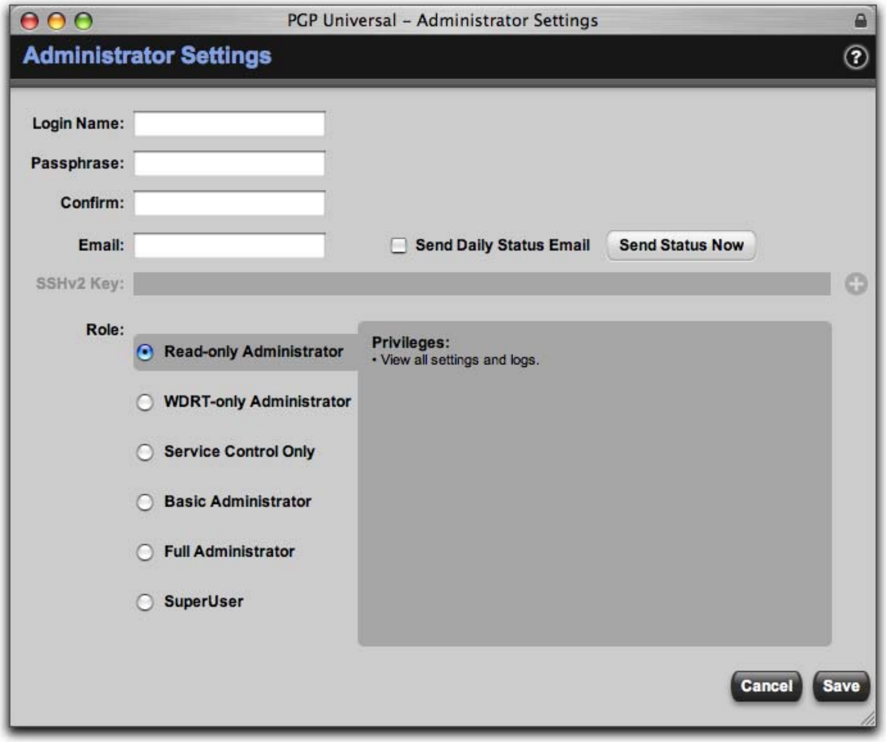
Using the Administrators card, you can create a new administrator, delete one or more administrators, sort the configured administrators listed on the Administrators card, view the settings of configured administrators, change their passphrases, and upload or remove the SSH v2 keys of SuperUser administrators.

Creating a New Administrator

To add a new administrator:

1 From the Users>Administrators card. click **Add Administrator**.

The Administrator Settings dialog appears.



Role: ● Read-only Administrator

Privileges:
• View all settings and logs.

2 In the **Login Name** field, enter a login name for the new administrator.

3 In the **Passphrase** field, enter a passphrase for this administrator.

4 In the **Confirm** field, enter the same passphrase again.

5 In the **Email** field, enter the email address of the new administrator.

6 Select the **Daily Status Email** checkbox if you want the new administrator to receive a daily status email for your system.

7 From the **Role** list, select the role for the new administrator.

8 The privileges for the selected role appear.

9 Click **Save**.

The new administrator is added.

Importing SSH v2 Keys

SuperUser administrators have the option of adding their SSH v2 key to the PGP Universal Server. The SSH v2 key acts as an authentication token and allows SuperUser administrators to access the command line of the PGP Universal Server by logging in with the username root.

> ⚠ Accessing the PGP Universal Server command line in this way may void portions of your PGP Support agreement. Contact PGP Support for more information.

To import an SSH v2 key:

1 Click the plus icon at the end of the **SSHv2 Key** field on the Administrator Settings dialog.

The Update SSH Public Key dialog appears.

2 Import the SSH v2 key file either by selecting a key file via the **Choose File** button or by pasting the SSH v2 public key block into the **Import Key Block** box.

3 Click **Import**.

The SSH key is imported.

Deleting Administrators

To delete one administrator:

1 From the Users>Administrators card, click the icon in the Delete column of the administrator you want to delete. Administrators cannot delete themselves.

A confirmation dialog appears.

2 Click **OK**.

The name of the deleted administrator is removed from the list.

To delete multiple administrators:

1 Specify the administrators you want to delete by selecting the appropriate check boxes on the far right side of each administrator's name.

2 Select **Delete Selected** from the Options menu on the bottom right corner of the Administrators card.

3 To delete all administrators, select **Delete All** from the Options menu.

A confirmation dialog appears.

4 Click **OK**.

The selected administrators are deleted from the list.

Inspecting and Changing the Settings of an Administrator

To inspect or change the settings of a configured administrator:

1. On the Administrators card, click the name of the administrator whose settings you wish to view.

   The Administrator Settings dialog appears.

2. You can enter a new email address, activate the daily status email, send an immediate status email, add an SSH v2 key if you have SuperUser status, or change the passphrase. You can also change other administrators' roles, but you cannot change your own role.

3. To change your own passphrase, click **Change Passphrase**, enter the current passphrase, enter a new passphrase, confirm the new passphrase, then click **Save**.

4. To change another administrator's passphrase, click **Reset Passphrase**, enter and confirm the new passphrase, and click **Save**.

5. Click **Save**.

   The Administrator Settings dialog disappears.

Daily Status Email

Any administrator can receive a daily or immediate status email.

To send an administrator the daily status email, from the Administrator Settings dialog select **Send Daily Status Email**. To send a status report now, click the **Send Status Now** button.

The status email provides information about the following:

- Software version number.
- Length of time the PGP Universal Server has been running.
- Warnings. For example, that there is a software update available.
- Data backup failures.
- Security. For example, failed administration login attempts and excessive PGP Universal Web Messenger login failures.
- Statistics. For example, viruses found, messages processed, encrypted, decrypted, in queue, and pending email address exclusions.
- License status.
- Organization Certificate status.
- Disk and CPU usage.

36 PGP Universal Satellite

This chapter describes PGP Universal Satellite.

PGP Universal Satellite is available for both Windows and Mac OS X systems. This chapter describes those aspects of PGP Universal Satellite that are common to both.

For information about the Windows version, refer to Chapter 38, "PGP Universal Satellite for Windows". For information specific to the Mac OS X version, refer to Chapter 37, "PGP Universal Satellite for Mac OS X".

Topics in this chapter include:

Overview

PGP Universal Satellite serves several important purposes:

- For internal users (email users in a domain being managed by a PGP Universal Server), it provides PGP security for messages all the way to their computer.
- For external users (email users external to an organization's PGP Universal Server), it is one way for them to become part of the Self-Managing Security Architecture (SMSA). It also provides security for email messages all the way to their computer and it allows them to use their favorite email client for sending and receiving PGP Universal Server messages.
- For both kinds of users, it gives them the option to create and manage their keys on their own computer, if allowed by the PGP Universal Server administrator.

> ! PGP Universal Satellite cannot be installed on a system with PGP Desktop 9.0 or greater. Beginning with PGP Desktop 9.0, PGP Universal Satellite functionality is built into PGP Desktop.

PGP Universal Satellite installation requires no input on the part of the person installing it. Once installed, PGP Universal Satellite gets its policy settings from a PGP Universal Server. **PGP Universal Satellite does not do anything to outbound email without a policy from a PGP Universal Server.**

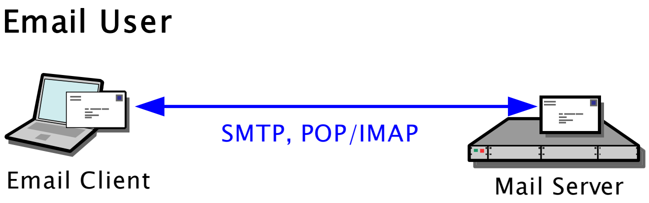
PGP Universal Satellite proxies SMTP traffic when the user sends email messages and POP and IMAP traffic when they retrieve email messages from their mail server.

PGP Universal Satellite also manages all sending and receiving of email via the MAPI protocol in an Exchange Server environment and via the Lotus Notes email client in a Domino Server environment.

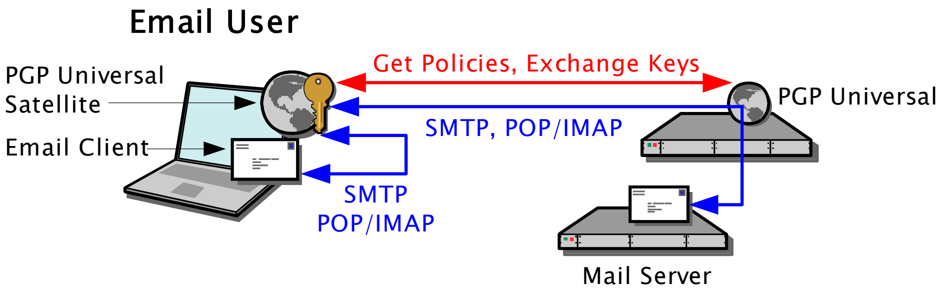
Connectivity to the PGP Universal Server on port 443 (HTTPS) is required for proper operation, in addition to the normal email protocols for internal non-MAPI users.

Technical Information

Before the PGP Universal Satellite software is installed on the email user's computer, their email client communicates with its associated mail server using SMTP to send email and POP or IMAP to retrieve email.



When installed, PGP Universal Satellite inserts itself into this process. It monitors the email traffic of the user and proxies their SMTP and POP or IMAP traffic, adding security (encrypting, decrypting, verifying, and signing) according to the policies it receives from its associated PGP Universal Server. It also gets policies and exchanges keys with the server over a link secured via SOAP/TLS.



Distributing the PGP Universal Satellite Software

PGP Universal Server supports the use of Microsoft Installer (.msi) package files for deploying and upgrading PGP Universal Satellite to your internal users (an executable is provided for external users).

The appropriate files are supplied on the PGP Universal Server documentation CD.

To deploy PGP Universal Satellite to internal users via the supplied MSI files:

1. Rename the installer to “PGPuniv.msi.”
2. Distribute the updater to your internal users and have them run it on their systems.

   This is often accomplished via mass software distribution utilities such as Microsoft SMS. If you do not intend to use this functionality, you should distribute the EXE versions of the installer instead.

   If your internal users do not have the Microsoft Windows Installer technology installed, they will need upgrade their system first, then run the updater.

To update PGP Universal Satellite using MSI files:

1. Make sure the filename of the updater is “PGPuniv.msi.”
2. Distribute “PGPuniv.msi” to your PGP Universal Satellite users.
3. Have them install it on their systems.

Configuration

How PGP Universal Satellite adds security to email traffic is based on two factors:

- the **deployment mode**, determined by the relationship of PGP Universal Satellite to the managed domain
- the **key mode**, chosen by the PGP Universal Satellite user from the allowed key modes set on the PGP Universal Server

Deployment Mode

There are two deployment modes for PGP Universal Satellite:

- **Internal:** PGP Universal Satellite is installed on the computer of an internal user, someone who is in an email domain being managed by a PGP Universal Server. PGP Universal Satellite gets its policies from the local PGP Universal Server, which can be placed internally or externally.

  In the case where an internal PGP Universal Satellite user is accessing a PGP Universal Server placed externally, PGP Universal Satellite cannot automatically determine what PGP Universal Server it should get its policy from. This information must be provided for it, a process called binding. Refer to "Binding" on page 317 for more information about binding a mail server to a PGP Universal Server in a PGP Universal Satellite policy.

- **External:** PGP Universal Satellite is installed on the computer of an external user, someone who is outside of the email domain being managed by a PGP Universal Server. PGP Universal Satellite gets its policies from a PGP Universal Server in the managed domain. This is the same PGP Universal Server that sent the Smart Trailer or PGP Universal Web Messenger message.

  It does not matter if the PGP Universal Server in the managed domain is placed internally or externally, as long as it is accessible to the external PGP Universal Satellite via HTTPS on port 443.

Key Mode

PGP Universal Satellite also works differently depending on the key mode associated with an applicable policy (one installation of PGP Universal Satellite can potentially have multiple key modes, one for each policy):

- In **Client Key Mode (CKM)**, all cryptographic operations are done by the computer on which PGP Universal Satellite is installed. The private key stays on the computer; the computer also handles all private key management.

- In **Guarded Key Mode (GKM)**, is the same as CKM, with one difference: an encrypted copy of the private key is stored on the PGP Universal Server (encrypted to the user's passphrase). The PGP Universal Server administrator cannot use the stored private key in GKM. GKM is useful if a key is accidentally deleted or if the user needs to access their key and policy from a different computer: the private key will be provided when needed from the PGP Universal Server. The user will need to use the same passphrase for the key from any system where this mobile key is used.

- In **Server Key Mode (SKM)**, all cryptographic operations are done by the computer on which PGP Universal Satellite is installed (with the exception of key generation); the PGP Universal Server temporarily sends the private key to PGP Universal Satellite via SOAP/TLS. The private key is stored only on the PGP Universal Server, and the PGP Universal Server handles all private key management. With SKM, the PGP Universal Server administrator has complete access to the private key material and can thus access all messages encrypted by the PGP Universal Satellite user.

If you are in an S/MIME environment and require ADK-like key recovery capabilities, you must operate S/MIME in SKM.

- In **Server Client Key Mode (SCKM)**, all cryptographic operations are done by the computer on which PGP Universal Satellite is installed. Additionally, an unencrypted copy of the encryption subkey is stored on the PGP Universal Server, while the signing subkey is held only on the computer on which PGP Universal Satellite is installed. All other key management is also handled by the user's computer. This mode ensures compliance with laws and corporate policies that require that signing keys not leave the control of the user while making sure that encryption keys are stored in case of emergency. SCKM requires a key with a separate signing subkey, which can be created for a new key with PGP Desktop or PGP Universal Satellite 9.5 or greater or added to an older PGP key using PGP Desktop 9.5 or greater.

Key modes are independently selectable for both the Internal User Policy (Internal User Policy > Policy Options: Default > Key Setup > Management tab) and the External User Policy (External User Policy > Policy Options > Key Management tab). PGP Universal Satellite users can select from any allowed mode.

To disable key generation, do not select any key mode.

Satellite Configurations

Putting these two concepts together — the deployment mode and the key mode — gives us six possible configurations for PGP Universal Satellite:

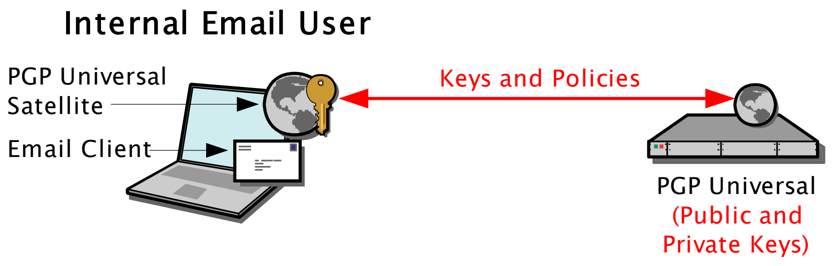
- Internal user, Server Key Mode (called Internal SKM)
- Internal user, Client Key Mode (called Internal CKM)
- Internal user, Server-Client Key Mode (called Internal SCKM)
- External user, Server Key Mode (called External SKM)
- External user, Client Key Mode (called External CKM)
- External user, Server-Client Key Mode (called External SCKM)

For the purposes of understanding PGP Universal Satellite configurations, CKM and GKM work the same way.

All Satellite configurations are described below.

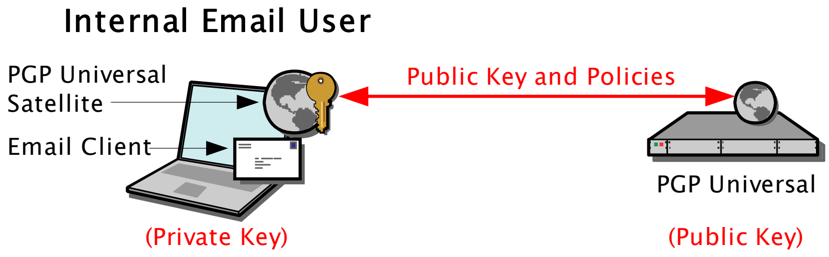
Internal SKM

Internal SKM requires the least effort on the part of the email user. After installation, PGP Universal Satellite automatically gets its policies from the local PGP Universal Server when the email user sends or retrieves mail. Because the PGP Universal Server is managing the keypair, the user doesn't have to do any configuration of PGP Universal Satellite.



Internal CKM

Some configuration is required by the email user with Internal CKM because they have the option of managing their key on their own computer.



When PGP Universal Satellite retrieves a policy that includes the option to manage its key locally, it displays the Satellite Key Setup Assistant, which asks the user to choose an allowed key mode, then to select a key source, if applicable.

The private key will stay on the email user's computer and *not* be sent to the PGP Universal Server. A technical exception to this rule is the ability to synchronize the key with the PGP Universal Server (Guarded Key Mode), which stores an encrypted, passphrase-protected version of the private key on the PGP Universal Server; the key is sent to the PGP Universal Server, but it is encrypted and passphrase-protected, so the PGP Universal Server can't do anything with it. The advantage to Guarded Key Mode is that the encrypted private key remains available to the user as they move between computers or between home and work, for example.

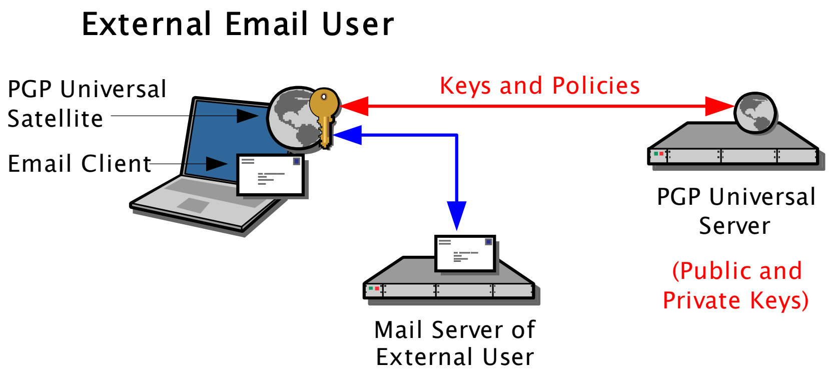
Internal SCKM

Internal SCKM allows internal users to manage their own key on their system, with a copy of the encryption subkey saved on their PGP Universal Server, allowing encrypted messages sent by the client to be decrypted at a later time if the user is unable or unwilling to decrypt them.

SCKM requires a key with a separate signing subkey, which can be created for a new key with PGP Desktop or PGP Universal Satellite 9.5 or greater or added to an older PGP key using PGP Desktop 9.5 or greater.

External SKM

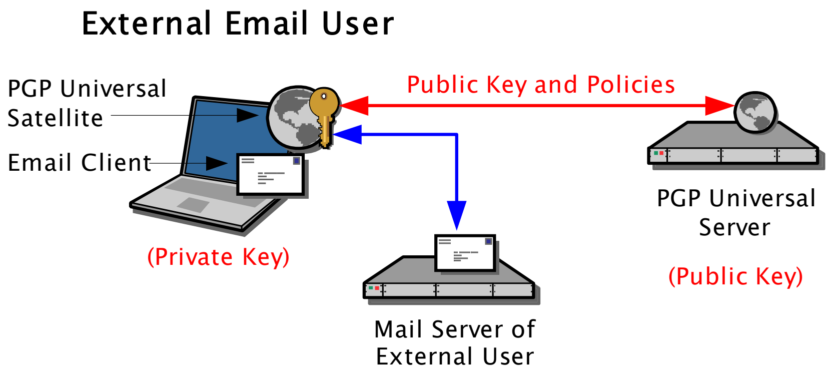
In External SKM, the email user will be joining the SMSA via a Smart Trailer or PGP Universal Web Messenger message. When they respond to the message, they will be asked to establish a passphrase to secure future messages. Next, they will choose a method of delivery for future messages from the managed email domain: PGP Universal Web Messenger, PGP Universal Satellite, or using an existing PGP Desktop key.



When they select the PGP Universal Satellite option, the PGP Universal Satellite installer will be downloaded to their computer. After installation, PGP Universal Satellite will automatically contact the PGP Universal Server that sent the Smart Trailer or PGP Universal Web Messenger message and download its policies. The key for this user will be created on and managed by the PGP Universal Server.

External CKM

External CKM users go through the same process as External SKM users except that instead of the PGP Universal Server automatically creating and managing a key for them, the user is given the options available through the Satellite Key Setup Assistant: first to choose an allowed key mode, then to specify the key to use.



The private key will stay on the email user's computer and *not* be sent to the PGP Universal Server. A technical exception to this rule is the ability to synchronize the key with the PGP Universal Server (Guarded Key Mode), which stores an encrypted, passphrase-protected version of the private key on the PGP Universal Server; the key is sent to the PGP Universal Server, but it is encrypted and passphrase-protected, so the PGP Universal Server cannot do anything with it. The advantage to Guarded Key Mode is that the encrypted private key remains available to the user as they move between computers or between home and work, for example.

External SCKM

External SCKM users will also be joining the SMSA via a Smart Trailer or PGP Universal Web Messenger message. Once PGP Universal Satellite is installed and the user selects the SCKM option, their encryption subkey will be copied to their PGP Universal Server, allowing encrypted messages to be decrypted if the user is unwilling or unable to decrypt them.

SCKM requires a key with a separate signing subkey, which can be created for a new key with PGP Desktop 9.5 or greater or added to an older key using PGP Desktop 9.5 or greater.

Switching Key Modes

It is possible to switch key modes:

1. In PGP Universal Satellite, click **Clear**.

   The next time PGP Universal Satellite needs the key of the user, the Satellite Key Setup Assistant will appear.

2. The PGP Universal Satellite user will be prompted to choose an allowed key mode and then to select a key source, if applicable.

   When the Satellite Key Setup Assistant is complete, the key mode has been switched.

Binding

To send and receive protected email, PGP Universal Satellite must be able to access a mail server to send and receive mail and a PGP Universal Server to get keys and policies.

In many cases, PGP Universal Satellite determines how to communicate with the appropriate mail server and PGP Universal Server automatically. There are two scenarios where it cannot do this automatically, however. In these cases, this information must be provided to it.

Make sure not to bind a mail server to a PGP Universal Server except for the two cases described below. If this is done, the PGP Universal Satellite user will not be able to send or receive email.

The two cases are:

- **Internal MAPI or Lotus Notes client running PGP Universal Satellite:** In a Microsoft Exchange or Domino Server environment, the PGP Universal Server is prohibited from being between the internal email client and the Exchange or Domino Server in the logical flow of data. In this situation, the PGP Universal Satellite can automatically determine its mail server (the Exchange or Domino Server), but it *cannot* automatically determine its PGP Universal Server; that information must be provided to it.

  MAPI and Lotus Notes email clients are only supported in the Windows version of PGP Universal Satellite.

- **Internal PGP Universal Satellite user accessing a PGP Universal Server in External Mode:** Same problem with this configuration. By definition, the PGP Universal Server is between the mail server and the Internet, thus making it impossible for the PGP Universal Satellite to automatically determine its PGP Universal Server. It must be told which PGP Universal Server to use.

> If PGP Universal Satellite is installed in either of the two cases described above and the mail server is **not** bound to a PGP Universal Server, and the end user then sends an email message outside of their email domain, the PGP Universal Server will create Server Key Mode keys for that user. The user will not have the option of other key modes (if allowed by policy). The user will also not be able to retrieve keys or policies until the mail server is bound to a PGP Universal Server in a PGP Universal Satellite policy.

There are two ways of "binding" a mail server and a PGP Universal Server in a PGP Universal Satellite policy: pre-binding and manual binding.

Pre-Binding

With pre-binding, you configure the PGP Universal Satellite installer with the PGP Universal Server and the mail server *before* the installer is downloaded and distributed to the end users. So with pre-binding, the installer comes to the end user with the correct information already configured in it.

To pre-bind a PGP Universal Satellite installer:

1. On the administrative interface of a PGP Universal Server, navigate to the Policy tab**.**
2. On the Internal Users Policy card, click **Download Client**.

   The Download PGP Clients dialog appears.
3. In the **Client** field, select **PGP Universal Satellite**.
4. In the **Platform** field, select **Windows** or **Mac OS X**, as appropriate.
5. Enable the **Customize** option.
6. In the **PGP Universal Server** field, enter the name of the appropriate PGP Universal Server.

   The name of the PGP Universal Server you are currently using is inserted by default.

7 In the **Mail Server Binding** field, enter the name of the mail server you want bound to the PGP Universal Server listed above for the PGP Universal Satellite installer you are creating. You can use wildcards.

If you are creating a binding for an internal MAPI email client, you **must** use the WINS name of the Exchange Server.

If you are creating a binding for an internal Lotus Notes email client, you **must** use the fully qualified domain name of the Domino server.

8 Click **Download**.

The PGP Universal Satellite installer is created with the information you supplied and downloaded.

9 Distribute the installer you just created to the appropriate end users and have them install it.

The policy with the binding information you specified will be created.

10 Have the end user send an email message; it can be to anyone.

The PGP Universal Server will automatically send an enrollment email message to the end user.

11 Have the end user open the message from the PGP Universal Server.

If the policy of the PGP Universal Server allows any of the client-managed key modes (CKM, GKM, or SCKM), the Satellite user will be prompted to configure a key, after which they can begin sending email securely.

If the policy of the PGP Universal Server does not allow Client Key Mode, the end user is done and can begin sending email securely.

Manual Binding

With manual binding, PGP Universal Satellite is first installed on the system of the end user, then a policy that includes the appropriate mail server and PGP Universal Server is created.

To manually bind a mail server and a PGP Universal Server in a policy:

1 Distribute a PGP Universal Satellite installer to the appropriate end users and have them install it on their systems.

2 After PGP Universal Satellite is installed, have the end user open the **Policy** tab of the PGP Universal Satellite user interface.

3 Click the **Add** button.

4 Add a policy for the appropriate PGP Universal Server.

5 Once the PGP Universal Server Policy is complete, create a policy for a Mail Server.

6 In the **Server** field, enter the name of the appropriate mail server.

If you are creating a binding for an internal MAPI email client, you **must** use the WINS name of the Exchange Server.

If you are creating a binding for an internal Lotus Notes email client, you **must** use the fully qualified domain name of the Domino server.

7. From the **Binding** drop-down list, select the PGP Universal Server you just added.
8. Close the PGP Universal Satellite user interface.
9. Have the end user send an email message; it can be to anyone.

   The PGP Universal Server will automatically send an enrollment email message to the end user.
10. Have the end user open the message they receive from the PGP Universal Server.

    If the policy of the PGP Universal Server allows Client Key Mode, the end user will be prompted to create a key. After they have created the key, they can begin sending email securely.

    If the policy of the PGP Universal Server does not allow Client Key Mode, the end user is done and can begin sending email securely.

Policy and Key or Certificate Retrieval

Because accidents happen, PGP Universal Server includes built-in support to assist PGP Universal Satellite users to retrieve lost policies and keys or certificates.

A policy could be lost if it is accidentally removed or if the computer hosting the policy stops working. A key or certificate could be lost because it has been cleared from a policy or the computer hosting the key or certificate stops working. For our purposes a "lost" policy or key/certificate is one that once existed but that is no longer available, for whatever reason.

If both a policy and a key/certificate are no longer available (if the computer hosting them stops working, for example), then the policy should be retrieved first, followed by the key/certificate.

Retrieving Lost Policies

The method used to retrieve a lost policy is different based on whether the PGP Universal Satellite user was in Internal or External Deployment Mode and whether you need to retrieve just the policy or the PGP Universal Satellite software and the policy.

Internal Deployment Mode

In Internal Deployment Mode, the PGP Universal Satellite software is installed on the computer of an internal user, a user who is in an email domain being managed by a PGP Universal Server. In this case, Satellite gets its policies from that local PGP Universal Server.

Need Policy Only

A PGP Universal Satellite user in Internal Deployment Mode who has lost their policy but still has Satellite software installed needs only to send or receive an email message and the missing policy will automatically be retrieved.

Need Satellite Software and Policy

A PGP Universal Satellite user in Internal Deployment Mode who has lost both their PGP Universal Satellite software and their policy needs to first reinstall the PGP Universal Satellite software and then retrieve their policies.

To reinstall PGP Universal Satellite software in Internal Deployment Mode:

1. Contact your PGP Universal Server administrator.
2. Follow instructions to retrieve the PGP Universal Satellite installer.
3. Install PGP Universal Satellite onto their computer.

To retrieve policies in Internal Deployment Mode:

1. Send or receive an email message.

   The appropriate policy is retrieved from the PGP Universal Server.

External Deployment Mode

In External Deployment Mode, the PGP Universal Satellite software is installed on the computer of an external user, a user who is not in an email domain being managed by a PGP Universal Server. In this case, PGP Universal Satellite gets its policies from the PGP Universal Server from which it received the PGP Universal Satellite software via a Smart Trailer or PGP Universal Web Messenger message.

Need Policy Only

A PGP Universal Satellite user in External Deployment Mode who has lost their policy but still has the PGP Universal Satellite software installed needs to retrieve the lost policy from the PGP Universal Server.

To retrieve a lost policy in External Deployment Mode:

- Log in to the PGP Universal Server that you originally got PGP Universal Satellite from by pointing your Web browser at **https://keys.domain.com** (where domain.com is the domain they originally got PGP Universal Satellite from, enter their passphrase, re-select PGP Universal Satellite as your delivery option, and click Choose Option. The ActiveX control will determine that you already have PGP Universal Satellite installed but don't have a policy, so it will download your policy for you.
- Access the PGP Universal Satellite user interface, create a new external policy (use the URL and email address that were part of the lost policy), and then click **Retrieve Policy**. The lost policy will be retrieved from the server.

Need Satellite Software and Policy

A PGP Universal Satellite user in External Deployment Mode who has lost both their Satellite software and their policy needs to both reinstall the Satellite software and retrieve the lost policy.

To reinstall Satellite software and retrieve a lost policy without the original Satellite installer:

1. Open a Web browser and access the Web interface of the PGP Universal Server from which they received the original PGP Universal Satellite installer.

   Use the URL **https://keys.<domain>**.

2. Log on to the PGP Universal Server using the passphrase that was established when you first downloaded the PGP Universal Satellite software.

3. Re-select **PGP Universal Satellite** as your delivery option and click **Choose Option**.

   The ActiveX control will determine that you do not have PGP Universal Satellite installed nor do you have a policy, so it will download and install both PGP Universal Satellite and your policy for you.

Retrieving Lost Keys or Certificates

The method of retrieving a lost key or certificate depends on the key mode of the user.

This section covers only retrieving lost keys/certificates. If you also need to retrieve the PGP Universal Satellite software and/or a policy, refer to "Retrieving Lost Policies" on page 320 for instructions. When the PGP Universal Satellite software and policy are in place, return to this section for key/certificate retrieval instructions.

SKM

In SKM, the private key/certificate is stored only on the server, and the server handles all private key management.

If a key/certificate is lost from a policy in SKM, because it resides on the server and not on the computer hosting the PGP Universal Satellite software, it will automatically be retrieved the next time an email message is sent or received. No action is required by the user to retrieve the key/certificate.

CKM and GKM

In CKM, the private key/certificate stays on the user's computer; it is only transmitted to the PGP Universal Server if the user chooses to store it there encrypted, which is GKM.

If a key or certificate is lost from a policy in CKM, PGP Universal Satellite will attempt to locate the key/certificate the next time it is needed. If the user synchronized their key/certificate with the server (GKM), the key/certificate will be retrieved at this point.

If PGP Universal Satellite cannot locate the key/certificate, or if the key/certificate has been manually cleared from the policy, PGP Universal Satellite will display the Key Wizard, which gives the user the option of importing the key/certificate from an exported file or reinitializing the account.

To import a private key/certificate from an exported file:

1 On the Key Source Selection screen, select **Import Key** and click **Next**.

2 Locate and select the ASC file that includes the appropriate key or certificate, then click **Import**.

The key is retrieved.

If a private key/certificate is permanently unretrievable, you should reinitialize the account so that the user will not continue to receive messages they cannot decrypt. Another reason you might want to reinitialize an account is if the private key/certificate has been compromised.

To reinitialize an account where the key has been lost:

1 On the Key Source Selection screen, select **Reinitialize Account** and click **Next**.

You are prompted for a key or certificate for the new account.

2 Select from create a new key/certificate, create a managed key/certificate (that is, Server Key Mode), or import a different, previously exported key or certificate. Make your selection and click **Next**.

The account is reinitialized.

To reinitialize an account where the key has been compromised, have the user click the Clear button. This will clear the compromised key from the account. When PGP Universal Satellite next needs the key, the Satellite Key Setup Assistant will appear and ask the Satellite user to set up a new key.

37 PGP Universal Satellite for Mac OS X

This chapter describes those aspects of the PGP Universal Satellite software that are specific to the Mac OS X version.

For general information about PGP Universal Satellite, refer to Chapter 36, "PGP Universal Satellite". For information specific to the Windows version, refer to Chapter 38, "PGP Universal Satellite for Windows".

Topics include:

Overview

PGP Universal Satellite for Mac OS X proxies SMTP traffic when the user is sending email messages and POP and IMAP traffic when the user is retrieving email messages from their mail server.

PGP Universal Satellite for Mac OS X runs on systems with Mac OS X 10.4 or greater. It has been tested with the following email clients:

- Apple Mail
- Microsoft Entourage
- Qualcomm Eudora

It should work without problems with any Internet-standards-based email client that runs on Mac OS X 10.4 or greater.

PGP Universal Satellite requires a PGP Universal Server; it provides no functionality at all without a policy from an associated PGP Universal Server.

System Requirements

Minimum system requirements for PGP Universal Satellite for Mac OS X are:

- Mac OS X 10.4 or greater
- 128 MB physical RAM
- 20 MB hard disk space

Obtaining the Installer

Internal users (email users in a domain being managed by a PGP Universal Server) should get the PGP Universal Satellite installer from their PGP Universal Server administrator (the PGP Universal Satellite installer is included on the PGP Universal Server CD and is downloadable from the PGP Universal Server's administrative interface). After installation, PGP Universal Satellite for Mac OS X communicates with the local PGP Universal Server to get its policies.

External users (email users external to an organization's PGP Universal Server) get access to the PGP Universal Satellite installer via a link in an email message from an internal user that includes a Smart Trailer or when they retrieve a message sent using PGP Universal Web Messenger mail (refer to Chapter 16, "Applying Key Not Found Settings to External Users" for more information). After installation, PGP Universal Satellite will access a URL to automatically download its policies from the appropriate PGP Universal Server.

Installation

PGP Universal Satellite for Mac OS X *cannot* be installed on a system with PGP Desktop. If you currently have PGP Desktop on your system, do not install PGP Universal Satellite for Mac OS X. If you are using a version of PGP Desktop prior to 9.0, you should upgrade. If you are using 9.0 or greater of PGP Desktop, you can configure PGP Desktop to do everything PGP Universal Satellite for Mac OS X does for you. See your PGP administrator for more information.

To install PGP Universal Satellite for Mac OS X:

1. Download the PGP Universal Satellite for Mac OS X installation file onto the computer.

   The file that is downloaded is **pgpuniversal.tar.gz**. Most Mac OS X systems should automatically extract the actual installer, PGP Universal Server.pkg.

   If this does not happen automatically, you can extract the installer using Stuffit Expander or with Terminal using the command:
   tar -xzf pgpuniversal.tar.gz.

2. Quit any open programs.

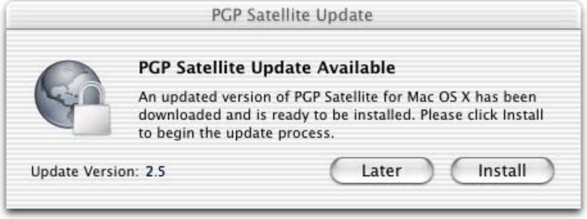
3 Double click the installer (**PGP Universal Server.pkg**).

4 Follow the on-screen instructions.

Updates

When the PGP Universal Server with which PGP Universal Satellite communicates receives an updated version of the PGP Universal Satellite software, it notifies PGP Universal Satellite of this the next time they communicate.

The PGP Universal Server Automatic Update screen displays automatically on the computer on which PGP Universal Satellite is installed.



PGP Satellite Update Available

An updated version of PGP Satellite for Mac OS X has been downloaded and is ready to be installed. Please click Install to begin the update process.

Update Version: 2.5

Once the installer application is downloaded, it can be installed in the same manner as described in "Installation" on page 325.

Files

PGP Universal Satellite both installs files onto the user's system and creates files when it is used.

The following files are installed onto the user's system during installation:

- /Library/Application Support/PGP/pgpdivert
- /Library/Application Support/PGP/pgpipfwtool.pl
- /Applications/PGP Universal Server.app

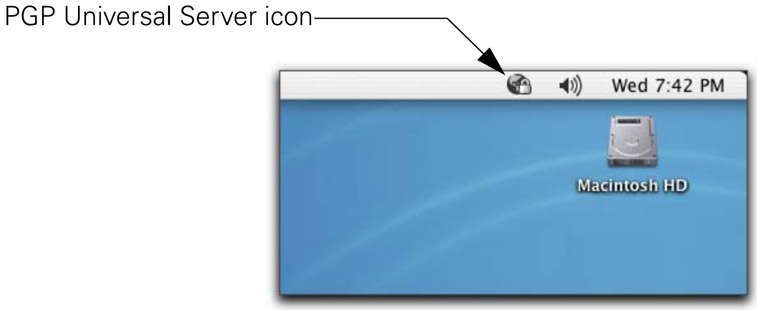
The following files are created when the user runs PGP Universal Satellite for Mac OS X:

- ~/Library/Preferences/com.pgp.universal.plist
- ~/Documents/PGP Universal Server/PGP Public Keyring.pkr
- ~/Documents/PGP Universal Server/PGP Private Keyring.skr
- ~/Library/Logs/PGP/PGPEngine*.log

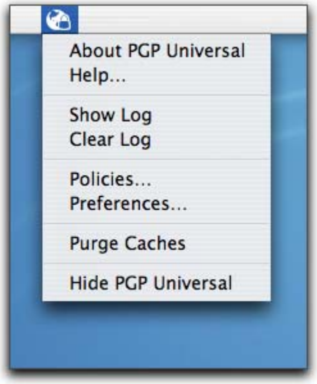
If your users are managing their own keys, PGP Corporation recommends backing up the keyring files (PGP Public Keyring.pkr and PGP Private Keyring.skr).

User Interface

PGP Universal Satellite has a minimal user interface. All functionality can be accessed via the PGP Universal Server icon in the Menu Bar.



Pull down the PGP Universal Server icon to display the PGP Universal Server menu.



Each of the commands on the PGP Universal Server menu are described below.

About PGP Universal Server

Selecting the About PGP Universal Server command displays the About PGP Universal Satellite screen.

This screen displays both the names of the people who helped to create PGP Universal Satellite and the version of PGP Universal Satellite being used.

You can also uninstall PGP Universal Satellite from the About PGP Universal Satellite screen.

To uninstall PGP Universal Satellite:

1 On the About PGP Universal Satellite screen, click **Uninstall**.

  A confirmation screen appears.

2 Click **OK**.

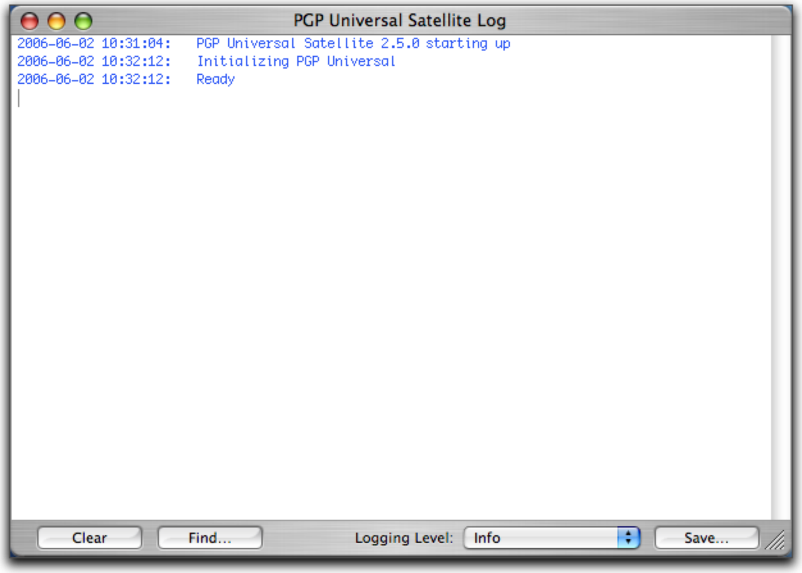
  PGP Universal Satellite is removed from your Mac OS X system.

Help

Selecting the Help command displays the PGP Universal Satellite for Mac OS X online help.

Show Log

Selecting the Show Log command displays the PGP Universal Satellite Log screen.



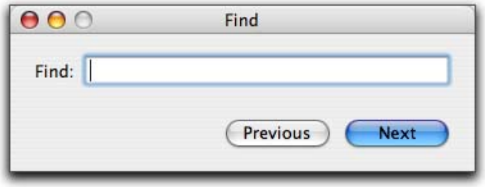
```
2006-06-02 10:31:04:    PGP Universal Satellite 2.5.0 starting up
2006-06-02 10:32:12:    Initializing PGP Universal
2006-06-02 10:32:12:    Ready
```

Logging Level: Info

The Log screen displays an entry for each action that PGP Universal Satellite takes. Each entry is date and time stamped.

In addition to viewing the log entries on the Log screen, you can select from the following options:

- **Clear**: Clears all entries from the log.
- **Find**: Displays the Find screen so that you can search for text in the log entries.



- **Logging Level**: Choose Info (the default) or Verbose. Note that Verbose logging can generate very large log files.
- **Save**: Lets you save the log to a file (if the checkbox Save as Rich Text (RTF) is checked, the file will be saved as an RTF file and retain its formatting; if the check box is unchecked, the log file will be saved as a text file and will lose all formatting).

Clear Log

The Clear Log command clears all entries from the log.

Policies

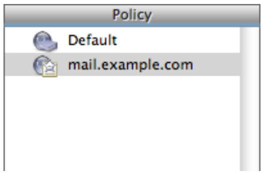
The Policies command displays the PGP Universal Server Policy screen, which lets you control the policy settings that apply to PGP Universal Satellite.

PGP Universal Satellite automatically manages your policy settings for you. Typically, there is no reason to modify the settings on this screen. Consult your PGP Universal Server administrator before making any changes.

Policy Section

The Policy section contains the following fields and buttons:

- **Policy list**: Shows the existing policies and the list of managed domains for each policy. Click on a policy to see its settings.



- **Add**: Lets you add a policy manually. Click the plus sign (**+**) button and then select the appropriate settings in the Server and/or Key sections.
- **Remove**: Click the minus sign (**–**) button to delete the selected policy.

Key Section

The Key section includes the Key box and three buttons: Change Passphrase, Clear Key, and Import.

The Key box displays information about the PGP key being used by the policy selected in the Policy list, if applicable. The information found on this screen includes: identification of the user (their name and email address), the key ID, type, size, creation date, expiration date, cipher, and fingerprint.

> Users can manage their key properties only if permitted by the PGP Universal Server administrator.

The three buttons in the Key section are:

- **Change Passphrase**: To change the passphrase for the key, click **Change Passphrase**, enter the existing passphrase for the key followed by the new passphrase, enter the new passphrase again, and finally click **OK**.
- **Clear Key**: Removes the key from PGP Universal Satellite.
- **Import**: To import a key, click **Import** and then locate and select the file of an exported keypair (mykey.asc, for example) on your computer. Click **Import** and a window with existing choices (keypairs) will be displayed: select the one you want to import and click **Import** again. The keypair you imported is now displayed in the Key section. You can only import keys whose private key was included when the key was exported. If the key includes only the public key portion, you cannot import it.

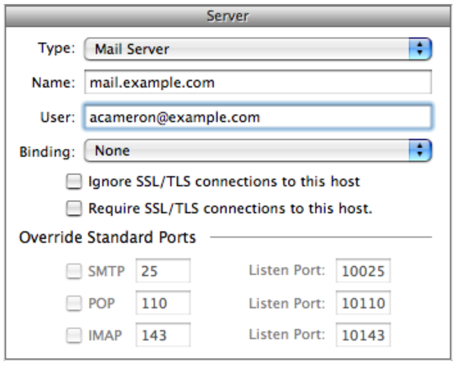
Server Section

There are three types of devices with which PGP Universal Satellite can interface. The settings available in the Server section depend on which of the three types of devices is selected:

- a standard Mail Server
- a PGP Universal Server Internal to your organization
- a PGP Universal Server External to your organization

Each of these three are described in more detail below.

Mail Server



Server

Type: Mail Server

Name: mail.example.com

User: acameron@example.com

Binding: None

□ Ignore SSL/TLS connections to this host

□ Require SSL/TLS connections to this host.

Override Standard Ports

□ SMTP	25	Listen Port:	10025
□ POP	110	Listen Port:	10110
□ IMAP	143	Listen Port:	10143

With the standard Mail Server selected, your users can change:

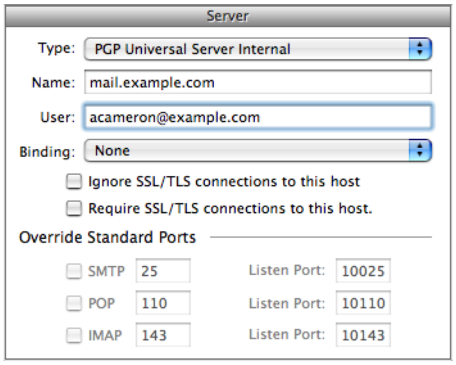
- **Name**: Shows the fully qualified domain name or IP address of the server that PGP Universal Satellite is interfacing with.
- **User**: Shows the username to which the policy applies.
- **Binding**: Binds a mail server (an Exchange Server, for example) to a PGP Universal Server.

  Make sure *not* to bind a mail server to a PGP Universal Server except for the two required cases: an internal MAPI or Lotus Notes client running PGP Universal Satellite or an internal PGP Universal Satellite user accessing a PGP Universal Server in External Mode. For more information, refer to "Binding" on page 317.
- **Ignore SSL/TLS connections to this host**: Check if you want PGP Universal Satellite to pass through and ignore data that is already encrypted by the email client using SSL/TLS.

  If SSL/TLS is being used to protect data going from the email client to the mail server, PGP Universal Satellite cannot encrypt it. If you want PGP Universal Satellite to be able to encrypt that data, you need to disable SSL/TLS in the email client.
- **Require SSL/TLS connections to this host**: Check if you want PGP Universal Satellite to require that data being sent to it be encrypted by the email client using SSL/TLS.

  If you enable this option, make sure to enable SSL/TLS in your email client, as unencrypted connections will be dropped.
- **SMTP**: This option is not available for mail servers.
- **POP**: This option is not available for mail servers.
- **IMAP**: This option is not available for mail servers.
- **Apply**: Click **Apply** to apply the selected settings.

PGP Universal Server Internal



Server

Type: PGP Universal Server Internal

Name: mail.example.com

User: acameron@example.com

Binding: None

□ Ignore SSL/TLS connections to this host

□ Require SSL/TLS connections to this host.

Override Standard Ports

□ SMTP 25 Listen Port: 10025

□ POP 110 Listen Port: 10110

□ IMAP 143 Listen Port: 10143

With PGP Universal Server Internal selected, your users can change:

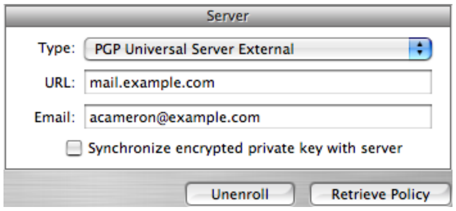
- **Name**: Shows the fully qualified domain name or IP address of the server that PGP Universal Satellite is interfacing with.

- **User**: Shows the username to which the policy applies.
- **Synchronize encrypted private key with server**: Lets Client Key Mode users store an encrypted copy of their private key on the PGP Universal Server. This is useful if a key is accidentally deleted or the user wants to access their key and the policy to which it applies from a different computer: the private key will be provided when needed, but since it is stored encrypted, the PGP Universal Server cannot do anything with it.
- **Ignore SSL/TLS connections to this host**: Check if you want PGP Universal Satellite to pass through and ignore data that is already encrypted by the email client using SSL/TLS.

  If SSL/TLS is being used to protect data going from the email client to the mail server, PGP Universal Satellite cannot encrypt it. If you want PGP Universal Satellite to be able to encrypt that data, you need to disable SSL/TLS in the email client.
- **Require SSL/TLS connections to this host**: Check if you want PGP Universal Satellite to require that data being sent to it be encrypted by the email client using SSL/TLS.

  If you enable this option, make sure to enable SSL/TLS in your email client, as unencrypted connections will be dropped.
- **SMTP**: Controls the port on which PGP Universal Satellite is listening for SMTP traffic. Standard ports for the protocol (as assigned by the IANA) are used by default. You can override the standard ports by clicking the checkbox and entering the desired port number for SMTP and its Listen Port. If the server supports SSL/TLS encryption, PGP Universal Satellite will automatically use it.
- **POP**: Controls the port on which PGP Universal Satellite is listening for POP traffic. Standard ports for the protocol (as assigned by the IANA) are used by default. You can override the standard ports by clicking the checkbox and entering the desired port number for POP and its Listen Port. If the server supports SSL/TLS encryption, PGP Universal Satellite will automatically use it.
- **IMAP**: Controls the port on which PGP Universal Satellite is listening for IMAP traffic. Standard ports for the protocol (as assigned by the IANA) are used by default. You can override the standard ports by clicking the checkbox and entering the desired port number for IMAP and its Listen Port. If the server supports SSL/TLS encryption, PGP Universal Satellite will automatically use it.
- **Apply**: Click **Apply** to apply the selected settings.

PGP Universal Server External



Type: PGP Universal Server External

URL: mail.example.com

Email: acameron@example.com

☐ Synchronize encrypted private key with server

With PGP Universal Server External selected, your users can change:

- **URL**: Shows the fully qualified domain name or IP address of the server that PGP Universal Satellite is interfacing with.
- **Email**: Shows the email address to which the policy applies.
- **Synchronize encrypted private key with server**: Lets Client Key Mode users store an encrypted copy of their private key on the PGP Universal Server. This is useful if a key is accidentally deleted or the user wants to access their key and the policy to which it applies from a different computer: the private key will be provided when needed, but since it is stored encrypted, the PGP Universal Server cannot do anything with it.
- **Unenroll**: Lets you tell the appropriate PGP Universal Server that you wish to be removed from its SMSA.
- **Retrieve Policy**: Click **Retrieve Policy** and then enter the passphrase you defined when you elected to become an external user. This passphrase is not the same one used for your key and is needed to retrieve your policy settings from the server.
- **Apply**: Click **Apply** to apply the selected settings.

Creating an External Policy

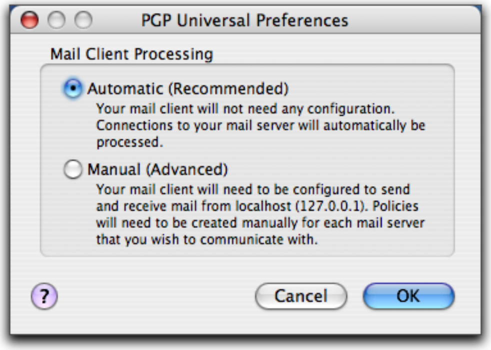
External policies are not created automatically; they must be added manually.

To manually add an external policy:

1. In the Policy section, click the plus sign (**+**) button.
2. In the Server section, pull down the **Type** menu and select **PGP Universal Server External**.
3. In the **URL** field, enter the fully qualified domain name of the external server. For example, **keys.example.com**.
4. In the **Email** field, enter your email address.
5. Click the **Retrieve Policy** button.

Preferences

The Preferences command displays the PGP Universal Server Preferences screen, which lets you control the preferences that apply to PGP Universal Satellite.



Mail Client Processing

● Automatic (Recommended)
Your mail client will not need any configuration. Connections to your mail server will automatically be processed.

○ Manual (Advanced)
Your mail client will need to be configured to send and receive mail from localhost (127.0.0.1). Policies will need to be created manually for each mail server that you wish to communicate with.

Mail Client Processing

- **Automatic**: This is the preferred configuration method. PGP Universal Satellite will automatically intercept and proxy connections from the email client to the mail server (or to the PGP Universal Server). In this mode, policies are automatically retrieved/created based on where the users are attempting to connect and the user name with which they are authenticating.
- **Manual**: This method is used for custom configurations and when required by the PGP Universal Server administrator.

  If this configuration is used, you will need to re-configure your email clients to retrieve mail from 127.0.0.1 (localhost). Additionally, you will need to create policies for the server to which you are trying to connect (keys.example.com, for example).

Purge Caches

The Purge Caches command purges PGP Universal Satellite's internal IMAP and POP message caches, the key cache, and the passphrase cache on your Mac OS X system.

PGP Universal Satellite for Mac OS X caches your passphrase as a convenience so that you don't have to enter it each time you want to sign or decrypt a message. Your passphrase is cached until the application quits, which occurs automatically on logout. Once the passphrase cache is purged, PGP Universal Satellite will require you to enter your password the next time it is needed.

> If you are operating in CKM (Client Key Mode) or using a PGP Desktop key, it is a good idea to purge your cache if you leave your computer. This will prevent someone from being able to sign/decrypt your messages while you are away.

To purge your caches:

1 Select the **Purge Caches** command from the PGP Universal Server menu.

The caches are purged.

Hide and Quit PGP Universal Satellite

The Hide PGP Universal Server command removes the PGP Universal Satellite icon from the Menu Bar, but leaves the application running. The Quit PGP Universal Server command removes the PGP Universal Satellite icon from the Menu Bar, but it also causes the application to quit.

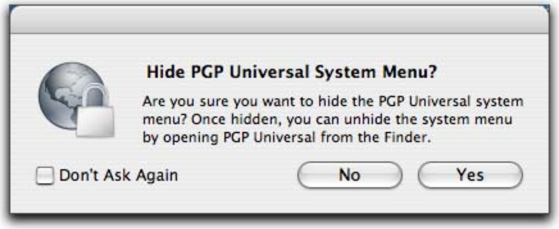
> If you quit PGP Universal Satellite, no email messages will be encrypted, decrypted, signed, or verified as they would be normally. You may not be able to decrypt messages sent to you, even after PGP Universal Satellite is restored. Also, no key management will be done while PGP Universal Satellite is not running.

To see the Quit PGP Universal Server command, hold down the Option (alt) key on the keyboard while pulling down the PGP Universal Server menu.

To hide the PGP Universal Satellite icon:

1 Pull down the PGP Universal Server Menu and select the **Hide PGP Universal Server** command.

A confirmation dialog appears.



Hide PGP Universal System Menu?

Are you sure you want to hide the PGP Universal system menu? Once hidden, you can unhide the system menu by opening PGP Universal from the Finder.

2 Click **Yes**.

To prevent the confirmation dialog from appearing in the future, put a checkmark next to **Don't Ask Again**.

The PGP Universal Server icon disappears from the Menu Bar.

To restore the PGP Universal Satellite icon if hidden:

1 Locate the PGP Universal Satellite application on your system.

The default location is in the Applications folder.

2 Double click the PGP Universal Satellite application.

The PGP Universal Satellite icon appears in the Menu Bar.

To quit PGP Universal Satellite:

1 Hold down the Option key, pull down the PGP Universal Server Menu, and then select the **Quit PGP Universal Server** command.

PGP Universal Satellite quits and the PGP Universal Server icon disappears.

To restart PGP Universal Satellite if the application is not running:

1 Locate the PGP Universal Satellite application on your system.

The default location is in the Applications folder.

2 Double click the PGP Universal Satellite application.

PGP Universal Satellite starts and its icon appears in the Menu Bar.

During the installation process you were asked if you wanted PGP Universal Satellite to start automatically after logging in. If you selected Yes, then restarting your computer also restarts PGP Universal Satellite. (If you selected No, then you will need to restart PGP Universal Satellite manually after a restart.)

38 PGP Universal Satellite for Windows

This chapter describes those aspects of the PGP Universal Satellite software that are specific to the Windows version.

For general information about PGP Universal Satellite, refer to Chapter 36, "PGP Universal Satellite". For information specific to the Mac OS X version, refer to Chapter 37, "PGP Universal Satellite for Mac OS X".

Topics in this chapter include:

Overview

PGP Universal Satellite for Windows proxies SMTP traffic when the user is sending email messages and POP and IMAP traffic when the user is retrieving email messages from their mail server. It also supports MAPI traffic in an Exchange Server environment and Lotus Notes email client (versions 5.x and above) traffic in a Domino Server environment.

PGP Universal Satellite for Windows runs on:

- Windows Vista (all 32-bit editions)
- Windows 2003 Server (SP 1)
- Windows XP (SP 2)
- Windows 2000 (SP 3)

Older Windows operating systems are not supported.

PGP Universal Satellite for Windows has been tested with the following email clients:

- Outlook XP, 2003, and 2007
- Outlook Express 6

- Qualcomm Eudora 6.1
- Mozilla 1.6

It should work without problems with any Internet-standards-based email client that runs on Windows, with email clients that support MAPI, and with Lotus Notes email clients.

Versions of Novell GroupWise prior to 6.5 may not work properly due to a lack of support for standard mail protocols.

PGP Universal Satellite requires a PGP Universal Server; it provides no functionality at all without a policy from an associated PGP Universal Server.

System Requirements

Minimum system requirements for PGP Universal Satellite for Windows are:

- Pentium 166 or greater processor or compatible
- Internet Explorer 6.0 or greater
- 64 MB physical RAM
- 20 MB hard disk space

Obtaining the Installer

Email users who are already part of the Self-Managing Security Architecture (SMSA) should get the PGP Universal Satellite installer from their PGP Universal Server administrator (the PGP Universal Satellite installer is included on the PGP Universal Server CD and can be downloaded from the PGP Universal Server administrative interface). After installation, PGP Universal Satellite communicates with the local PGP Universal Server to get its policies.

Email users outside the SMSA get access to the PGP Universal Satellite installer via a link in an email message from an internal user that includes a Smart Trailer or when they retrieve a message sent using PGP Universal Web Messenger mail (refer to Chapter 16, “Applying Key Not Found Settings to External Users” for more information).

External PGP Universal Satellite for Windows users also are sent an ActiveX® control that assists them with both installing and updating their PGP Universal Satellite software. The ActiveX control is clearly labeled as being from PGP Corporation.

In these cases, PGP Universal Satellite will follow a URL to download its policies from the appropriate PGP Universal Server.

Installation

PGP Universal Satellite for Windows *cannot* be installed on a system with PGP Desktop. If you currently have PGP Desktop on your system, do not install PGP Universal Satellite for Windows. If you are using a version of PGP Desktop prior to 9.0, you should upgrade. If you are using 9.0 or greater of PGP Desktop, you can configure PGP Desktop to do everything PGP Universal Satellite for Windows does for you. See your PGP administrator for more information.

Installing PGP Universal Satellite for Windows is different for internal PGP Universal Satellite users and external users.

Internal users simply need to get the installer and run it. External users need to download an Active X component and approve it to be installed and allowed to run.

To install PGP Universal Satellite for Windows for internal users:

1 Download the PGP Universal Satellite installer onto the computer.

2 Double click the installer application.

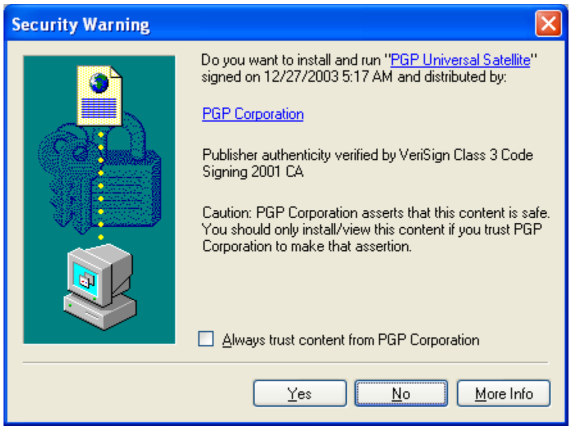
3 Follow the on-screen instructions.

To install PGP Universal Satellite for Windows for external users:

1 As part of the process of interacting with a PGP Universal Server via a Smart Trailer or PGP Universal Web Messenger message, the Future Message Delivery Options screen appears.

2 Select **PGP Universal Satellite** and click **Choose Option**.

The PGP Universal Satellite ActiveX control asks for permission to install and run



Do you want to install and run "PGP Universal Satellite" signed on 12/27/2003 5:17 AM and distributed by:

PGP Corporation

Publisher authenticity verified by VeriSign Class 3 Code Signing 2001 CA

Caution: PGP Corporation asserts that this content is safe. You should only install/view this content if you trust PGP Corporation to make that assertion.

□ Always trust content from PGP Corporation

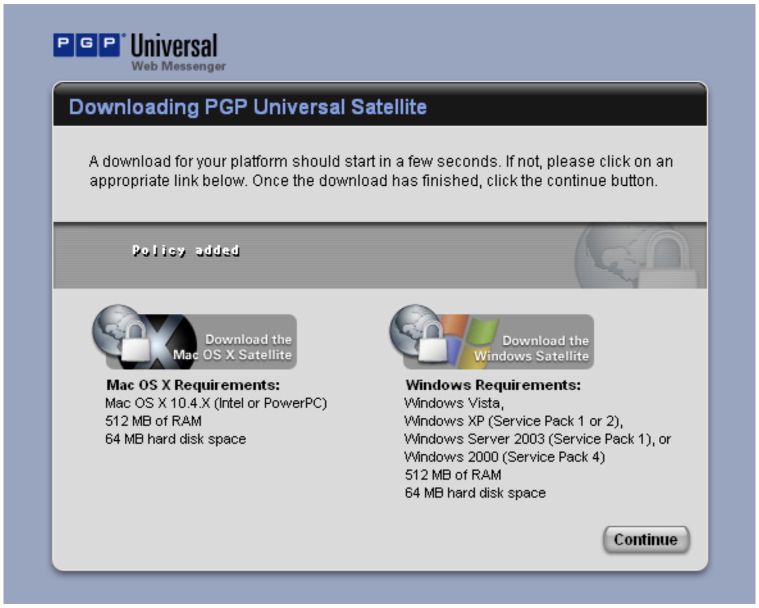
3 Click **Yes**.

4 Agree to the End User License Agreement.

You are prompted for permission to download the installer application.

5 Click **Yes**.

PGP Universal Satellite begins installing and the following screen appears.


PGP Universal
Web Messenger
Policy added
Download the Mac OS X Satellite
Download the Windows Satellite
Continue

Downloading PGP Universal Satellite

A download for your platform should start in a few seconds. If not, please click on an appropriate link below. Once the download has finished, click the continue button.

Mac OS X Requirements:
Mac OS X 10.4.X (Intel or PowerPC)
512 MB of RAM
64 MB hard disk space

Windows Requirements:
Windows Vista,
Windows XP (Service Pack 1 or 2),
Windows Server 2003 (Service Pack 1), or
Windows 2000 (Service Pack 4)
512 MB of RAM
64 MB hard disk space

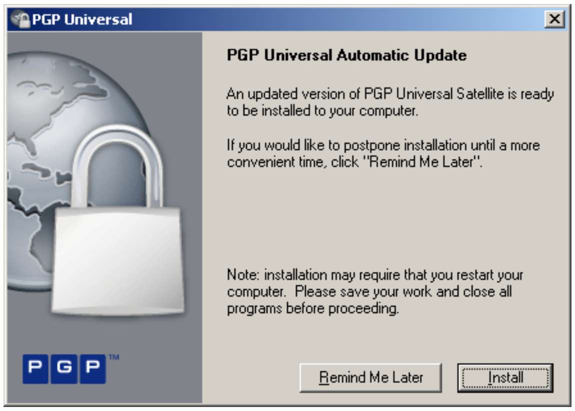
6 When the install is complete, click **Continue**.

The system prompts you to reboot.

Updates

When PGP Universal Satellite communicates with a PGP Universal Server that is running a newer version, PGP Universal Satellite will have the option of updating its software.

The PGP Universal Server Automatic Update screen displays automatically on the computer on which PGP Universal Satellite is installed.



PGP Universal Automatic Update

An updated version of PGP Universal Satellite is ready to be installed to your computer.

If you would like to postpone installation until a more convenient time, click "Remind Me Later".

Note: installation may require that you restart your computer. Please save your work and close all programs before proceeding.

Click **Install** to begin the installation.

Click **Remind Me Later** to be reminded in 18 hours.

Files

The files that are created and/or used by PGP Universal Satellite are stored on the user's computer at:

C:\Documents and Settings\<username>\Application Data\PGP Corporation\PGP Universal Server

If your users are managing their own keys, PGP Corporation recommends backing up the keyring files (*secring.skr* and *pubring.pkr*).

MAPI Support

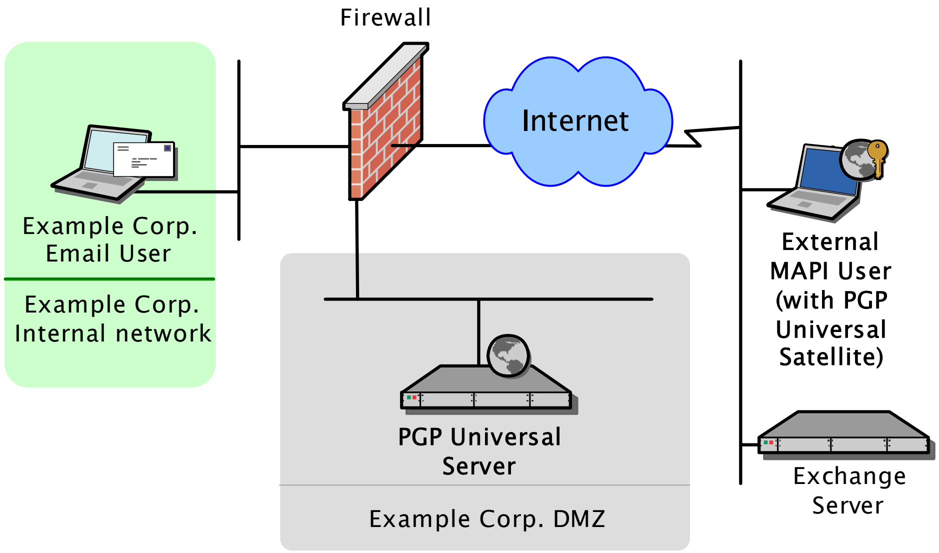
MAPI (Messaging Application Programming Interface), which is a messaging architecture and a client interface used in Microsoft Exchange Server environments, is supported in PGP Universal Satellite for Windows.

MAPI support in PGP Universal Satellite for Windows means you get both PGP message security all the way to your users' computers and the other features that MAPI makes available. MAPI support is available for both internal and external Satellite users.

External MAPI Configuration

For external email users using PGP Universal Satellite, MAPI is no different than using POP or IMAP.

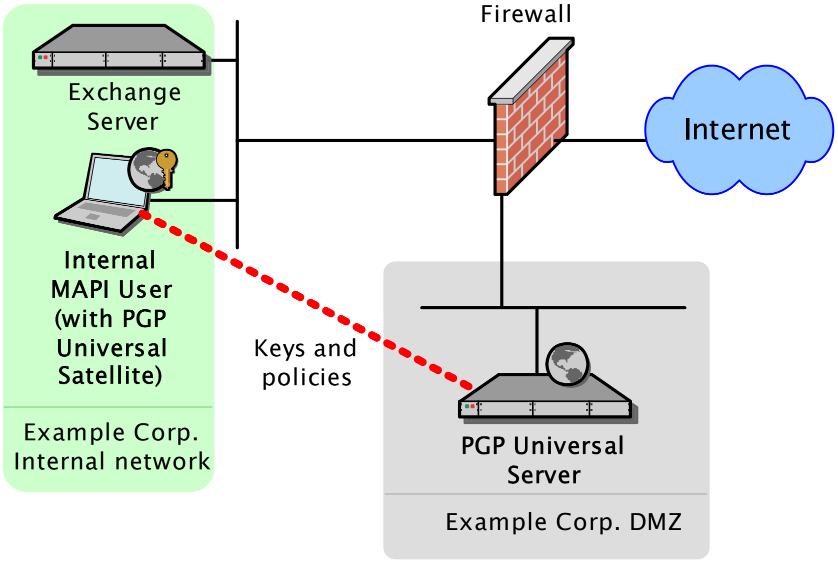
The external PGP Universal Satellite gets its policies from a PGP Universal Server in the managed domain. This is the same PGP Universal Server that sent the Smart Trailer or PGP Universal Web Messenger message.



It does not matter if the PGP Universal Server in the managed domain is in Internal or External Mode as long as it is accessible to the external PGP Universal Satellite via HTTPS on the well-known port 443.

Internal MAPI Configuration

For internal email users using PGP Universal Satellite, MAPI requires a slightly different configuration because the MAPI client must connect directly to its Exchange Server.



In this configuration, email goes from the internal MAPI user with PGP Universal Satellite to the Exchange Server and then on to its destination. PGP Universal Satellite gets its keys and policies from a PGP Universal Server (to which it is "bound" (refer to "Binding" on page 317 for more information about binding).

The advantages to this configuration include full support for MAPI features and full security for email messages, as messages are stored encrypted on the Exchange Server and are encrypted all the way to the computer of the email user.

In some cases with internal Server Key Mode (SKM) users connecting to a PGP Universal Server in External Mode, messages will be decrypted by the server before arriving at the client; use Client Key Mode (CKM) or Guarded Key Mode (GKM) keys to ensure end-to-end security (refer to "Key Mode" on page 313 for more information).

Using MAPI

External users who are using PGP Universal Satellite do not have to do anything to begin sending and receiving messages securely. When they downloaded their copy of PGP Universal Satellite it included the appropriate policy from a PGP Universal Server.

Because an email client that uses MAPI must always interface directly with a Microsoft Exchange Server, internal MAPI users need to bind their Exchange Server to their PGP Universal Server in a PGP Universal Satellite policy.

There are two ways to bind an Exchange Server to a PGP Universal Server to support internal MAPI users:

- **Pre-binding the PGP Universal Satellite installer:** With pre-binding, the PGP Universal Server administrator configures the PGP Universal Satellite installer with the name of the PGP Universal Server and the WINS name of the mail server before the installer is downloaded and distributed to end users
- **Manual binding:** With manual binding, PGP Universal Satellite is first installed on the system of the end user, then a policy that includes the appropriate mail server (Exchange Server) and PGP Universal Server is created.

Both methods are described in "Binding" on page 317.

Lotus Notes Support

Lotus Notes is a groupware application that supports messaging, calendaring, and scheduling capabilities. The Lotus Notes email client (versions 5.x and above) is supported in PGP Universal Satellite for Windows.

(Support for Lotus Notes email clients is not included in PGP Universal Satellite for Mac OS X.)

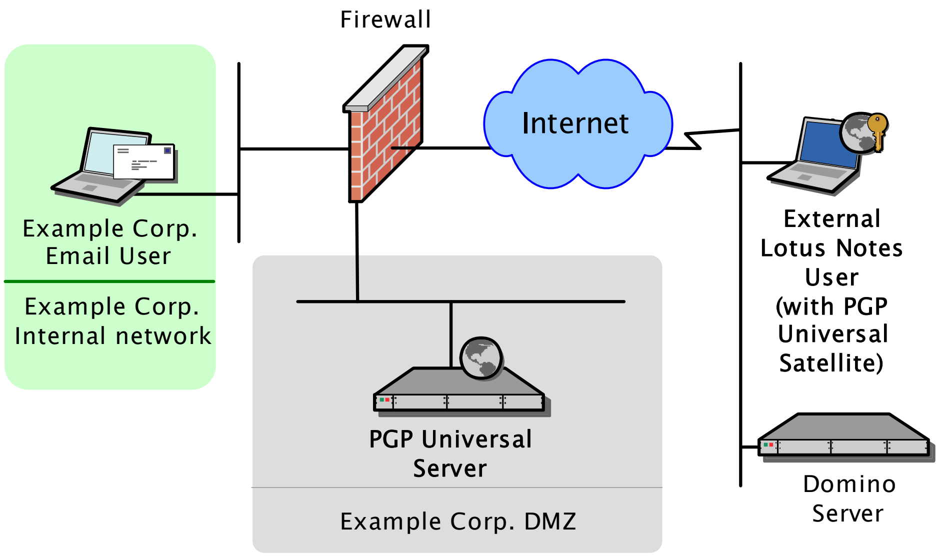
Support for Lotus Notes email clients in PGP Universal Satellite for Windows means you get both PGP message security all the way to your users' computers and the other features that Lotus Notes makes available.

Lotus Notes email client support is available for both internal and external PGP Universal Satellite users.

External Lotus Notes Configuration

For external email users, using a Lotus Notes email client is no different than using a POP or IMAP email client.

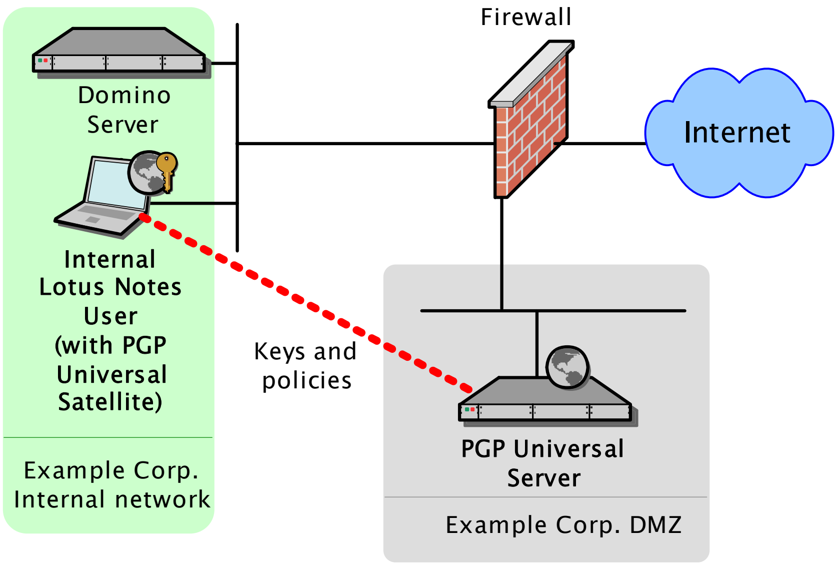
The external PGP Universal Satellite gets its policies from a PGP Universal Server in the managed domain. This is the same PGP Universal Server that sent the Smart Trailer or PGP Universal Web Messenger message.



It does not matter if the PGP Universal Server in the managed domain is in Internal or External Mode, as long as it is accessible to the external PGP Universal Satellite via HTTPS on the well-known port 443.

Internal Lotus Notes Configuration

For internal PGP Universal Satellite users, Lotus Notes requires a slightly different configuration because the Lotus Notes email client must connect directly to its Domino Server.



In this configuration, email goes from the internal Lotus Notes user to the Domino Server and then on to its destination. PGP Universal Satellite gets its keys and policies from a PGP Universal Server to which it is "bound" (refer to "Binding" on page 317 for more information about binding).

The advantages to this configuration include full support for Lotus Notes features and full security for email messages, as messages are stored encrypted on the Domino Server and stay encrypted all the way to the computer of the Lotus Notes email user.

In some cases with internal Server Key Mode (SKM) users connecting to a PGP Universal Server in External Mode, messages will be decrypted by the PGP Universal Server before arriving at the client; use Client Key Mode (CKM) keys to ensure end-to-end security (refer to "Key Mode" on page 313 for more information about SKM and CKM).

Using Lotus Notes

External Lotus Notes users who are using PGP Universal Satellite do not have to do anything to begin sending and receiving messages securely. When they downloaded their copy of PGP Universal Satellite it included the appropriate policy from a PGP Universal Server.

Because a Lotus Notes email client must always interface directly with a Domino Server, internal Lotus Notes users need to bind their Domino Server to their PGP Universal Server in a PGP Universal Satellite policy.

There are two ways to bind a Domino Server to a PGP Universal Server to support internal Lotus Notes users:

- **Pre-binding the PGP Universal Satellite installer:** With pre-binding, the PGP Universal Server administrator configures the PGP Universal Satellite installer with the name of the PGP Universal Server and the fully qualified domain name of the mail server before the installer is downloaded and distributed to end users.
- **Manual binding:** With manual binding, PGP Universal Satellite is first installed on the system of the end user, then a policy that includes the appropriate mail server (Domino Server) and PGP Universal Server is created.

Both methods are described in more detail in "Binding" on page 317.

Notes IDs

All PGP Universal Server keys have SMTP email address associated with them: **josem@example.com**, for example.

The keys of internal Lotus Notes email client users have their Notes ID on their key in addition to a SMTP email address: **CN=josem/O=notes6@notes6**, for example. (External users will never have a Notes ID on their key, as contact with external users is always using their SMTP email addresses.)

The keys of internal Lotus Notes email client users have both addresses, the SMTP email address and the Notes ID, because requests for the key from PGP Universal Satellite for Windows could specify either address.

Notes IDs can be seen in the Primary Email column of the Internal Users card, as well as the User Information screen for a Lotus Notes email client user.

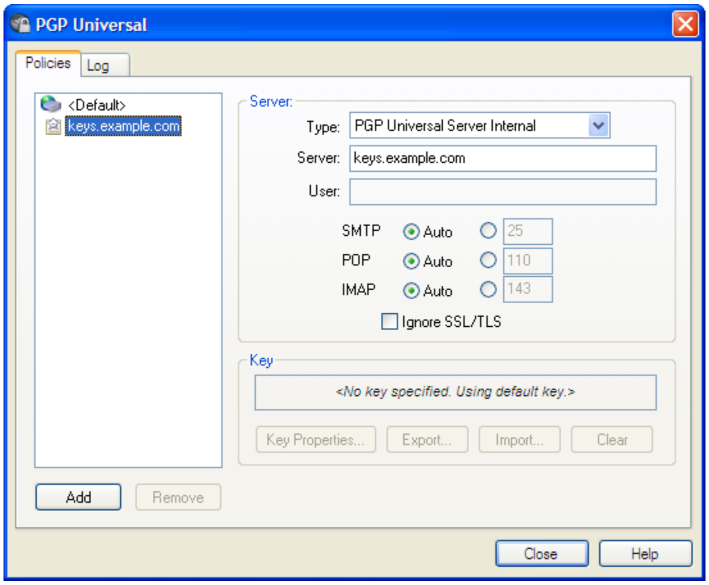
User Interface

PGP Universal Satellite for Windows has a minimal user interface. There are two tabs: Policy and Log. You can also access PGP Universal Satellite functions from the Windows tray icon.

The Policy Tab

The Policy tab lets the user control the policy settings that apply to it and import their PGP keys (if they have a PGP key, of course).

PGP Universal Satellite automatically manages policy settings. There is typically no reason for your users to modify their settings on the Policy tab.



PGP Universal

Policies | Log

<Default>
keys.example.com

Server:

Type: PGP Universal Server Internal

Server: keys.example.com

User:

SMTP ● Auto ○ 25

POP ● Auto ○ 110

IMAP ● Auto ○ 143

□ Ignore SSL/TLS

Key

<No key specified. Using default key.>

The fields on the Policy tab include:

Some fields are only available when a particular Server Type is selected. These fields are noted in the text.

- **Policies list:** Shows the existing policies and each policy's list of managed email domains. Click on a policy to see its settings.
- **Add:** Lets you add a policy manually. Click **Add**, then select the appropriate settings in the Server and Key sections.
- **Remove:** Deletes the selected policy.

- **Type:** Shows what type of device PGP Universal Satellite is interfacing with. There are three options: a PGP Universal Server Internal to your organization, a PGP Universal Server External to your organization, or a standard Mail Server.
- **Server:** Shows the fully qualified domain name or IP address of the server with which PGP Universal Satellite is interfacing. *Does not appear when Type is set to PGP Universal Server External.*
- **URL:** Shows the URL to the PGP Universal Server that PGP Universal Satellite is interfacing with. *Appears only when Type is set to PGP Universal Server External.*
- **User:** Shows the username to which the policy applies. This field is read only. *Appears only when Type is set to PGP Universal Server Internal.*
- **Email:** Shows the email address to which the policy applies. *This field is editable only when Type is set to PGP Universal Server External.*
- **Binding:** Binds a mail server (an Exchange Server, for example) to a PGP Universal Server. *Appears only when Type is set to Mail Server.*

  Make sure not to bind a mail server to a PGP Universal Server except for the two required cases: an internal MAPI or Lotus Notes client running PGP Universal Satellite or an internal PGP Universal Satellite user accessing a PGP Universal Server in External Mode. For more information, refer to "Binding" on page 317.
- **SMTP:** Controls the port on which PGP Universal Satellite is listening for SMTP traffic. The default is Auto, which means the well-known ports (as assigned by the IANA) for the protocol will be used. You can specify a different port by selecting the editable box and entering the desired port number (the default is the SMTP well-known port 25). If the server supports SSL/TLS encryption, it will automatically be used by PGP Universal Satellite.
- **POP:** Controls the port on which PGP Universal Satellite is listening for POP traffic. The default is Auto, which means the well-known ports (as assigned by the IANA) for the protocol will be used. You can specify a different port by selecting the editable box and entering the desired port number (the default is the POP well-known port 110). If the server supports SSL/TLS encryption, it will automatically be used by PGP Universal Satellite.
- **IMAP:** Controls the port on which PGP Universal Satellite is listening for IMAP traffic. The default is Auto, which means the well-known ports (as assigned by the IANA) for the protocol will be used. You can specify a different port by selecting the editable box and entering the desired port number (the default is the IMAP well-known port 143). If the server supports SSL/TLS encryption, it will automatically be used by PGP Universal Satellite.
- **Ignore SSL/TLS:** Check if you want PGP Universal Satellite to pass through and ignore any data that is already encrypted by the email client using SSL/TLS.

  If SSL/TLS is being used to protect data going from the email client to the mail server, PGP Universal Satellite cannot secure it. If you want PGP Universal Satellite to be able to encrypt or sign that data, you need to disable SSL/TLS in the email client.
- **Key box:** Shows the PGP key that is used by this policy to protect email messages.

If new users are added to a policy, the default key for that policy is automatically used unless the user has explicitly cleared the key from the policy.

- **Key Properties:** Displays a dialog that lets you examine the properties of the key. The information found on the Key Properties dialog includes: identification of the user (usually the name and email address of the user to whom the key belongs), the key ID, type, size, creation date, expiration date, cipher, fingerprint, synchronization status with the server, and the ability to change the key's passphrase.

  The synchronization status with the server, which lets the owner of the key keep an encrypted, passphrase-protected copy of their private key on the server, can be changed at any time.

  To change the passphrase for the key, click the **Change Passphrase** button, enter the existing passphrase for the key and press **OK**, enter the new passphrase, enter the new passphrase again, and finally click **OK**.

- **Export:** Lets you export the key. Available only if allowed by the PGP Universal Server administrator. To export a key, click **Export**, select a location, specify a file name, select a file type, decide whether to include the private key, then click **Save**.

- **Import:** Lets you import an existing **keypair**; that is, you can only import keys whose private key was included when the key was exported. If the key includes only the public key portion, you cannot import it. *Available only if allowed by the PGP Universal Server administrator. To import a key, click* **Import***, locate and select the file of the key, click* **Open***, and then click* **OK** *when asked if you want to import the key.*

- **Clear:** Removes the key from PGP Universal Satellite. *Available only if allowed by the PGP Universal Server administrator.*

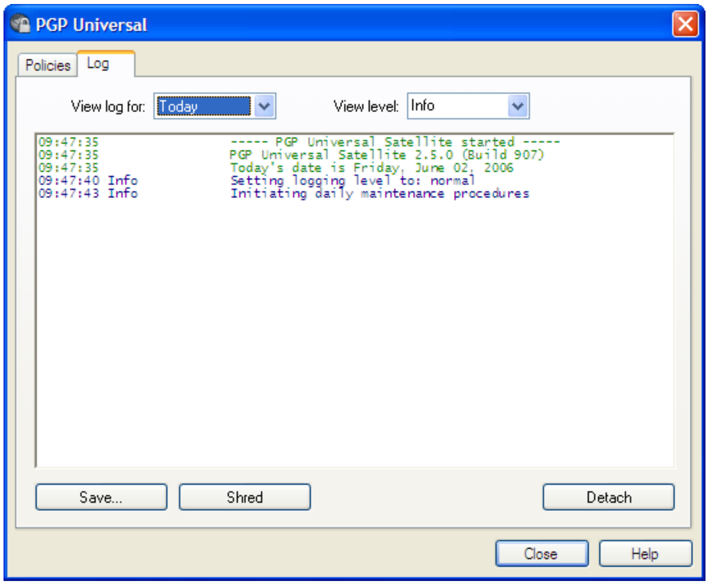
- **Retrieve Policy:** Click to retrieve policy settings from the PGP Universal Server. *Available only for External policies.*

The Log Tab

The Log tab displays log entries for actions taken by PGP Universal Satellite. The Log tab lets you verify that PGP Universal Satellite is processing your mail. It can also be useful for troubleshooting purposes,

PGP Universal Satellite has two logging levels: Normal and Verbose. Normal entries have three color-coded levels of severity (Error, Warn, and Info). Verbose logging adds a fourth type (Verbose) of log entry.

Verbose logging can generate very large log files; in order to prevent inadvertently large log files, the logging level will automatically revert to the Normal level when the log window is closed.



View log for: Today

View level: Info

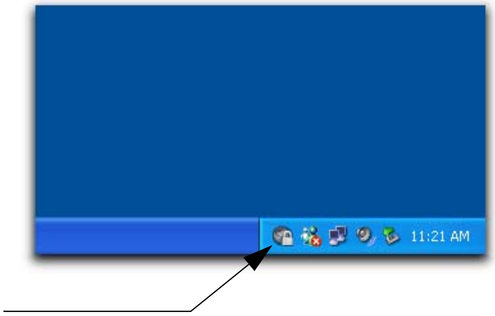
```
09:47:35                 ----- PGP Universal Satellite started -----
09:47:35                 PGP Universal Satellite 2.5.0 (Build 907)
09:47:35                 Today's date is Friday, June 02, 2006
09:47:40 Info            Setting logging level to: normal
09:47:43 Info            Initiating daily maintenance procedures
```

The fields on the Log tab include:

- **View log for:** Select the day for the logs you wish to view.
- **View level:** Select the minimum severity of log entries you wish to view: **Error**, **Warn**, **Info**, or **Verbose**. Selecting Verbose will set the logging level to Verbose. Verbose logging can generate very large log files; in order to prevent inadvertently large log files, the logging level will automatically revert to the Normal level when the log window is closed.
- **List of log entries:** Shows the time stamp and the description of the log entry.
- **Save:** Lets you save the log entries to a text or RTF file.
- **Shred:** Lets you delete all log entries.
- **Detach:** Lets you detach the Log tab into a separate dialog, which can be resized for easier viewing.

The Satellite Tray Icon

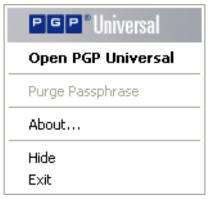
The PGP Universal Satellite tray icon provides access to Satellite functions.



PGP Universal Server Satellite tray icon

The PGP Universal Satellite tray icon is hidden by default when PGP Universal Satellite is installed. To see the PGP Universal Satellite tray icon if it is hidden, click **Start** > **Programs** > **PGP Universal Server**.

Right-click the PGP Universal Satellite tray icon to display the menu.



Each of the commands on the menu are described below.

Open PGP Universal Server

This command opens PGP Universal Satellite and displays the Policy tab.

Purge Passphrase

This command purges from memory any cached passphrases.

PGP Universal Satellite for Windows caches your passphrase as a convenience so that you do not have to enter it each time you want to sign or decrypt a message. Your passphrase is cached until the application quits, which occurs automatically on logout.

Technical note: Server Key Mode (SKM) users do not actually have a passphrase. The PGP Universal Server maintains the private key and provides it to PGP Universal Satellite when needed. So for SKM users, Purge Passphrase actually purges the private key from memory.

Once the passphrase cache is purged, you will have to enter your password the next time it is needed.

If you are operating in Client Key Mode (CKM) or using a PGP Desktop key, it is a good idea to purge your passphrase cache if you leave your computer. This will prevent someone from being able to use your cached passphrase to sign/decrypt your messages while you are away.

To purge the passphrase cache:

1 Select **Purge Passphrase** from the PGP Universal Satellite menu.

The passphrase cache is purged.

About PGP Universal Server

Select **About** to display the About PGP Universal Satellite dialog.

This screen displays both the names of the people who helped to create PGP Universal Satellite and the version of PGP Universal Satellite being used.

Click **OK** to close the About PGP Universal Satellite dialog.

Hide

The **Hide** command removes the PGP Universal Satellite icon from the Windows tray, but leaves the application running.

To hide the PGP Universal Satellite for Windows tray icon:

1 Right click the PGP Universal Satellite tray icon and select **Hide**.

The PGP Universal Server icon disappears from the Menu Bar.

To restore the PGP Universal Satellite tray icon if hidden:

1 Click **Start** --> **All Programs** --> **PGP Universal Server**.

The Policy tab appears on your screen and the PGP Universal Satellite icon appears in the Windows tray.

Exit

The **Exit** command removes the PGP Universal Satellite icon from the Windows tray *and* causes the application to quit.

If you quit PGP Universal Satellite for Windows, no email messages will be encrypted, decrypted, signed, or verified until it is restarted. Also, no key management will be done while PGP Universal Satellite is not running.

To exit PGP Universal Satellite for Windows:

1 Right click the PGP Universal Satellite tray icon and select **Exit**.

If you email client is open, you will see a message telling you that exiting prevents PGP Universal Satellite from protecting your email and to close all open email applications before proceeding.

2 Click **OK**.

The PGP Universal Satellite application quits and the PGP Universal Satellite icon disappears from the Windows tray.

To restart the PGP Universal Satellite for Windows application:

1 Click **Start** --> **All Programs** --> **PGP Universal Server**.

The Policy tab appears on your screen and the PGP Universal Satellite icon appears in the Windows tray.

Restarting your computer also restarts PGP Universal Satellite if the application is not running.

39 Configuring the Integrated Keyserver

This chapter describes the Keyserver service, which is integrated into every PGP Universal Server and holds the public keys of internal users.

You can configure Keyserver options from the Services>Keyserver card.

Topics include:

- "Overview"
- "Configuring the Keyserver Service" on page 354

Overview

Every PGP Universal Server includes an integrated keyserver that is populated with the public keys of your internal users. When an internal user sends a message to another internal user, the PGP Universal Server goes to the keyserver to find the public key of the recipient to secure the message.

Depending on how your network is configured, the PGP Universal Servers of other organizations can also contact your keyserver to look for public keys. External users' PGP Desktop applications can do the same.

The keyserver is always on if the service is enabled, but PGP Universal Server administrators can control access to it via the Keyserver card. You can block or allow access to the keyserver by specified IPs and hostnames.

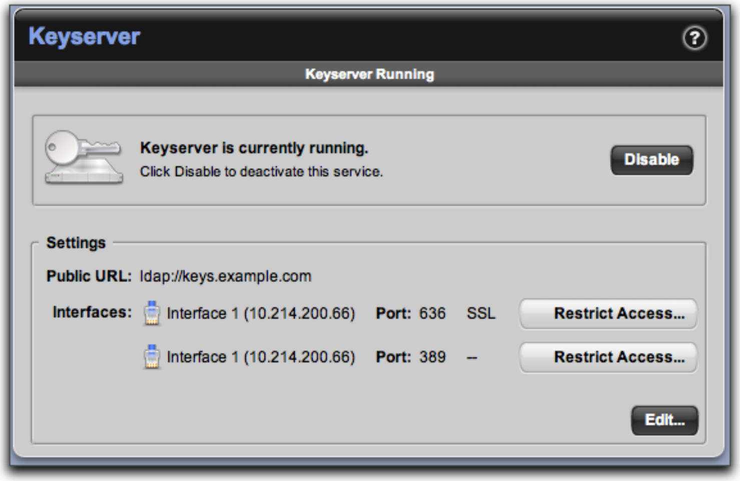
If you have the PGP Verified Directory activated, the keyserver will receive vetted user-submitted keys from the PGP Verified Directory. See Chapter 31, "Configuring the PGP Verified Directory"

Configuring the Keyserver Service

You can allow access to the keyserver through non-SSL/TLS service, SSL/TLS service, or both.

To configure the Keyserver service:

1. Go to Services>Keyserver. On the Keyserver card, click the **Enable** button to enable the service.
2. To disable the Keyserver service, click the **Disable** button on the Keyserver card.



Keyserver is currently running.
Click Disable to deactivate this service.

Settings

Public URL: ldap://keys.example.com

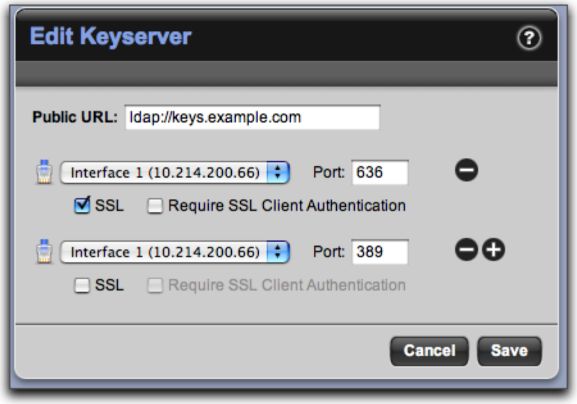
Interfaces: Interface 1 (10.214.200.66) Port: 636 SSL

Interface 1 (10.214.200.66) Port: 389 --

To configure the Keyserver service:

1 From the Services>Keyserver card, click **Edit**.

The Edit Keyserver card appears.



Public URL: ldap://keys.example.com

Interface 1 (10.214.200.66) Port: 636

☑ SSL □ Require SSL Client Authentication

Interface 1 (10.214.200.66) Port: 389

□ SSL □ Require SSL Client Authentication

2 In the **Public URL** field, enter the keyserver's network name. If the keyserver is behind a load balancer, this name may be different from the PGP Universal Server's network name.

Anytime the Public Keyserver URL changes, that information on the Organization Key will immediately change. On user keys, the URL information will be updated the next time the Organization Key signature is renewed.

3 In the **Interface** field, select the appropriate interface for the Keyserver from the drop-down list.

4 In the **Port** field, enter a port number for the Keyserver to listen on or keep the default setting. The default port for the first interface connector is port 389. The SSL default is port 636.

The above two fields establish the interface and port on which the Keyserver will be established.

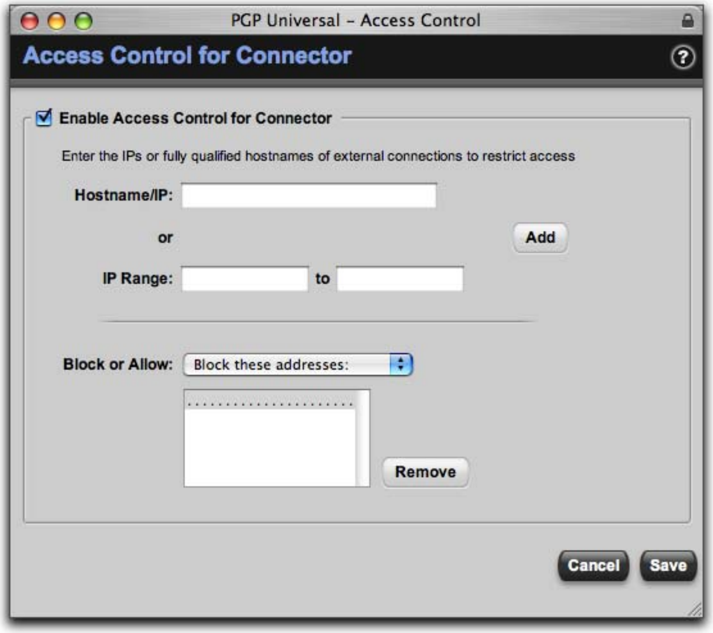
5 Put a check in the **SSL** checkbox to require that connections to the Keyserver be over SSL.

6 Put a check in the **Require SSL Client Authentication** checkbox to require that client connections be SSL-authenticated.

7 Click the plus sign icon to add another network interface, and select the appropriate interface, port, and SSL information.

8 Click **Save** to save changes and return to the Keyserver card.

9 For each interface you enabled, you have the option of clicking **Restrict Access** and establishing access control for the connection on the Access Control for Connector dialog:



☑ Enable Access Control for Connector

Enter the IPs or fully qualified hostnames of external connections to restrict access

Hostname/IP:

or

IP Range: to

Block or Allow: Block these addresses:

- Put a checkmark next to **Enable Access Control for Connector** to enable access control.
- In the **Hostname/IP** field, enter a hostname or IP address, then click **Add**. What you enter here will go onto the list in the **Block or Allow** field below. If you enter a hostname like **example.com**, the name will be resolved to an IP address.
- In the **IP Range** fields, enter starting and ending IP addresses for an IP address range, then click **Add**. What you enter here will go onto the list in the **Block or Allow** field below.
- In the **Block or Allow** field, select **Block these addresses** or **Allow only these addresses**, as appropriate, for the IP addresses or ranges in the box below.

To remove an IP address or range from the box, select it then click **Remove**.

10 Click **Save** to close the Access Control for Connector dialog.

SECTION 7

Managing Your PGP Universal Server

This section describes how to monitor and manage your PGP Universal Server.

40 System Graphs

This chapter describes system graphs, a feature that graphically displays information about your PGP Universal Server.

Topics in this chapter include:

Overview

Select **Reporting>Graphs** to view the graph screen. There are four system graphs:

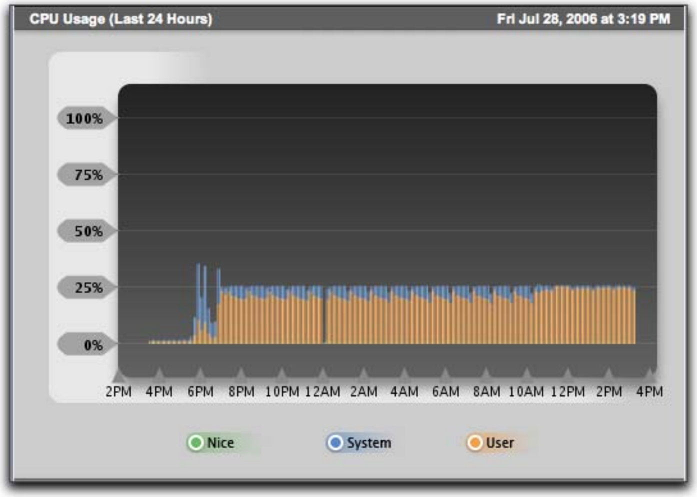
- CPU usage (Last 24 hours)
- Message activity
- Recipient statistics
- Recipient domain statistics

Click **Refresh** (at the top of the System Graphs screen) to refresh the information in the graphs.

CPU Usage

The CPU Usage graph displays information about the CPU usage of the hardware hosting your PGP Universal Server in the last 24 hours. The following categories are shown:

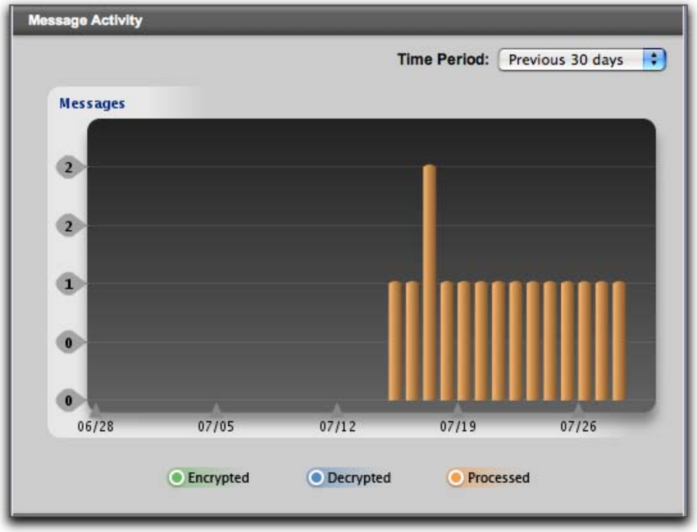
- **Nice**. Shows CPU usage by processes running at a lower priority than any other processes; it is mostly used for low-importance background tasks and rarely shows much activity on PGP Universal Servers. Nice processes only run when the CPU is not running any other task.
- **System**. Shows CPU usage by the PGP Universal Server software.
- **User**. Shows CPU usage by PGP Universal Server users.



Message Activity

The Message Activity graph shows the number of messages the PGP Universal Server encrypted, decrypted, and processed for the specified time period.

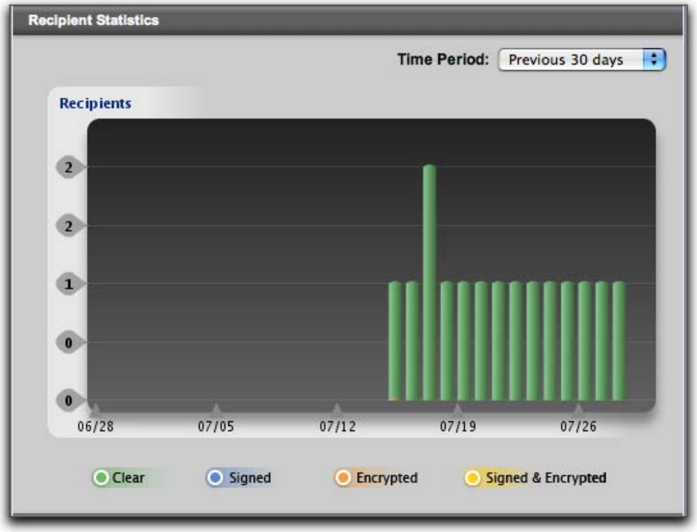
Available time periods are the previous 30 days, previous 6 months, and previous year.


Time Period: Previous 30 days

Recipient Statistics

The Recipient Statistics graph shows the number of recipients (internal and external) getting messages sent in the clear, sent signed, sent encrypted, and sent signed and encrypted.

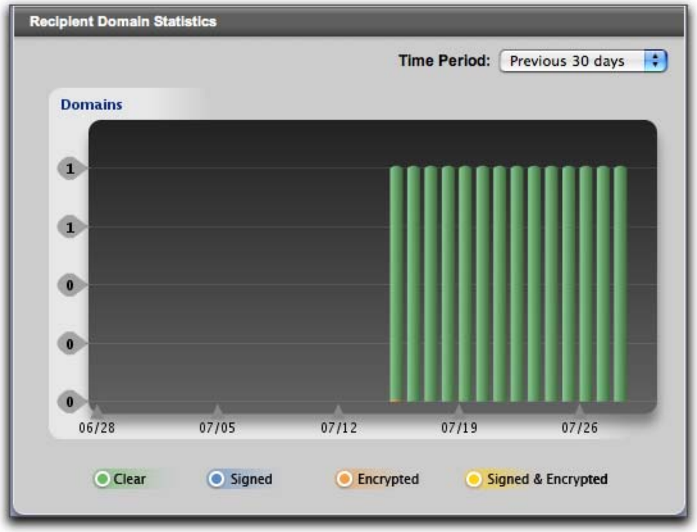
Available time periods are the previous 30 days, previous 6 months, and previous year.



Recipient Domain Statistics

The Recipient Domain Statistics graph shows the number of domains receiving messages sent in the clear, sent signed, sent encrypted, and sent signed and encrypted.

Available time periods are previous 30 days, previous 6 months, previous year.



41 System Logs

This chapter tells you about the PGP Universal Server system logs.

Topics in this chapter include:

Overview

The System Logs card lists and time stamps each action a PGP Universal Server takes. Analysis of the logs can help you determine how your configuration of the server and the policies you have established are affecting your email.

The list shows the most recent events at the top.

The list can be filtered by what actions were logged, date the action occurred, time the action occurred, and type of message (Information, Warnings, Notices, and Errors). There are 10 possible types of actions:

- **Administration** logs are audit logs of configuration changes made through the administration console interface.
- **Backup** logs provide information about events such as data and configuration restoration, and automatic and manual backups.
- **Client** logs display messages about connections made from PGP Universal Satellite, for example.
- **Cluster** logs include messages about cluster join events and data replication notices.
- **Ignition Key** logs record events such as adding and removing ignition keys and using ignition keys to unlock the server.
- **Mail** logs record mail proxy activities such as PGP Universal Server finding recipient keys, IMAP connections, and the starting and stopping of mail services.
- **Postfix** logs display events associated with sending mail messages.
- **Update** logs provide information about software-update specific actions.
- **Verified Directory** logs include information about events such as user submission of keys and key-verification email.

- **Web Messenger** logs display events such as users logging in and out of the service and messages being sent.

You can also search the log and save a copy of the log as a text file at any time.

Filtering the Log View

You can filter the log view based on multiple criteria.

To filter the view of the system log:

1. Select **Reporting>Logs**.
2. Click the current **Log** selection and select the appropriate logged action from the drop-down list.

   The list of log entries re-displays, showing only those entries for the appropriate action for the selected date.
3. To change the type of entries shown in the list, check the **Display** types you want to see and uncheck the types you don’t want to see, then click **Find**:

   – **Information** shows informative log entries, events of low importance.

   – **Notice** shows notification log entries, important events like starting and stopping processes.

   – **Warnings** shows warning log entries, indicating possible problems.

   – **Errors** shows error log entries, for example, serious and non-fatal errors.

   The list of log entries re-displays each time you choose a filter.
4. To change the range of dates and times displayed, select **1 page**, **1 hour**, **6 hours**, etc., from the menu on the right. You can move between time periods one at a time by clicking the arrows.

Searching the Log Files

Searches are not case–sensitive.

To perform a simple search in the list of log entries for a particular word or phrase:

1. Enter the word or phrase in the **Search** field.
2. Check **Regular expressions**, as appropriate.
3. Choose any of the Log and Display types.
4. Click **Search**.

The list of log entries re-displays to show logs containing the word or phrase for which you searched.

To perform an advanced search based on days of the week, or dates and times:

1. Click **advanced**.
2. Enter a word or phrase in the **Search** field, if necessary.
3. Check **Regular expressions**, as appropriate.
4. Choose any of the Log and Display types.
5. Enter the dates and times of the logs you want to view.
6. Click **Search**.

   The list of log entries shows those entries time stamped at the times you specified for the selected dates.

Exporting a Log File

You may want to save a log file to examine it offline or you may want to save a record of log messages. The log file is a text file, so you can open it with any text editor.

Click the **Export Log** button to save a log file.

Enabling External Logging

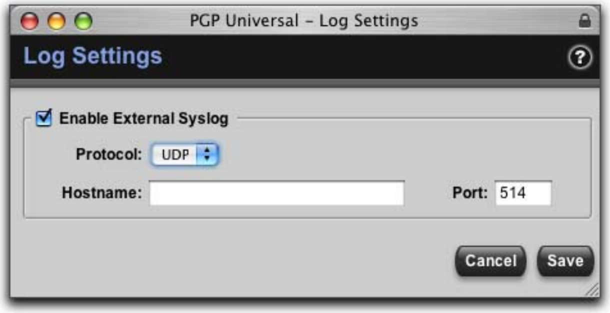
Log Settings lets you enable external system logging, which means you can send all log messages to an existing remote syslog server for central log gathering. Keeping logs for all of your systems in one location can help with log analysis.

When external syslog is enabled, the logs for the following PGP Universal Server services are sent to the syslog server: administration, software updates, clustering, backups, Web Messenger, Verified Directory, Postfix, and mail. The logs of some generic services, such as cron (the system task scheduler), are sent as well.

To configure the log settings:

1. Click on the **Settings** button.

   The Log Settings dialog appears.



☑ Enable External Syslog

Protocol: UDP

Hostname:

Port: 514

2 Put a checkmark next to **Enable External Syslog**.

3 Choose the desired **Protocol** to use to send the logs (UDP or TCP) from the drop-down list.

The default protocol and port values are the most common values; they should be used unless you are certain you must use different values.

4 Specify the **Hostname** to which to send them.

5 Enter the desired **Port** number or use the default.

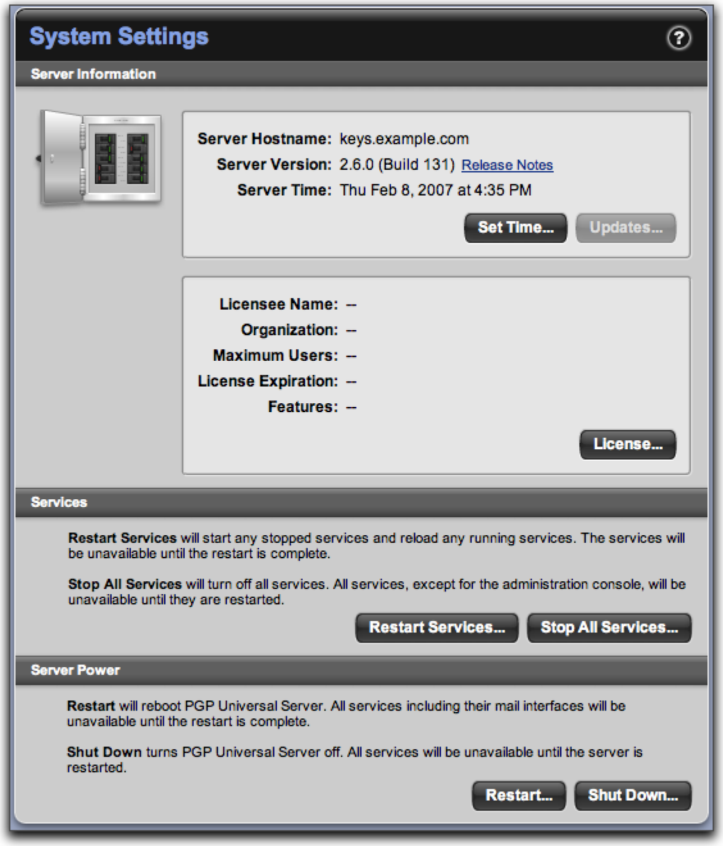
6 Click **Save**.

42 Shutting Down and Restarting Services and Power

This chapter discusses things you can do using the System Settings card.

Overview

The System Settings card, found at **System>General Settings**, shows data about the PGP Universal Server you are using, lets you set the time for the server, update your license, stop and restart services, and shut down and restart the server.



System Settings

Server Information

Server Hostname: keys.example.com
Server Version: 2.6.0 (Build 131)
Server Time: Thu Feb 8, 2007 at 4:35 PM

Licensee Name: --
Organization: --
Maximum Users: --
License Expiration: --
Features: --

Services

Restart Services will start any stopped services and reload any running services. The services will be unavailable until the restart is complete.

Stop All Services will turn off all services. All services, except for the administration console, will be unavailable until they are restarted.

Server Power

Restart will reboot PGP Universal Server. All services including their mail interfaces will be unavailable until the restart is complete.

Shut Down turns PGP Universal Server off. All services will be unavailable until the server is restarted.

PGP Universal Server

The Server Information section displays the version of the server currently installed and any important information or cautions that apply (a system update that's ready to be installed, for example). It also includes links to software updates and licensing information.

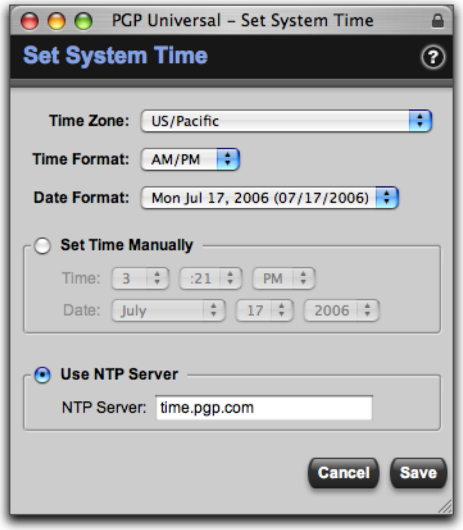
Setting the Time

You need to set the time for your PGP Universal Server so that it knows what time it is; this is especially important for time-based operations such as scheduled backups.

To set the time:

1 Click **Set Time**.

The Set System Time dialog appears.



PGP Universal – Set System Time

Set System Time

Time Zone: US/Pacific

Time Format: AM/PM

Date Format: Mon Jul 17, 2006 (07/17/2006)

○ Set Time Manually

Time: 3 :21 PM

Date: July 17 2006

● Use NTP Server

NTP Server: time.pgp.com

2 Select the appropriate time zone from the **Time Zone** drop-down list.

3 Select your preferred time and date formats.

4 Select either **Set Time Manually** and then set the correct time or **Use NTP Server** and use the default NTP (time.pgp.com) server or specify a different one.

5 Click the **Save** button.

Updating Software

To update the software, click **Updates**.

The Software Updates screen appears. See Chapter 48, "Updating PGP Universal Server Software" for more information.

Licensing a PGP Universal Server

To enter, change, or view licensing information for this PGP Universal Server:

1 Click **License**.

The Enter License Information dialog appears.

2 In the **Licensee Name** field, enter the name of the person who owns the license.

> ⓘ If you have used your license number for authorization in the past, you must enter your name and organization exactly the way you did the first time. If you are unable to authorize your software successfully and you have ruled out problems with your network connection, please contact PGP Support (**www.pgp.com/support/**).

3 In the **Licensee Organization** field, enter the name of the organization that owns the license.

4 In the **Licensee Email** field, enter the email address of the person who owns the license.

5 In the **License Number** field, enter the license number for this server.

6 If you have been sent a license authorization from the PGP License Administrator, click **Manual**, then paste the license authorization into the **License Authorization** box.

Unless you have unusual network problems, you should have no need for manual authorization.

7 Click **Save**.

If there is a problem with the authorization, an error message appears at the top of the Enter License Information dialog.

If the authorization is successful, the System Settings card appears with the license information filled in.

Downloading the Release Notes

To download the *Release Notes*, click *Release Notes* in the Server Information section. The *Release Notes* for your version of the software appears.

Shutting Down and Restarting the PGP Universal Server Software Services

Services lets you shut down and restart the software services provided by PGP Universal Server; the hardware and the administrative interface are not affected. Restarting restarts any stopped services and reloads any running services; the server does not accept connections until the restart is complete. Stopping services shuts down all services until they are restarted; the server does not accept connections during this time.

Services include:

- PGP Universal Web Messenger
- Keyserver
- PGP Verified Directory
- Mail proxies

- Clustering communication
- Client software communication

To restart services when services are running, click **Restart Services**.

The server software is restarted. An confirmation message appears at the top of the screen when the restart is complete.

To stop all services, click **Stop All Services**.

All software services are stopped. An confirmation message appears at the top of the screen when the services are stopped.

To start all services when the services are stopped, click **Start All Services**.

All software services start. A confirmation message appears when the services are started.

Shutting Down and Restarting the PGP Universal Server Hardware

Server Power lets you restart or shut down the hardware on which your PGP Universal Server is running. Restarting stops all server functionality until the automatic restart is complete. Shut down stops all server functionality until the server is manually restarted.

To restart the PGP Universal Server, click **Restart**.

The PGP Universal Server restarts.

To shut down the PGP Universal Server, click **Shut Down**.

The PGP Universal Server shuts down.

You must manually restart the server to restore operation.

43 Configuring SNMP Monitoring

This chapter describes how to configure PGP Universal Server to allow network management applications to monitor system information for the device on which PGP Universal Server is installed, and to send system and application information to an external destination.

You can configure SNMP options from the **Services>SNMP** card.

Topics include:

Overview

SNMP enables a network management application to monitor the health and activity of the PGP Universal Server software and the computer on which it is installed. The network management application can poll the PGP Universal Server on a regular basis to extract information. Polling means that the network management application periodically queries the PGP Universal Server to get the desired status information, and SNMP is the protocol it uses.

You can configure all polling settings, including polling cycles, on the network management application. You can poll the following system information, as part of the standard MIB:

- The number of instances of certain running processes
- System memory usage
- Disk usage
- System load information

You can also download PGP custom MIBs that allow you to poll for messaging statistics, including the following:

- The number of messages processed that day
- The number of messages encrypted and/or signed that day
- The number of messages decrypted that day
- The number of messages processed total
- The number of messages encrypted and/or signed total
- The number of messages decrypted total

- The number of viruses found that day
- The number of messages currently in the mail queue

You can also set up the PGP Universal Server to use SNMP to send out trap information to one or more specified hosts or IP addresses. Traps are triggers set off by certain network events. You can configure the SNMP service to send out an alert every time the following events occur:

- When the number of certain processes drops to zero
- When the amount of available swap space drops too low
- When a disk has less than 20% free space
- When the 1-minute system load average rises above 4.0
- When the 5-minute system load average rises above 1.0
- When the 15-minute system load average rises above 1.0

Downloading the Custom MIB File

PGP Corporation provides a custom MIB extension to allow you to poll for PGP Universal Server-specific information. The MIB files are called PGP-UNIVERSAL-MIB.mib and PGP-SMI.mib. The root Object ID (OID) for the PGP Universal Server custom MIB set is .1.3.6.1.4.1.17766.1.1.1, which is .iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).pgp(17766).products(1).pgpuniversal(1).messaging(1).

To download the custom MIB files:

1. From the Services>SNMP card, click **Download PGP MIBs**.
2. Save the zipped file mibs.zip to your desktop.

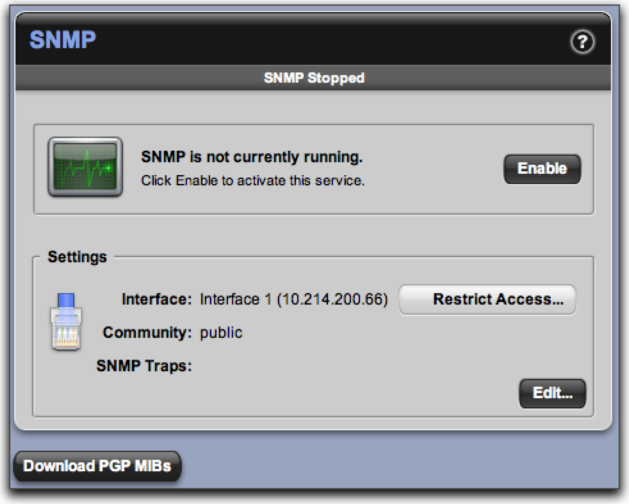
   The MIB files download to your desktop.
3. Unzip mibs.zip, and extract the files PGP-UNIVERSAL-MIB.mib and PGP-SMI.mib.
4. Depending on which SNMP browser you are using, you may need to compile the MIBs before you can add them to the browser. The MIB files are formatted as text and may need to be converted to a database form before they can be used. Consult the documentation for your SNMP browser.
5. Import the MIBs to your SNMP browser.

Configuring the SNMP Service

To enable the SNMP service:

1. On the Services>SNMP card, click the **Enable** button to enable the service.

2 To disable the SNMP service, click the **Disable** button on the SNMP card.



SNMP

SNMP Stopped

SNMP is not currently running.
Click Enable to activate this service.

Settings

Interface: Interface 1 (10.214.200.66)

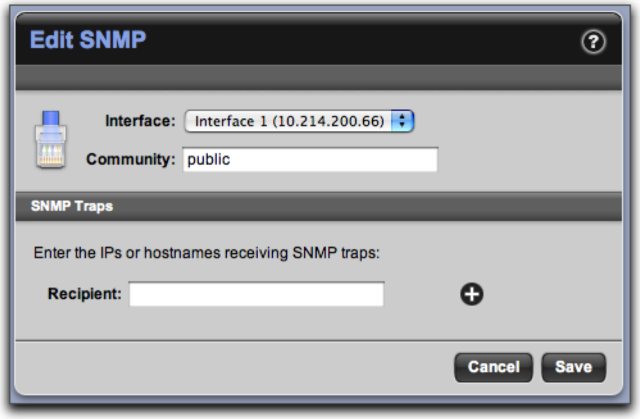
Community: public

SNMP Traps:

To configure the SNMP service:

1 From the SNMP card, click the **Edit** button.

The Edit SNMP card appears.



Edit SNMP

Interface: Interface 1 (10.214.200.66)

Community: public

SNMP Traps

Enter the IPs or hostnames receiving SNMP traps:

Recipient:

2 In the **Interface** field, select the interface on which you want to allow SNMP polling of the PGP Universal Server.

You cannot specify a port because the standard port for SNMP traffic is always port 161.

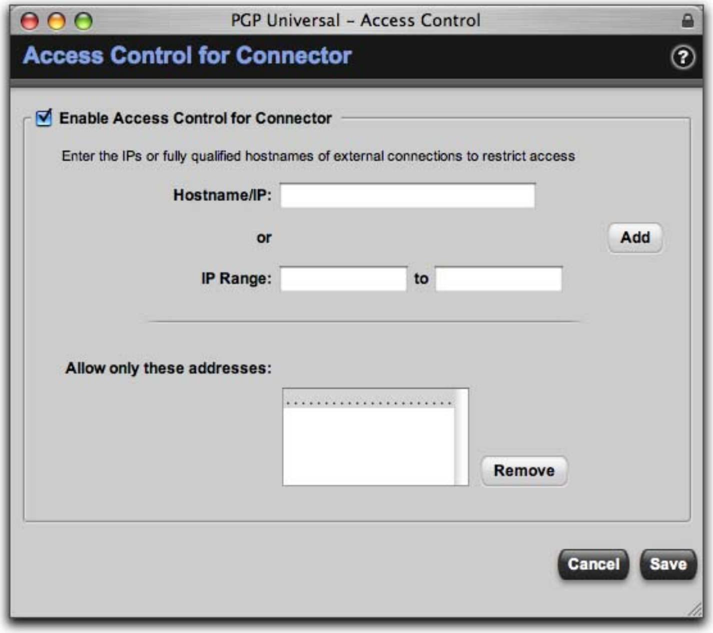
3 In the **Community** field, enter the community name, also called the community string. The community name acts as a password, allowing the network management application to poll the PGP Universal Server. You will need to enter the same community name in your SNMP browser.

4 In the **SNMP Traps Recipient** field, enter the IP or hostname you want to receive SNMP trap data.

5 Click the plus sign icon next to the Recipient field to add another recipient. There is no limit to the number of IPs you can add.

6 Click **Save** to save changes and return to the SNMP card.

7 You have the option of clicking **Restrict Access** and establishing access control for the connection on the Access Control for Connector dialog:


PGP Universal – Access Control
Access Control for Connector
?
☑ Enable Access Control for Connector
Enter the IPs or fully qualified hostnames of external connections to restrict access
Hostname/IP:
or
Add
IP Range:
to
Allow only these addresses:
Remove
Cancel
Save

- Put a checkmark next to **Enable Access Control for Connector** to enable access control.
- In the **Hostname/IP** field, enter a hostname or IP address, then click **Add**. What you enter here will go onto the list in the **Allow only these addresses** field below. If you enter a hostname like **example.com**, the name will be resolved to an IP address.
- In the **IP Range** fields, enter starting and ending IP addresses for an IP address range, then click **Add**. What you enter here will go onto the list in the **Allow only these addresses** field below.

  To remove an IP address or range from the box, select it and click **Remove**.

8 Click **Save** to close the Access Control for Connector dialog.

44 Setting Network Interfaces

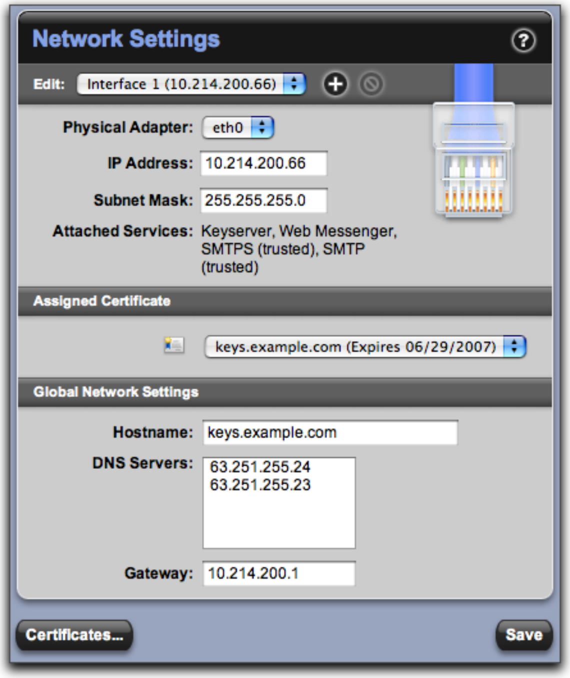
This chapter tells you about network settings and how to modify them. It also describes certificates and tells you how to work with them.

Topics in this chapter include:

- "Overview"
- "Changing Interface Settings" on page 376
- "Adding Interface Settings" on page 376
- "Deleting Interface Settings" on page 376
- "Editing Global Network Settings" on page 377
- "Assigning a Certificate" on page 377
- "Working with Certificates" on page 377

Overview

The Network Settings card lets you view and change the settings for the interfaces the PGP Universal Server is using to attach to your network.



Network Settings

Edit: Interface 1 (10.214.200.66)

Physical Adapter: eth0

IP Address: 10.214.200.66

Subnet Mask: 255.255.255.0

Attached Services: Keyserver, Web Messenger, SMTPS (trusted), SMTP (trusted)

Assigned Certificate

keys.example.com (Expires 06/29/2007)

Global Network Settings

Hostname: keys.example.com

DNS Servers: 63.251.255.24
63.251.255.23

Gateway: 10.214.200.1

These settings will have been originally configured using the Setup Assistant. You can have more than one network interface. Each interface must have its own IP address.

You can also use the Network Settings card to manage the certificates your PGP Universal Server uses.

If you want to change the network settings of any Primary or Secondary cluster member, you will need to break up the cluster first, change the settings, and reestablish the cluster. See Chapter 45, "Clustering your PGP Universal Servers" for information on clusters and network settings.

Changing Interface Settings

To change the settings of an interface:

1. Select the interface whose settings you want to change from the **Edit** drop-down list.
2. Establish the appropriate settings for the **Physical Adapter** (the physical network cards on your hardware), **IP Address**, and **Subnet Mask** fields.
3. Click **Save**.

Adding Interface Settings

To add an interface:

1. Click the Add icon.

   A new interface number appears in the Edit field; it will be numbered sequentially from the highest existing interface number.
2. Establish the appropriate settings for the **Physical Adapter**, **IP Address**, and **Subnet Mask** fields.
3. Click **Save**.

   The new interface is added.

Deleting Interface Settings

To delete an interface:

1. Click the Delete icon to the right of the Edit field.

   A confirmation dialog appears.

> You may need to reassign services assigned to the interface you are trying to delete **before** you can delete the interface. A message will tell you which services need to be reassigned.

2 Click **OK**.

Editing Global Network Settings

Your PGP Universal Server needs to have a hostname and needs to know about domain name servers (DNS) it can use. These will have been configured when you first accessed your server using the Setup Assistant; existing settings can be changed here.

To edit the global network settings:

1 In the **Hostname** field, enter a fully qualified domain name for the server (keys.example.com, for example).

2 In the **DNS Servers** box, remove the IP address of an existing DNS server or add the IP address of a new DNS server.

3 In the **Gateway** box, enter the IP for the network gateway.

4 Click **Save**.

Assigning a Certificate

When you assign a certificate to an interface, any service bound to that interface will automatically use the certificate for SSL/TLS traffic.

To assign a certificate to an interface:

1 In the Assigned Certificate section of the Network Settings card, click the drop-down list.

The SSL/TLS certificates that can be assigned to the interface shown at the top of the Network Settings card appear.

2 Select the appropriate certificate, then click **Save**.

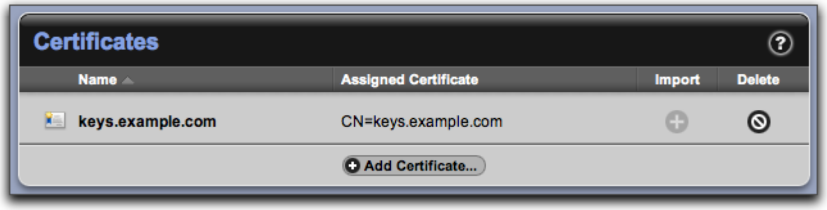
The certificate you selected is assigned to the interface.

For information about adding certificates to the list, see “Working with Certificates” on page 377.

Working with Certificates

To see the Certificates card, navigate to the Network Settings card (System>Network in the administrative interface) and click the Certificates button in the lower left corner of the screen.

The Certificates card lets you view existing certificates, import existing certificates, and generate self-signed certificates and new certificate requests.



Name	Assigned Certificate	Import	Delete
keys.example.com	CN=keys.example.com	⊕	⦸

The Setup Assistant automatically creates a self-signed certificate for use with SSL/TLS traffic. Because this certificate is self signed, it may not be trusted by email or Web browser clients. Specific behavior in response to this self-signed certificate depends on the specific email or web browser client and its security settings.

PGP Corporation recommends you obtain a valid SSL/TLS certificate for each of your servers from a public Certificate Authority, such as GeoTrust, available at the PGP Online Store (www.pgpstore.com). Not doing so will lead to incompatibilities with some email clients and Web browsers.

You can also use pre-existing keys and certificates for SSL/TLS traffic (you must import them first so that they appear on the Certificate card, then you can assign them using the Certificate Assignment card).

Most commonly, these keys and certificates are used in conjunction with Apache Web servers to provide secure communications between Web browsers and Web servers.

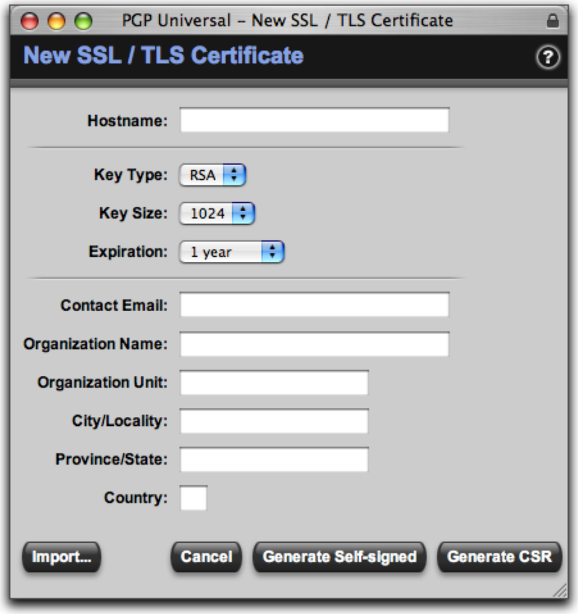
Importing an Existing Certificate

If you have an existing certificate you would like to assign to an interface, you must import it first.

To import a certificate:

1 Click **Add Certificate** on the Certificates card.

The New SSL/TLS Certificate dialog appears.



PGP Universal – New SSL / TLS Certificate

New SSL / TLS Certificate

Hostname:

Key Type: RSA

Key Size: 1024

Expiration: 1 year

Contact Email:

Organization Name:

Organization Unit:

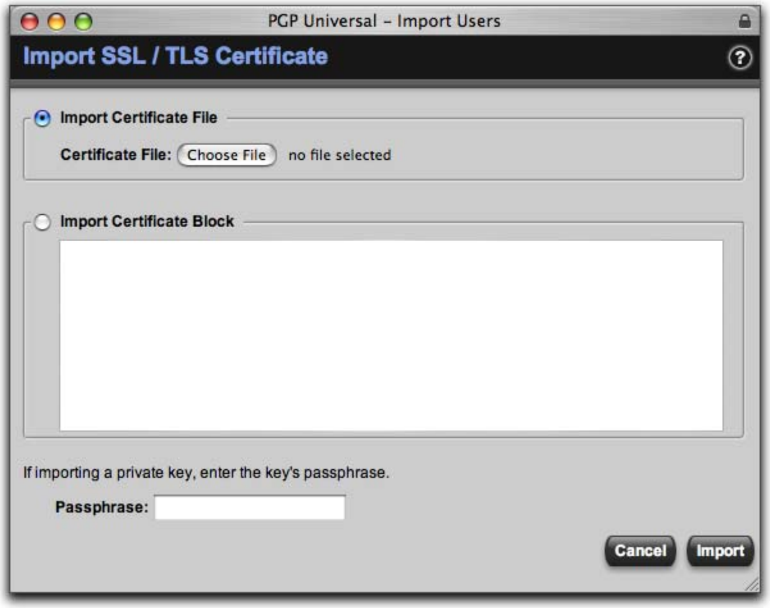
City/Locality:

Province/State:

Country:

2 Click **Import**.

The Import SSL/TLS Certificate screen appears.



PGP Universal – Import Users

Import SSL / TLS Certificate

● Import Certificate File

Certificate File: Choose File no file selected

○ Import Certificate Block

If importing a private key, enter the key's passphrase.

Passphrase:

3 Select **Import Certificate File** and use the **Choose File** button to locate the file of the PKCS #12 certificate.

If you have a native Apache-style SSL/TLS certificate, you can paste both the public and private portions of the certificate into the **Import Certificate Block** box in any order.

4 If the certificate you are importing has a passphrase, enter it in the **Passphrase** field.

5 Click **Import**.

The Import SSL/TLS Certificate screen disappears. The certificate you just added appears on the Certificate card. It can now be assigned to an interface.

Generating a Certificate Request

Services that the PGP Universal Server runs that use the SSL protocol require a server-side SSL/TLS certificate, which includes the DNS name for the IP address on which the service is running. To issue a certificate, the CA vendor needs information found in a certificate request.

To generate a certificate request:

1 Click **Add Certificate** on the Certificates card.

The New SSL/TLS Certificate dialog appears.

2 Enter the PGP Universal Server domain name in the **Hostname** field.

3 In the **Key Type** field, the only supported option is **RSA**.

4 In the **Key Size** field, select **1024**, **1536**, or **2048** from the drop-down list.

5 In the **Expiration** field, select **6 months**, **1 year**, **2 years**, **3 years**, or **5 years** from the drop-down list.

6 Enter an email address in the **Contact Email** field.

7 Enter your organization's name in the **Organization Name** field.

8 Enter your organization's unit designation in the **Organization Unit** field.

9 Enter a city or locality, as appropriate, in the **City/Locality** field.

10 Enter a state or province, as appropriate, in the **Province/State** field. Do not abbreviate the state or province name. For example, enter "California," not "CA."

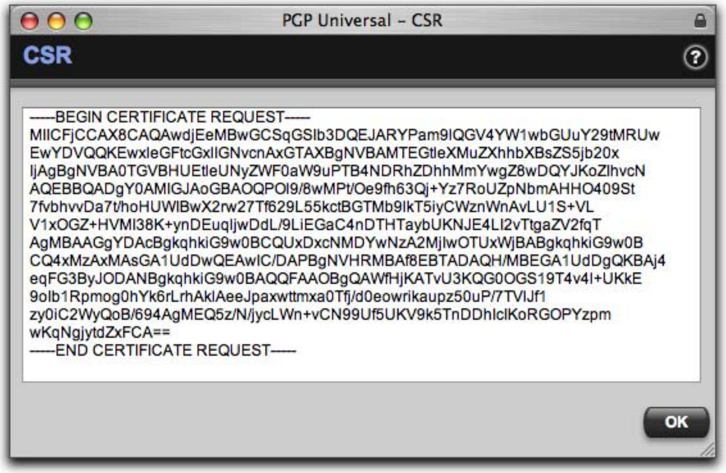
11 Enter a country in the **Country** field.

12 To generate a self-signed certificate that you can use right away, click **Generate Self-signed** after you have entered all the values; a new, self-signed certificate will be created, which you can then assign to an interface. Skip the rest of this procedure because it does not apply.

13 To generate a certificate signing request (CSR), click **Generate CSR**. If you choose this option, the certificate will appear on the Certificate card labeled "Pending" and you will subsequently need to add the certificate once it has been validated and returned by the Certificate Authority (CA).

The New SSL/TLS Certificate dialog disappears. The certificate request is created with the settings you specified.

The CSR dialog appears, showing the certificate request.



```
-----BEGIN CERTIFICATE REQUEST-----
MIICFjCCAX8CAQAwdjEeMBwGCSqGSIb3DQEJARYPam9lQGV4YW1wbGUuY29tMRUw
EwYDVQQKEwxleGFtcGxlIGNvcnAxGTAXBgNVBAMTEGtleXMuZXhhbXBsZS5jb20x
IjAgBgNVBA0TGVBHUEtleUNyZWF0aW9uPTB4NDRhZDhhMmYwgZ8wDQYJKoZIhvcN
AQEBBQADgY0AMIGJAoGBAOQPOI9/8wMPt/Oe9fh63Qj+Yz7RoUZpNbmAHHO409St
7fvbhvvDa7t/hoHUWIBwX2rw27Tf629L55kctBGTMb9IkT5iyCWznWnAvLU1S+VL
V1xOGZ+HVMI38K+ynDEuqIjwDdL/9LiEGaC4nDTHTaybUKNJE4LI2vTtgaZV2fqT
AgMBAAGgYDAcBgkqhkiG9w0BCQUxDxcNMDYwNzA2MjIwOTUxWjBABgkqhkiG9w0B
CQ4xMzAxMAsGA1UdDwQEAwIC/DAPBgNVHRMBAf8EBTADAQH/MBEGA1UdDgQKBAj4
eqFG3ByJODANBgkqhkiG9w0BAQQFAAOBgQAWfHjKATvU3KQG0OGS19T4v4I+UKkE
9oIb1Rpmog0hYk6rLrhAkIAeeJpaxwttmxa0Tfj/d0eowrikaupz50uP/7TVIJf1
zy0iC2WyQoB/694AgMEQ5z/N/jycLWn+vCN99Uf5UKV9k5TnDDhIcIKoRGOPYzpm
wKqNgjytdZxFCA==
-----END CERTIFICATE REQUEST-----
```

14 Copy the contents of the CSR dialog to a file, then click **OK**.

15 Submit this file to your CA.

The CA will send the certificate back to you when they have approved it.

16 When the certificate request has been approved, add the pending certificate (it will appear on the Certificates card), and then assign it to an interface using the Certificate Assignment card.

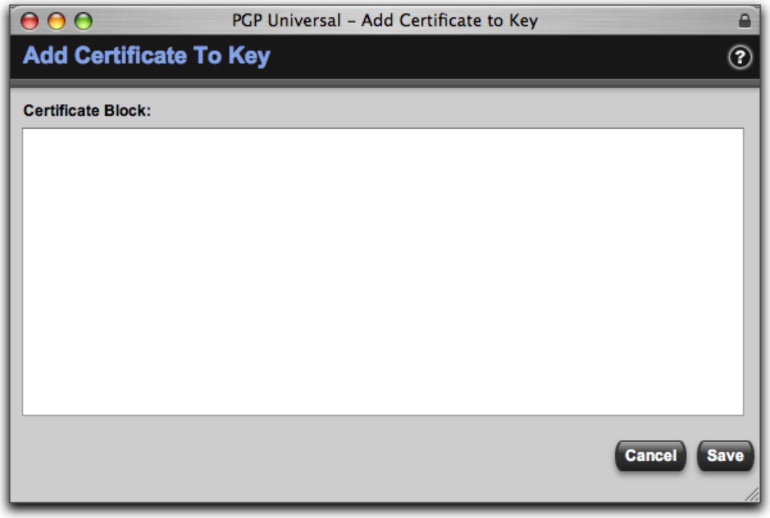
Adding a Pending Certificate

When you send a certificate request, the certificate will appear on the Certificate card listed as pending. When the certificate request is approved, you need to add the pending certificate before it can be assigned to an interface.

To add a pending certificate:

1 Click the plus-sign icon in the Import column of the pending certificate you are adding.

The Add Certificate to Key dialog appears.



2 Paste the validated certificate file that was sent to you by the CA into the **Certificate Block** box.

3 Click **Save**.

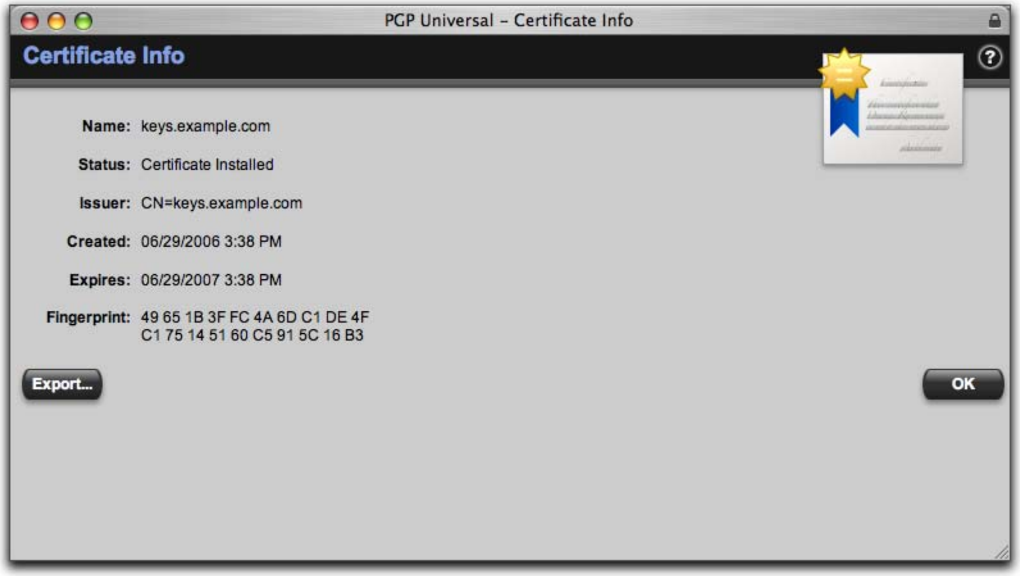
The Add Certificate to Key dialog disappears. The certificate is ready for inspection and can be assigned to an interface.

Inspecting a Certificate

To inspect the settings of a certificate:

1 Click the name of the certificate whose settings you want to inspect.

The Certificate Info dialog appears.



Name: keys.example.com

Status: Certificate Installed

Issuer: CN=keys.example.com

Created: 06/29/2006 3:38 PM

Expires: 06/29/2007 3:38 PM

Fingerprint: 49 65 1B 3F FC 4A 6D C1 DE 4F C1 75 14 51 60 C5 91 5C 16 B3

2 Inspect the information about the certificate you selected. You may need to click **more** to see all the certificate data, which will appear in a pop-up dialog.

3 Click **OK**.

The Certificate Info dialog disappears.

Exporting a Certificate

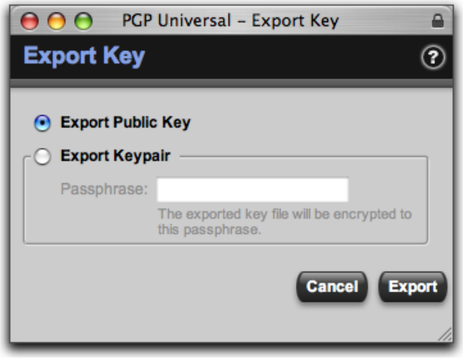
To export a certificate to a PKCS #12 file:

1 Click the name of the certificate you want to export.

The Certificate Info dialog appears.

2 Click **Export**.

The Export Key dialog appears.



● Export Public Key

○ Export Keypair

Passphrase:

The exported key file will be encrypted to this passphrase.

3 To export the certificate with just the public key, select **Export**.

4 To export the certificate with the private key, select **Export Keypair** and enter a passphrase to protect the exported key file, then click **Export**.

5 Specify a location you want to save the file to, then click **Save**.

The certificate is saved to a PKCS #12 file.

Deleting a Certificate

To delete a certificate:

1 Click the Delete icon of the certificate you want to delete.

A confirmation dialog appears.

2 Click **OK**.

The confirmation dialog disappears. The certificate is deleted.

45 Clustering your PGP Universal Servers

This chapter describes the Clustering feature, which allows multiple PGP Universal Servers in an organization to synchronize with each other.

Topics include:

Overview

When you have two or more PGP Universal Servers operating in your organization, you can configure them to synchronize with each other; this arrangement is called a "cluster."

In a cluster, one of the PGP Universal Servers is designated as the Primary server for the cluster; all other cluster members are designated as Secondary servers. The Secondary servers in a cluster synchronize their users, keys, managed domains, and policies with the Primary server. Cached keys found in the mailflow are also replicated across the cluster.

> Be careful joining an already-configured PGP Universal Server into a cluster. All users and policies on the joining server will be deleted and replaced with those of the Primary server.

While a Secondary cluster member becomes unavailable and disconnected from the Primary, it will not receive synchronized data. If the Secondary is disconnected for more than 24 hours, when it reconnects to the Primary it will execute a resynchronization. Resynchronizing data may take several hours, particularly if PGP Universal Web Messenger is in High Availability Mode. All services on the Secondary are stopped while resynchronization occurs.

Benefits of clustering include lower overhead (spreading the system load between the PGP Universal Servers in the cluster means greater throughput) and the ability for email services to continue working even if one of the servers in the cluster goes down, including the Primary server.

If you create a cluster that includes a PGP Universal Server in a gateway placement and an internal user sends an email message to an internal user in Server Key Mode, that message may not be encrypted, to prevent recipients from receiving messages they cannot decrypt. You can avoid unencrypted messages in this scenario by using Client Key Mode instead of Server Key Mode or by not using servers in a gateway placement in a cluster. Disabling the *No Encryption for Regular Internal Users* rule on the Outbound chain will also prevent this problem.

Updates to the PGP Universal Server software are not propagated between cluster members; all PGP Universal Servers in a cluster must update their own software.

PGP Corporation recommends that all members of a cluster use the same version of the PGP Universal Server software. If you need to update to version 2.6 from a previous version, refer to the *PGP Universal Server Upgrade Guide* for more information. If you are updating from version 2.x to any later version of 2.x, first update the Primary server, the update the Secondary servers. The cluster members will temporarily be running different versions of the software, but they will continue to share cluster data.

Clustering and PGP Universal Web Messenger

If you have multiple PGP Universal Servers clustered together, you can choose to store PGP Universal Web Messenger user account information in either of 2 modes.

- High Availability Mode replicates new PGP Universal Web Messenger user accounts on all clustered universal servers running the service. All external user account information exists on all members of the cluster. If a cluster member is not functioning, PGP Universal Web Messenger users will still be able to use the service.
- Home Server Mode assigns a home PGP Server for each new PGP Universal Web Messenger user account. All account information for an external user exists on a single cluster member.

  When the PGP Universal Web Messenger service is running, PGP Universal Web Messenger performs load balancing by spreading new email accounts between the PGP Universal Servers in a cluster. Every 10 minutes the server recalculates its load-balancing decision. New PGP Universal Web Messenger accounts are created on the server that currently hosts the fewest number of accounts. All future email for a specific external user will be stored on the assigned server in the cluster (chosen at account creation time), allowing for better load balancing. If you remove a Secondary server from a cluster, all the PGP Universal Web Messenger email stored on that Secondary is lost.

  If you add a new Secondary cluster member while High Availability Mode is enabled, PGP Universal Web Messenger user data will not automatically be transferred to the new Secondary. Contact PGP Support (www.pgp.com/support) for help transferring the data.

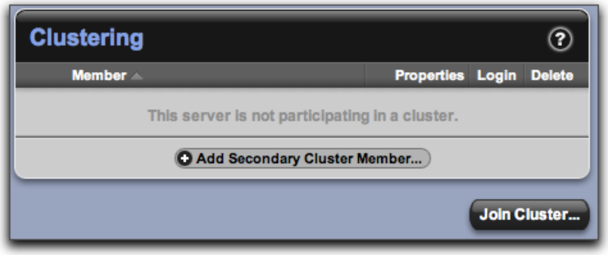
  Refer to Chapter 30, "Configuring PGP Universal Web Messenger" for more information on High Availability Mode.

If a PGP Universal Server in a cluster does go down in Home Server Mode, the PGP Universal Web Messenger inboxes of the users on that server will not be available until you bring back up that server.

Cluster Status

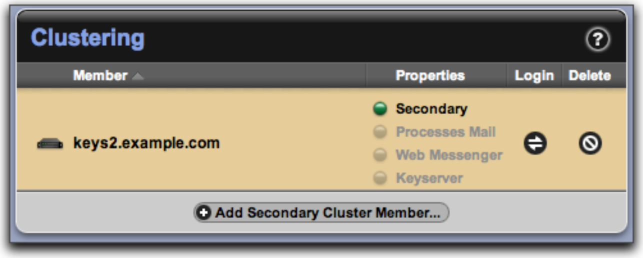
You can quickly determine the cluster status of a PGP Universal Server by looking at the Clustering card. The Clustering card shows a list of the IP/hostnames and properties of all the other servers in the cluster.

- If there are no member IP addresses or hostnames in the list and you can see the message “This server is not participating in a cluster,” then the server is not in a cluster.



This server is not participating in a cluster.

- If the top item in the Properties column says “Secondary,” then the machine you are looking at is a Primary server that has at least one Secondary server in the cluster. The member name showing in the Clustering card is a Secondary server.

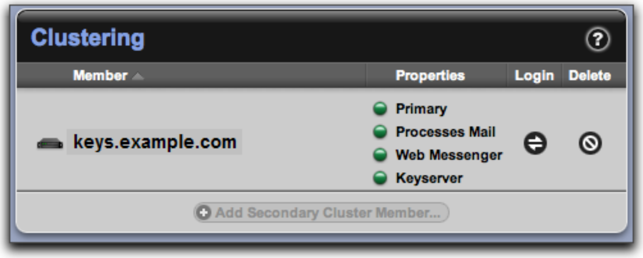


Member	Properties	Login	Delete
keys2.example.com	● Secondary ○ Processes Mail ○ Web Messenger ○ Keyserver	⊖	⊘

Because this is a Primary server in the cluster, **Add Secondary Cluster Member** is shown in bold type (thus selectable) and the **Join Cluster** button is disabled because it is only used by Secondary servers to join a cluster.

The other items in the Properties column indicate functions for which the Secondary server(s) is configured. The Login icon lets you log in to the Secondary server(s) if you need to make configuration changes. The Delete icon lets you delete the Secondary server from the cluster.

- If the top item in the Properties column says “Primary,” then the machine you are looking at is a Secondary server. The top member showing in the Clustering card is a Primary server. Any other IP/hostnames belong to other Secondary cluster members.



Clustering

Member	Properties	Login	Delete
keys.example.com	Primary Processes Mail Web Messenger Keyserver		

Because this is a Secondary server, **Add Secondary Cluster Member** is disabled (because you cannot add a Secondary server to another Secondary server) as is the **Join Cluster** button, because the server is already a member of a cluster.

- You can log into other members of the cluster from the Clustering card. Click the icon in the Login column for the cluster member you want to log into.

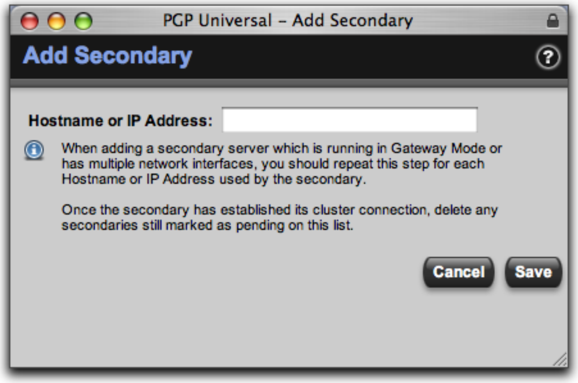
Creating Clusters

This procedure can be used at any time to create a cluster. You can designate which server will act as Primary and which as Secondary in the cluster when you are first configuring the PGP Universal Server during setup. However, any server can act as Primary as long as it is not already Secondary to any other server. Note that if you make an already-configured server into a Secondary server, it will lose all its configured information and take on all the information on the Primary server.

Add Secondaries to your cluster one at a time. After adding the Secondary to the Primary, join it immediately to the cluster before adding another Secondary. Adding multiple Secondaries before joining any of them causes data not to replicate across the cluster.

To create a cluster:

1 On the Primary server, use **Add Secondary Cluster Member** on the Clustering card of the administrative interface to add the Secondary server(s) in the cluster.



PGP Universal – Add Secondary

Add Secondary

Hostname or IP Address:

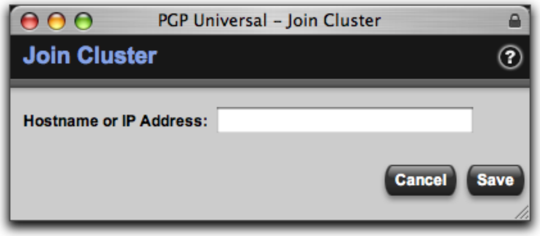
When adding a secondary server which is running in Gateway Mode or has multiple network interfaces, you should repeat this step for each Hostname or IP Address used by the secondary.

Once the secondary has established its cluster connection, delete any secondaries still marked as pending on this list.

You will need to know either the hostname or the IP address of the Secondary servers. The Secondary servers you add will appear as pending on the Clustering card.

2 What you do next depends on whether the Secondary server is already configured:

– If the Secondary server is already configured, on the Secondary servers, use the **Join Cluster** button to join the cluster.



You will need to know either the hostname or the IP address of the Primary server.

– If the Secondary server you added is not yet configured, click the button in the Login column to access the Setup Assistant on the Secondary Server and begin configuring the server.

Deleting Clusters

If you need to dismantle a cluster, the recommended procedure is:

1 On the Primary server in the cluster, delete the Secondary servers.

2 On the Secondary servers, delete the Primary server.

Changing Network Settings in Clusters

Changing the network settings of any Primary or Secondary cluster member will keep the servers from communicating with each other. To change network settings, you will have to remove the servers from the cluster, change the settings, and then reestablish the cluster. Make sure all the cluster members now have the correct hostname and IP address information. See Chapter 44, "Setting Network Interfaces" for information on network settings.

Managing Secondary Settings in Clusters

Setting up a cluster in intended to spread the system load. Some settings are inherited by the Secondary servers from the Primary. The settings you can configure directly on the Secondary server help you balance the amount of work done by each PGP Universal Server. You can manage the following settings directly on a Secondary server:

- Mail proxy settings
- Mail routes

- Services; for example, you can turn on and off PGP Universal Web Messenger, keyserver functionality, SNMP polling and traps, and the PGP Verified Directory. However, you will not be able to change the settings associated with the services; those are inherited from the Primary.
- Licensing
- Network settings
- Backup and restore
- Downloading and installing software updates
- Purging the key cache
- Directory synchronization
- PGP Verified Directory User key vetting

46 Protecting PGP Universal Server with Ignition Keys

This chapter describes the Ignition Key feature, which protects your PGP Universal Server in the event an unauthorized person gains physical control of the hardware.

Topics include:

Overview

Ignition Keys protect the data on your PGP Universal Server (your Organization Key, internal and external user keys in SKM mode, and optionally PGP Universal Web Messenger messages) in case an unauthorized person gains physical control of your PGP Universal Server.

The Ignition Keys card shows the current status of the PGP Universal Server at the top of the screen: for example, **Server is unlocked**. It also lists all Ignition Keys currently configured on the PGP Universal Server. If there are no Ignition Keys configured, **There are currently no ignition keys** appears.

There are two types of Ignition Keys:

- **Hardware Token**. When you insert a PKCS#11 token in the PGP Universal Server, the PGP Universal Server will detect it and allow you to use it as an Ignition Key. The token must contain a single key, which must be protected by a PIN. You can cache the token's PIN so that you do not need to enter the PIN at restart, just have the token present.
- **Soft-Ignition Passphrase**. A passphrase you specify protects the PGP Universal Server.

If the PGP Universal Server is protected by an ignition key, the following information is stored encrypted on the server:

- PGP Universal Web Messenger messages, if you choose it. Enable this option on the Services>Web Messenger card. See Chapter 30, "Configuring PGP Universal Web Messenger" for more information.
- Internal and external user private (SKM) keys.
- Whole Disk Recovery Tokens.

- Organization key, public and private.
- Cluster shared secrets.

Using the Ignition Key feature, you can provide several levels of protection for the hardware hosting your PGP Universal Server:

- No ignition key protection.
- Soft-ignition key with passphrase-only protection (no hardware token).
- Hardware ignition key with PIN cached.
- Hardware ignition key with PIN uncached.

You can create as many Ignition Keys as you like; any combination of hardware token keys and soft-ignition passphrase keys. If you have multiple administrators, for example, you might want to create separate Ignition Keys for each administrator.

If you configure one or more Ignition Keys, but they are not available when the PGP Universal Server is restarted, the Organization Key can be used to unlock the server.

During normal operation, the PGP Universal Server is unlocked; it automatically locks on restart if you have ignition keys enabled. You can manually lock a PGP Universal Server only by rebooting it; you cannot use the administrative interface to lock it.

You can unlock a PGP Universal Server in any of the following ways:

- By inserting a hardware token Ignition Key with a cached PIN. In this case, the PGP Universal Server will be unlocked automatically.
- By inserting a hardware token Ignition Key with an uncached PIN, and then supplying the PIN.
- By supplying a configured soft-ignition passphrase.

Changing the Organization Key deletes Ignition Keys. If you have hard or soft token Ignition Keys configured, regenerating the Organization Key will delete them.

Ignition Keys and Clustering

Ignition Keys are synchronized throughout the cluster; any Ignition Key can be used to unlock any PGP Universal Server in the cluster. However, each PGP Universal Server in the cluster must be unlocked independently on startup.

If a cluster member is locked, that status will be visible on the cluster screen.

Preparing Hardware Tokens to be Ignition Keys

Before you can add a hardware token Ignition Key, you must prepare the token. Currently only the Athena ASEKey USB token can be used as a hardware Ignition Key.

To use an Athena token as a hardware Ignition Key token with PGP Universal Server, the Athena token must have a PGP keypair on it. The only way to get a PGP keypair onto an Athena ASEKey token is using PGP Desktop. One of the PGP Universal Server CDs you received contains a copy of PGP Desktop and the necessary USB token drivers.

The token must have one keypair and a PIN to function as an Ignition Key.

To put a PGP keypair onto an Athena ASEKey token.

1 Obtain an Athena ASEKey USB token.

This is the only token that can be used as an Ignition Key with PGP Universal Server 2.6.

2 Install PGP Desktop 9.6 for Windows onto a Windows system (if you don't already have a Windows system with PGP Desktop installed).

You will use PGP Desktop on this Windows system to either create a keypair on your Athena token or copy an existing keypair to the token.

3 Install the Athena driver software onto the Windows system.

The Athena driver software was included with your PGP Universal Server Installation CDs. The filename is ASECard Crypto Toolkit 3.1b.msi; it includes the ASEKey drivers and the PKCS#11 library. However, if you do not have access to the Installation CDs, you can get the driver software from the Athena website.

4 Once the Windows system has both PGP Desktop for Windows 9.6 and the Athena driver software installed, open PGP Desktop.

5 Insert the Athena ASEKey token into an available USB port on the Windows system.

6 You have two options for getting a PGP keypair onto your Athena ASEKey token: you can create a new PGP keypair directly on the token or you can use the **Send To** context menu to send an existing PGP keypair to the token.

7 To create a new PGP keypair on your Athena ASEKey token, pull down the File menu and select **New PGP Key**.

When the PGP Key Generation Assistant appears, make sure to check the **Generate Key on Token** option, then click **Next**.

8 On the Name and Email Assignment screen, enter a name and an email address (if you plan on using this PGP keypair only as an Ignition Key for PGP Universal Server, you can leave the Primary Email field empty; no email address on a keypair means no messages will be encrypted to the key nor can it be uploaded to the PGP Global Directory. You will be asked if you want to continue without an email address; click Yes.). Click **Next**.

9 On the Passphrase Assignment screen, enter the PIN of your Athena ASEKey token (which will now also be used as the passphrase for keypair); the default for Athena tokens is eight 1s (11111111); click **Next**.

10 PGP Desktop generates the key on the token. When the process completes, click **Next**.

11 On the PGP Global Directory Assistant screen, click **Skip** so that the public key is not sent to the PGP Global Directory. When PGP Desktop reappears, click the **Smartcard Keys** item in the PGP Keys Control box; the PGP keypair you just created should appear on the right.

12 To copy an existing PGP keypair to your Athena ASEKey token, click the **All Keys** item in the PGP Keys Control box. Right click the keypair you want to send to the token (it must be a 1024-bit RSA keypair, not just a public key).

13 On the context menu that appears, slide down to **Send To**, then over to **Smartcard** (if **Smartcard** is grayed out, the selected key doesn't meet the requirements to be on the token).

A warning message explains that the passphrase for the selected keypair will change to the PIN of the token; click **OK**.

14 Enter the current passphrase for the selected keypair, then click **OK**.

15 Enter the PIN of the Athena ASEKey token, then click **OK**.

The keypair is copied to the token.

16 As the default PIN for Athena tokens is publicly known, you need to change it immediately.

The Athena ASEKey token now has a PGP keypair on it. It can be used as a hardware Ignition Key with a PGP Universal Server.

Configuring a Hardware Token Ignition Key

To add a hardware token Ignition Key:

1 On the Ignition Keys card, click **Add Ignition Key**.

The Add Ignition Key dialog box appears.

2 Insert the hardware token you wish to use. The system will read the token's manufacturer and serial number.

3 In the **Ignition Key Name** field, enter a name for the Ignition Key you are creating.

4 Select **Hardware Token**.

5 If you want to store the token's PIN on the PGP Universal Server so that you do not need to enter it on restart, enable **Cache PIN** and enter the PIN for the token you are using.

Caching the token's PIN can save time when you are restarting the PGP Universal Server, but it also lowers security.

If you leave the token in the server and cache the PIN, the server will be unlocked automatically at restart, for example in the event of a power failure. This option is useful if the box is installed in a remote location, because you will not have to go there to enter the PIN. However, this option compromises the security of using an Ignition Key.

6 Click **Save**.

The Ignition Keys card appears; the Ignition Key you just created displays on the list.

Configuring a Soft-Ignition Passphrase Ignition Key

To add a soft-ignition passphrase Ignition Key:

1 On the Ignition Keys card, click **Add Ignition Key**.

The Add Ignition Key dialog box appears.

2 In the **Ignition Key Name** field, enter a name for the Ignition Key you are creating.

Soft-Ignition Passphrase is already selected.

3 In the **Passphrase** field, enter a passphrase for this Ignition Key.

4 In the **Confirm** field, enter the same passphrase again.

5 Click **Save**.

The Add Ignition Key dialog disappears; the Ignition Key you just created appears on the list.

Deleting Ignition Keys

At some point you may no longer need an Ignition Key.

To delete an Ignition Key:

1 Click the icon in the Delete column of the Ignition Key you want to delete.

A confirmation dialog appears, asking if you are sure you want to delete this Ignition Key.

2 Click **OK**.

The Ignition Key is deleted.

Deleting the Ignition Key means all formerly protected data is no longer protected.

47 Backing Up and Restoring System and User Data

This chapter describes PGP Universal Server's backup and restore capabilities.

You can configure Backup options from the System>System Backups card.

Topics include:

Overview

Your data is important. To help make sure that it doesn't get lost, PGP Universal Server supports backing up your data in two ways: scheduled backups and on-demand backups.

Backup files, whether scheduled or on-demand, are always encrypted to your Organization Key before they are sent to the backup location.

Backup files can be stored on the PGP Universal Server, or they can be automatically sent via FTP or SCP to a location you specify. If your remote host is temporarily unavailable, the backup file is stored on the PGP Universal Server until the host becomes available. Make sure that you get the backup file from the host in binary format, not ASCII.

Backups include all information necessary to restore the PGP Universal Server to its exact condition when the backup was created, including proxy and policy settings, as well as keys and user information. PGP Corporation recommends making periodic backups of all of your PGP Universal Servers. Each backup is a full backup.

The System Backups list shows both pending backups (if scheduled) and existing backups.

PGP Universal Server also supports multiple ways of restoring data from a backup.

It is not possible to upload backups of 2GB or larger through the PGP Universal Web interface. Contact PGP Support (www.pgp.com/support) for help restoring your data.

Creating Backups

PGP Universal Server supports two kinds of backups:

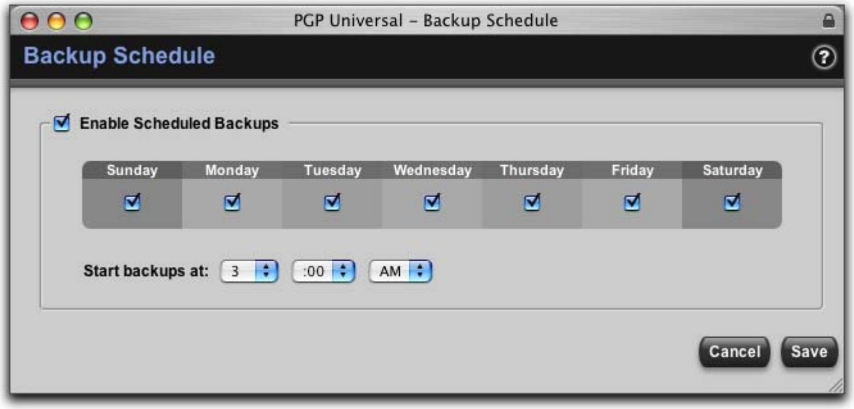
- **Scheduled backups**. You set up a schedule so that backups of your data are made automatically.
- **On-demand backups**. You create a backup immediately.

Scheduling Backups

To schedule automatic backups:

1 On the System>System Backups screen of the administrative interface, click **Backup Schedule**.

The Backup Schedule dialog appears.



☑ Enable Scheduled Backups

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
☑	☑	☑	☑	☑	☑	☑

Start backups at: 3 :00 AM

2 Click **Enable Scheduled Backups**.

3 Put checkmarks in the boxes under the names of the days of the week you want backups performed.

4 Specify a time for the backups to begin in the **Start backups at** field.

5 Click **Save**.

Performing On-Demand Backups

To create a backup right now, on the System>System Backups screen of the administrative interface, click **Backup Now**.

A backup of your data is performed immediately. When the backup is complete, it displays in the Backups list.

Configuring the Backup Location

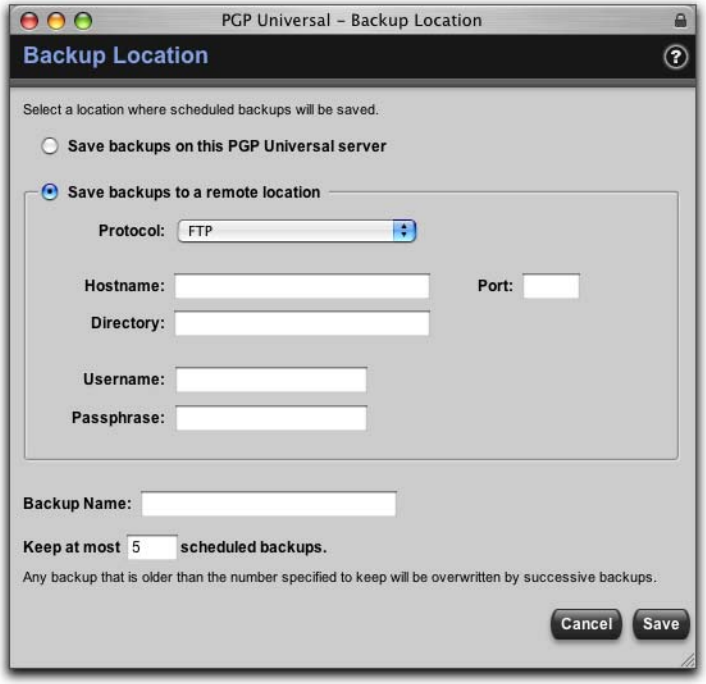
By default, backups are saved to the local disk on the PGP Universal Server. You can specify another location to save backup files to instead. Backup files will then be automatically sent to that location via FTP or SCP.

If you change your backup location, you will not be able to restore from backups stored on the old location, even though the backup files still appear listed on the System Backups page.

To configure the backup location:

1 On the System>System Backups screen of the administrative interface, click **Backup Location**.

The Backup Location dialog appears.



PGP Universal – Backup Location

Backup Location

Select a location where scheduled backups will be saved.

○ Save backups on this PGP Universal server

● Save backups to a remote location

Protocol: FTP

Hostname:

Port:

Directory:

Username:

Passphrase:

Backup Name:

Keep at most 5 scheduled backups.

Any backup that is older than the number specified to keep will be overwritten by successive backups.

2 Choose **Save backups on this PGP Universal Server**, or to have backups saved to a remote location, select **Save backups to a remote location**.

3 Select **FTP**, **SCP Password Authentication**, or **SCP Keypair Authentication**.

4 Enter the backup location hostname in the **Hostname** field.

5 Enter the port number in the **Port** field. The default FTP port is 21. The default SCP port is 22.

6 Specify a **Directory** to which to save the backup. The default backup directory is the FTP or SCP home directory for the username you choose.

7 Enter a valid login name for the location you are saving the backup to in the **Username** field.

8 Enter a valid passphrase for the login name you specified in the **Passphrase** field.

9 If you chose **SCP Keypair Authentication**, import an SSHv2 Key by clicking the Add icon. The Update SSH Key dialog appears.

   a If you do not have an SSH keypair, choose **Generate and Import New Key**. Select the appropriate key size and type.

   b If you already have an SSH keypair, choose **Import Key File**, import your keypair, and enter a passphrase.

   c Click **Import**. The Update SSH Key dialog disappears and the keypair appears in the Backup Location dialog.

10 Enter a name for your backup files into the **Backup Name** field.

11 Specify how many backups you want to save at a time. Once you have saved that number of backups, the oldest backup will be overwritten by the newest backup file.

12 Click **Save**.

   The Backup Location dialog disappears.

You can download your SSH keypair and place the public part of the key onto another server to use to validate logins on that server.

Restoring From a Backup

PGP Universal Server supports three ways of restoring data from an existing backup file:

- **On-demand restore**, where you restore a server that is up and running to the data saved in an existing backup file. This is useful if data has been lost or corrupted but the PGP Universal Server is still up and running.
- **Configuration restore**, where you use the data in an existing backup file to configure a replacement PGP Universal Server. This is useful when you need to replace a PGP Universal Server because it is no longer functional.
- **Specific-version restore**, where you have a backup created by a version of the PGP Universal Server software and you need to restore that backup using a PGP Universal Server running that same version.

Restoring On-Demand

There are two ways to restore server data from a backup.

- On the System Backups screen, click the icon in the Restore column of the backup from which you want to restore.
- If you have a backup file on your system that is *not* on the list of backups but from which you would like to restore, click **Upload Backup**, locate the backup file, then click **Restore**. The PGP Universal Server will be restored from the backup file you specified.

It is not possible to upload backups of 2GB or larger through the PGP Universal Web interface. Contact PGP Support (www.pgp.com/support) for help restoring your data.

The PGP Universal Server is restored to the state when the backup was performed.

Restoring Configuration

You can do a configuration restore when you are configuring a new PGP Universal Server or when reinstalling PGP Universal Server 2.6.

On PGP Universal Server 2.6, you can only restore backed-up data from version 2.5.3 or later. Refer to the *PGP Universal Server 2.6 Release Notes* for details on upgrading and restoring data.

Remember that you must have stored the backup in a location other than the PGP Universal Server itself, if you want to restore the data after upgrading.

Begin by connecting to the new PGP Universal Server for the first time, which brings up the Setup Assistant, as described in Chapter 7, "Setting Up the PGP Universal Server." Restoring from a backup restores everything configured, including proxy and policy settings, as well as keys and user information. If you want to upgrade to 2.6 from a previous version and restore your configuration, see the *PGP Universal Server Upgrade Guide*.

If the PGP Universal Server software you are using for your configuration restore is a different version than was used to make the backup file from which you are restoring, you may have problems performing the restore. If this is the case, refer to "Restoring from a Different Version" on page 403 for more information.

To restore backed-up data during the configuration of a server:

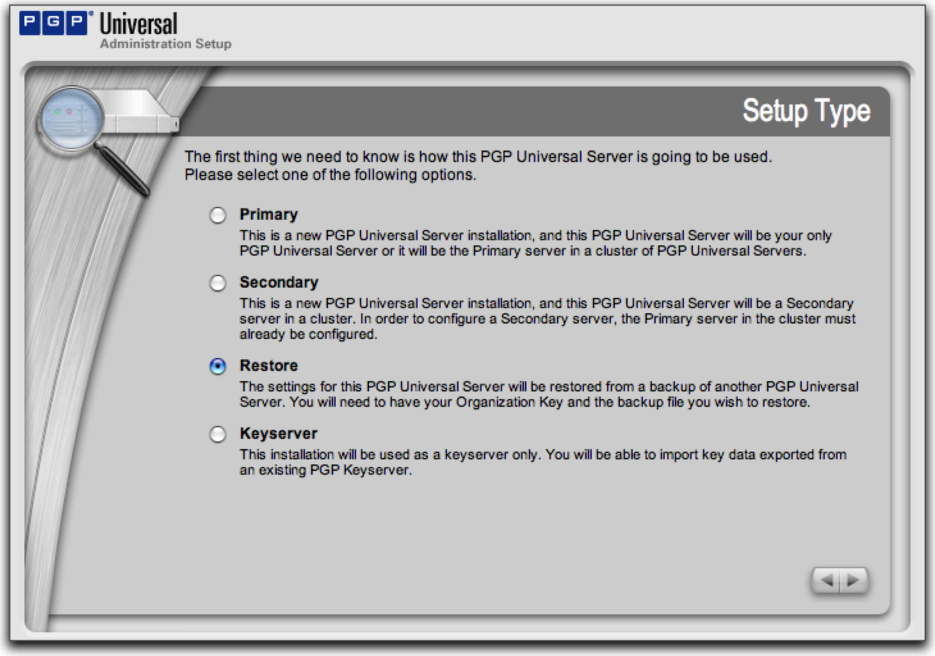
1 Access the Setup Assistant for the new server.

2 On the Welcome screen, read the text and then click the **Forward** button.

The End User License Agreement screen appears.

3 Read the text, click the **I Agree** button at the end, then click the **Forward** button.

The Setup Type screen appears.



Setup Type

The first thing we need to know is how this PGP Universal Server is going to be used. Please select one of the following options.

○ **Primary**
This is a new PGP Universal Server installation, and this PGP Universal Server will be your only PGP Universal Server or it will be the Primary server in a cluster of PGP Universal Servers.

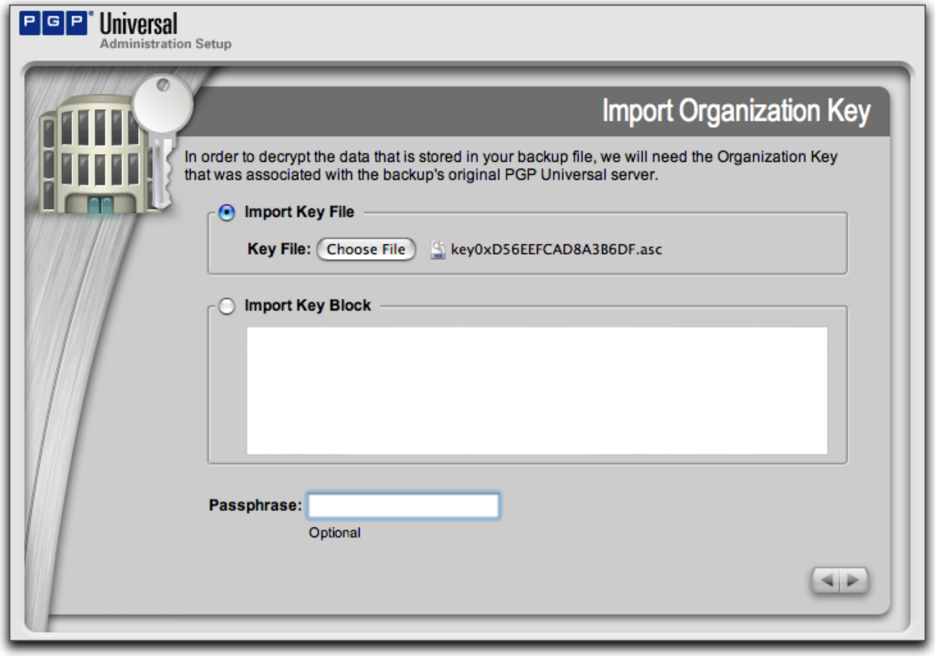
○ **Secondary**
This is a new PGP Universal Server installation, and this PGP Universal Server will be a Secondary server in a cluster. In order to configure a Secondary server, the Primary server in the cluster must already be configured.

● **Restore**
The settings for this PGP Universal Server will be restored from a backup of another PGP Universal Server. You will need to have your Organization Key and the backup file you wish to restore.

○ **Keyserver**
This installation will be used as a keyserver only. You will be able to import key data exported from an existing PGP Keyserver.

4 Select **Restore**, then click the **Forward** button.

The Import Organization Key screen appears.



Import Organization Key

In order to decrypt the data that is stored in your backup file, we will need the Organization Key that was associated with the backup's original PGP Universal server.

● **Import Key File**

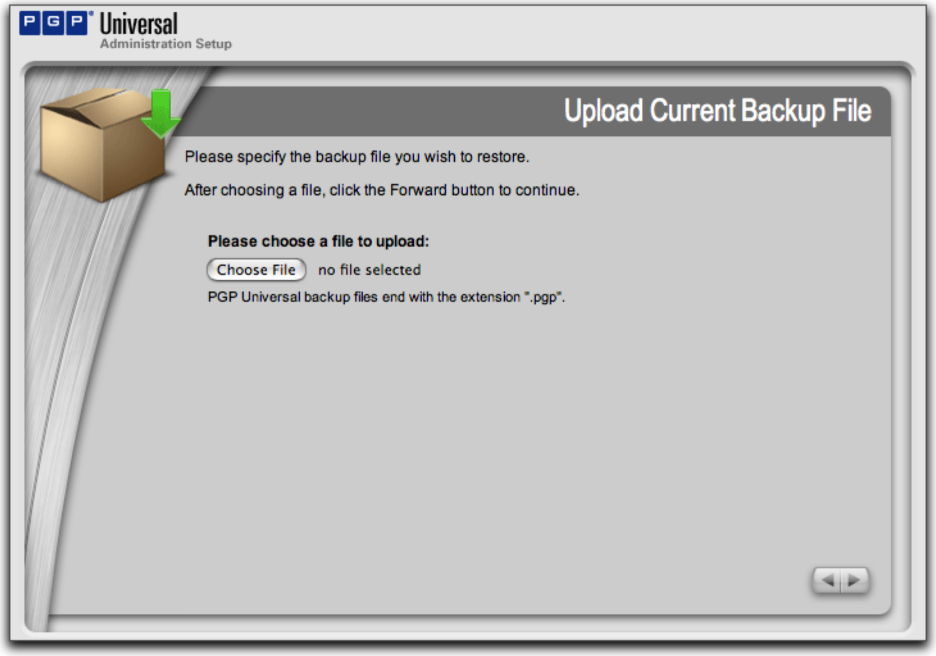
Key File: Choose File key0xD56EEFCAD8A3B6DF.asc

○ **Import Key Block**

Passphrase:
Optional

5 Copy your Organization Key and paste it into the box or import a file containing the key, then click the **Forward** button.

The Upload Current Backup File screen appears.



Please specify the backup file you wish to restore.

After choosing a file, click the Forward button to continue.

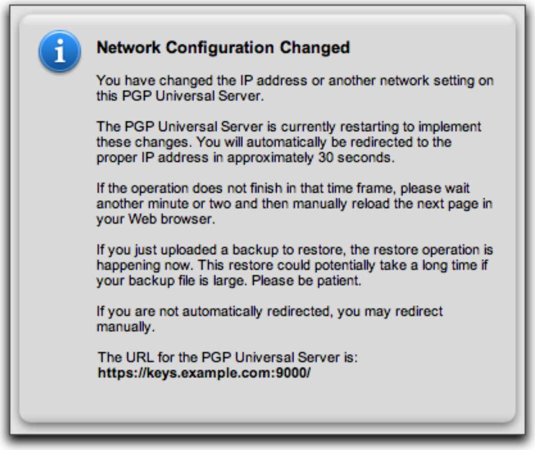
Please choose a file to upload:

no file selected

PGP Universal backup files end with the extension ".pgp".

6 Click **Choose File**, select the backup file from which you want to restore, then click **OK**.

The Network Configuration Changed screen appears and the server restarts automatically.



Network Configuration Changed

You have changed the IP address or another network setting on this PGP Universal Server.

The PGP Universal Server is currently restarting to implement these changes. You will automatically be redirected to the proper IP address in approximately 30 seconds.

If the operation does not finish in that time frame, please wait another minute or two and then manually reload the next page in your Web browser.

If you just uploaded a backup to restore, the restore operation is happening now. This restore could potentially take a long time if your backup file is large. Please be patient.

If you are not automatically redirected, you may redirect manually.

The URL for the PGP Universal Server is:
https://keys.example.com:9000/

You will be redirected to the PGP Universal Server administrative interface.

The server will be configured with the settings from the backup file you selected.

Restoring from a Different Version

Restoring from a backup may not work if the PGP Universal Server software you are using to perform the restore is a different version than was used to make the backup file.

ⓘ On PGP Universal Server 2.6, you can only restore backed-up data from version 2.5.3 or later. Refer to the *PGP Universal Server 2.6 Release Notes* for details on upgrading and restoring data.

If a version mismatch is preventing you from restoring directly from a backup, a specific-version restore will let you restore from the backup file.

Remember that you must have stored the backup in a location other than the PGP Universal Server itself, if you want to restore the data after reinstalling the software.

To perform a specific-version restore:

1 Reinstall the PGP Universal Server software using the original CD or download you received from PGP Corporation.

2 Use the software update feature to update the PGP Universal Server software to the same version as was used to create the backup file.

Refer to Chapter 48, "Updating PGP Universal Server Software," for more information about the software update feature.

3 On the System Backups screen, click the icon in the Restore column of the backup from which you want to restore.

If the backup file from which you want to restore is not on the list of backups, click **Upload Backup**, locate the backup file, then click **Restore**.

The PGP Universal Server is restored from the backup file.

48 Updating PGP Universal Server Software

This chapter tells you how to manage software updates for your PGP Universal Server.

Test software updates on staging servers before implementing them in large live production environments. This allows you to easily return to a previous version if you run into problems.

Overview

The Software Updates card lets you control how and when updates to PGP Universal Servers and PGP Universal Satellite are handled.

You cannot update the software of a PGP Universal Server unless it has been licensed.

PGP Corporation will make updates available periodically to provide support for new security patches or new software releases by other vendors. Updates for PGP Universal Satellite will also be made available this way. (New versions of PGP Universal Satellite install over the existing version.)

The file format for PGP Universal Server updates is .pup.

The PGP Universal Server must not be behind a proxy server, unless it is a transparent proxy, to receive update information automatically.

The list on the Software Updates card shows all updates available and uninstalled for your PGP Universal Server. Updates have to be installed in the appropriate order, so only the update that should be installed next has its install icon active (all other updates have their install icon disabled).

The list shows the name of the update, the version, the size, the date of the last action for that update, and the Install icon.

After the update installs, all users logged in at the time of the update will need to log back into the server. All mail connections shut down during the installation, so any mail sent to the PGP Universal Server during the short update period will be rejected, and the mail client or other sender will resend the message.

Updates to the PGP Universal Server software are not propagated among cluster members; all PGP Universal Servers in a cluster must update their own software.

ⓘ PGP Corporation recommends that all members of a cluster use the same version of the PGP Universal Server software. If you update the software of one member of a cluster, you must update the software of all of the others as well. First update the Primary server, then update the Secondary servers. The cluster members will temporarily be running different versions of the software, but they will continue to share cluster data. If you need to update to version 2.6 from a previous version, refer to the *PGP Universal Server Upgrade Guide* for more information.

Manual update installers are also available via PGP Support (**www.pgp.com/support/**) for customers with network issues or problems auto-updating.

Inspecting Update Packages

Click the name of the update you want to inspect. When the Update Information dialog appears, you can read the information about the update. Click **OK** to close the dialog.

Establishing Software Update Settings

The Software Update Settings button lets you control how updates are received and if they are installed automatically.

To establish software update settings:

1 Click **Software Update Settings**.

The Software Update Settings dialog appears.

2 To have your PGP Universal Server automatically retrieve updates, select **Retrieve updates over the network**. If you would like updates installed automatically when downloaded, put a checkmark next to **Install Automatically**.

3 To prevent your PGP Universal Server from automatically retrieving software updates, select **Do not retrieve updates over the network**. You will have to manually retrieve updates if you choose this option.

4 If you want to see what beta releases of the PGP Universal Server software are available, check **Include beta releases when checking for updates**.

5 Click **Save**.

Checking for New Updates

The Check For Updates button lets you manually check for new updates.

Click **Check For Updates** to check for new updates. If a new update is found, it will appear on the list.

Uploading Update Packages

The Upload Update Packages link lets you retrieve update packages you may have saved on your hard drive. You can upload the package, and then install it as you would any other update package.

1 Click **Upload Update Packages** to upload an update package from your hard drive.

The Upload Update dialog appears.

2 Browse to find the file you want, then click **Upload**.

The update package will appear on the list.

Manually Installing an Update

The Install icon lets you manually install an update. This is only necessary if you are not having updates installed automatically. If you are installing updates manually, you must install them in the order in which they were received, if you are installing more than one.

Click the icon in the Install column to manually install an update.

The text in the Date of Last Action column says "Currently Installing" while the install is in progress.

After the update installs, you will need to log back into the server.

Glossary

Additional Decryption Key (ADK)

A special key to which messages are encrypted, in addition to the recipient. Using an ADK is a way to reconstruct a message if the recipient is unable or unwilling to so (the holder of the ADK can decrypt any message that was encrypted to the ADK), or if required by regulations or corporate policy.

administrative interface

A Web-based interface that gives you control over every aspect of the operation of a PGP Universal Server.

Advanced Encryption Standard (AES)

NIST-approved encryption standards, usually used for the next 20 to 30 years. Rijndael, a block cipher designed by Joan Daemen and Vincent Rijmen, was chosen as the new AES in October 2000.

algorithm (encryption)

A set of mathematical rules (logic) used in the processes of encryption and decryption.

algorithm (hash)

A set of mathematical rules (logic) used in the processes of message digest creation and key/signature generation.

asymmetric encryption

Also known as public-key encryption. Encryption where one key is used to encrypt a message (the public key) and another to decrypt the message (the private key).

authentication

The determination of the origin of encrypted information through the verification of someone’s digital signature or someone’s public key by checking its unique fingerprint.

authorization

To convey official sanction, access, or legal power to an entity.

authorization certificate

An electronic document to prove someone's access or privilege rights, also to prove an individual is who he or she claims to be.

back up

To copy data to a second location as a precaution in case the main version becomes unavailable.

cache

A portion of memory that holds recently accessed data; designed to speed up subsequent access to the same data.

CAST

A 64-bit block cipher using a 64-bit key, six S-boxes with 8-bit input and 32-bit output, developed in Canada by Carlisle Adams and Stafford Tavares.

certificate

An electronic document attached to a public key by a trusted third party, which provides proof that the public key belongs to a legitimate owner and has not been compromised.

Certificate Authority (CA)

A trusted third party who creates certificates that consist of assertions on various attributes and binds them to an entity and/or to a public key.

certification

Endorsement of information by a trusted entity.

ciphertext

Plaintext converted into a secretive format through the use of an encryption algorithm. An encryption key can unlock the original plaintext from ciphertext.

clear-signed message

Messages that are digitally signed, but not encrypted.

cluster

Two or more PGP Universal Servers working together in an organization where users, keys, managed domains, and policies are synchronized between Primary and one or more Secondary servers. Clustering provides security, scalability, and reliability for the servers in the cluster.

Corporate Signing Key (CSK)

A public key that is designated by the security officer of a corporation as the system-wide key that all corporate users trust to sign other keys.

conventional encryption

Encryption that relies on a common passphrase instead of public key cryptography. The file is encrypted using a session key, which encrypts using a passphrase you are asked to choose.

crypto API (CAPI)

Microsoft’s crypto API for Windows-based operating systems and applications.

cryptography

The art and science of creating messages that have some combination of being private, signed, and unmodified with non-repudiation.

cryptosystem

A system comprised of cryptographic algorithms, all possible plaintext, ciphertext, and keys.

Data Encryption Standard (DES)

A 64-bit block cipher, symmetric algorithm also known as Data Encryption Algorithm (DEA) by ANSI and DEA-1 by ISO. Widely used for more than 20 years; adopted in 1976 as FIPS 46.

data integrity

A method of ensuring information has not been altered by unauthorized or unknown means.

decryption

A method of unscrambling encrypted information so that it becomes legible again. The recipient's private key is used for decryption.

demilitarized zone (DMZ) A subnetwork that sits between a trusted internal network, such as a corporate private LAN, and an untrusted external network, such as the Internet.

dictionary attack A calculated brute force attack to reveal a password by trying obvious and logical combinations of words.

Diffie-Hellman The first public key algorithm, invented in 1976, using discrete logarithms in a finite field.

direct trust An establishment of peer-to-peer confidence.

domain A subnetwork composed of a group of clients and servers under the control of one security database. Dividing LANs into domains improves performance and security.

domain name An organization's unique name on the Internet. For example, *example.com* is a domain name.

Domain Name System (DNS) An Internet service that translates domain names into the corresponding IP address. Humans like domain names because they are easier to remember. For the Internet to work, however, the actual IP address must be known. Hence the need for the translation from domain name to IP address.

DNS server A server on the Internet that translates domain names into the corresponding IP address.

email Short for “electronic mail.”

email address A “name” in a specific format that identifies a particular user on a particular email system. On the Internet, email addresses use the following syntax: “user@domain name”; for example, “jsmith@example.com”. Email addresses must be unique.

encryption A method of scrambling information to render it unreadable to anyone except the intended recipient, who must decrypt it to read it.

File Transfer Protocol (FTP) An Internet protocol used for transferring files.

firewall A software or hardware/software combination that protects the perimeter of a network against unauthorized access to that network.

FTP server A server that supports the File Transfer Protocol (FTP).

fully qualified domain name

The full name of a system, consisting of its local hostname and its domain name, including a top-level domain (com and edu are top-level domains). "server.example.com" is a fully qualified domain name; "server" is the local hostname, "example" is the domain name, and "com" is the top-level domain.

gateway

A device on a network that serves as an entrance to another network. In an enterprise, the gateway is a computer that routes data from the computers inside the local network to destinations outside the local network. For people connecting from their homes via an Internet Service Provider (ISP), an ISP computer is their gateway to the Internet.

Gateway Placement

One of the two mail processing modes of a PGP Universal Server (the other is Internal Placement). A gateway placed server logically sits between your mail server and the Internet. The server encrypts outgoing SMTP email and decrypts incoming SMTP email. Email stored on your mail server is stored unencrypted.

hash function

A one-way function that takes an input message of arbitrary length and produces a fixed-length digest.

hierarchical trust

A graded series of entities that distribute trust in an organized fashion, commonly used in ANSI X.509 issuing certifying authorities.

HyperText Transfer Protocol (HTTP)

A protocol commonly used on the World Wide Web for the exchange of HTML documents.

implicit trust

Implicit trust is reserved for keypairs located on your local keyring. If the private portion of a keypair is found on your keyring, PGP solutions assume that you are the owner of the keypair and that you implicitly trust yourself.

Internal Placement

One of the two mail processing modes of a PGP Universal Server (the other is Gateway Placement). An internally placed server logically sits between your email users and your mail server. The server encrypts outgoing SMTP email and decrypts incoming POP and/or IMAP email. Email stored on your mail server is stored encrypted.

International Data Encryption Algorithm (IDEA)

A 64-bit block symmetric cipher using 128-bit keys based on mixing operations from different algebraic groups. Considered one of the strongest algorithms.

International Organization for Standardization (ISO)

Responsible for a wide range of standards, such as the OSI model and international relationship with ANSI on X.509.

Internet Message Access Protocol (IMAP)

An Internet protocol for retrieving email that is stored on an email server. A newer protocol than POP.

Internet Engineering Task Force (IETF)

The main standards organization for the Internet. The IETF is an open, international community of network designers, operators, vendors, and researchers who coordinate the operation, management, and evolution of the Internet. They also resolve short- and mid-range protocol and architectural issues and are a major source of proposals for protocol standards.

Internet Protocol (IP) address

An identifying number for a computer or other device on a TCP/IP network. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be zero to 255. For example, 192.168.1.1 could be an IP address.

integrity

Assurance that data is not modified (by unauthorized persons) during storage or transmittal.

introducer

A person or organization allowed to vouch for the authenticity of someone’s public key. You designate an introducer by signing their public key.

key

A digital code used to encrypt and sign and decrypt and verify messages and files. Keys come in keypairs and are stored on keyrings.

key length

The number of bits representing the key size; the longer the key, the stronger it is.

keypair

A public key and its complementary private key. In public-key cryptosystems, such as the PGP system, each user has at least one keypair.

keyring

A set of keys. Each user has two types of keyrings: a private keyring and a public keyring.

keyserver

A repository for keys and certificates. Some keyservers, such as keyserver.pgp.com, are available to the public. Many enterprises also have keyservers that are available only to members of the enterprise.

Learn Mode

A special mode of the PGP Universal Server where it handles traffic normally (including creating keys for users) but doesn’t encrypt or decrypt any messages.

Lightweight Directory Access Protocol (LDAP)

A protocol that supports access and search operations on directories containing information such as names, phone numbers, and addresses across otherwise incompatible systems over the Internet. PGP Universal Server supports synchronizing PGP Universal Server with an existing LDAP directory.

log

To record an action; to enter a record into a log file. A file that lists actions that have occurred. For example, Web servers maintain log files listing every request made to the server.

mail queue

A list of email messages.

message digest

A compact "distillate" of your message or file checksum. It represents your message, such that if the message were altered in any way, a different message digest would be computed from it.

message integrity check (MIC)

Originally defined in PEM for authentication using MD2 or MD5. Micalg (message integrity calculation) is used in secure MIME implementations.

messaging API (MAPI)

A programming interface from Microsoft that enables a client application to send to and receive mail from Microsoft Exchange Server or a Microsoft Mail messaging system.

meta-introducer

A trusted introducer of trusted introducers.

Multipurpose Internet Mail Extensions (MIME)

An open set of specifications that offers a way to interchange text in languages with different character sets and multimedia email among many different computer systems that use Internet mail standards.

Network Time Protocol (NTP)

An Internet protocol used to synchronize the system's clock with a reference time source on a different server.

non-repudiation

Preventing the denial of previous commitments or actions.

one-way hash

A function of a variable string to create a fixed-length value representing the original pre-image, also called message digest, fingerprint, or message integrity check (MIC).

Organization Key

A special keypair used to sign all user keys that the PGP Universal Server creates and to encrypt server backups. The private key portion of the keypair is used for both functions. Make sure you create a backup of your Organization Key in case there's a problem with your PGP Universal Server. If you have a server backup and a backup of the Organization Key, you can restore the PGP Universal Server.

passphrase

An easy-to-remember phrase used for better security than a single password; key crunching converts it into a random key.

password

A sequence of characters or a word that a subject submits to a system for purposes of authentication, validation, or verification.

PGP/MIME

An IETF standard (RFC 2015) that provides privacy and authentication using the Multipurpose Internet Mail Extensions (MIME) security content types described in RFC1847; deployed in PGP 5.0 and later versions.

PGP

An application and protocol (RFC 2440) for secure email and file encryption developed by Phil R. Zimmermann. Originally published as freeware, the source code has always been available for public review. PGP encryption uses a variety of algorithms such as IDEA, RSA, DSA, MD5, SHA-1 for providing encryption, authentication, message integrity, and key management. PGP encryption is based on the "Web-of-Trust" model and has worldwide deployment.

PGP Universal Satellite

The PGP Universal Satellite software is a small program that resides on the computer of the email user. It allows email to be encrypted all the way to and from the desktop, and it is one way for external users to participate in PGP Universal Server's Self-Managing Security Architecture (SMSA). It also allows users the option of controlling their keys locally.

PGP Universal Server

A device you add to your network that provides encryption, decryption, and digital signatures with little user interaction. The server automatically creates and maintains a Self-Managing Security Architecture (SMSA) by monitoring authenticated users and their email traffic. You can also send protected messages to addresses that aren't part of the SMSA.

PGP Universal Web Messenger mail

A method used by the PGP Universal Server system to deal with users who are not currently part of the SMSA. PGP Universal Web Messenger mail gives the recipient a way to securely read a message and several ways to become part of the SMSA.

plaintext

Normal, legible, unencrypted, unsigned text.

Post Office Protocol (POP)

An Internet protocol for retrieving email that is stored on an email server. An older protocol than IMAP.

port

An endpoint to a logical, not physical, connection on TCP/IP networks. The port number identifies what type of port it is. For example, port 80 is used for HTTP traffic.

private key

The secret portion of a keypair; used to sign and decrypt information. A user's private key should be kept secret, known only to the user.

public key

One of two keys in a keypair: used to encrypt information and verify signatures. A user's public key can be widely disseminated to colleagues or strangers. Knowing a person's public key does not help anyone discover the corresponding private key.

public key infrastructure (PKI)

A certificate system that verifies and authenticates the validity of each party involved in a transaction.

random number

An important aspect to many cryptosystems and a necessary element in generating a unique key(s) that are unpredictable to an adversary. True random numbers are usually derived from analog sources and usually involve the use of special hardware.

revocation

Retraction of certification or authorization.

request for comment (RFC)

An IETF document, either FYI (For Your Information) RFC sub-series that serve as overviews and introductions or STD RFC sub-series that identify specify Internet standards. Each RFC has an RFC number by which it is indexed and by which it can be retrieved (www.ietf.org).

Rijndael

A block cipher designed by Joan Daemen and Vincent Rijmen, chosen as the new Advanced Encryption Standard (AES). It is considered to be both faster and smaller than its competitors. The key size and block size can be 128-bit, 192-bit, or 256-bit and either can be increased by increments of 32 bits.

RSA

Short for RSA Data Security, Inc.; or referring to the principals Ron Rivest, Adi Shamir, and Len Adleman; or referring to the algorithm they invented. The RSA algorithm is used in public key cryptography and is based on the fact that it is easy to multiply two large prime numbers together, but hard to factor them out of the product.

secure channel

A means of conveying information from one entity to another such that an adversary does not have the ability to reorder, delete, insert, or read (SSL, IPSec, whispering in someone’s ear).

Secure Multipurpose Mail Extension (S/MIME)

A proposed standard developed by Deming software and RSA Data Security, Inc. for encrypting and/or authenticating MIME data. S/MIME defines a format for the MIME data, the algorithms that must be used for interoperability (RSA, RC2, SHA-1), and the additional operational concerns such as ANSI X.509 certificates and transport over the Internet. PGP Universal Server supports both S/MIME and OpenPGP encryption protocols.

Secure Shell (SSH)

A program that provides strong authentication and secure connections over insecure networks so that a user can log into another computer over a network, execute commands on a remote machine, or move files from one machine to another.

Secure Sockets Layer (SSL)

Developed by Netscape to provide security and privacy over the Internet. Supports server and client authentication and maintains the security and integrity of the transmission channel. Operates at the transport layer and mimics the “sockets library,” allowing it to be application-independent. Encrypts the entire communication channel and does not support digital signatures at the message level.

Self-Managing Security Architecture (SMSA)

A traditional PKI is a certificate system that verifies and authenticates the validity of each party involved in a transaction. PGP Universal Server, however, automatically creates and maintains a security architecture by monitoring authenticated users and their email traffic. We call this a “self-managing” security architecture (SMSA). PGP Universal Server uses the SMSA it creates to secure messages between the members of the SMSA.

Setup Assistant

A series of screens that steps you through the initial configuration of your PGP Universal Server.

session key

The secret (symmetric) key used to encrypt each set of data on a transaction basis. A different session key is used for each communication session.

sign

To apply a signature.

signature

A digital code created with a private key. Signatures allow authentication of information by the process of signature verification. When you sign a message or file, the PGP program uses your private key to create a digital code that is unique to both the contents of the message and your private key. Anyone can use your public key to verify your signature.

Simple Mail Transfer Protocol (SMTP)

An Internet protocol for sending email messages. Most Internet email systems use SMTP to send email between email servers. Email clients retrieve email using IMAP or POP.

Simple Object Access Protocol (SOAP)

A lightweight, XML-based messaging protocol for encoding the information in a Web service request and response messages before sending them over a network. SOAP messages are independent of any OS or protocol and may be sent using many Internet protocols, including HTTP, MIME, or SMTP.

Smart Trailer

Text added to a message that is sent to the recipient unencrypted. The text tells the recipient that the message could have been encrypted if the recipient were a member of the SMSA. The Smart Trailer includes a link to a location on the PGP Universal Server where the recipient can download the PGP Universal Satellite software, software the recipient can install on his/her machine to become part of the SMSA.

strong passphrase

A passphrase consisting of at least one of each of the following: a lowercase letter, an uppercase letter, a number, and a punctuation mark.

subnet

A portion of a network with a common address component. On TCP/IP networks, subnets are defined as all devices whose IP addresses have the same prefix. For example, all devices with IP addresses that start with 192.168.1. would be part of the same subnet.

subnet mask

A mask used to determine what subnet an IP address belongs to. An IP address has two components, the network address and the host address. On a Class B network, the first two octets of an IP address (192.168, for example) identify the network address; the second two octets (168.1, for example) identify a specific host on the network. Subnetting lets an administrator further divide the host portion of the address into two or more subnets by reserving a part of the host address to identify the subnet.

symmetric encryption

Also known as conventional, secret key, and single key algorithms; the encryption and decryption key are either the same or can be calculated from one another. Two sub-categories exist: block and stream.

timestamping

Recording the time of creation or existence of information.

Transport Layer Security (TLS) Protocol

Provides communications privacy over the Internet. It allows client/server applications to communicate in a way designed to prevent eavesdropping, tampering, or message forgery. The PGP Universal Server uses the TLS protocol for authentication between the server and Microsoft Exchange servers. Defined in RFC 2246; based on the Secure Sockets Layer version 3.0 protocol.

TripleDES

An encryption configuration in which the DES algorithm is used three times with three different keys. Also known as 3DES.

trusted

A public key is said to be trusted by you if it has been validated by you or by someone you have designated as an introducer.

trusted introducer

Someone whom you trust to provide you with keys that are valid. When a trusted introducer signs another person’s key, you trust that the person’s key is valid and you do not need to verify the key before using it.

Twofish

A new 256-bit block cipher, symmetric algorithm. Twofish was one of five algorithms the U.S. National Institute of Standards and Technology (NIST) considered for the Advanced Encryption Standard (AES).

user identification

A text phrase that identifies a keypair. For example, one common format for a user ID is the owner's name and email address. The user ID helps users (both the owner and colleagues) identify the owner of the keypair.

username

The name by which a user is identified by a particular system. One person can have a different name for each system on which he or she participates.

validity

Indicates the level of confidence that the key actually belongs to the alleged owner.

verification

The act of comparing a signature created with a private key to its public key. Verification proves that the information was actually sent by the signer and that the message has not been subsequently altered by anyone else.

Web of Trust

A distributed trust model used by the PGP system to validate the ownership of a public key where the level of trust is cumulative, based on the individual's knowledge of the introducers.

X.509

An ITU-T digital certificate that is an internationally recognized electronic document used to prove identity and public key ownership over a communication network. It contains the issuer's name, the user's identifying information, and the issuer's digital signature, as well as other possible extensions. PGP Universal Server supports both PGP keys and X.509 certificates.

Index