



FORUM SENTRY™ VERSION 9

FTP SECURITY GUIDE



Legal Marks

No portion of this document may be reproduced or copied in any form, or by any means – graphic, electronic, or mechanical, including photocopying, taping, recording, or information retrieval system – without expressed permission from Forum Systems, Inc.

FORUMOST™ Firmware, Forum Systems XMLSec™ WebAdmin, Forum Systems XML Security Appliance™, Forum Sentry™, Forum Presidio™, Forum XWall™, Forum Sentry™ Web Services Gateway, Forum Presidio™ OpenPGP Gateway, Forum FIA Gateway™, Forum XWall Type-PCI™, Forum XWall® Web Services Firewall and Forum XRay™ are trademarks and registered trademarks of Forum Systems, Inc.

All other products are trademarks or registered trademarks of their respective companies.

Copyright © 2002-2024 Forum Systems, Inc. – All Rights Reserved.

Forum Sentry™ Version 9 FTP Security Guide, published May 2024.

D-ASF-SE-012398

Table of Contents

Contents

Contents	3
INTRODUCTION TO THE FTP SECURITY GUIDE	1
Audience for the FTP Security Guide	1
FTP POLICIES AND FTP USER POLICIES	2
FTP User Policies	7
How Appliance Binds FTP and FTP User Policies - Example 2	10
FTP User Policy Terms	11
FTP Policies and FTP User Policies With and Without SSL or TLS Examples	14
OPENPGP KEY POLICIES	29
OpenPGP Key Pairs and Public Certificates	29
OpenPGP Key Policy Examples	31
Import an OpenPGP Key Pair Stored in One File from a File Upload	32
Import an OpenPGP Key Pair Stored in One File Pasted from the Clipboard	34
View OpenPGP Key Pair Details	39
View or Edit OpenPGP Key Settings	40
Edit Number of Days in Advance of Expiry Notification Setting	40
Import an OpenPGP Key Pair Stored in Multiple Files	41
Import an OpenPGP Public Certificate	44
View OpenPGP Public Certificate Details	46
Export OpenPGP Keys	47
Export All OpenPGP Key Pairs as a Keyring	47
Export OpenPGP Keys From OpenPGP Key Details Screen	49
Add a Comment to an OpenPGP Key	51
Validate OpenPGP Key Pairs	52
Export an OpenPGP Key Pair or OpenPGP Public Certificate	53
Generate an OpenPGP Key Pair	55
Delete an OpenPGP Key Pair or OpenPGP Public Certificate	55
OPENPGP KEY POLICIES	57
ASCII Armor Format Options	58
OpenPGP Policy Details Screen Terms	59
OpenPGP Operation Flowchart	60
OpenPGP Network Policy Examples	61
Add an OpenPGP Encrypt Policy Using ASCII Armor	62
Add an OpenPGP Signature Policy	64
Add an OpenPGP Verify Policy	66
Add an OpenPGP Sign and Encrypt Policy	68
Add an OpenPGP Decrypt and Verify Policy	70
SFTP POLICIES	86
SFTP Listener Policies	86
SFTP Listener Policy Screen Terms	87
SFTP Remote Policies	88
SFTP Remote Policy Screen Terms	89
SFTP Proxy Policies	90
SFTP Proxy Policy Screen Terms	91
SSH KEY POLICIES	92
SSH Key Policy Screen Terms	92
Create an SSH Key	92
Import an SSH Public Key or Key Pair	92
APPENDICES	93

Appendix A - FTP Error Codes	93
Appendix B - Constraints of FTP Security Guide	97
Appendix C - Specifications in FTP Security Guide	98
INDEX	99

INTRODUCTION TO THE FTP SECURITY GUIDE

Audience for the FTP Security Guide

The *Forum Systems Sentry™ Version 9 FTP Security Guide* is for System Administrators who will manage:

- FTP/FTPS policies and FTP over SSL/TLS* policies.
- FTP User policies and FTP over SSL/TLS* User policies.
- SFTP Policy Transfers
- OpenPGP key pairs and Certificates received from third parties.
- OpenPGP key generation.
- OpenPGP Encrypt, OpenPGP Decrypt & Verify, OpenPGP Sign, OpenPGP Verify as well as OpenPGP Sign & Encrypt policies.
- Encrypt, decrypt & verify, sign, verify, and encrypt & sign with OpenPGP over FTP.
-
- Compression/decompression of inbound and outbound documents.

* Transport Layer Security

Conventions Used

A red asterisk (*) aligned with a field term means that this field is required. In this and other documentation, the Web Administration Interface is referred to as the WebAdmin and the Forum XML Security Appliance™ is referred to as the 'device', 'product' or 'system'.

In this document, all data or commands that must be entered or selected are displayed in boldface. Example:

User name: **johnsmith**
Password: *********

UI screens which display a STATUS column represent the following states:

- Green status light = enabled policy.
- Yellow status light = a required functional element of this policy is disabled.
- Red status light = disabled policy.

Throughout this and other documents in the Documentation Set, repetitive actions such as:

- View / edit a policy.
- Enable / disable a policy.
- Delete a policy.
- Rename a policy.
- Limit display of policies with Search or Max Results fields.

are not shown. For more information, refer to the Common Operations section of the *Forum Systems Sentry™ Version 9 Web-based Administration Guide*.

Customers with plug-in licenses on the system, confirm that your Integration License is visible on the General Info screen under the SUPPORTED FEATURES section.

Any specifications and constraints referenced in this volume appear in the Appendices of this volume.

FTP POLICIES AND FTP USER POLICIES

FTP Policies

The Network Policies screen manages FTP policies, their settings and status in the system, tracks existing policies, port settings and policy parameters that listeners map to on the system. FTP policies use the FTP transmission protocol and are created by clicking the **New** button on the Network Policies screen. You may create, edit/view and delete policies as well as enable/disable FTP policies.

Note: Selecting the + prefacing an FTP policy name link reveals a listing of all Virtual Directories associated with that policy. Only FTP policies which have the “Process as XML” option checked may have associated virtual directories.

FTP Policies with Encryption and Decryption

FTP policies allow users to add OpenPGP over FTP when the product processes inbound or outbound documents; in particular encrypted or decrypted documents.

FTP Error Codes

FTP error codes are error codes that are returned to the client when the system fails to process data. During run-time, if the system cannot process a request of response on an FTP/FTPS policy or FTP/FTPS user policy, an error code is returned to the client. For information on FTP error codes, refer to the FTP Error Code Table section of this document.

Overview of FTPS

FTPS is a protocol in which secure FTP sessions can be achieved. The security function is performed by the Secure Socket Layer (SSL) and/or Transport Layer Security (TLS). Initially, connections are unsecured (as opposed to HTTPS where the connection is secured immediately) and the FTPS client and server negotiate for secure FTP control and data connections.

Two de-facto FTPS standards are supported in the product; ‘AUTH SSL’ and ‘AUTH TLS’. The ‘AUTH SSL’ standard has been deprecated over the last couple of years, but still has momentum in some installations. The ‘AUTH TLS’ has been widely adopted because of its adherence to RFC 2228 – “FTP Security Extensions” and additional impetus from Paul Ford-Hutchinson’s “Securing FTP with TLS” RFC draft. The product supports the above standards in both client and server applications.

FTP over SSL or TLS Policies

FTP over Secure Socket Layers/Transport Layer Security (SSL/TLS) policies use the FTPS protocol for securing FTP over SSL/TLS. FTP over SSL/TLS policies allow users to utilize FTP over SSL/TLS when the product processes inbound or outbound documents; including OpenPGP encrypted or decrypted documents.

FTP over SSL or TLS Policy Prerequisites

Follow the listed sequence to create an FTP over SSL policy:

1. create a key pair.
2. create an SSL policy that refers to the key pair.
3. create an FTP policy that refers to an SSL policy.

ZIP Archives with FTP Policies

Currently, the system supports for ZIP archives that have only one entry. If the incoming ZIP archive contains more than one entry, then only the first entry will be decompressed and any remaining entries will be ignored. All files will be named .zip on placement on remote servers.

Network Policy Terms for FTP Policies and FTP over SSL or TLS Policies

While creating an FTP policy or FTP over SSL/TLS policy, please consider the following:

TERM	DEFINITION
Name	The identifier for this Network policy.
Status	<ul style="list-style-type: none">• Green status light = enabled policy.• Yellow status light = a required functional element of this policy is disabled.• Red status light = disabled policy. <p>Network policies are automatically enabled upon creation when the network topology option matches the Network policy.</p>
Protocol	The protocol that is supported by this Network policy, or FTP.
Listener Address	The IP address of the system.
Remote Address	The IP address of the back end server.

Note: FTP policies, FTP over SSL/TLS policies, FTP User policies, and FTP over SSL/TLS User policies share system resources; therefore, Forum Systems recommends limiting the number of active policies to 32.

FTP Policy Terms

While creating an FTP or FTP over SSL/TLS policy, please consider the following:

FIELD NAME	DEFINITION
FTP NETWORK POLICY	
Name	The identifier for this FTP policy.
Process as XML	This feature is available only with an upgrade to the Forum product so ignore this checkbox.
User Policy Rule	<p>FTP user policy rules manage exactly how FTP Users should be processed. REQUIRED means that when a user authenticates with the system, they MUST have a valid FTP User policy that corresponds to the provided user name and password. The user is then authenticated on the system and routed properly using the settings specified in the FTP User policy.</p> <p>If the user who is transmitting an FTP session matches with the user name and password, then the Remote and OpenPGP policies specified in this policy are applied.</p> <p>If a valid user who is transmitting an FTP session logs on to the product but there is no FTP User policy which exists for that user, the login will fail.</p> <p>The REQUIRED FTP user policy rule forces all users to authenticate with the product.</p> <p>OPTIONAL means if the user name provided at authentication time (in the Local Authentication section of the FTP User policy) matches an FTP User policy, the settings of the FTP User policy will apply.</p> <p>If the user name provided at authentication time (in the Local Authentication section of the FTP User policy) does not match an FTP User policy, then the settings for the FTP listener itself (FTP policy) will be used. Authentication will be performed on the back end FTP server.</p> <p>IGNORED is a state that disregards any FTP User policies and processes all transactions with the configuration of the FTP listener itself (FTP policy). The back end FTP server is used to authenticate the user.</p> <p>Note: The Required, Ignored and Optional settings are for authentication at the back end. If authentication is never achieved, Administrators will not be allowed to log into the FTP server.</p>
LISTENER	
Listener IP	The IP address that the product will listen for connections on. The listener IP is the IP alias or the IP address of the device port on the product.
Listener Port	The port number that the product listens for connections on.
Read Timeout	Read timeout in minutes for holding open connection that is idle.
Override PASV IP Address	Override the Listener IP address when responding to the PASV command. This is useful when within a DMZ behind a firewall.
PASV IP	IP address that will be used to respond to the PASV command.

Address	
FTP over SSL/TLS	With the FTP over SSL/TLS checked, you are creating an FTP over SSL/TLS network policy.
SSL Termination Policy	The SSL Termination policy selected to bind to this FTP over SSL network policy.
SSL Initiation Policy	The SSL Initiation policy selected to bind to this FTP over SSL network policy.
FTPS Mode	<p>Explicit: FTP client issue a specific command to the FTP server after establishing a connection. The default FTP server port is used..</p> <p>Implicit: automatically begins with an SSL connection as soon as the FTP client connects to an FTP server. In implicit security, the FTP server defines a specific port for the client (990) to be used for secure connections</p>
DEFAULT REMOTE	
Prevent user@host Syntax	<ul style="list-style-type: none"> With the Prevent user@host Syntax checkbox checked, you are specifying that the product will proxy all traffic to the remote server IP or host name and remote port defined. When checked, any attempts to use the user@host Syntax proxy will not be allowed. With the Prevent user@host Syntax checkbox unchecked, the product will allow users to proxy to the specified host using the product's proxy capabilities.
Remote Server IP or Host Name	IP address or host name of your back end FTP server.
Remote Port	Requests processed by the Service policy will be sent to this port on the back end FTP server. For example, FTP traffic generally uses Port 21.
FTP over SSL/TLS	With the FTP over SSL/TLS checked, you are creating an FTP over SSL network policy.
SSL Remote Policy	The SSL Initiation policy selected to bind to this FTP over SSL network policy.
FTPS Mode	<p>Explicit: FTP client issue a specific command to the FTP server after establishing a connection. The default FTP server port is used..</p> <p>Implicit: automatically begins with an SSL connection as soon as the FTP client connects to an FTP server. In implicit security, the FTP server defines a specific port for the client (990) to be used for secure connections</p>
OpenPGP GET	The OpenPGP GET drop down list includes all OpenPGP policies. Use OpenPGP GET control actions to select which OpenPGP policy to use for a GET (data from FTP server to FTP client) operation. Select None if you are not interested in applying any policy at all.
OpenPGP PUT	The OpenPGP PUT drop down list includes all OpenPGP policies. Use OpenPGP PUT control actions to select which OpenPGP policy to use for a PUT (data from FTP client to FTP server) operation. Select None if you are not interested in applying any policy at all.

FIELD NAME	DEFINITION
OPENPGP	
OpenPGP GET	The OpenPGP GET drop down list includes all OpenPGP policies. Use OpenPGP GET control actions to select which OpenPGP policy to use for a GET (data from FTP server to FTP client) operation. Select None if you are not interested in applying any policy at all.
OpenPGP PUT	The OpenPGP PUT drop down list includes all OpenPGP policies. Use OpenPGP PUT control actions to select which OpenPGP policy to use for a PUT (data from FTP client to FTP server) operation. Select None if you are not interested in applying any policy at all.
DATA COMPRESSION	
[None]	Use [None] to select no data compression at all.
ZIP-Compress	Use this option to compress data using the ZIP compression algorithm.
ZIP-Decompress	Use this option to decompress data using the ZIP compression algorithm.
GZIP-Compress	Use this option to compress data using the GZIP compression algorithm.
GZIP-Decompress	Use this option to decompress data using the GZIP compression algorithm.
COMMENT	
Comment	Enter any relevant comments about this policy in the Comment field.
CREATED / MODIFIED	
Created/ Modified	The system populated a date/timestamp and comment text for any FTP User policies that may be bound to this FTP policy.
FTP USER POLICY	
FTP User Policy	FTP User policies are visible only after they have been created.

FTP User Policies

The FTP User policy screen is a subset of the FTP policies screen. FTP User policies allow you to enforce more granular routing and security decisions based on local authentication credentials and remote authentication credentials, if configured. The FTP User Policy screen overrides the FTP policy configuration. Generally you may specify OpenPGP policies generically for the listeners, but the product allows you to override these by a variety of settings on FTP User policies.

The FTP User policy screen is an optional feature. If a new FTP User policy feature is configured, it overrides the “DEFAULT REMOTE” and OPENPGP policies in the FTP policy. With this more granular control over an FTP transaction, the system provides more authentication features. FTP User policies allow you to setup authentication credentials to access the local FTP server on the system and also the remote authentication credentials of the back end FTP server.

Note: All OpenPGP users specific to FTP sessions are managed through the FTP policy screen, not through the Users screen. When creating an FTP user from the FTP USER POLICY screen, consider that this user is a separate user from any LDAP user or Forum user visible on the Users screen.

Interactions Between FTP Policies and FTP User Policies

Once you have created your first FTP policy, click an FTP policy name link to return to the bottom of the FTP Policy details screen.

Note: Only after you create the first policy will you see the table and table headers under which this policy will be listed.

Before Creating First FTP User Policy

NETWORK POLICIES > FTP NETWORK POLICY

FTP NETWORK POLICY

Name*:

Process as XML: ☐

User Policy Rule:

LISTENER

Listener IP*:

Listener Port*:

FTP over SSL/TLS: ☐

SSL Listener Policy:

Auth Mode: ☒ TLS ☐ SSL

DEFAULT REMOTE

Prevent user@host Syntax: ☐

Remote Server*:

Remote Port*:

FTP over SSL/TLS: ☐

SSL Remote Policy:

Auth Mode: ☒ TLS ☐ SSL

OPENPGP

OpenPGP GET:

OpenPGP PUT:

DATA COMPRESSION

Compression GET:

Compression PUT:

FTP USERS

☐ **FTP USER POLICY**

CREATED

No items to display

After Creating First FTP User Policy

NETWORK POLICIES > FTP NETWORK POLICY

FTP NETWORK POLICY

Name*:

Process as XML: ☐

User Policy Rule:

LISTENER

Listener IP*:

Listener Port*:

FTP over SSL/TLS: ☐

SSL Listener Policy:

Auth Mode: ☒ TLS ☐ SSL

DEFAULT REMOTE

Prevent user@host Syntax: ☐

Remote Server*:

Remote Port*:

FTP over SSL/TLS: ☐

SSL Remote Policy:

Auth Mode: ☒ TLS ☐ SSL

OPENPGP

OpenPGP GET:

OpenPGP PUT:

DATA COMPRESSION

Compression GET:

Compression PUT:

COMMENT

Comment:

CREATED/MODIFIED

Created: Oct 12, 2004 1:48 AM Modified: Oct 12, 2004 1:48 AM

FTP USERS

<input type="checkbox"/> FTP USER POLICY	CREATED	MODIFIED
<input type="checkbox"/> FTP_TransportR	Oct 12, 2004 1:52 AM	Oct 12, 2004 1:52 AM

How Appliance Binds FTP and FTP User Policies - Example 1

The following graphics display an FTP policy (FTP_SSL_DomesticVendors) and how an FTP User policy (FTP_SSL_VendorCenters) is bound to it:

FTP Network Policy Options

NETWORK POLICIES > FTP NETWORK POLICY

FTP NETWORK POLICY

Name*:

Process as XML: ☐

User Policy Rule:

LISTENER

Listener IP*:

Listener Port*:

FTP over SSL/TLS: ☒

SSL Listener Policy: **For FTP over SSL / TLS, select an SSL Termination Policy with Auth Mode.**

Auth Mode: ☐ TLS ☒ SSL

DEFAULT REMOTE

Prevent user@host Syntax: ☐

Remote Server IP or Host Name*:

Remote Port*:

FTP over SSL/TLS: ☒

SSL Remote Policy: **For FTP over SSL / TLS, select an SSL Initiation Policy with Auth Mode.**

Auth Mode: ☐ TLS ☒ SSL

OPENPGP

OpenPGP GET:

OpenPGP PUT:

DATA COMPRESSION

Compression GET:

Compression PUT: **For transforming data, select compression control actions for PUTs and GETs.**

COMMENT

Comment:

CREATED/MODIFIED

Created: Mar 23, 2005 12:16 PM Modified: Has Not Been Modified

FTP USERS

☐ **FTP USER POLICY** **CREATED**

☒ **FTP_SSL_VendorCenters** Mar 23, 2005 12:23 PM **Delete**

This FTP User Policy is bound to this FTP Network Policy.

For using this Network policy with OpenPGP, bind OpenPGP Policies to OpenPGP GET and PUT control actions .

OPENPGP POLICIES

OPENPGP POLICY	TYPE
<input type="checkbox"/> PGP_Dave_DecVer	Decrypt & Verify
<input type="checkbox"/> PGP_Dave_Encrypt	Encrypt
<input type="checkbox"/> PGP_Dave_SigEnc	Sign & Encrypt
<input type="checkbox"/> PGP_Dave_Sign	Sign
<input type="checkbox"/> PGP_Dave_Verify	Verify
<input type="checkbox"/> PGP_Sandy_DecVer	Decrypt & Verify
<input type="checkbox"/> PGP_Sandy_SigEnc	Sign & Encrypt

Figure 2: Binding an FTP Policy to an FTP User Policy with various SSL or TLS Options and OpenPGP Policies and Compression Action Options.

How Appliance Binds FTP and FTP User Policies - Example 2

FTP User Policy Options

NETWORK POLICIES > FTP NETWORK POLICY

FTP USER POLICY
Policy Name*: FTP_SSL_VendorCent

LOCAL AUTHENTICATION
System user: marysmith

REMOTE AUTHENTICATION
☐ Use system user
☒ Use non-system user
 Remote User Name*: admin1
 Remote Password: michellecote
 Confirm Remote Password:

REMOTE SERVER
 Remote IP Address: 11.11.11.57
 Remote Port: 27
 FTP over SSL/TLS: ☒
 SSL Remote Policy: SSL_Init_Danielle
 Auth Mode: ☐ TLS ☒ SSL

OPENPGP
 OpenPGP Get: [None]
 OpenPGP Put: [None]

DATA COMPRESSION
 Compression GET: GZIP - Decompress
 Compression PUT: GZIP - Compress

COMMENT
 Comment:

For FTP over SSL / TLS, select an SSL initiation Policy with Auth Mode.

SSL_Init_Danielle
 SSL_Init_Danielle
 SSL_Init_Walter
 SSL_Policy_527873370

For using this User Network policy with OpenPGP, bind OpenPGP Policies to OpenPGP GET and PUT control actions .

[None]
 [None]
 PGP_Dave_DecVer
 PGP_Dave_Encrypt
 PGP_Dave_SigEnc
 PGP_Dave_Sign
 PGP_Dave_Verify
 PGP_Sandy_DecVer
 PGP_Sandy_SigEnc

OPENPGP POLICIES

OPENPGP POLICY	TYPE
<input type="checkbox"/> PGP_Dave_DecVer	Decrypt & Verify
<input type="checkbox"/> PGP_Dave_Encrypt	Encrypt
<input type="checkbox"/> PGP_Dave_SigEnc	Sign & Encrypt
<input type="checkbox"/> PGP_Dave_Sign	Sign
<input type="checkbox"/> PGP_Dave_Verify	Verify
<input type="checkbox"/> PGP_Sandy_DecVer	Decrypt & Verify
<input type="checkbox"/> PGP_Sandy_SigEnc	Sign & Encrypt

For transforming data, select compression control actions for PUTs and GETs.

[None]
 ZIP - Compress
 ZIP - Decompress
 GZIP - Compress
 GZIP - Decompress

Save

Figure 3: How an FTP User Policy is Bound to an FTP Policy with various SSL or TLS Options and OpenPGP Policies and Compression Action Options.

FTP User Policy Terms

While creating an FTP User policy or an FTP over SSL/TLS User policy, please consider the following:

FIELD NAME	DEFINITION
FTP USER POLICY	
Policy Name	The identifier for this FTP user policy.
LOCAL AUTHENTICATION	
System user	From the System user drop down list, select the user whose credentials will be presented to the FTP server.
	Note: As of Release 5.1, local users no longer exist for local authentication. All users are managed from the USERS screen.
REMOTE AUTHENTICATION	
User system user	With the Use system user option, the credentials presented to the remote server are those of the user policy name selected. This user must have Enable for basic auth on so their password is clear text.
User non-system user	With the Use non-system user option, the credentials presented to the remote server are those of the remote user name / remote password entered.
Remote User Name	Remote User Name applies to the user name for a non-system user when authenticating to the remote server. The Remote User Name may be from 0-unlimited keyboard characters.
Remote Password	Remote Password is the password of the remote server that traffic will be forwarded to during this FTP session. The Remote Password may be from 0-unlimited keyboard characters.
Confirm Remote Password	For verification purposes, re-enter your Remote Password.

FIELD NAME	DEFINITION
REMOTE SERVER	
Remote IP Address	Remote IP Address is the IP of your back end FTP server.
Remote Port	Remote Port is the port on the back end FTP server that the product is forwarding traffic to. For example, FTP traffic generally uses Port 21.
FTP over SSL/TLS	With the FTP over SSL/TLS checked, you are creating an FTP over SSL User policy.
SSL Remote Policy	The SSL Initiation policy selected to bind to this FTP over SSL User policy.
FTPS mode	<p>Explicit: FTP client issue a specific command to the FTP server after establishing a connection. The default FTP server port is used..</p> <p>Implicit: automatically begins with an SSL connection as soon as the FTP client connects to an FTP server. In implicit security, the FTP server defines a specific port for the client (990) to be used for secure connections</p>
OPENPGP	
OpenPGP GET	<p>The OpenPGP GET drop down list includes all OpenPGP policies. Use OpenPGP GET control actions to select which OpenPGP policy to use for a GET operation (transfer of data from FTP server to FTP client). Data is processed with the OpenPGP operation in the policy while it flows from the FTP server to the FTP client.</p> <p>Select None to apply no FTP User policy to this FTP policy action.</p>
OpenPGP PUT	<p>The OpenPGP PUT drop down list includes all OpenPGP policies. Use OpenPGP PUT control actions to select which OpenPGP policy to use for a PUT operation (transfer data from FTP client to FTP server). Data is processed with the OpenPGP operation in the policy while it flows from the FTP client to the FTP server.</p> <p>Select None to apply no FTP User policy to this FTP policy action.</p>
DATA COMPRESSION	
[None]	Use [None] to select no data compression at all.
ZIP-Compress	Use this option to compress data using the ZIP compression algorithm.
ZIP-Decompress	Use this option to decompress data using the ZIP compression algorithm.
GZIP-Compress	Use this option to compress data using the GZIP compression algorithm.
GZIP-Decompress	Use this option to decompress data using the GZIP compression algorithm.
COMMENT	
Comment	Enter any relevant comments in the Comment field.

Note: When selecting one compression mode on a PUT (for example, GZIP-compress) you may want to select the complementary compression mode on a GET (GZIP-decompress).

Data compression may or may not be used in conjunction with OpenPGP operations. Consider that OpenPGP encryption **always** compresses data by default **prior** to encryption, and OpenPGP signing **always** compresses data by default **after** signing. Therefore, even though it is not prohibited, there is minimum benefit to be gained from associating a data compression action with these specific OpenPGP operations.

Administrators may, however, gain benefit from applying compression with OpenPGP Decrypt & Verify and OpenPGP Verify policies. For example, if an OpenPGP GET operation is linked to an OpenPGP Verify policy, and a GET ZIP-Compress action is specified, then the data will be compressed using the ZIP algorithm **after** it has been verified. Similarly, if an OpenPGP PUT operation is linked to an OpenPGP Decrypt & Verify policy, and a PUT ZIP-Compress action is specified, then the data will be compressed using the ZIP algorithm **after** it has been decrypted.

Data compression or decompression is always the **last** operation performed on the data for PUT control actions, and the **first** operation for GET control actions. Resulting zip/gzip compressed files will have extensions .zip and .gz as appropriate.

As of Release 5.1, local users no longer exist. All users are managed from the USERS screen.

FTP Policies and FTP User Policies With and Without SSL or TLS Examples

Examples for FTP and FTP User policies include:

- Add an FTP Policy.
- Add an FTP over SSL/ TLS User Policy.

Follow these steps to:

- ## Adding an FTP Policy with an Associated OpenPGP Policy

This operation assumes that, at minimum, one OpenPGP Decrypt & Verify policy has been previously created.

NETWORK POLICIES > FTP NETWORK POLICY

FTP NETWORK POLICY

Name*:

Labels:

Process as XML: ☐

User Policy Rule:

LISTENER

Use Device IP: ☐

Listener IP*:

Listener Port*:

Read Timeout(minutes)*:

Override PASV IP Address: ☐

PASV IP Address:

Enable PASV Port Range: ☐

Start PASV Range:

End PASV Range:

FTP over SSL/TLS: ☐

SSL Listener Initiation Policy:

SSL Listener Termination Policy:

FTPS Mode: ☒ Explicit ☐ Implicit

DEFAULT REMOTE

Prevent user@host Syntax: ☐

Remote Server*:

Remote Port*:

Use PASV IP: ☒

FTP over SSL/TLS: ☐

SSL Remote Initiation Policy:

SSL Remote Termination Policy:

FTPS Mode: ☒ Explicit ☐ Implicit

OPENPGP

OpenPGP GET:

OpenPGP PUT:

DATA COMPRESSION

Compression GET:

COMMENT

Comment:

- Navigate to the **Network Policies** screen and click **New**.

- On the NEW NETWORK POLICY screen, select the **FTP** radio button and then click **Next**.
- On the FTP NETWORK POLICY screen, in the Name field, enter the **name** for this policy.
- Skip the Process as XML checkbox.
- Retain the default (Optional) setting in the Use Policy Rule drop down list.

Note: Use the User policy rules drop down list to set an override option that toggles FTP Users policies to be Required, Optional or Ignored. Although you are setting this override option now, you have not connected the FTP User to this FTP policy yet. The override is active when you create an FTP User policy. When working with FTP User policies, consider that:

- A) When the FTP User policy is set to REQUIRED or OPTIONAL, the FTP User policy becomes bound to the FTP policy and the FTP User policy will now override the settings on the associated FTP policy.
- B) When the FTP User policy is set to REQUIRED, only FTP User policies attached to FTP Server policies will be able to log in and use the product.
- X) When the FTP User policy is set to OPTIONAL, only users that exist as an FTP User policy or as a user of a back end FTP server can log in.
- Δ) When the FTP User policy is set to IGNORED, this option processes all transactions with the configuration of the FTP listener itself (FTP policy). The back end FTP server is used to authenticate the user.

During run-time, it is at this point in processing documents that the user would be authenticated on the FTP server. If user authentication were to fail, then OpenPGP GET or PUT control actions (steps 17 and 18) and data compression actions (steps 19 and 20) would never take place.

- In the Listener IP field, enter the **listener IP address**.
- In the Listener Port field, enter the **listener port**.
- Skip the FTP over SSL/TLS checkbox.
- Skip the SSL Listener Policy drop down list.
- Skip the FTPS Mode radio buttons.
- Skip the Prevent user@host Syntax checkbox.
- In the Remote Server IP or Host Name field, enter the **remote server IP**.
- In the Remote Port field, enter the **remote port**.
- Skip the FTP over SSL/TLS checkbox.
- Skip the SSL Remote Policy drop down list.
- Skip the FTPS Mode radio buttons.
- From the OpenPGP GET drop down list, select an **OpenPGP Policy** as the OpenPGP key pair to associate with this FTP policy.

Note: The OpenPGP GET drop down list contains the OpenPGP policies to use for FTP decryption using OpenPGP. Remember, you decrypt and verify inbound documents with an OpenPGP key pair applied to an OpenPGP Decrypt & Verify policy. PGP_Dave_DecVer is an OpenPGP Decrypt & Verify policy that was created using Dave's OpenPGP key pair.

- Leave the OpenPGP PUT drop down option selected to None.

Note: The OpenPGP PUT drop down list contains the OpenPGP policies to use for FTP encryption using OpenPGP.

- From the Compression GET drop down list, select **GZIP-Decompress**.
- Retain the default Compression PUT control action (None).
- Skip the Comment field.
- Click **Create**. The NETWORK POLICIES screen refreshes.

NETWORK POLICIES				
FTP Policies				
<input type="checkbox"/> NAME	STATUS	PROTOCOL	LISTENER ADDRESS	REMOTE ADDRESS
<input type="checkbox"/> FTP_DomesticTransports	●	FTP	10.5.6.92:21	11.11.11.11:21
<input type="checkbox"/> PoPOverFTPJeff	●	FTP	10.5.6.55:21	11.11.11.55:21
IBM MQ Listener Policies				
<input type="checkbox"/> NAME	STATUS	PROTOCOL	LISTENER ADDRESS	MODE
<input type="checkbox"/> MqListenerPolicy-0	●	JMS/MQ	192.168.0.1:1414	Sync
<input type="button" value="Delete"/> <input type="button" value="Enable"/> <input type="button" value="Disable"/> <input type="button" value="New"/>				

Now you can add the FTP User Policy by editing the FTP policy just created. This operation is shown next.

Adding an FTP User Policy with an Associated OpenPGP Policy

An FTP User policy can be added immediately after creating your first FTP policy or later. The New command at the bottom of the FTP NETWORK POLICY screen is not available until you have created an FTP Server policy. This example assumes that an FTP policy has previously been created.

- Select an **FTP policy name** link.
- On the FTP NETWORK POLICY details screen, at the bottom, create a new FTP User Policy by clicking **New**.

NETWORK POLICIES > FTP NETWORK POLICY > FTP U

FTP USER POLICY

Policy Name*:

LOCAL AUTHENTICATION

System user:

REMOTE AUTHENTICATION

☐ Use system user

☒ Use non-system user

Remote User Name*:

Remote Password:

Confirm Remote Password:

REMOTE SERVER

Remote IP Address:

Remote Port:

FTP over SSL/TLS: ☐

SSL Remote Policy:

Auth Mode: ☐ TLS ☐ SSL

OPENPGP

OpenPGP Get:

OpenPGP Put:

DATA COMPRESSION

Compression GET:

Compression PUT:

COMMENT

Comment:

Create

- On the FTP USER POLICY screen, in the Policy Name field, enter a **name**.
- Under LOCAL AUTHENTICATION, from the System user drop down list, select a **System user**.

Note: Under LOCAL AUTHENTICATION, select the System user whose credentials are presented to the FTP server.

Under REMOTE AUTHENTICATION, select the Use system user option when selecting which user policy credentials are presented to the remote server. Select the Use non-system user option when a user not on the Forum system whose credentials will be presented to the remote server. This option also requires the non-system users' password.

- Under REMOTE AUTHENTICATION, select the **Use non-system user** radio button.

Note: The Remote User Name is the name of the user associated with this FTP User policy and identifies whose credentials are presented to the remote server. The Remote User Name and Remote Password are used by the product to authenticate outgoing users. The Remote User Name and Remote Password may be from 0-unlimited keyboard characters.

- In the Remote User Name field, enter the **user name** of a user to be authenticated on the remote server.
- In the Remote Password field, enter the **password** for this user.
- In the Confirm Remote Password field, re-enter the **password** for this user.
- In the Remote IP Address field, enter the **remote IP** entered earlier for the FTP policy remote IP address.
- In the Remote Port field, enter the **remote port**
- Skip the FTP over SSL/TLS checkbox.
- Skip the SSL Remote Policy drop down list.
- Skip the FTPS mode radio buttons.
- Leave the OpenPGP GET drop down list selected to None.

Note: With the None option selected for OpenPGP GET, you are retaining the defaulted option set earlier in the FTP policy. The OpenPGP GET control action is assigned to the PGP_Sandy_Encrypt policy. Remember, you decrypt inbound documents with an OpenPGP key pair applied to an OpenPGP Decryption policy.

- From the OpenPGP PUT drop down list, select **PGP_Dave_Encrypt** as the OpenPGP Encryption Policy to use for overriding the FTP policy so that the product will manage encryption via OpenPGP over FTP.

Note: The OpenPGP PUT drop down list contains the OpenPGP policies to use for FTP encryption using OpenPGP. This action applies encryption for inbound documents to OpenPGP over FTP by assigning the PUT control action to the FTP policy named FTP_DomesticTransports. Remember, you encrypt outbound documents with an OpenPGP public Certificate applied to an OpenPGP Encryption policy.

- Leave the Compression GET drop down list selected to None.
- From the PUT drop down list, select **ZIP-Compress**.

Note: The Compression GET drop down list contains data compression options for inbound documents. The Compression PUT drop down list contains data compression options for outbound documents.

- Skip the Comment field.
- Click **Create** and the FTP POLICY details screen refreshes, revealing the new FTP User policy at the bottom of the screen.

FTP USERS		
<input type="checkbox"/> FTP USER POLICY	CREATED	MODIFIED
<input type="checkbox"/> FTP_TransportB	Mar 22, 2005 6:22 PM	-
<div> Delete New </div>		

Add an FTP over SSL or TLS Policy

Follow these steps to add an FTP over SSL/TLS policy. This example displays adding an FTP over SSL policy:

NETWORK POLICIES				
FTP Policies				
<input type="checkbox"/> NAME	STATUS	PROTOCOL	LISTENER ADDRESS	REMOTE ADDRESS
<input type="checkbox"/> FTP_DomesticTransports	●	FTP	10.5.6.92:26	11.11.11.56:26
<input type="checkbox"/> PGPOverFTPJeff	●	FTP	10.5.6.55:21	11.11.11.55:21
IBM MQ Listener Policies				
<input type="checkbox"/> NAME	STATUS	PROTOCOL	LISTENER ADDRESS	MODE
<input type="checkbox"/> MqListenerPolicy-0	●	JMS/MQ	192.168.0.1:1414	Sync
<div>Delete Enable Disable New</div>				

NETWORK POLICIES > NEW NETWORK POLICY

NETWORK POLICY PROTOCOL

☐ HTTP

☐ Group Remote

☒ FTP

☐ SMTP

☐ TIBCO Rendezvous

☐ IBM Websphere MQ

☐ TIBCO EMS

Next

- Navigate to the **Network Policies** screen and click **New**.
- On the NEW NETWORK POLICY screen, select the **FTP** radio button and then click **Next**.

NETWORK POLICIES > FTP NETWORK POLICY

FTP NETWORK POLICY

Name*:

Process as XML: ☐

User Policy Rule:

LISTENER

Listener IP*:

Listener Port*:

FTP over SSL/TLS: ☒

SSL Listener Policy:

Auth Mode: ☐ TLS ☒ SSL

DEFAULT REMOTE

Prevent user@host Syntax: ☐

Remote Server IP or Host Name*:

Remote Port*:

FTP over SSL/TLS: ☒

SSL Remote Policy:

Auth Mode: ☐ TLS ☒ SSL

OPENPGP

OpenPGP GET:

OpenPGP PUT:

DATA COMPRESSION

Compression GET:

Compression PUT:

COMMENT

Comment:

FTP USERS

<input type="checkbox"/>	FTP USER POLICY	CREATED	MODIFIED
After creating the FTP policy you will be able add FTP user policies.			

- On the FTP NETWORK POLICY screen, in the Name field, enter the **name** for this policy.
- Skip the Process as XML checkbox.
- From the Use Policy Rule drop down list, select **Required**.

Note: Use the User policy rules drop down list to set an override option that toggles FTP Users policies to be Required, Optional or Ignored. Although you are setting this override option now, you have not connected the FTP User to this FTP policy yet. The override is active when you create an FTP User policy. When working with FTP User policies, consider that:

- A) When the FTP User policy is set to **REQUIRED** or **OPTIONAL**, the FTP User policy becomes bound to the FTP policy and the FTP User policy will now override the settings on the associated FTP policy.
- B) When the FTP User policy is set to **REQUIRED**, only FTP User policies attached to FTP Server policies will be able to log in and use the product.
- X) When the FTP User policy is set to **OPTIONAL**, only users that exist as an FTP User policy or as a user of a back end FTP server can log in.
- Δ) When the FTP User policy is set to **IGNORED**, this option processes all transactions with the configuration of the FTP listener itself (FTP policy). The back end FTP server is used to authenticate the user.

- In the Listener IP field, enter the **listener IP address**.
- In the Listener Port field, enter the **listener port**.
- Check the **FTP over SSL/TLS** checkbox.
- From the SSL Listener Policy drop down list, select an **SSL Termination policy**.
- Aligned with FTPS mode, check the **SSL** radio button.
- Skip the Prevent user@host Syntax checkbox.
- In the Remote Server IP or Host Name field, enter the **remote server IP**.
- In the Remote Port field, enter the **remote port**.
- Check the **FTP over SSL/TLS** checkbox.
- From the SSL Remote Policy drop down list, select an **SSL Initiation policy**.
- Aligned with FTPS mode, check the **SSL** radio button.

Note: At this point, the FTP over SSL actions have been set in steps 10 and 16. Administrators may continue to add additional values to the balance of this screen. For example, to set OpenPGP PUT and GET control actions to this FTP policy and to add data compression actions to this FTP policy.



- From the OpenPGP GET drop down list, select an **OpenPGP Policy**.
- From the OpenPGP PUT drop down list, select **OpenPGP Policy**.
- From the Compression GET drop down list, select **ZIP-Decompress**.
- From the Compression PUT drop down list, select **ZIP-Compress**.

Note: The PUT, GET and DATA COMPRESSION settings are beyond achieving SSL/ TLS, and Administrators may or may not apply these settings, based on their needs.

- Click **Create**. The NETWORK POLICIES screen refreshes.

NETWORK POLICIES

FTP Policies

<input type="checkbox"/>	NAME	STATUS	PROTOCOL	LISTENER ADDRESS	REMOTE ADDRESS
<input type="checkbox"/>	<u>FTP DomesticTransports</u>		FTP	10.5.6.92:26	11.11.11.56:26
<input type="checkbox"/>	<u>FTP SSL DomesticVendors</u>		FTP	10.5.6.57:27	11.11.11.57:27

Now you can add an FTP over SSL/TLS User Policy by editing FTP_SSL_DomesticVendors policy. This operation is shown next.

Add an FTP over SSL or TLS User Policy

Follow these steps to add an FTP over SSL/TLS User policy:

The screenshot shows two web interface sections. The top section, titled "FTP Policies", contains a table with four rows, each with a checkbox and a text link: "NAME", "FTP_DomesticTransports", "FTP_SSL_DomesticVendors", and "PGPOverFTPJA". A mouse cursor is hovering over the "PGPOverFTPJA" link. The bottom section, titled "FTP USERS", contains a table with a header row: "FTP USER POLICY", "CREATED", and "MODIFIED". Below the header, it says "No items to display". At the bottom right of this section are two buttons: "Delete" and "New". A mouse cursor is hovering over the "New" button.

FTP Policies	
<input type="checkbox"/>	NAME
<input type="checkbox"/>	FTP_DomesticTransports
<input type="checkbox"/>	FTP_SSL_DomesticVendors
<input type="checkbox"/>	PGPOverFTPJA

FTP USERS		
<input type="checkbox"/> FTP USER POLICY	CREATED	MODIFIED
No items to display		
		Delete New

- Navigate to the **Network Policies** screen, and edit the FTP policy by clicking on this **FTP policy name** link.
- On the FTP NETWORK POLICY details screen, at the bottom, create a new FTP User Policy by clicking **New**.

NETWORK POLICIES > FTP NETWORK POLICY > FTP U

FTP USER POLICY

Policy Name*:

LOCAL AUTHENTICATION

System user:

REMOTE AUTHENTICATION

☐ Use system user

☒ Use non-system user

Remote User Name*:

Remote Password:

Confirm Remote Password:

REMOTE SERVER

Remote IP Address:

Remote Port:

FTP over SSL/TLS: ☒

SSL Remote Policy:

Auth Mode: ☐ TLS ☒ SSL

OPENPGP

OpenPGP Get:

OpenPGP Put:

DATA COMPRESSION

Compression GET:

Compression PUT:

COMMENT

Comment:

Create

- On the FTP USER POLICY screen, in the Policy Name field, enter a **name** for this FTP User policy.
- Under LOCAL AUTHENTICATION, from the System user drop down list, select a **System user**.

Note: Under LOCAL AUTHENTICATION, select the System user whose credentials are presented to the FTP server.

Under REMOTE AUTHENTICATION, select the Use system user option when selecting which user policy credentials are presented to the remote server. Select the Use non-system user option when a user not on the Forum system whose credentials will be presented to the remote server. This option also requires the non-system users' password.

- Under REMOTE AUTHENTICATION, select the **Use non-system user** radio button.

Note: The Remote User Name is the name of the user associated with this FTP User policy and identifies whose credentials are presented to the remote server. The Remote User Name and Remote Password are used by the product to authenticate outgoing users. The Remote User Name and Remote Password may be from 0-unlimited keyboard characters.

- In the Remote User Name field, enter the **user name** of a user to be authenticated on the remote server.
- In the Remote Password field, enter the **password** for this user.
- In the Confirm Remote Password field, re-enter the **password** for this user.
- In the Remote IP Address field, enter the **remote IP** entered earlier for the FTP policy remote IP address.
- In the Remote Port field, enter the **remote port**.
- Check the **FTP over SSL/TLS** checkbox.
- From the SSL Remote Policy drop down list, select an **SSL Initiation Policy name**.
- Aligned with FTPS mode, select the **SSL** radio button.

Note: At this point, the FTP over SSL action has been set in step 15. Administrators may continue to add additional values to the balance of this screen. For example, to set OpenPGP PUT and GET control actions to this FTP policy and to add data compression actions for this FTP policy.

- From the OpenPGP GET drop down list, select an **OpenPGP Policy**.
- From the OpenPGP PUT drop down list, select an **OpenPGP Policy**.
- From the Compression GET drop down list, select **GZIP-Decompress**.
- From the Compression PUT drop down list, select **GZIP-Compress**.

Note: The PUT, GET and DATA COMPRESSION settings are beyond achieving SSL/ TLS, and Administrators may or may not apply these settings, based on their needs.

- Skip the Comment field.
- Click **Create** and the FTP NETWORK POLICY details screen refreshes, revealing the new FTP User policy (**FTP_SSL_VendorCenters**) at the bottom of the screen.

FTP USERS		
<input type="checkbox"/> FTP USER POLICY	CREATED	MODIFIED
<input type="checkbox"/> FTP_SSL_VendorCenters	Mar 23, 2005 12:23 PM	-
<div> Delete New </div>		

OPENPGP KEY POLICIES

The Keys screen provides a workspace for managing PKCS and OpenPGP key pairs and public certificates. Key pairs and public certificates should be named for the owner of the key, who may be someone in your organization, or a customer.

Sort by Name and Sort by Expiration

The KEYS screen may also be toggled between Sort by Name or Sort by Expiration views. To sort by name, click the **Sort by Name** link. To sort by expiration, click the **Sort by Expiration** link.

OpenPGP Key Pairs and Public Certificates

The Keys screen serves, in part, as the repository for OpenPGP key pairs, OpenPGP public certificates and generated OpenPGP keys. Key pairs and public certificates should be named for the owner of the key, who may be someone in your organization, or a customer.

OpenPGP key pairs and OpenPGP public certificates do not include a notion of a Signer group, Certificate Authority or Root CA. Instead, these are peer-to-peer keys. Before importing OpenPGP keys, verify that the fingerprint is valid with a phone call or face-to-face visit, reading aloud the sender's fingerprint, which they will verify for you.

You may:

- import an OpenPGP key pair stored in one or multiple files from a file upload.
- import an OpenPGP key pair stored in one or two files pasted from the clipboard.
- import an OpenPGP key pair stored in multiple files.
- import an OpenPGP public certificate.
- view OpenPGP key pairs, public certificate details and settings.
- export an OpenPGP key pair or OpenPGP public certificate.
- validate an OpenPGP key pair.
- generate an OpenPGP key pair.
- delete an OpenPGP key pair or OpenPGP public certificate unless referenced elsewhere on the product.
- filter display of OpenPGP Keys policy view with the Search or Max Results field.

The product allows only one physical representation of a key at one time. When an OpenPGP key pair is held in two separate files (the OpenPGP public certificate and the OpenPGP private key), both keys are combined into one key pair, and it is this combined key pair that is applied during any operations that call for the key pair.

Note: The product supports OpenPGP key sizes from 1024 to 4096 bits.

OpenPGP Key Protocols Supported

The product supports the following OpenPGP key protocols:

- ElGamal
- Diffie Hellman/DSS
- RSA v3 and v4 up to key size 4096
- OpenPGP

The ElGamal protocol is an asymmetric ciphering method digital signatures and plaintext.

The Diffie-Hellman protocol allows two users to exchange a secret key over an insecure medium without any prior secrets.

The RSA v3 and v4 protocols include keys from 1024 to 4096 bits in size.

The OpenPGP protocol is an open specification for Pretty Good Privacy® (PGP® *) which provides algorithms and formats of OpenPGP processed objects as well as the MIME framework for exchanging these via e-mail or other transport protocols.

* PGP and Pretty Good Privacy are the Registered Trademarks of PGP Corporation.

OpenPGP Key Formats Supported

The product supports ASCII OpenPGP key format.

OpenPGP Algorithms Supported

The product supports 3-DES, CAST-5 and AES OpenPGP key algorithms.

OpenPGP Key Sizes

OpenPGP keys may be from 1024 to 4096 bits in size.

OpenPGP Key Policy Examples

Examples for OpenPGP Key policies include:

- Import an OpenPGP Key Pair Stored in One File from File Upload.
- Import an OpenPGP Key Pair Stored in One File Pasted from the Clipboard.
- View OpenPGP Key Details.
- View OpenPGP Key Settings.
- Import an OpenPGP Key Pair Stored in Multiple Files.
- Import an OpenPGP Public Certificate.
- View OpenPGP Public Certificate Details.
- Export OpenPGP Keys From the OpenPGP Keys Details Screen.
- Add a Comment to an OpenPGP Key.
- Validate OpenPGP Key Pairs.
- Export an OpenPGP Key Pair or OpenPGP Public Certificate.
- Export All OpenPGP Keys as a Keyring.
- Validate an OpenPGP Key Pair.
- Generate an OpenPGP Key Pair.
- Delete an OpenPGP Key Pair or OpenPGP Public Certificate.

Note: For information on editing / viewing, or filtering display of OpenPGP keys, refer to the Common Operations section of the *Forum Systems Sentry™ Version 9 Web-based Administration Guide*. If attempting to delete an OpenPGP key pair or OpenPGP public certificate referenced elsewhere on the product, the following message appears:

The screenshot shows a web interface titled "KEYS". At the top, a red error message states: "Cannot remove. Another policy depends on this policy". Below this is a table of keys with columns: NAME, TYPE, SIZE, STATUS, CREATED, IMPORTED, and LAST USED. The table lists various keys, including OpenPGP Key Pairs and Certificates. At the bottom, there is a search bar, a "max results" dropdown set to "1000", and buttons for "Show", "Settings", "Delete", "Import", and "New".

	NAME	TYPE	SIZE	STATUS	CREATED	IMPORTED	LAST USED
<input checked="" type="checkbox"/>	PGP_Dave	OpenPGP Key Pair	1024/2048	Active	2002-09-03		Never been
<input type="checkbox"/>	PGP_Joemitchell	OpenPGP Key Pair	1024/2048	Active	2002-09-03		Never been
<input type="checkbox"/>	PGP_Sandy	OpenPGP Key Pair	1024/1536	Active	2002-09-03		Never been
<input type="checkbox"/>	PGP_davemonroe	OpenPGP Key Pair	1024/3072	Active	2002-09-03		Never been
<input type="checkbox"/>	ABC_Corp_SSL	Key Pair	1024	Active			
<input type="checkbox"/>	ABC_Corp_SSL_cert	Certificate	1024	Active			
<input type="checkbox"/>	Danielle	Key Pair	2048	Active			
<input type="checkbox"/>	Danielle_cert	Certificate	2048	Active			
<input type="checkbox"/>	JackKantos	Key Pair	1024	Active			
<input type="checkbox"/>	JackKantos_cert	Certificate	1024	Active			
<input type="checkbox"/>	Mark_cert	Certificate	1024	Active			
<input type="checkbox"/>	NewHampshire	Key Pair	512	Active			
<input type="checkbox"/>	NewHampshire_0_cert	Certificate	512	Active			
<input type="checkbox"/>	NewHampshire_1_cert	Certificate	2048	Active			
<input type="checkbox"/>	Walter	Key Pair	2048	Active			
<input type="checkbox"/>	Walter_cert	Certificate	2048	Active			
<input type="checkbox"/>	testkey1	Key Pair	1024	Active			

Import an OpenPGP Key Pair Stored in Two Files Pasted from the Clipboard in the same manner described in Import an OpenPGP Key Pair Stored in One File Pasted from the Clipboard.

To delete an OpenPGP key pair or any OpenPGP public key, discover which Server policy or OpenPGP policy it references, delete that policy, and then the key pair or public key will be accessible for deletion. In the case of Server policies, you may un-reference the key by resetting the OpenPGP GET and/or OpenPGP PUT to NONE and saving the Server policy.

Import an OpenPGP Key Pair Stored in One File from a File Upload

Always verify with the originator that the fingerprint of an OpenPGP key pair received is the same as the fingerprint sent before importing an OpenPGP key pair. This example displays importing an OpenPGP key pair that is contained in one file. This OpenPGP key pair will be associated with an FTP Server and FTP User policy. For more information, refer to Add an FTP Server Policy and Add an FTP User Policy sections.

The **Settings** command is visible only after an initial key is created on the system.

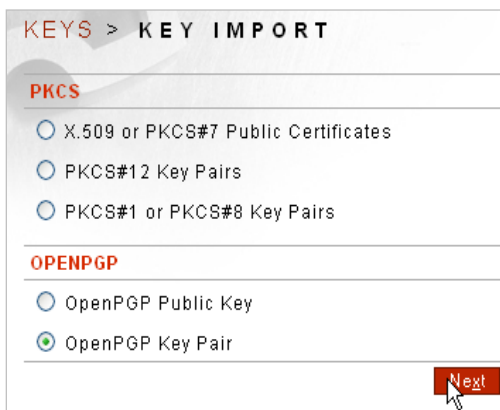
KEYS

Show Compact ViewSort By Name

<input type="checkbox"/>	NAME	TYPE	SIZE	STATUS	CREATED	IMPORTED	LAST USED	EXPIRATION	EM
<input type="checkbox"/>	ABC_Corp_SSL	Key Pair	1024	Active					
<input type="checkbox"/>	ABC_Corp_SSL_cert	Certificate	1024	Active					

13 items found. Search max results 2

ShowSettingsDeleteImportNew



KEYS > KEY IMPORT

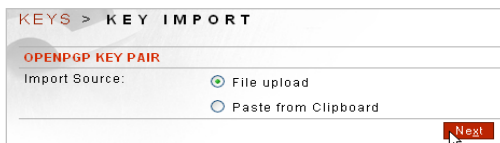
PKCS

- ☐ X.509 or PKCS#7 Public Certificates
- ☐ PKCS#12 Key Pairs
- ☐ PKCS#1 or PKCS#8 Key Pairs

OPENPGP

- ☐ OpenPGP Public Key
- ☒ OpenPGP Key Pair

[Next](#)



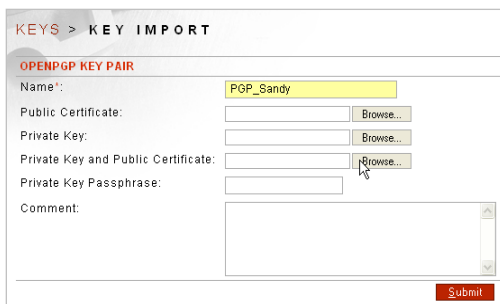
KEYS > KEY IMPORT

OPENPGP KEY PAIR

Import Source:

- ☒ File upload
- ☐ Paste from Clipboard

[Next](#)



KEYS > KEY IMPORT

OPENPGP KEY PAIR

Name*:

Public Certificate: [Browse...](#)

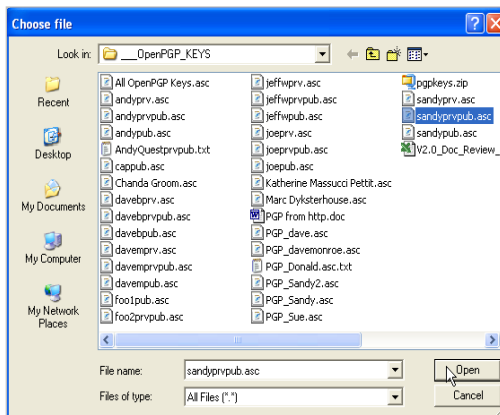
Private Key: [Browse...](#)

Private Key and Public Certificate: [Browse...](#)

Private Key Passphrase:

Comment:

[Submit](#)



KEYS > KEY IMPORT

OPENPGP KEY PAIR

Name: PGP_Sandy

Public Certificate: Browse...

Private Key: Browse...

Private Key and Public Certificate: *_KEYS\sandyprivpub.asc Browse...

Private Key Passphrase:

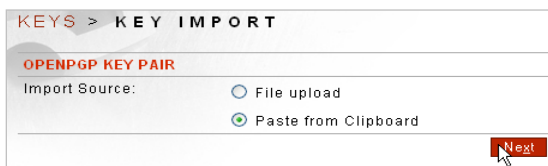
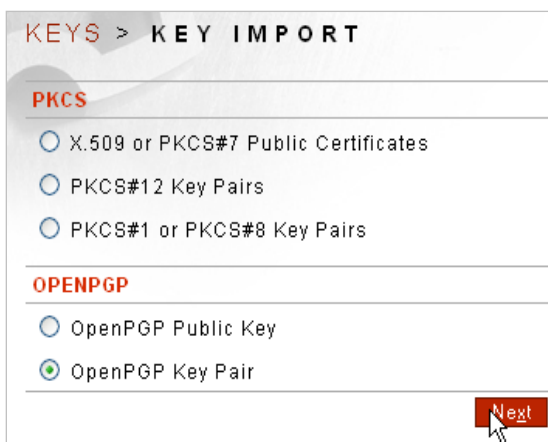
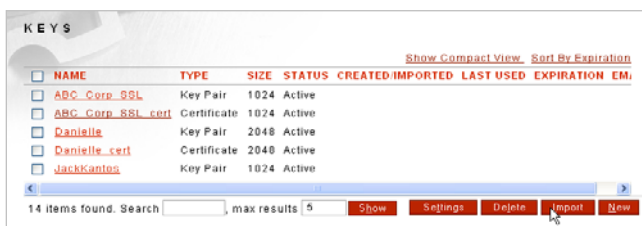
Comment: OpenPGP key for Sandy

- Navigate to the **Keys** screen, and click **Import**.
- On the KEY IMPORT screen, click the **OpenPGP Key Pair** radio button, and then click **Next**.
- On the KEY IMPORT screen, select the **File Upload** radio button, and then click **Next**.
- On the OPENPGP KEY PAIR details screen, in the Name field, enter the **Name** for this OpenPGP Key Pair.
- Skip the Public Certificate and Private Key fields.
- Click **Browse** aligned with the Private Key and Public Certificate field to navigate your file system. The Choose file screen appears. Click the **OpenPGP Key Pair**, and then click **Open**. This file must adhere to the **.asc** file format. The OpenPGP Key Pair populates the File name field and the screen closes.
- When initially creating your OpenPGP private key, you had also created a password; enter this **Private Key Passphrase** in the Private Key Passphrase field.
- In the Comment field, enter any relevant **comment** for this key pair.
- Click **Submit**. The Keys screen refreshes.

Note: It is not possible to reload a key. If you create a key and wish to edit it, you must first delete the key, and then re-create the key.

Import an OpenPGP Key Pair Stored in One File Pasted from the Clipboard

When importing a Key Pair stored in one file by pasting it from the clipboard, be sure to paste it into the correct text box. Follow these steps to import an OpenPGP Key Pair stored in one file by pasting it from the clipboard:



KEYS > KEY IMPORT

OPENPGP KEY PAIR

Name:

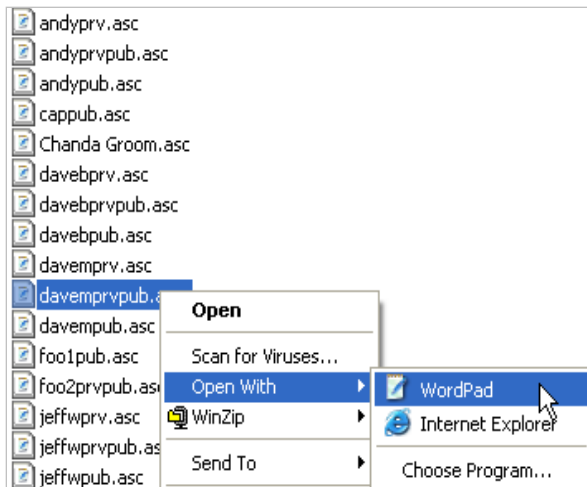
Paste Public Certificate (PEM format):

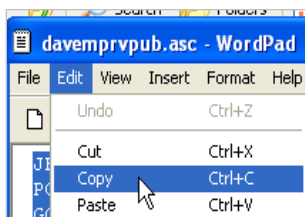
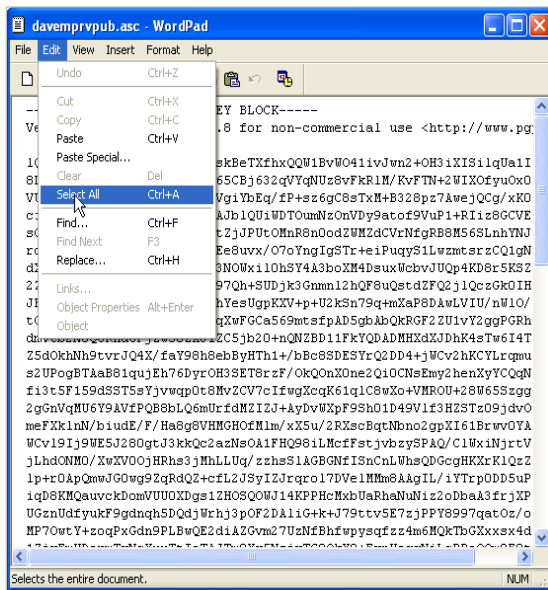
Paste Private Key (PEM format):

Paste Private Key and Public Certificate (PEM format):

Private Key Passphrase:

Comment:





KEYS > KEY IMPORT

OPENPGP KEY PAIR

Name:

PGP_DaveM

Paste Public Certificate (PEM format):

Paste Private Key (PEM format):

Paste Private Key and Public Certificate (PEM format):

```

xxTtIaTAJm0Xw5MzjyTC90kX8+FvnWoggNiLcPBeQ0m0F9t7T2QSf0LC9org+BW
A77FFRI78cV24u117j3SYELzKzP2ZQp+as6HPPh2UqEjwnUvvoSWtt30eYlvvuguX
o1bC13lIPpYpNM1D6ucYYzgH1HCS7AWd7kobMUG2gTm0bvJi6Ya2IPEAME2Zb3A
fwln9zU9gu32pJ8Nt07WzSYiuTmYoV3K+QtDoxcC1bKxxLFwXqrQhdt860JESvHS
+ueAjZ0D/f0bVW3/vS6eLGN/qkaMS1zXVAD41okARgQYEQIABgUCFXUWRgAKCRL
kr1yJxXWwNODAJ0Yf5JL4dooXeF02KYqVCNVV5FLSQCeIS1GmoJfBT2c0Le2nR0v
XOTLi7I=
=Jbg6
-----END PGP PUBLIC KEY BLOCK-----

```

Private Key Passphrase:

.....

Comment:

OpenPGP key for Dave Miller

Submit

KEYS

[Show Compact View](#)
[Sort By Expiration](#)

<input type="checkbox"/>	NAME	TYPE	SIZE	STATUS	CREATED/IMPORTED	LAST USED
<input type="checkbox"/>	ABC_Corp_SSL	Key Pair	1024	Active		
<input type="checkbox"/>	ABC_Corp_SSL_cert	Certificate	1024	Active		
<input type="checkbox"/>	Danielle	Key Pair	2048	Active		
<input type="checkbox"/>	Danielle_cert	Certificate	2048	Active		
<input type="checkbox"/>	JackKantos	Key Pair	1024	Active		
<input type="checkbox"/>	JackKantos_cert	Certificate	1024	Active		
<input type="checkbox"/>	Mark_cert	Certificate	1024	Active		
<input type="checkbox"/>	NewHampshire	Key Pair	512	Active		
<input type="checkbox"/>	NewHampshire_0_cert	Certificate	512	Active		
<input type="checkbox"/>	NewHampshire_1_cert	Certificate	2048	Active		
<input type="checkbox"/>	PGP_DaveM	OpenPGP Key Pair	1024/3072	Active	2002-09-03	Never beer
<input type="checkbox"/>	PGP_Sandy	OpenPGP Key Pair	1024/1536	Active	2002-09-03	Never beer
<input type="checkbox"/>	testkey1	Key Pair	1024	Active		
<input type="checkbox"/>	Walter	Key Pair	2048	Active		
<input type="checkbox"/>	Walter_cert	Certificate	2048	Active		

15 items found. Search

max results 1000

Show

Settings

Delete

Import

New

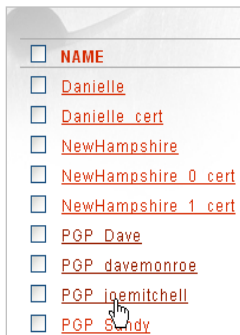
- Navigate to the **Keys** screen, and click **Import**.
- On the KEY IMPORT, click the **OpenPGP Key Pair** radio button, and then click **Next**.
- On the KEY IMPORT details screen, select the **Paste from Clipboard** radio button, and then click **Next**.
- On the KEY IMPORT summary screen, in the Name field, enter the **Name** for this OpenPGP Key Pair.
- Navigate your file system to locate the OpenPGP key pair. Right-click on the **file name** with your mouse, and select **Open**. A system dialog appears.
- Select the **Select the program from a list** radio button, and click **OK**. The Open with dialog appears.
- Select **WordPad**, and then click **OK**.
- The key pair file opens. From the **Edit** menu, select **Select All**. Type **<Control C>** to copy the contents, or select **Copy** from the **Edit** menu.
- Return to the OPENPGP KEY IMPORT screen. With your cursor positioned in the Paste Private Key and Public Certificate (PEM format) text box, enter **<Control V>** to paste the contents into the text box.

Note: With the OpenPGP key pair held in two files, copy the public certificate portion of the file and then paste it in the Paste Public Certificate text box. Next, copy the private key portion of the file and then paste it in the Paste Private Key text box.

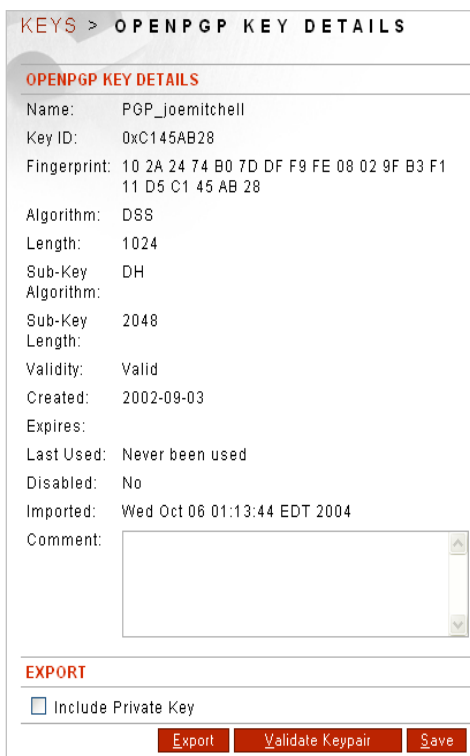
- In the Private Key Passphrase field, enter the **passphrase** for this key.
- In the Comment field, enter any relevant **comment** for this key.
- Click **Submit**. The Keys screen refreshes.

View OpenPGP Key Pair Details

Administrators may view, but not edit, OpenPGP key details. Follow these steps to view OpenPGP Key Pair details:



A list of OpenPGP keys with checkboxes next to each name. The names are: NAME, Danielle, Danielle_cert, NewHampshire, NewHampshire_0_cert, NewHampshire_1_cert, PGP Dave, PGP davemonroe, PGP joemitchell, and PGP Sudy. A mouse cursor is pointing at the checkbox next to PGP joemitchell.



KEYS > OPENPGP KEY DETAILS

OPENPGP KEY DETAILS

Name: PGP_joemitchell
Key ID: 0xC145AB28
Fingerprint: 10 2A 24 74 B0 7D DF F9 FE 08 02 9F B3 F1
11 D5 C1 45 AB 28
Algorithm: DSS
Length: 1024
Sub-Key: DH
Algorithm:
Sub-Key: 2048
Length:
Validity: Valid
Created: 2002-09-03
Expires:
Last Used: Never been used
Disabled: No
Imported: Wed Oct 06 01:13:44 EDT 2004
Comment:

EXPORT

☐ Include Private Key

Export Validate Keypair Save

- Navigate to the **Keys** screen, and click a **Key name** link. The OPENPGP KEY DETAILS screen appears with private key fingerprint data visible.
- Click the **Keys** link on the Navigator to return to the Keys screen.

View or Edit OpenPGP Key Settings

The Settings command manages the following values:

- Number of Days in Advance of Expiry to send an email.
- Number of OpenPGP key pairs in the system available for exporting as a keyring.

Note: The Export command is visible only after at least one OpenPGP key is added to the system.

For information about exporting all OpenPGP key pairs in the system, refer to the Exporting All OpenPGP Key Pairs as a Keyring section.

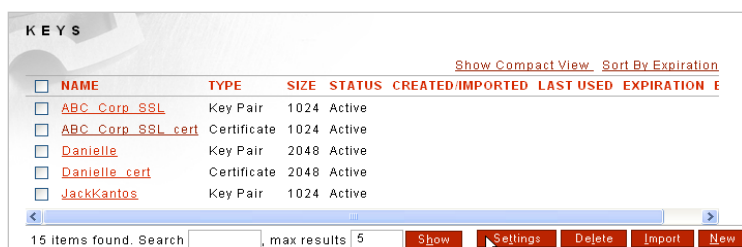
Edit Number of Days in Advance of Expiry Notification Setting

When an OpenPGP key is expiring, the number of days in advance of this expiration to send an email alert provides a key expiry warning to Administrators.

Note: See the *Forum Systems Sentry™ Version 9 System Management Guide* for details on configuring email alerts

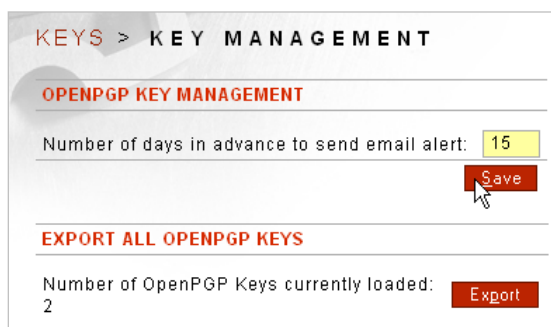
The number of days in advance to send email alert option is provided on the **Keys** screen, under **Settings**. The **Settings** command is visible only after an initial key is created on the system.

The default is 1 day; however, Administrators may want to increase this time to allow for acquiring a fresh OpenPGP key pair.



The screenshot shows the 'KEYS' screen with a table of keys and a search bar. The table has columns: NAME, TYPE, SIZE, STATUS, CREATED/IMPORTED, LAST USED, and EXPIRATION. There are 15 items found, and the search bar is set to 'max results 5'. The 'Settings' button is highlighted.

NAME	TYPE	SIZE	STATUS	CREATED/IMPORTED	LAST USED	EXPIRATION
ABC_Corp_SSL	Key Pair	1024	Active			
ABC_Corp_SSL_cert	Certificate	1024	Active			
Danielle	Key Pair	2048	Active			
Danielle_cert	Certificate	2048	Active			
JackKantos	Key Pair	1024	Active			



The screenshot shows the 'KEYS > KEY MANAGEMENT' screen. The 'OPENPGP KEY MANAGEMENT' section has a field for 'Number of days in advance to send email alert:' with a value of 15. The 'Save' button is highlighted. The 'EXPORT ALL OPENPGP KEYS' section has a field for 'Number of OpenPGP Keys currently loaded:' with a value of 2. The 'Export' button is highlighted.

KEYS > KEY MANAGEMENT

OPENPGP KEY MANAGEMENT

Number of days in advance to send email alert: 15

Save

EXPORT ALL OPENPGP KEYS

Number of OpenPGP Keys currently loaded: 2

Export

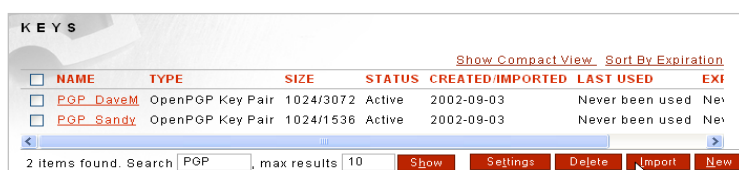
- Navigate to the **Keys** screen.
- On the KEYS , select **Settings**.
- On the KEY MANAGEMENT , in the Number of days in advance to send email alert field, overwrite the default of 1, and then enter the **number of days** in advance of an OpenPGP key pair expiration to be notified via an email alert.
- Click **Save**.

Import an OpenPGP Key Pair Stored in Multiple Files

Always verify with the originator that the fingerprint of an OpenPGP key pair received is the same as the fingerprint sent before importing an OpenPGP key pair. You may import an OpenPGP key pair by two methods:

- Either import an OpenPGP key pair by loading a single key in the *Private Key and Public Certificate field*.
- Or import an OpenPGP private key (held in one file) and an OpenPGP public key (held in another file) by loading the OpenPGP private key in the *Private Key field*, and then loading the OpenPGP public key in the *Public Certificate field*. With this option, **these two actions must be performed during the same operation**.

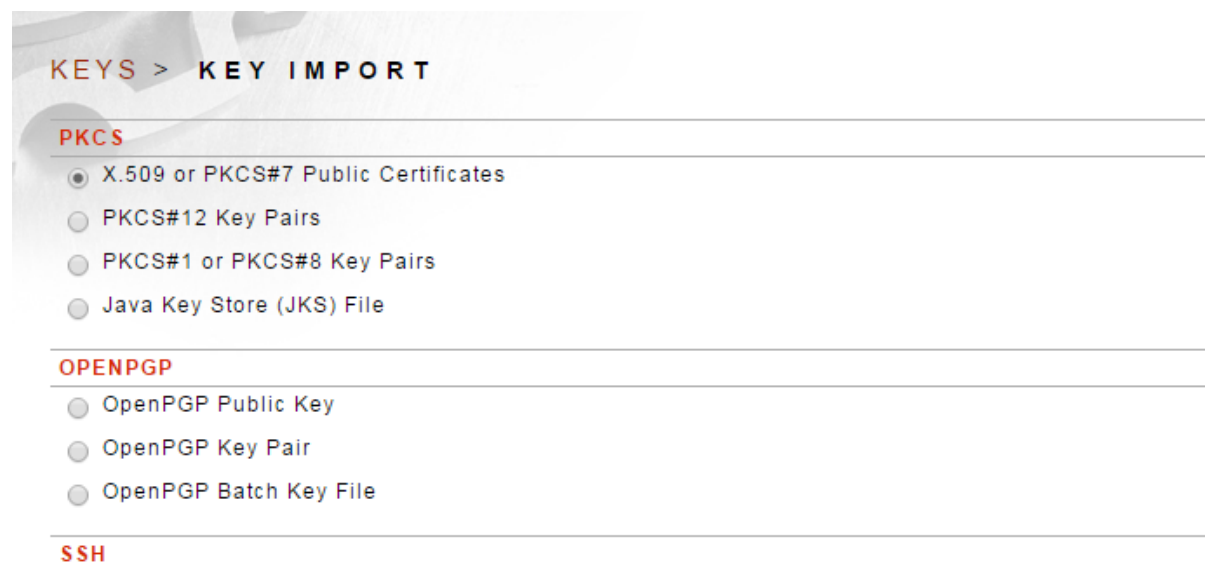
This example displays importing an OpenPGP key pair that is contained in two separate files. This OpenPGP key pair will be associated with an FTP Server and FTP User policy. For more information, refer to Add an FTP Server Policy and Add an FTP User Policy sections.



The screenshot shows a table titled 'KEYS' with columns: NAME, TYPE, SIZE, STATUS, CREATED/IMPORTED, LAST USED, and EXPIRATION. Two rows are visible, both for 'OpenPGP Key Pair' type, with names 'PGP_DaveM' and 'PGP_Sandy'. Below the table are search and action buttons.

NAME	TYPE	SIZE	STATUS	CREATED/IMPORTED	LAST USED	EXPIRATION
PGP_DaveM	OpenPGP Key Pair	1024/3072	Active	2002-09-03	Never been used	Never
PGP_Sandy	OpenPGP Key Pair	1024/1536	Active	2002-09-03	Never been used	Never

2 items found. Search: PGP, max results: 10. Buttons: Show, Settings, Delete, Import, New.



The screenshot shows the 'KEYS > KEY IMPORT' page. It has sections for PKCS (X.509 or PKCS#7 Public Certificates, PKCS#12 Key Pairs, PKCS#1 or PKCS#8 Key Pairs, Java Key Store (JKS) File) and OPENPGP (OpenPGP Public Key, OpenPGP Key Pair, OpenPGP Batch Key File). The 'SSH' section is also visible at the bottom.

KEYS > KEY IMPORT

PKCS

- ☒ X.509 or PKCS#7 Public Certificates
- ☐ PKCS#12 Key Pairs
- ☐ PKCS#1 or PKCS#8 Key Pairs
- ☐ Java Key Store (JKS) File

OPENPGP

- ☐ OpenPGP Public Key
- ☐ OpenPGP Key Pair
- ☐ OpenPGP Batch Key File

SSH



The screenshot shows the 'OPENPGP KEY PAIR' section. It has an 'Import Source:' label with two radio buttons: 'File upload' (selected) and 'Paste from Clipboard'. A 'Next' button is at the bottom right.

KEYS > KEY IMPORT

OPENPGP KEY PAIR

Import Source: ☒ File upload ☐ Paste from Clipboard

Next

KEYS > KEY IMPORT

OPENPGP KEY PAIR

Name*:

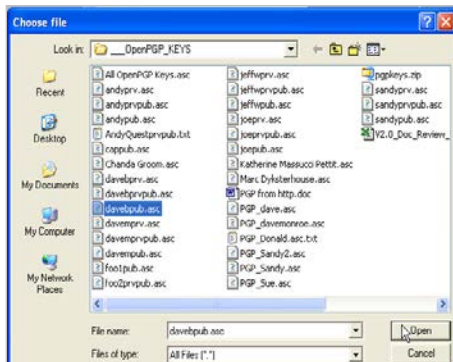
Public Certificate:

Private Key:

Private Key and Public Certificate:

Private Key Passphrase:

Comment:



KEYS > KEY IMPORT

OPENPGP KEY PAIR

Name*:

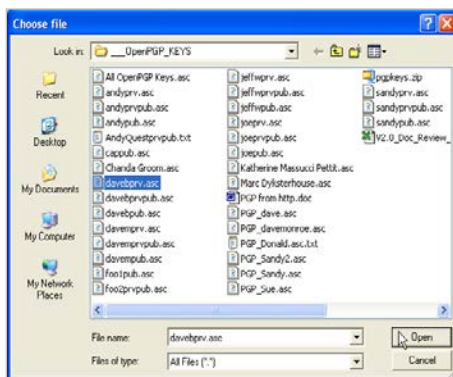
Public Certificate:

Private Key:

Private Key and Public Certificate:

Private Key Passphrase:

Comment:



KEYS > KEY IMPORT

OPENPGP KEY PAIR

Name*:

Public Certificate:

Private Key:

Private Key and Public Certificate:

Private Key Passphrase:

Comment:

- Navigate to the **Keys** screen, and click **Import**.
- On the KEY IMPORT , click the **OpenPGP Key Pair** radio button, and then click **Next**.
- On the OPENPGP KEY PAIR, click the **File upload** radio button, and then click **Next**.
- On the OPENPGP KEY PAIR details screen, in the Name field, enter the **Name** for this OpenPGP Key Pair.
- Click **Browse** aligned with the Public Certificate field to navigate your file system. The Choose file screen appears. Click the **OpenPGP Public Certificate**, and then click **Open**. This file must adhere to the **.asc** file format. The OpenPGP Public Certificate populates the File name field and the screen closes.
- Click **Browse** aligned with the Private Key field to navigate your file system. The Choose file screen appears. Click the **OpenPGP Private Key**, and then click **Open**. This file must adhere to the **.asc**, **der** or **ber** file format. The OpenPGP Private Key populates the File name field and the screen closes.
- Skip the Private and Public Certificate field.
- When initially creating your private key, you had also created a password; enter this **Private Key Passphrase** in the Private Key Passphrase field.
- In the Comment field, enter any relevant **comment** for this OpenPGP key pair.
- Click **Submit**.

Note: It is not possible to reload a key. If you create a key and wish to edit it, first you must delete the key, and then re-create the key.

Also a batch key import option has been added which lets you import keys in bulk.

Import an OpenPGP Public Certificate

Always verify with the originator that the fingerprint of an OpenPGP public certificates received is the same as the fingerprint sent before importing an OpenPGP public certificates.

KEYS

[Show Compact View](#) [Sort By Expiration](#)

<input type="checkbox"/>	NAME	TYPE	SIZE	STATUS	CREATED/IMPORTED	LAST USED	EXPI
<input type="checkbox"/>	PGP_DaveR	OpenPGP Key Pair	1024/2048	Active	2002-09-03	Never been used	200
<input type="checkbox"/>	PGP_DaveM	OpenPGP Key Pair	1024/3072	Active	2002-09-03	Never been used	Nev
<input type="checkbox"/>	PGP_Sandy	OpenPGP Key Pair	1024/1536	Active	2002-09-03	Never been used	Nev

3 items found. Search max results [Show](#) [Settings](#) [Delete](#) [Import](#) [New](#)

KEYS > KEY IMPORT

PKCS

☐ X.509 or PKCS#7 Public Certificates

☐ PKCS#12 Key Pairs

☐ PKCS#1 or PKCS#8 Key Pairs

OPENPGP

☒ OpenPGP Public Key

☐ OpenPGP Key Pair

[Next](#)

KEYS > KEY IMPORT

OPENPGP PUBLIC KEY

Import Source: ☒ File upload

☐ Paste from Clipboard

[Next](#)

KEYS > KEY IMPORT

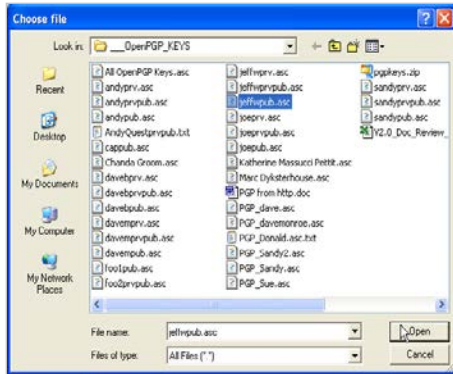
OPENPGP PUBLIC KEY

Name*:

Public Certificate*: [Browse...](#)

Comment:

[Submit](#)



KEYS > KEY IMPORT

OPENPGP PUBLIC KEY

Name*:

Public Certificate*:

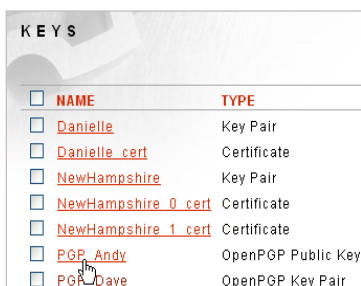
Comment:

- Navigate to the **Keys** screen, and click **Import**.
- On the KEY IMPORT, click the **OpenPGP Public Key** radio button, and then click **Next**.
- On the OPENPGP PUBLIC KEY screen, click the **File upload** radio button, and then click **Next**.
- On the OPENPGP PUBLIC KEY details screen, in the Name field, enter the **Name** for this OpenPGP public key.
- Click **Browse** aligned with the Public Certificate field to navigate your file system. The Choose file screen appears. Click the **OpenPGP Public Key**, then click **Open**. This file must adhere to the **.asc** file format. The OpenPGP Public Key populates the File name field and the screen closes.
- In the Comment field, enter any relevant **comment**.
- Click **Submit**.

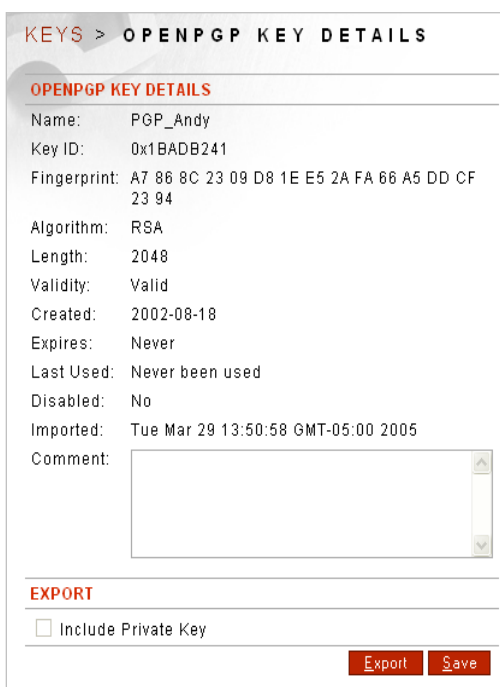
Note: It is not possible to reload a key. If you create a key and wish to edit it, first you must delete the key, and then re-create the key.

View OpenPGP Public Certificate Details

OpenPGP public certificate details may be viewed, but not edited. Follow these steps to view details of an OpenPGP public certificate:



<input type="checkbox"/>	NAME	TYPE
<input type="checkbox"/>	Danielle	Key Pair
<input type="checkbox"/>	Danielle_cert	Certificate
<input type="checkbox"/>	NewHampshire	Key Pair
<input type="checkbox"/>	NewHampshire_0_cert	Certificate
<input type="checkbox"/>	NewHampshire_1_cert	Certificate
<input type="checkbox"/>	PGP_Andy	OpenPGP Public Key
<input type="checkbox"/>	PGP_Dave	OpenPGP Key Pair



KEYS > OPENPGP KEY DETAILS

OPENPGP KEY DETAILS

Name: PGP_Andy
Key ID: 0x1BADB241
Fingerprint: A7 86 8C 23 09 D8 1E E5 2A FA 66 A5 DD CF 23 94
Algorithm: RSA
Length: 2048
Validity: Valid
Created: 2002-08-18
Expires: Never
Last Used: Never been used
Disabled: No
Imported: Tue Mar 29 13:50:58 GMT-05:00 2005
Comment:

EXPORT

☐ Include Private Key

- Navigate to the **Keys** screen, and click a **Key name** link. The OPENPGP KEY DETAILS screen appears with fingerprint data visible.
- Click the **Keys** link on the Navigator to return to the Keys screen.

Export OpenPGP Keys

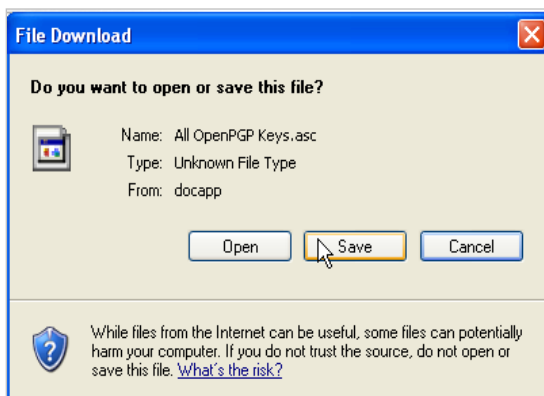
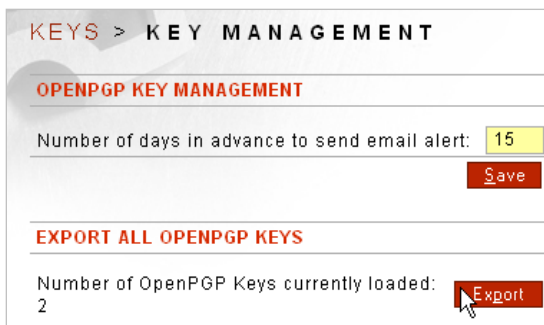
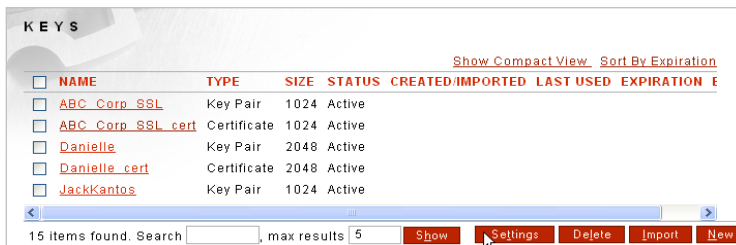
You may export OpenPGP Key Pairs and OpenPGP Public Certificates by either:

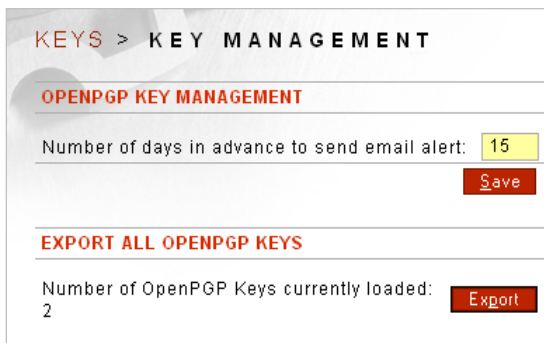
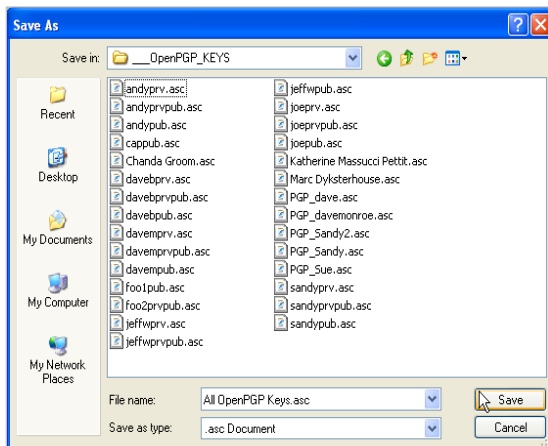
- selecting the **KEYS** screen and then the Settings screen, and using the **Export** button to export all OpenPGP key pairs as a keyring,
- or selecting the **KEYS** screen, and then selecting a specific OpenPGP Key link, and from the OPENPGP KEY DETAILS screen, selecting the **Export** button.

Export All OpenPGP Key Pairs as a Keyring

The **Settings** command is visible only after an initial key is created on the system.

You may export all OpenPGP Public keys and Key Pairs into a single ASCII Armored file.





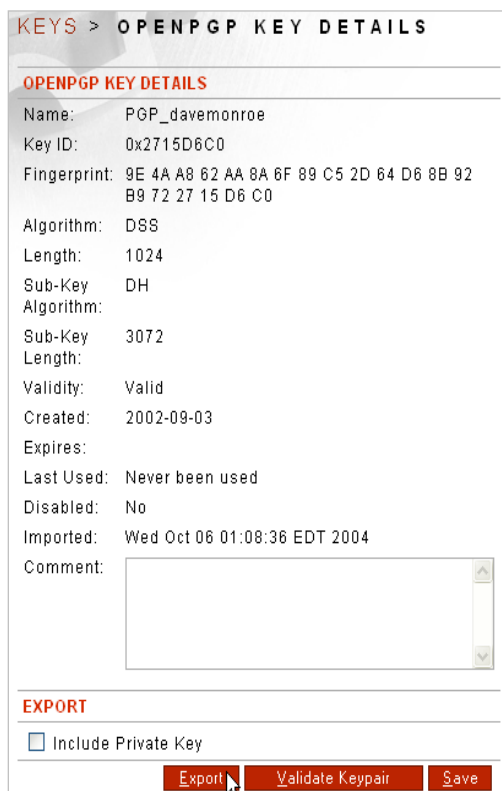
- Navigate to the **Keys** screen.
- On the KEYS screen, select **Settings**.
- On the OPENPGP KEY MANAGEMENT screen, select **Export** and the File Download dialog appears.
- Select **Save**, and the Save As dialog appears.
- Navigate to the location to save the OpenPGP key pairs, and click **Save**.

Export OpenPGP Keys From OpenPGP Key Details Screen

When exporting an OpenPGP key, you are not removing it from the product, only exporting a copy of it to a file on your local system. You can not re-import saved keys unless they are first deleted from the product.

When exporting an OpenPGP key, the OpenPGP KEY DETAILS screen offers two choices:

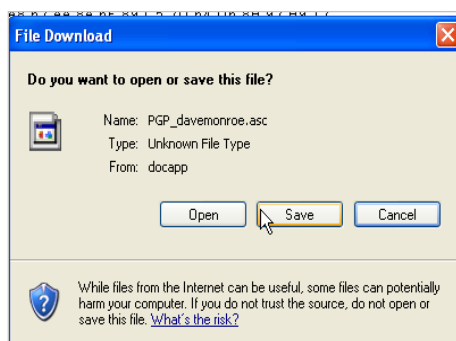
- Export the OpenPGP private key and public key by checking the **Include Private Key** checkbox, and then clicking **Export**.
- Export the OpenPGP public key only by clicking **Export**.

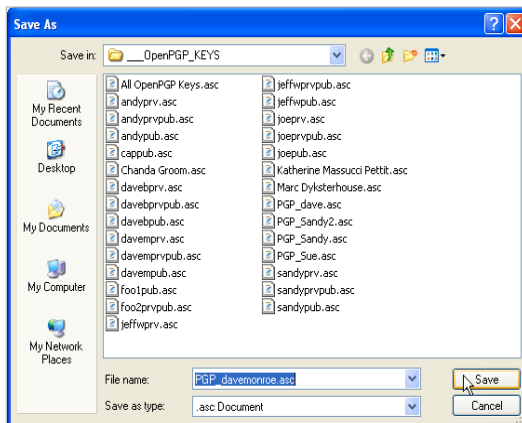


The screenshot shows the 'KEYS > OPENPGP KEY DETAILS' screen. It displays the following information:

- NAME:** PGP_davemonroe
- Key ID:** 0x2715D6C0
- Fingerprint:** 9E 4A A8 62 AA 8A 6F 89 C5 2D 64 D6 8B 92 B9 72 27 15 D6 C0
- Algorithm:** DSS
- Length:** 1024
- Sub-Key:** DH
- Algorithm:**
- Sub-Key:** 3072
- Length:**
- Validity:** Valid
- Created:** 2002-09-03
- Expires:**
- Last Used:** Never been used
- Disabled:** No
- Imported:** Wed Oct 06 01:08:36 EDT 2004
- Comment:** (empty text area)

Below the details is an **EXPORT** section with a checkbox labeled 'Include Private Key' (which is unchecked). At the bottom are three buttons: 'Export', 'Validate Keypair', and 'Save'. A mouse cursor is pointing at the 'Export' button.





- Navigate to the **Keys** screen, and select an **OpenPGP key name** link.
- On the OPENPGP KEY DETAILS screen, select **Export**.
- On the File Download dialog, select **Save**. The Save As dialog appears with the OpenPGP keys filename already pre-populating the File name field.
- Select **Save**.

Add a Comment to an OpenPGP Key

From the KEY DETAILS screen, Administrators may add a comment that will be saved for this OpenPGP Key.

KEYS > OPENPGP KEY DETAILS

OPENPGP KEY DETAILS

Name: PGP_davemonroe
Key ID: 0x2715D6C0
Fingerprint: 9E 4A A8 62 AA 8A 6F 89 C5 2D 64 D6 8B 92 B9 72 27 15 D6 C0
Algorithm: DSS
Length: 1024
Sub-Key Algorithm: DH
Sub-Key Length: 3072
Validity: Valid
Created: 2002-09-03
Expires:
Last Used: Never been used
Disabled: No
Imported: Wed Oct 06 01:08:36 EDT 2004
Comment: key for Dave Monroe, first OpenPGP key entered in the new system 5/1/2005.

EXPORT

☐ Include Private Key

[Export](#) [Validate Keypair](#) [Save](#)

- Navigate to the **Keys** screen, and select an **OpenPGP key name** link.
- On the OPENPGP KEY DETAILS screen, add a **Comment** in the Comment field, and then select **Save**.

Validate OpenPGP Key Pairs

When validating an OpenPGP key pair, the OpenPGP Key Pair is checked to see if it is complementary, whether the private key password stored in the system is correct and that the key has not expired. The result of checking the validation will be shown on the screen and also logged in the Audit logs.

KEYS > OPENPGP KEY DETAILS

OPENPGP KEY DETAILS

Name: PGP_davemonroe
Key ID: 0x2715D6C0
Fingerprint: 9E 4A A8 62 AA 8A 6F 89 C5 2D 64 D6 8B 92 B9 72 27 15 D6 C0
Algorithm: DSS
Length: 1024
Sub-Key: DH
Sub-Key Algorithm: 3072
Sub-Key Length: 3072
Validity: Valid
Created: 2002-09-03
Expires:
Last Used: Never been used
Disabled: No
Imported: Wed Oct 06 01:08:36 EDT 2004
Comment: key for Dave Monroe, first OpenPGP key entered in the new system 5/1/2005.

EXPORT

☐ Include Private Key

Export Validate Keypair Save

- Navigate to the **Keys** screen, and select an **OpenPGP key name** link.
- On the OPENPGP KEY DETAILS screen, select **Validate Keypair**.

Note: The Validate Keypair command checks that the keypair is complementary and has not expired.

KEYS > OPENPGP KEY DETAILS

Keypair PGP_davemonroe is valid

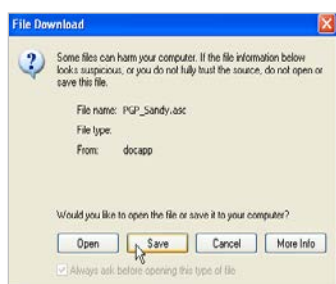
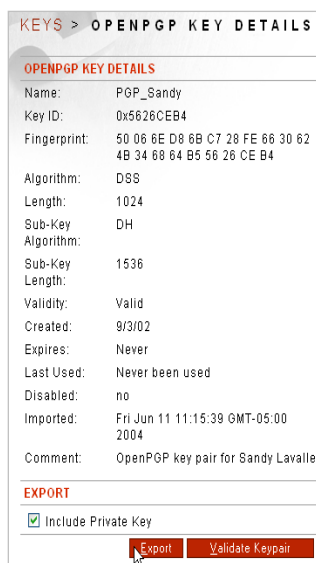
OPENPGP KEY DETAILS

Name: PGP_davemonroe
Key ID: 0x2715D6C0
Fingerprint: 9E 4A A8 62 AA 8A 6F 89 C5 2D 64 D6 8B 92 B9 72 27 15 D6 C0
Algorithm: DSS
Length: 1024
Sub-Key: DH
Sub-Key Algorithm:

- The screen refreshes with a confirmation message (Keypair <keypair name> is valid) visible at the top of the screen.

Export an OpenPGP Key Pair or OpenPGP Public Certificate

You may export an OpenPGP key pair or OpenPGP public certificate in the same manner. When exporting an OpenPGP key pair, you may also export the private key along with the key pair. This example displays exporting an OpenPGP key pair:



Generate an OpenPGP Key Pair

Follow these steps to generate a new OpenPGP key pair.



KEYS > NEW KEY

GENERATE NEW KEY

☐ PKCS Key Pair

☒ OpenPGP Key Pair

Next

KEYS > OPENPGP KEY GENERATION

GENERATE NEW OPENPGP KEY

Key Name*: PGP_Terry

User Name*: terrimalone

Email*: tmalone@test.forumsys.com

Algorithm: RSA

Size: 2048

Expiration Date: 6/11/05

☒ Never Expires

Passphrase*:

Confirm Passphrase*:

Comment: OpenPGP key pair for Terry Malone

Create

- Navigate to the **Keys** screen, and click **New**.
- On the NEW KEY screen, click the **OpenPGP Key Pair** radio button, and then click **New**.
- On the OPENPGP KEY GENERATION screen, in the Key Name field, enter the **name** of this new OpenPGP key.
- In the User Name field, enter the **user name** that corresponds with this key.
- In the Email field, enter the **email address** of this user.
- From the Algorithm drop down list, select Diffie-Hellman/DSS or RSA.
- From the Size drop down list, select the size of this key.
- Either accept the current date as the Expiration Date for this key, or check the Never Expires checkbox.
- In the Passphrase field, enter the **passphrase** for this OpenPGP key.
- Re-enter the **Passphrase** in the Confirm Passphrase field.
- In the Comment field, enter any relevant **comment**.
- Click **Create** and the OPENPGP KEY GENERATION IN PROGRESS message appears.

Note: Forum Systems recommends that when generating an OpenPGP key, you also export it to retain a copy of this key in a secure location.

Delete an OpenPGP Key Pair or OpenPGP Public Certificate

Before deleting an OpenPGP key pair or OpenPGP public certificate, you might want to review details of the OpenPGP key first. This example displays deleting an OpenPGP key pair. Deleting an OpenPGP public certificate or OpenPGP private key is performed in the same manner.

KEYS

[Show Compact View](#) [Sort By Expiration](#)

<input type="checkbox"/>	NAME	TYPE	SIZE	STATUS	CREATED/IMPORTED	LAST USED	E
<input type="checkbox"/>	PGP_DaveB	OpenPGP Key Pair	1024/2048	Active	2002-09-03	Never been used	2
<input type="checkbox"/>	PGP_DaveM	OpenPGP Key Pair	1024/3072	Active	2002-09-03	Never been used	1
<input type="checkbox"/>	PGP_Jeff	OpenPGP Public Key	1024/1536	Active	2002-09-03	Never been used	1
<input checked="" type="checkbox"/>	PGP_Joe	OpenPGP Public Key	1024/2048	Active	2002-09-03	Never been used	1
<input type="checkbox"/>	PGP_Sandy	OpenPGP Key Pair	1024/1536	Active	2002-09-03	Never been used	1

5 items found. Search max results [Show](#) [Settings](#) [Delete](#) [Import](#) [New](#)

- Navigate to the **Keys** screen and check the checkbox aligned with an OpenPGP Key Pair.
- The “Are you sure you want to delete the checked keys?” message appears. Click **OK**.

OPENPGP KEY POLICIES

The OpenPGP screen allows Administrators to manage system OpenPGP key policies. The different types of OpenPGP Key policies are:

- Encrypt
- Decrypt
- Verify
- Decrypt & Verify
- Sign & Encrypt

Administrators may link these different policies with FTP to use the FTP-OpenPGP feature of the product, thereby applying one or more OpenPGP operations to content arriving and leaving the product via FTP.

OpenPGP encryption, OpenPGP decryption & verification and OpenPGP signing provides a method of encrypting, decrypting & verifying and signing with one OpenPGP key on the system.

OpenPGP verification leverages all the keys on the system.

OpenPGP encryption and signing provides a method of both encrypting and signing in one step.

The product supports the RFC 2440 and RFC 1991 specifications. In addition, the product supports the application of the different OpenPGP operations to unlimited large file transfers. OpenPGP policies can include 128 simultaneous open streams, limited by the disk capacity on a client or server.

The operations that may be performed on OpenPGP Policies include:

- Add an OpenPGP Encrypt policy.
- Add an OpenPGP Decrypt & Verify policy.
- Add an OpenPGP Sign policy.
- Add an OpenPGP Verify policy.
- Add an OpenPGP Sign & Encrypt policy.
- Add encrypt, decrypt & verify, sign, verify or sign & encrypt with OpenPGP over FTP
- Edit / View an OpenPGP policy.
- Limit display of an OpenPGP policy view with Search and Max Results field.
- Delete an OpenPGP policy.

File Size Constraints with OpenPGP Operations

The OpenPGP implementation supports RFC 2440 streaming, which allows processing of unlimited file size documents. The maximum document size that can be successfully processed, however, is practically limited by the disk space available on the client and server.

ASCII Armor Format Options

ASCII armor format is an encoding process that provides data in binary format to be transformed into textual format. This option is available on OpenPGP Sign, OpenPGP Sign & Encrypt and OpenPGP Encrypt policies.

Encoding Options

Encoding options specify how the encrypted data is encoded, which has implications on the maximum document size allowed for encryption. The product supports the following encoding:

- Unlimited - RFC 2440
- Legacy - RFC 1991

RFC 2440

RFC 2440 encoding is used for unlimited length encoding.

RFC 1991

RFC 1991 encoding is used for legacy compatibility; it is used for fixed length encoding. The maximum document size allowed is 100MB.

Note: For more information on FTP PUT and FTP GET commands, refer to the FTP Policies and FTP User Policies section.

OpenPGP Policy Details Screen Terms

The following table displays the terms and definitions found on the OpenPGP Policy Details screen:

TERM	DEFINITION
OPENPGP POLICY	
Name	The name of the OpenPGP policy.
Mode	<p>Encrypt mode is accomplished with an OpenPGP key pair or OpenPGP public certificate. Therefore, the OpenPGP encrypt operation presents a current listing of all OpenPGP key pairs and OpenPGP public certificates that are currently loaded in the Keys screen. The OpenPGP encrypt operation implicitly performs a document compression prior to the encryption.</p> <p>Decrypt & Verify blended modes are accomplished with an OpenPGP private key and a public certificate. Therefore, the OpenPGP decrypt & verify operation presents the current listing of OpenPGP key pairs and public certificates that are currently loaded in the Keys screen. If the source document is encrypted but not signed, this operation will perform only the required decryption. Conversely, if the source document is signed and encrypted, this operation will perform both the required decryption and signature verification in this exact order.</p> <p>Sign mode is accomplished with an OpenPGP key pair. Therefore, the OpenPGP sign operation presents a current listing of OpenPGP key pairs that are currently loaded in the Keys screen. The OpenPGP sign operation implicitly performs a document compression after the signature.</p> <p>Verify mode uses a specific verification key pair or public key.</p> <p>Sign & Encrypt blended modes are accomplished with an OpenPGP key pair. This operation presents a current listing of all OpenPGP key pairs and OpenPGP public certificates that are currently loaded in the Keys screen. This operation implicitly performs a document compression after the signature and prior to the encryption.</p>
Append File Extension	Allows users to append a filename extension to outgoing files when creating Encrypt, Sign, and Sign & Encrypt OpenPGP policies. This text field accepts a maximum of three alphanumeric characters. When a user enters an extension, the outgoing file will be given that extension.
DECRYPTION	
Key Pair	The selected Key Pair used for decryption.
ENCRYPTION	
Certificate or Key Pair	The selected certificate or Key Pair used for encryption.
Use ASCII Armor	When checked, applies ASCII Armor format to the encrypted data.
Encoding	<p>Unlimited – RFC 2440 applied RFC 2440 encoding (unlimited document size).</p> <p>Legacy – RFC 1991 applies RFC 1991 encoding for legacy compatibility (100MB maximum document size allowed).</p>

TERM	DEFINITION
SIGNATURE	
Key Pair	The selected Key Pair used for signing.
Use ASCII Armor	When checked, applies ASCII Armor format to the signed data.
VERIFICATION	
Certificate or Key Pair	The selected Certificate or Key Pair used for verification.
COMMENT	
Comment	A text box used for comments (optional).

OpenPGP Operation Flowchart

The following graphic displays a typical scenario for integrating OpenPGP policies with FTP policies:

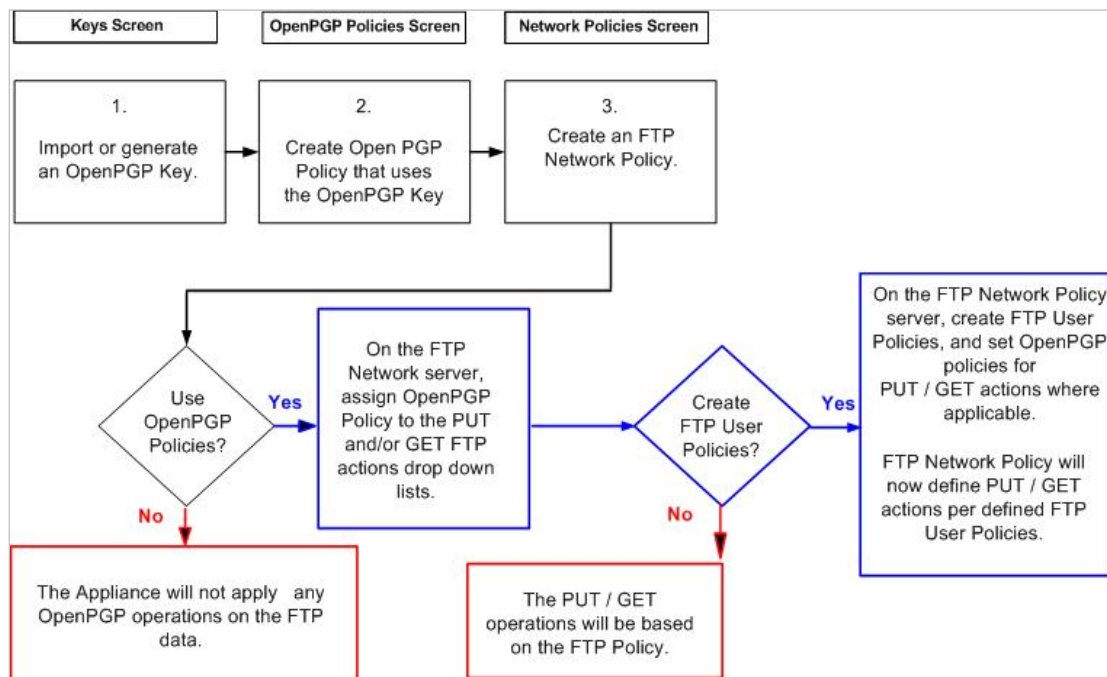


Figure 1: OpenPGP Flowchart for Setting OpenPGP Security Policies.

Note: You may perform FTP / OpenPGP operations with or without an associated FTP User policy.

How FTP Sessions Interrelate with OpenPGP Policies

If there is a change to an OpenPGP policy via the WebAdmin UI that is being used by an FTP policy, the changes do not take effect on open FTP sessions using that FTP policy. The Administrator will have to bounce that FTP policy via the WebAdmin UI to pick up the changes in the OpenPGP policy.

OpenPGP Network Policy Examples

Examples for OpenPGP Policies include:

- Add an OpenPGP Encrypt Policy.
- Add an OpenPGP Signature Policy.
- Add an OpenPGP Verify Policy.
- Add an OpenPGP Sign & Encrypt Policy.
- Add an OpenPGP Decrypt & Verify Policy.
- Add Encrypt, Decrypt & Verify, Sign, Verify, or Sign & Encrypt with OpenPGP over FTP.

Add an OpenPGP Encrypt Policy Using ASCII Armor

Follow these steps to create an OpenPGP Encrypt policy:

Note: OpenPGP Encrypt policies can be specified with or without ASCII Armor and the Encoding option.

OPENPGP POLICIES

☐ **OPENPGP POLICY**

	TYPE	CREATED	MODIFIED
No items to display			

0 items found. Search , max results 1000 Show Delete New

OPENPGP POLICIES > OPENPGP POLICY DET

OPENPGP POLICY

Name*:

Mode:

- ☒ Encrypt
- ☐ Decrypt & Verify
- ☐ Sign
- ☐ Verify
- ☐ Sign & Encrypt

Append File Extension:

DECRYPTION

Key Pair:

ENCRYPTION

Certificate or Key Pair:

- PGP_Dave
- PGP_davemonroe
- PGP_Joemitchell
- PGP_Sandy

Use ASCII Armor: ☒

Encoding:

SIGNATURE

Key Pair:

Use ASCII Armor: ☐

VERIFICATION

Certificate or Key Pair:

COMMENT

Comment:

Save

OPENPGP POLICIES			
<input type="checkbox"/> OPENPGP POLICY	TYPE	CREATED	MODIFIED
<input type="checkbox"/> PGP Dave Encrypt	Encrypt	May 2, 2005 1:39 PM	-
1 items found. Search <input type="text"/> , max results 1000 <input type="button" value="Show"/> <input type="button" value="Delete"/> <input type="button" value="New"/>			

- Navigate to the **OPENPGP POLICIES** screen, and click **New**.
- On the OPENPGP POLICY DETAILS screen, overwrite this name and enter a unique **OpenPGP Policy Name** in the Name field.
- Aligned with Mode, check the **Encrypt** radio button.
- In the Append File Extension field, enter a **file extension (asc)**.

Note: The Append File Extension field allows users to append a filename extension to outgoing files when creating Encrypt, Sign, and Sign & Encrypt OpenPGP policies. This text field accepts a maximum of three alphanumeric characters.

- Skip the DECRYPTION section.
- In the ENCRYPTION section, select one or more **OpenPGP Key Pair(s)** or **Certificate(s)** from the Certificate or Key Pair drop down list.

Note: To select more than one Certificate or Key Pair, select the first **Certificate**, hold down the **Control** key, and then select the **second Certificate**.

- Check the **Use ASCII Armor** checkbox (optional).
- From the Encoding drop down list, select an **encoding** option.
- Skip the SIGNATURE section.
- Skip the VERIFICATION section.
- Enter any relevant text in the **Comment** text box (optional).
- Click **Create**.

Add an OpenPGP Signature Policy

Follow these steps to create an OpenPGP Sign policy:

Note: OpenPGP Sign policies can be specified with or without ASCII Armor. Currently, OpenPGP Sign policies can not be configured with the Encoding option; therefore, signatures are generated by default in the RFC 2440 format. This choice of defaulting to the new format can result in incompatibility of older tools using signatures.

OPENPGP POLICIES			
<input type="checkbox"/> OPENPGP POLICY	TYPE	CREATED	MODIFIED
<input type="checkbox"/> PGP_Dave_Encrypt	Encrypt	May 2, 2005 1:39 PM	-
1 items found. Search <input type="text"/> , max results 1000 Show Delete New			

OPENPGP POLICIES > OPENPGP POLICY DET

OPENPGP POLICY

Name*:

PGP_Sign_Dave

Mode:

☐ Encrypt

☐ Decrypt & Verify

☒ Sign

☐ Verify

☐ Sign & Encrypt

Append File Extension:

DECRYPTION

Key Pair:

PGP_Dave

ENCRYPTION

Certificate or Key Pair:

PGP_Dave

PGP_davemonroe

PGP_joemitchell

PGP_Sandy

Use ASCII Armor:

☐

Encoding:

Unlimited - RFC 2440

SIGNATURE

Key Pair:

PGP_Dave

Use ASCII Armor:

☒

VERIFICATION

Certificate or Key Pair:

PGP_Dave

COMMENT

Comment:

Create

OPENPGP POLICIES			
<input type="checkbox"/> OPENPGP POLICY	TYPE	CREATED	MODIFIED
<input type="checkbox"/> PGP_Dave_Encrypt	Encrypt	May 2, 2005 1:39 PM	-
<input type="checkbox"/> PGP_Sign_Dave	Sign	May 2, 2005 1:40 PM	-
2 items found. Search <input type="text"/> max results <input type="text"/> <input type="button" value="Show"/> <input type="button" value="Delete"/> <input type="button" value="New"/>			

- Navigate to the **OPENPGP POLICIES** screen, and click **New**.
- On the OPENPGP POLICY DETAILS screen, overwrite this name and enter a unique **OpenPGP Policy Name** in the Name field.
- Aligned with Mode, check the **Sign** radio button.
- Skip the Append File Extension field.
- Skip the DECRYPTION section.
- Skip the ENCRYPTION section.
- In the SIGNATURE section, select an **OpenPGP Key Pair** from the Key Pair drop down list.
- Check the **Use ASCII Armor** checkbox (optional).
- Skip the VERIFICATION section.
- Enter any relevant text in the **Comment** text box (optional).
- Click **Create**.

Add an OpenPGP Verify Policy

Follow these steps to create an OpenPGP Verify policy:

OPENPGP POLICIES			
<input type="checkbox"/> OPENPGP POLICY	TYPE	CREATED	MODIFIED
<input type="checkbox"/> PGP_Dave_Encrypt	Encrypt	May 2, 2005 1:39 PM	-
<input type="checkbox"/> PGP_Sign_Dave	Sign	May 2, 2005 1:40 PM	-
2 items found. Search <input type="text"/> , max results <input type="text"/> 1000 <input type="button" value="Show"/> <input type="button" value="Delete"/> <input type="button" value="New"/>			

OPENPGP POLICIES > OPENPGP POLICY DET

OPENPGP POLICY

Name*:PGP_Dave_Verify

Mode:

☐ Encrypt

☐ Decrypt & Verify

☐ Sign

☒ Verify

☐ Sign & Encrypt

Append File Extension:

DECRYPTION

Key Pair:

PGP_Dave

ENCRYPTION

Certificate or Key Pair:

PGP_DavePGP_davemonroePGP_joemitchellPGP_Sandy

Use ASCII Armor:☐

Encoding:

Unlimited - RFC 2440

SIGNATURE

Key Pair:

PGP_Dave

Use ASCII Armor:☐

VERIFICATION

Certificate or Key Pair:

PGP_Dave

COMMENT

Comment:

Create

OPENPGP POLICIES				
<input type="checkbox"/> OPENPGP POLICY	TYPE	CREATED	MODIFIED	
<input type="checkbox"/> PGP_Dave_Encrypt	Encrypt	May 2, 2005 1:39 PM	-	
<input type="checkbox"/> PGP_Dave_Verify	Verify	May 2, 2005 1:42 PM	-	
<input type="checkbox"/> PGP_Sign_Dave	Sign	May 2, 2005 1:40 PM	-	
3 items found. Search <input type="text"/> , max results <input type="text"/> 1000 <input type="button" value="Show"/> <input type="button" value="Delete"/> <input type="button" value="New"/>				

- Navigate to the **OpenPGP POLICIES** screen, and click **New**.
- On the OPENPGP POLICY DETAILS screen, overwrite this name and enter a unique **OpenPGP Policy Name** in the Name field.
- Aligned with Mode, check the **Verify** radio button.
- Skip the Append File Extension field.
- Skip the DECRYPTION section.
- Skip the ENCRYPTION section.
- Skip the SIGNATURE section.
- In the VERIFICATION section, select an **OpenPGP Key Pair** or **Certificate** from the Certificate or Key Pair drop down list.
- Enter any relevant text in the **Comment** text box (optional).
- Click **Create**.

Add an OpenPGP Sign and Encrypt Policy

Follow these steps to create a blended OpenPGP Sign & Encrypt policy:

Note: The blended OpenPGP Sign & Encrypt policy may be added with or without ASCII Armor.

OPENPGP POLICIES				
<input type="checkbox"/> OPENPGP POLICY	TYPE	CREATED	MODIFIED	
<input type="checkbox"/> PGP_Dave_Encrypt	Encrypt	May 2, 2005 1:39 PM	-	
<input type="checkbox"/> PGP_Dave_Verify	Verify	May 2, 2005 1:42 PM	-	
<input type="checkbox"/> PGP_Sign_Dave	Sign	May 2, 2005 1:40 PM	-	
3 items found. Search <input type="text"/> , max results 1000 Show Delete New				

OPENPGP POLICIES > OPENPGP POLICY DET

OPENPGP POLICY

Name*:

Mode:

- ☐ Encrypt
- ☐ Decrypt & Verify
- ☐ Sign
- ☐ Verify
- ☒ Sign & Encrypt

Append File Extension:

DECRYPTION

Key Pair:

ENCRYPTION

Certificate or Key Pair:

Use ASCII Armor: ☐

Encoding:

SIGNATURE

Key Pair:

Use ASCII Armor: ☐

VERIFICATION

Certificate or Key Pair:

COMMENT

Comment:

[Create](#)

OPENPGP POLICIES				
<input type="checkbox"/> OPENPGP POLICY	TYPE	CREATED	MODIFIED	
<input type="checkbox"/> PGP Dave Encrypt	Encrypt	May 2, 2005 1:39 PM	-	
<input type="checkbox"/> PGP Dave Verify	Verify	May 2, 2005 1:42 PM	-	
<input type="checkbox"/> PGP Sandy SigEnc	Sign & Encrypt	May 2, 2005 1:45 PM	-	
<input type="checkbox"/> PGP Sign Dave	Sign	May 2, 2005 1:40 PM	-	
4 items found. Search <input type="text"/> , max results <input type="text" value="1000"/> <input type="button" value="Show"/> <input type="button" value="Delete"/> <input type="button" value="New"/>				

- Navigate to the **OPENPGP POLICIES** screen, and click **New**.
- On the OPENPGP POLICY DETAILS screen, overwrite this name and enter a unique **OpenPGP Policy Name** in the Name field.
- Aligned with Mode, check the **Sign & Encrypt** radio button.
- Skip the Append File Extension field.
- Skip the DECRYPTION section.
- In the ENCRYPTION section, select one or more **OpenPGP key pair(s)** or **Certificate(s)** from the Certificate or Key Pair drop down list.
- Skip the Use ASCII Armor checkbox (optional).
- In the SIGNATURE section, select an **OpenPGP Key Pair** from the Key Pair drop down list.
- Skip the VERIFICATION section.
- Enter any relevant text in the **Comment** text box (optional).
- Click **Create**.

Add an OpenPGP Decrypt and Verify Policy

Follow these steps to create a blended OpenPGP Decrypt & Verify policy:

OPENPGP POLICIES				
<input type="checkbox"/> OPENPGP POLICY	TYPE	CREATED	MODIFIED	
<input type="checkbox"/> PGP_Dave_Encrypt	Encrypt	May 2, 2005 1:39 PM	-	
<input type="checkbox"/> PGP_Dave_Verify	Verify	May 2, 2005 1:42 PM	-	
<input type="checkbox"/> PGP_Sandy_SigEnc	Sign & Encrypt	May 2, 2005 1:45 PM	-	
<input type="checkbox"/> PGP_Sign_Dave	Sign	May 2, 2005 1:40 PM	-	
4 items found. Search <input type="text"/> , max results 1000 Show Delete New				

OPENPGP POLICIES > OPENPGP POLICY DET

OPENPGP POLICY

Name*:

PGP_Sandy_DecVer

Mode:

☐ Encrypt

☒ Decrypt & Verify

☐ Sign

☐ Verify

☐ Sign & Encrypt

Append File Extension:

DECRYPTION

Key Pair: PGP_Sandy

ENCRYPTION

Certificate or Key Pair: PGP_Dave
PGP_davemonroe
PGP_Joemitchell
PGP_Sandy

Use ASCII Armor: ☐

Encoding: Unlimited - RFC 2440

SIGNATURE

Key Pair: PGP_Dave

Use ASCII Armor: ☐

VERIFICATION

Certificate or Key Pair: PGP_Dave

COMMENT

Comment:

Create

OPENPGP POLICIES				
<input type="checkbox"/> OPENPGP POLICY	TYPE	CREATED	MODIFIED	
<input type="checkbox"/> PGP_Dave_Encrypt	Encrypt	May 2, 2005 1:39 PM	-	
<input type="checkbox"/> PGP_Dave_Verify	Verify	May 2, 2005 1:42 PM	-	
<input type="checkbox"/> PGP_Sandy_DecVer	Decrypt & Verify	May 2, 2005 1:46 PM	-	
<input type="checkbox"/> PGP_Sandy_SigEnc	Sign & Encrypt	May 2, 2005 1:45 PM	-	
<input type="checkbox"/> PGP_Sign_Dave	Sign	May 2, 2005 1:40 PM	-	
5 items found. Search <input type="text"/> , max results <input type="text" value="1000"/> Show Delete New				

- Navigate to the **OPENPGP POLICIES** screen, and click **New**.
- On the OPENPGP POLICY DETAILS screen, overwrite this name and enter a unique **OpenPGP Policy Name** in the Name field.
- Aligned with Mode, check the **Decrypt & Verify** radio button.
- Skip the Append File Extension field.
- In the DECRYPTION section, select an **OpenPGP key pair** from the Key Pair drop down list.
- Skip the ENCRYPTION section.
- Skip the SIGNATURE section.
- Skip the VERIFICATION section.

Note: When creating an OpenPGP Decrypt & Verify policy, the verification Certificate or Key Pair drop down is disabled because the system checks your uploaded keys on the fly, as the document is being processed, to find the matching public key for verification. If the encrypted document **does not** contain an enclosed signed document, then the document is decrypted, and the verification step is skipped.

Conversely, if the encrypted document **does** contain an enclosed signed document, but a matching verification public key is **not found** in your uploaded keys, then verification is not performed. However, in both these cases, decryption proceeds as usual.

- Enter any relevant text in the **Comment** text box (optional).
- Click **Create**.

Add Encryption with OpenPGP over FTP

Administrators may link Decrypt & Verify, Sign, Verify, or Sign & Encrypt in the same manner described for setting set encryption with OpenPGP over FTP. Use the following sequence to set encryption with OpenPGP over FTP that will be delivered in ASCII format:

Note: Not all graphics are shown in this instruction.



OPENPGP POLICY > **OPENPGP POLICY DATA**

OPENPGP POLICY

Name: PGP_Dave_Encrypt

Mode:

- ☒ Encrypt
- ☐ Decrypt & Verify
- ☐ Sign
- ☐ Verify
- ☐ Sign & Encrypt

Append File Extension:

OPENPGP POLICIES	
<input type="checkbox"/> OPENPGP POLICY	TYPE
<input type="checkbox"/> PGP Dave Encrypt	Encrypt
<input type="checkbox"/> PGP Dave Verify	Verify
<input type="checkbox"/> PGP Sandy DecVer	Decrypt & Verify
<input type="checkbox"/> PGP Sandy SigEnc	Sign & Encrypt
<input type="checkbox"/> PGP Sign Dave	Sign

- Navigate to the **Keys** screen and import an OpenPGP key pair to use for encryption. Refer to the Import OpenPGP Key Pair in One File section for instructions.
- Navigate to the OPENPGP Policies screen and add an OpenPGP Encryption Policy that uses this OpenPGP key pair, and includes the **Use ASCII Armor** option. Refer to the Add OpenPGP Encrypt Policy section for instructions.
- From the Encoding drop down list, select an **encoding**.
- Enter any relevant **comment** in the Comment field (optional).
- Click **Create**. The OPENPGP POLICIES screen refreshes.

NETWORK POLICIES				
IBM MQ Listener Policies				
<input type="checkbox"/> NAME	STATUS	PROTOCOL	LISTENER ADDRESS	MODE
<input type="checkbox"/> MqListenerPolicy-0	●	JMS/MQ	192.168.0.1:1414	Sync
<div> Delete Enable Disable New </div>				

NETWORK POLICIES > NEW
NETWORK POLICY

NETWORK POLICY
PROTOCOL

☐ HTTP
☐ Group Remote
☒ FTP
☐ SMTP
☐ TIBCO Rendezvous
☐ IBM Websphere MQ
☐ TIBCO EMS

[Next](#)

NETWORK POLICIES > FTP NETWORK POLICY

FTP NETWORK POLICY

Name*: PGPOverFTPJeff
 Process as XML: ☐
 User Policy Rule: Required ▾

LISTENER

Listener IP*: 10.5.6.55
 Listener Port*: 21
 Read Timeout(minutes)*: 0
 Override PASV IP Address: ☐
 PASV IP Address:
 FTP over SSL/TLS: ☐
 SSL Listener Policy: SSL_Policy_Joyce ▾ [Edit](#)
 Auth Mode: ☒ TLS ☐ SSL

DEFAULT REMOTE

Prevent user@host Syntax: ☐
 Remote Server*: 11.11.11.55
 Remote Port*: 21
 FTP over SSL/TLS: ☐
 SSL Remote Policy: SSL_Init ▾ [Edit](#)
 Auth Mode: ☒ TLS ☐ SSL

OPENPGP

OpenPGP GET: [None] ▾
 OpenPGP PUT: PGP_Dave_Encrypt ▾ [Edit](#)

DATA COMPRESSION

Compression GET: [None] ▾
 Compression PUT: [None] ▾

COMMENT

Comment:

Create

FTP USERS

<input type="checkbox"/>	FTP USER POLICY	CREATED	MODIFIED

After creating the FTP policy you will be able to add FTP user policies.

- From the **Network Policies** screen, create a new FTP policy by clicking **New**.
- On the NETWORK POLICY TYPE screen, select the **FTP** radio button, and then click **Next**.
- On the FTP NETWORK POLICY screen, in the Name field, enter the **name** for this policy.

- Skip the Process as XML checkbox.
- From the Use Policy Rule drop down list, select **Required**.
- In the Listener IP field, enter the **listener IP address**.
- In the Listener Port field, enter the **listener port**.
- Skip Read timeout(minutes)
- Skip Override PASV IP Address
- Skip the FTP over SSL/TLS checkbox.
- Skip the SSL Listener Policy drop down list.
- Skip the FTPS mode radio buttons.
- Skip the Prevent user@host Syntax checkbox.
- In the Remote Server IP or Host Name field, enter the **remote server IP**.
- In the Remote Port field, enter the **remote port**.
- Skip the FTP over SSL/TLS checkbox.
- Skip the SSL Remote Policy drop down list.
- Skip the FTPS mode radio buttons.
- Leave the OpenPGP GET drop down list selected to None.
- From the OpenPGP PUT drop down list, select an **OpenPGP Policy name**.
- Leave the Compression GET drop down list selected to None.
- Leave the Compression PUT drop down list selected to None.
- Click **Create**. The NETWORK POLICIES screen refreshes.

NETWORK POLICIES					
FTP Policies					
<input type="checkbox"/>	NAME	STATUS	PROTOCOL	LISTENER ADDRESS	REMOTE ADDRESS
<input type="checkbox"/>	PGPoverFTPJeff	●	FTP	10.5.6.55:21	11.11.11.55:21
IBM MQ Listener Policies					
<input type="checkbox"/>	NAME	STATUS	PROTOCOL	LISTENER ADDRESS	MODE
<input type="checkbox"/>	MaListenerPolicy-0	●	JMS/MQ	192.168.0.1:1414	Sync
<input type="button" value="Delete"/> <input type="button" value="Enable"/> <input type="button" value="Disable"/> <input type="button" value="New"/>					

FTP USERS		
<input type="checkbox"/>	FTP USER POLICY	CREATED
No items to display		
<input type="button" value="Delete"/> <input type="button" value="New"/>		

- Edit the FTP policy by clicking on this **FTP policy** link.
- On the FTP POLICY details screen, at the bottom of the FTP POLICY details screen, create a new FTP User Policy by clicking **New** in the FTP USER POLICY section.

Note: When working with FTP User policies, consider that:

- With the User policy rule set to REQUIRED or OPTIONAL, the FTP User policy becomes bound to the FTP policy and the FTP User policy will now override the settings on the associated FTP policy.
- With the User policy rule set to REQUIRED, only FTP User policies attached to FTP policies will be able to log in and use the product.
- With the User policy rule set to OPTIONAL, only users that exist as an FTP User policy or a user of a back end FTP server can log in.
- When the FTP User policy is set to IGNORED, this option processes all transactions with the configuration of the FTP listener itself (FTP policy). The back end FTP server is used to authenticate the user.

NETWORK POLICIES > FTP NETWORK POLICY > FTP USER POLICY

FTP USER POLICY

Policy Name*:

LOCAL AUTHENTICATION

System user:

REMOTE AUTHENTICATION

☐ Use system user

☒ Use non-system user

Remote User Name*:

Remote Password:

Confirm Remote Password:

REMOTE SERVER

Remote IP Address:

Remote Port:

FTP over SSL/TLS: ☐

SSL Remote Policy:

Auth Mode: ☒ TLS ☐ SSL

OPENPGP

OpenPGP Get:

OpenPGP Put:

DATA COMPRESSION

Compression GET:

Compression PUT:

COMMENT

Comment:

- On the FTP USER POLICY screen, in the Policy Name field, enter a **name** for this FTP User policy.
- Under LOCAL AUTHENTICATION, select the System user from the System user drop down list.
- Under REMOTE AUTHENTICATION, select the **Use non-system user** radio button.

Note: Under REMOTE AUTHENTICATION, select the Use system user option when selecting which user policy credentials are presented to the remote server.

Select the Use non-system user option when a user not on the Forum system whose credentials will be presented to the remote server. This option also requires the non-system users' password.

- In the Remote User Name field, enter the **user name** of a user to be authenticated on the remote server.

- In the Remote Password field, enter the **password** for this user.
- In the Confirm Remote Password field, re-enter the **password** for this user.

Note: The Remote User Name is the name of the user associated with this FTP User policy and identifies whose credentials are presented to the remote server. The Remote User Name and Remote Password are used by the product to authenticate outgoing users. The Remote User Name and Remote Password may be from 0-unlimited keyboard characters.

- In the Remote IP Address field, enter the **remote IP** entered earlier for the FTP policy remote IP address.

Note: The Remote IP address/port on this FTP User policy must match with the Remote IP address/port of the FTP policy it is bound to. With this option, the credentials presented to the remote IP address of the FTP policy (entered earlier) are those of the non-system user.

- In the Remote Port field, enter the **remote port**.
- Skip the FTP over SSL/TLS checkbox.
- Skip the SSL Remote Policy drop down list.
- Skip the FTPS mode radio buttons.
- From the OpenPGP Get drop down list, select an **OpenPGP Policy name** as the OpenPGP Decrypt & Verify Policy to use for overriding this FTP policy so that the product will manage decryption and verification via OpenPGP over FTP.

Note: The OpenPGP GET drop down list contains the OpenPGP policies to use for FTP actions using OpenPGP.

- From the OpenPGP Put drop down list, select an **OpenPGP Policy name** as the OpenPGP Sign & Encrypt Policy to use for overriding this FTP policy so that the product will manage signing and encryption via OpenPGP over FTP.

Note: The OpenPGP PUT drop down list contains the OpenPGP policies to use for FTP actions using OpenPGP.

- From the Compression GET drop down list, select **ZIP-Decompress**.
- From the Compression PUT drop down list, select **ZIP-Compress**.
- In the Comment field, enter any relevant **comment** (optional).
- Click **Create** and the FTP NETWORK POLICY details screen refreshes.

Now, selecting the FTP policy just created opens the FTP policy details screen. At the bottom of the screen, under FTP Users, the newly created FTP User policy is visible.

FTP USERS			
<input type="checkbox"/>	FTP USER POLICY	CREATED	MODIFIED
<input type="checkbox"/>	FTPJeffBulkEncrypt	Mar 22, 2005 5:30 PM	Mar 22, 2005 5:30 PM
		Delete	New

•

[Redacted]

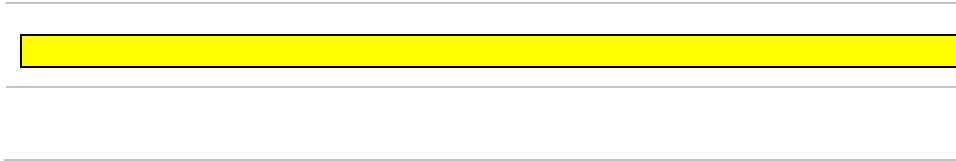
-

[Redacted]



Interactions Between FTP Policies and FTP User Policies

Once you have created your first FTP policy, click an FTP policy name link to return to the bottom of the FTP Policy details screen.



[Redacted]

-

-

[Redacted]

-

[Redacted]

-

[Redacted]

-

-

[Redacted]

-

[Redacted]

-

[Redacted]

- From the OpenPGP PUT drop down list, select

[Redacted]

-

[Redacted]

-

-

-

-

-

-

SFTP POLICIES

SFTP policies provide client, server, and proxy options to handle Secure FTP (SFTP) traffic flow. SFTP policies appear as an option under Network Policies and allow for creating a Listener, Remote, or Proxy policy type.

SFTP Listener Policies

The Network Policies screen manages SFTP policies, their settings and status in the system, tracks existing policies, port settings and policy parameters that listeners map to on the system. SFTP Listener policies are used to accept connection from inbound clients.

NETWORK POLICIES > SFTP LISTENER POLICY

SFTP LISTENER POLICY

Name*:

SftpListenerPolicy

Labels:

Use Device IP:

☒

Listener IP*:

0.0.0.0

Listener Port*:

22

Listener SSH Key:

serverDsaKey [Edit](#)

IP ACL Policy:

Unrestricted [Edit](#)

Template Name:

Default Template [Edit](#)

☐ **Send Response To Client**

SFTP Remote Policy:

Banner:

ALLOWED AUTHENTICATIONS

☒ **Password**

User ACL:

[Allow All]

☐ **Public Key**

SSH Keys:

Create

The settings represent the IP, Port, and SSH key to use for the listener. Further setting include optional IP level access control and error template. Response to the client is also an optional setting to provide a default response back to the client after successful transfer of SFTP information. The Allowed Authentication settings allow the policy to accept username, SSH keys, or both.

SFTP Listener Policy Screen Terms

Please consider the following terms when working with SFTP listener policies.

TERM	DEFINITION
Name	The identifier for this SFTP policy.
Use Device IP	Uses the current device IP as the default IP. This setting allows the policy to dynamically bind to the IP address of the Sentry host when the policy configuration is transferred to other Sentry instances.
Listener IP	Rather than using the device IP, this setting explicitly sets the IP address for the SFTP listener service.
Listener Port	The port for the SFTP listener service
Listener SSH Key	The SSH policy to use for the SFTP transactions
IP ACL Policy	(optional) The IP Access Control policy to restrict the Client IP sources allowed to communicate with this policy
Template Name	The error template to use for responses back to the client
Send Response To Client	(optional) Enables Sentry to send a response back to the client after successful SFTP transaction. This requires an SFTP Remote Policy and an optional Banner message to send to the client.
Allowed Authentications	This determines whether to allow username and password, SSH Keys, or both.

SFTP Remote Policies

The Network Policies screen manages SFTP remote policies, their settings and status in the system, tracks existing policies, port settings and policy parameters that listeners map to on the system. SFTP Remote policies are used to send SFTP transactions to remote SFTP endpoints (or respond back to the client).

NETWORK POLICIES > SFTP REMOTE POLICY

SFTP REMOTE POLICY

Name*:

SftpRemotePolicy

Remote Server*:

Remote Port*:

22

Directory:

Transfer Mode:

Binary ▾

☐ Verify Server Key

Known Hosts:

▾

Process Response:

☐

AUTHENTICATION

☒ Propagate Credentials

☐ Specify Credentials

Username:

Password:

Confirm Password:

☐ Public Key Authentication

Username:

Remote SSH Key:

serverDsaKey ▾ [Edit](#)

Create

The settings represent the remote server communication parameters to configure, including Remote Server IP and Port, the directory to publish the transaction to, the transfer mode (ASCII / Binary) and whether to verify the remote SSH key. Authentication settings enable propagation of credentials presented to Sentry on an SFTP Listener Policy, or specifying username credentials, or SSH credentials.

SFTP Remote Policy Screen Terms

Please consider the following terms when working with SFTP Remote policies.

TERM	DEFINITION
Name	The identifier for this SFTP policy.
Remote Server	The IP address or hostname of the target SFTP server
Remote Port	The port for the SFTP target server (default is Port 22)
Directory	The directory to publish the transaction once the connection is established
Transfer Mode	Binary or Text (ASCII) transfer mode
Verify Server Key	(optional) Verify the Server SSH Key against a Known Hosts policy to ensure that the endpoint SSH Key has been deemed a known trusted server
Process Response	Used to determine if the response from this policy is to be send to the Task Groups for document processing
Authentication	<ul style="list-style-type: none">• Propagate Credentials Will use the credentials presented to Sentry on the inbound SFTP listener policy• Specify Credentials Allows a username and password to be specified for username based authentication.• Public Key Authentication Allows an SSH Key policy to be specified to use for SSH Key authentication

SFTP Proxy Policies

The Network Policies screen manages SFTP proxy policies, their settings and status in the system, tracks existing policies, port settings and policy parameters that listeners map to on the system. SFTP Proxy policies are used to receive SFTP transactions and then send to remote SFTP endpoints (or respond back to the client).

NETWORK POLICIES > SFTP NETWORK POLICY

SFTP NETWORK POLICY

Name*:

SftpPolicy

Process:

☐

LISTENER

Use Device IP:

☐

Listener IP*:

10.5.1.196

Listener Port*:

22

Listener SSH Key:

serverDsaKey

Edit

ALLOWED AUTHENTIFICATIONS

☒ Password

Use ACL:

[Allow All]

☐ Public Key

Authorized SSH Keys:

REMOTE

Remote Server*:

Remote Port*:

22

☐ Verify Server Key

Known Hosts:

REMOTE AUTHENTICATION

☒ Propagate Credentials

☐ Specify Credentials

Username:

Password:

Confirm Password:

☐ Public Key Authentication

Username:

Remote SSH Key:

serverDsaKey

Edit

Create

The settings represent the listener policy configuration settings to accept inbound SFTP and the remote server communication parameters to communicate with a remote SFTP instance. These settings are described in detail in the preceding SFTP Listener Policy and SFTP Remote Policy sections.

SFTP Proxy Policy Screen Terms

Please consider the following terms when working with SFTP Proxy policies.

TERM	DEFINITION
Name	The identifier for this SFTP policy.
Remote Server	The IP address or hostname of the target SFTP server
Remote Port	The port for the SFTP target server (default is Port 22)
Directory	The directory to publish the transaction once the connection is established
Transfer Mode	Binary or Text (ASCII) transfer mode
Verify Server Key	(optional) Verify the Server SSH Key against a Known Hosts policy to ensure that the endpoint SSH Key has been deemed a known trusted server
Process Response	Used to determine if the response from this policy is to be send to the Task Groups for document processing
Authentication	<ul style="list-style-type: none">• Propagate Credentials Will use the credentials presented to Sentry on the inbound SFTP listener policy• Specify Credentials Allows a username and password to be specified for username based authentication.• Public Key Authentication Allows an SSH Key policy to be specified to use for SSH Key authentication

SSH KEY POLICIES

The Keys screen provides a workspace for managing SSH keys. SSH Keys can be generated directly on Sentry, or imported from other sources into Sentry.

KEYS

<input type="checkbox"/>	NAME	TYPE	SIZE	STATUS
<input type="checkbox"/>	serverDsaKey	SSH Key Pair	1024	Active
<input type="checkbox"/>	serverDsaKey_pub	SSH Public Key	1024	Active
<input type="checkbox"/>	serverKey	SSH Key Pair	1024	Active
<input type="checkbox"/>	serverKey_pub	SSH Public Key	1024	Active
<input type="checkbox"/>	serverRsaKey	SSH Key Pair	1024	Active
<input type="checkbox"/>	serverRsaKey_pub	SSH Public Key	1024	Active
<input type="checkbox"/>	test4	Key Pair	1024	Active
<input type="checkbox"/>	test4_0_cert	Certificate	1024	Active
<input type="checkbox"/>	test4_1_cert	Certificate	1024	Active
<input type="checkbox"/>	test4_2_cert	Certificate	1024	Active
<input type="checkbox"/>	test4_3_cert	Certificate	1024	Active

16 items found. Search max results [Show](#)

SSH Key Policy Screen Terms

Please consider the following terms when working with SSH Key policies.

TERM	DEFINITION
Name	The identifier for this SSH Key policy.
Algorithm	Specify the algorithm to use for the SSH key generation. Options include SSH1_RSA, SSH2_RSA, and SSH2_DSA
Key Size	The size of the generated SSH Key. Options include 1024, 2048, and 4096.
Passphrase	The passphrase to use for the generated SSH Key

Create an SSH Key

To create a new SSH Key, go to the Keys screen and click the **New** button. In the Wizard, choose the OpenSSH Key Pair option. On the next screen, enter the Key policy name, algorithm, key size, and passphrase, then click the “Create” button to generate the key.

Import an SSH Public Key or Key Pair

To import an SSH Key or Key Pair, go to the Keys screen and click the **Import** button. In the Wizard, choose the “SSH Public Key”, or the “SSH Key Pair” option. On the next screen, choose to upload from file, or paste from clipboard.

APPENDICES

Appendix A - FTP Error Codes

The following table displays a list of FTP error codes and their descriptions. Some of these error codes return different messages depending on the situation.

FTP ERROR CODE	DESCRIPTION
110	"Restart marker reply"
120	"Service ready in <something> minutes"
125	"Data connection already open; transfer starting"
150	"File status okay; about to open data connection" in response to a data transfer command (LIST, NLST, RETR, STOR, STOU, APPE) when about to read data from or write data to the client
200	"Command <command> okay"
200	"Command PORT okay" if PORT command is well formed
200	"Directory changed to <something>"
202	"Command <command> not implemented, superfluous at this site"
211	"FtpServer Connected to <something> Connected from <something> Logged in as <something> End of status"
211	"System status, or system help reply"
212	"Directory status"
213	"File status"
214	"Syntax: <command> <arguments>"
214	"The following commands are implemented. <list of commands> End of help"
214	"Unknown command <command>"
215	"<something> Type: FtpServer"
220	"Service ready for new user"
220	"Service ready for new user" when the system is ready for login
221	"Goodbye" in response to the QUIT command
221	"Service closing control connection"
225	"Can't open data connection"
226	"Closing data connection"

FTP ERROR CODE	DESCRIPTION
227	"Entering Passive Mode (<something>)" if PASV command succeeds on the system
230	"User logged in, proceed" if login succeeds on the system
234	"<command> <argument> successful" *
250	"Requested file action okay, completed"
250	"Requested file action okay, completed. Generated file: <something>"
257	""<something>' created"
257	""<something>' deleted"
257	""<something>' is current directory"
331	"Guest login ok, send your complete e-mail address as password"
331	"User name okay, need password for <username>" if USER command needs a password
332	"Need account for login"
350	"Requested file action pending further information"
350	"Restarting at <position>. Send STORE or RETRIEVE to initiate transfer"
421	"Invalid response from server" if the remote server does not prompt for login when we first connect to it
421	"Proxy unable to connect to server" if the remote server could not be contacted
421	"Proxy unable to resolve server address" if the remote server specified by the FTP policy could not be resolved
421	"Remote server closed connection; closing client connection" if the system receives a 421 response on the remote control connection
421	"Service not available, closing control connection" if USER command discovered the maximum number of users are already logged in
425	"Can't open data connection"
426	"Connection closed; transfer aborted"
431	"No such directory"
450	"Requested file action not taken"

FTP ERROR CODE	DESCRIPTION
451	<p>"Requested action aborted" (message may vary) for most errors during a data transfer command (LIST, NLST, RETR, STOR, STOU, APPE), examples:</p> <ul style="list-style-type: none"> • Server didn't return 227 in response to PASV command, or returned malformed 227 response • Appliance was unable to create server socket to use for remote PORT command, or remote returned an error in response to PORT command • Opening client data socket failed
451	"Requested action aborted. <argument>"
451	<p>OpenPGP Encryption failed: Use BINARY FTP transfer mode.</p> <p>If an Encryption or Signature operation is performed over ASCII FTP transfer mode and the user has not selected the "Use ASCII Armor" option for the corresponding OpenPGP policy, then the FTP transfer will fail. This is to prevent the binary encrypted or signed data from getting corrupted as a result of sending non-printable binary over the FTP ASCII transfer channel. The user must either switch to binary FTP transfer mode, or they must select the "Use ASCII Armor" option for the OpenPGP policy if they wish to use ASCII FTP transfer mode.</p>
451	<p>OpenPGP Decryption failed: Use BINARY FTP transfer mode.</p> <p>For Decryption and Verification operations, if the FTP policy detects that the incoming file is in binary OpenPGP format but the FTP transfer mode is ASCII, then the decryption or verification operation will fail. The user must perform the operation using binary FTP transfer mode. If the incoming file from the remote server is in the OpenPGP ASCII ARMORED format, then the user can chose either ASCII or BINARY FTP transfer mode as both modes will not corrupt the incoming PGP ASCII ARMORED data.</p>
451	<p>OpenPGP Signature failed: Use BINARY FTP transfer mode.</p> <p>If an Encryption or Signature operation is performed over ASCII FTP transfer mode and the user has not selected the "Use ASCII Armor" option for the corresponding OpenPGP policy, then the FTP transfer will fail. This is to prevent the binary encrypted or signed data from getting corrupted as a result of sending non-printable binary over the FTP ASCII transfer channel. The user must either switch to binary FTP transfer mode, or they must select the "Use ASCII Armor" option for the OpenPGP policy if they wish to use ASCII FTP transfer mode.</p>
451	<p>OpenPGP Signature Verification failed: Use BINARY FTP transfer mode.</p> <p>For Decryption and Verification operations, if the FTP policy detects that the incoming file is in binary OpenPGP format but the FTP transfer mode is ASCII, then the decryption or verification operation will fail. The user must perform the operation using binary FTP transfer mode. If the incoming file from the remote server is in the OpenPGP ASCII ARMORED format, then the user can chose either ASCII or BINARY FTP transfer mode as both modes will not corrupt the incoming PGP ASCII ARMORED data.</p>
452	"Requested action not taken"

FTP ERROR CODE	DESCRIPTION
500	"Syntax error, command <command> unrecognized"
501	"<argument>' is not a valid argument"
501	"<argument>' is not a valid directory"
501	"<argument>' is not a valid pathname"
501	"Syntax error in parameters or arguments" if PORT command is malformed
501	"Syntax error in parameters or arguments" if USER command did not specify a user name
502	"Command <command> not implemented"
503	"Bad sequence of commands" if a file transfer is in progress and an FTP command other than ABOR or QUIT is sent
504	"Command <command> not implemented for that parameter"
521	"<something>' already exists"
521	"Data connection cannot be opened with this PROT setting" *
530	"Access Denied" if login fails on the system
530	(message varies) if remote login fails because of an I/O failure
532	"Need account for storing files"
534	"Invalid protection level" *
550	"File <argument> unavailable"
550	"Requested action not taken" if PASV command fails on the system
550	SSL required on the control channel *
550	TLS required on the control channel *
552	"Requested file action aborted"
553	"Requested action not taken"

* Specific to FTPS.

In some situations, errors from the remote server are proxied directly back to the client. In these cases, Forum Systems cannot predict what the error message will be. In others, the error code from the remote server is used, but with an error message generated by the system from the set of standard FTP error messages.

Appendix B - Constraints of FTP Security Guide

ELEMENT	CONSTRAINTS	CHAR COUNT
OpenPGP Key Name	Unique, case sensitive and accepts underscores and dashes.	5-32
OpenPGP Private Key Passphrase	Case sensitive and accepts underscores and dashes.	6-255
OpenPGP Key Size	1024-4096 bits	N/A
Enabled Server Policies at one time	Unlimited *	N/A
FTP Policy Name and FTP over SSL/TLS Policy Name	Unique, case sensitive and accepts underscores and dashes.	5-32
FTP User Policy Name and FTP over SSL/TLS User Policy Name	Unique, case sensitive and accepts underscores and dashes.	5-32
Remote User Name	Unlimited keyboard characters.	0-unlimited
Remote Password	Unlimited keyboard characters.	0-unlimited
OpenPGP Encrypt Policy, OpenPGP Decrypt & Verify Policy, OpenPGP Sign Policy, OpenPGP Verify Policy, OpenPGP Sign & Encrypt Policy	Unique and accepts underscores and dashes.	1-32
Append File Extension field	Allows users to append a filename extension to outgoing files when creating Encrypt, Sign, and Sign & Encrypt OpenPGP policies. Accepts a maximum of three alphanumeric characters.	3

Appendix C - Specifications in FTP Security Guide

FTP Policies and FTP over SSL/TLS Policies	Unlimited *
FTP over SSL/TLS Policies	Unlimited *
FTP User Policies	The number of FTP User Policies on one FTP policy is unlimited.
FTP over SSL/TLS User Policies	The number of FTP User Policies on one FTP policy is unlimited.
Simultaneous FTP connections	The system supports unlimited large file transfers with streaming OpenPGP policies. OpenPGP policies can include 128 simultaneous open streams, limited by the disk capacity on a client or server.
The maximum document size for RFC 1991 encoding compliance	100MB
The maximum document size for RFC 2440 encoding compliance	Unlimited
The overall maximum number of FTP simultaneous connections for indefinite length RFC 2440 encoding	128 Example: 127 connections (Unlimited – RFC 2440) 1 connection (Legacy – RFC 2440)

* Limited only by disk space.

INDEX

add an FTP over SSL/TLS policy.....	21
add an FTP over SSL/TLS User policy	25
add an OpenPGP Verify policy	66
add blended OpenPGP Sign & Encrypt policy.....	68
add FTP policy and configure OpenPGP security	15
add OpenPGP Decrypt & Verify policy	70
add OpenPGP Encrypt policy	62
add OpenPGP Sign policy	64
ASCII	30
ASCII armor format	58
changing OpenPGP policy settings during an FTP session	60
conventions used	1
delete an OpenPGP key pair	55
delete an OpenPGP public key	55
delete OpenPGP key pair or OpenPGP public certificate unless referenced elsewhere	31
Diffie-Hellman.....	30
ElGamal.....	30
Encoding options.....	58
encrypt	
adding for OpenPGP over FTP.....	72
export all OpenPGP keys into ASCII Armored file	47
export an OpenPGP key pair	53
export OpenPGP keys from Key Details screen.....	49
FTP error code specific to FTPS.....	94, 96
FTP error code table	
run-time.....	93
FTP over SSL/TLS option for FTP over SSL/TLS network policy.....	5
FTP over SSL/TLS option for FTP over SSL/TLS User policy.....	12
FTP over SSL/TLS option for the listener	5
FTP policy	
name	4
terms	4
FTP User policy.....	7
adding	18
examples.....	14
name	11
remote Password	77
terms	11
FTPS	2
FTPS standards	
AUTH SSL	2
AUTH TLS.....	2
generate an OpenPGP key pair	55
GZIP - Compress	6, 12
GZIP - Decompress	6, 12
Ignored FTP User policy rule	4
import an OpenPGP key pair from multiple files.....	41
import an OpenPGP key pair from one file	32

import an OpenPGP public certificates	44, 52
import OpenPGP Key Pair stored in one file by pasting from clipboard	34
Keys	
number of days in advance of OpenPGP key expiry to send an alert email	40
Keys screen	29, 92
listener address for FTP policy.....	3
listener IP	4
listener port.....	4
Network Policies screen terms for FTP policies and FTP over SSL/TLS	3
OpenPGP	
RFC 2440 specification.....	57
OpenPGP algorithms supported	30
OpenPGP GET	5, 6, 12
OpenPGP key expiry alert settings	40
OpenPGP key formats supported	30
OpenPGP Key policy	
examples.....	31
OpenPGP key protocols supported	30
OpenPGP key sizes supported	30
OpenPGP keys	29
about exporting	49
add comment	51
OpenPGP network policy	
examples.....	61
OpenPGP over FTP	
about	2
OpenPGP policy	
Append File Extension.....	63
ASCII armor format encoding for encryption	59
ASCII armor format encoding for signing	60
certificate or key pair for verification	60
Decrypt & Verify mode.....	59
Encrypt mode.....	59
Encrypt with Append File Extension	59
key pair for decryption	59
key pair for encryption	59
key pair for signing.....	60
Legacy – RFC 1991 for encryption.....	59
RFC 2440 for encryption.....	59
Sign & Encrypt mode	59
Sign mode.....	59
unlimited – RFC 2440 for encryption	59
Verify mode.....	59
OpenPGP protocol	30
OpenPGP PUT.....	5, 6, 12
OpenPGP Screen	57
Optional FTP User policy rule	4
PKCS keys	29
policy name for Policy	3
policy name for Tibco-EMS policy..	87, 89, 91, 92
prevent user@host syntax	5
protocol for FTP policy	3
Remote address for FTP policy	3
Remote IP address with FTP User policy	12
Remote Password with FTP User policy.....	11
Remote Port	5

Remote port with FTP User policy	12
remote server IP or host name	5
Remote User Name with FTP User policy	11
Required FTP User policy rule	4
RSA v3 and v4	30
select multiple Key Pair or Certificate names	
OpenPGP Encrypt policy	63
Settings command	
visible only when	32
sort by name	
with OpenPGP keys	29
SSL Listener Policy	5
SSL Remote Policy p[roxy for FTP over SSL network policy	5
SSL Remote Policy with FTP over SSL User policy	12
status of a Network policy	3
view OpenPGP key details	39
view OpenPGP public certificate details	46
ZIP - Compress	6, 12
ZIP - Decompress	6, 12
ZIPs with more than one entry	2