IRONPORT®
SYSTEMS

IronPort Encryption Appliance 6.5

CONFIGURATION MANUAL

COPYRIGHT

Part Number: 421-0234

Revision Date: August 6, 2009

IRONPORT SYSTEMS® , INC.

IronPort Systems, Inc.
950 Elm Ave.
San Bruno, CA 94066

CONTACTING IRONPORT CUSTOMER SUPPORT

If you have purchased support directly from IronPort Systems, you can request support by phone, email, or online 24 hours a day, 7 days a week. During office hours (24 hours per day, Monday through Friday, excluding U.S. holidays), an engineer will contact you within an hour of your request. To report a critical issue that requires urgent assistance outside of our office hours, contact IronPort using the following information.

U.S. toll-free: 1 (877) 641-IRON (4766)

International: www.ironport.com/support/contact_support.html

Support Portal: www.ironport.com/support

If you have purchased support through a reseller or other entity, contact the supplier for support of your IronPort products.

Table of Contents

CHAPTER 1

Applications

This chapter contains information on the IronPort Encryption appliance applications, including using pre-defined applications and adding and configuring new ones.

This chapter contains the following sections:

ABOUT APPLICATIONS

The IronPort Encryption appliance uses applications to define the behavior of the system when sending messages. Typically, you would use the pre-defined applications that are shipped with the product. However, under some circumstances (for example, multiple branding) you would need to create new applications. When you create a new application, you define the behavior of that application by assigning an application type to it. For example, if you create a new application named 'Billing Statements' that you want to be encrypted and sent in a Secure Envelope, you could select the Registered Envelope application type. For information about adding, configuring, and managing applications on the IronPort Encryption appliance, see "Managing Applications" on page 13.

PRE-DEFINED APPLICATIONS

An IronPort Encryption appliance application is a processor pipeline defined to process mail messages.

- Offline Envelope

  Sends encrypted Secure Envelopes that can be opened offline. For more information see the section on the Registered Envelope application.

- Offline Envelope - Enrolled

  Sends encrypted Secure Envelopes that can be opened offline where the key used to decrypt the envelope is the registered recipient's password. For more information, see the section on the Registered Envelope application.

- Registered Envelope - Enrolled

  Sends encrypted Secure Envelopes where the key used to decrypt the envelope is stored online by the *key server*. For more information, see the section on the Registered Envelope application.

- Registered Envelope - CRES

  Sends encrypted Cisco Registered Envelope Service envelopes, where the key used to decrypt the envelope is stored online by the Cisco Registered Envelope key server. For more information, see the section on the Registered Envelope - CRES application.

- Secure Mailbox

  Sends a notification to the recipient and stores the message so that it can be retrieved through a secure webmail system.

- Resend

  Resends any message using original or new security credentials.

- SMTP Delivery

  Sends email messages using SMTP.

- Queue Message

  When using application chaining, this is typically the first application the message goes through. This application allows you to hold messages until the recipient enrolls.

- Bounce - User Locked

  Email messages that are identified by the User Status matcher as having been sent to a user with a 'Locked' status are sent to this application. This application adds an error message and sends the message to the Bounce application.

- bounce

  Handles bounced emails.

- error

  A repository where error-flagged messages are sent.

APPLICATION TYPES

When you create an application for the IronPort Encryption appliance, you must assign an application type to designate its behavior. The majority of application types have a corresponding sample application to illustrate the proper configurations, etc. The following is a list of all application types.

- Add Header and Footer
- Anti-Virus
- Archive
- Automatic Registration
- Bounce Handler
- Bounce Processor
- Clone Message
- Custom
- Email Formatter
- Email Queue
- Gateway Encrypt
- Large Attachments
- Modify Headers
- Notification
- PDF Secure
- PGP Decrypt and Verify Signature
- PGP Encrypt and Sign
- PGP Harvest
- Registered Envelope
- Registered Envelope Opener
- Secure Mailbox
- Recipient Modifier
- Remove Attachments
- Replace Message Body
- Resend
- S/MIME Decrypt
- S/MIME Encrypt and Sign

- S/MIME Harvest and Verify Signature
- SMTP Delivery
- Storage
- User Mapper

See the following sections for information about specific application types.

Add Header and Footer

Use this application type to take the body of the message and add headers and footers to it. In the Details tab, there are three configuration parameters specific to this application type:

- **Use Incoming Encoding:** Use the body charset and CTE of the incoming message in the modified message sent out by this application.
- **Body Charset:** The charset to use on the body of the outgoing message. This is only used if the Use Incoming Encoding parameter is checked or if the incoming charset fails.
- **Body CTE:** The CTE to use on the body of the outgoing message. This is only used if the Use Incoming Encoding parameter is checked or if the incoming charset fails.

Anti-Virus

Scans messages for viruses.

Automatic Registration

This application type checks to see if a user exists for the email address. If the user does not exist in our system, it will automatically create a Websafe user and mailbox. Note that this it is only intended to be used with systems that use some sort of external authentication since the password is automatically generated.

In the Details tab, there are three configuration parameters specific to Auto Registration App.

- **Default Disk Quota:** Websafe mailbox quota size.
- **Default Expiration Period (days):** Websafe message expiry.
- **Default unread Notification Period (days):** Sends a notification email to the sender if the email has not been read within a certain period.

In the LDAP tab, these are the configuration parameters specific to Auto Registration App.

- **Enable LDAP:** Used to enable LDAP to populate the user information.
- **LDAP Host:** Hostname of the LDAP server.
- **LDAP Port:** Port of the LDAP server.
- **User Name:** Username to login to the LDAP server.
- **Password:** Password to authenticate against the LDAP server.
- **Search Filter:** LDAP query to run to locate the user.

- **Search Base:** Base DN to do LDAP query.
- **Enable Subtree Search:** Enables you to recursively search the LDAP server.
- **Always Create User:** Creates the user even if the user does not exist in the LDAP server. Note that minimal information will be used to create the user.
- **Email Attribute:** Email address.

These parameters are read from the configured LDAP server and updated in the registration information for each user.

- **Notify Email Attribute:** Notification email address.
- **First Name Attribute:** First name of the user.
- **Last Name Attribute:** Last name of the user.
- **Company Name Attribute:** Name of the company the user belongs to.
- **Passphrase Attribute:** Contains the passphrase.

Bounce Handler

The Bounce Handler application type is provided to handle messages that are sent from the encryption server and get bounced back from the outside world. It is usually used in combination with a matcher that recognizes bounced mail.

- **Update Unrecognized Bounces in Tracking Database** - If checked, bounces in response to unknown messages are tracked.
- **Forward Unrecognized Bounces -** If checked, bounces in response to unknown messages are forwarded.
- **Unrecognized Bounce Forward Address** - Address bounces in response to unknown messages are forwarded to.
- **Next for Unrecognized Bounce** - Next Router RuleSet or application to process unrecognized bounces.
- **Forward Recognized Bounces** - If checked, bounces in response to known messages are forwarded.
- **Recognized Bounce Forward Address Prefix** - Local address (value before '@' sign) to forward bounces in response to known messages to.
- **Prefix Custom Tracking Table Value**
- **Recognized Bounce Forward Address Suffix** - Domain name (value after '@' sign) to forward bounces in response to known messages to.
- **Suffix Custom Tracking Table Value**
- **Convert Custom Tracking Table To Message Headers**
- **Tracking Service Name** - Tracking service's JNDI name.

- **Enable Tracking** - If checked, tracks outgoing email.
- **Next for Recognized Bounce** - Next Router RuleSet or application to process recognized bounces.

To use the BounceHandler application type, create an application following the instructions later in this chapter and select Bounce Handler from the Type drop-down.

Bounce Processor

The Bounce Processor application type allows you to define an application to handle messages that downstream MTAs return because they cannot deliver them. It analyzes the incoming bounced messages and updates the tracking tables.

Clone Message

Use this application type to clone a MIME message. The intent of this application type is to create a copy of the incoming message and send it to two different applications for further processing. This application type has two paths that can be configured by the Admin, the original message will be sent to the first "next" application configured. The cloned message will be sent to the second "next" application. The original message will not modified in any way.

In the Details tab, there are two configuration parameters specific to Clone Message App.

- **Next for Original Message:** The name of the application that the original message will be sent to.
- **Next for Cloned Message:** The name of the application that the cloned message will be sent to.

Custom

Use this application type when writing your own custom application. It is recommended that you have in-depth knowledge of the system before using this feature.

Email Formatter

Takes a XHTML document and transforms it into different output document types like PDF, PS, XML & RTF. The underlying parser is Apache-FOP. The converted document can then be handed over to the next application or ruleset if needed. The application takes a multipart MIME message and locates the text/XHTML attachments and converts them to the format specified in the X-Header and adds the converted document back to the MIME message. The X-Header should be of the format: X-PostX-FOP_*<target_doc_type>*. An example is X-PostX-FOP_PDF. You can set-up a matcher-mailet path using the HasHeader matcher to deliver mail to the Email Formatter App. If you are transforming the input doc to a PDF file, you have an option to specify DRM properties such as allowing the copy function. You can also specify the edit function using pdfencrypt.properties in the conf directory. When selected, the Auto Correct HTML configuration parameter will correct and convert HTML to XHTML which can be used to convert to PDF, PCF, etc.

Email Queue

This application allows you to hold messages until the recipient has registered.

Gateway Encrypt

Unpacks and processes messages that were sent using the Gateway Encrypt version of the desktop plug-ins for Microsoft Outlook and Lotus Notes.

Large Attachments

Stores large attachments on the server where they can be retrieved securely, and replaces the attachments with links to the files on the server.

Modify Headers

Modifies message headers, including adding or updating a new header or deleting an existing message header.

Notification

Sends notification emails. Notification emails can be sent to the recipients of the original message, the sender, or a custom recipient such as an admin.

PDF Secure

Use this application for signing and/or encrypting all of the PDF attachments present in a message, based on user configuration. The signing is done inline using a PKCS12 certificate and the encryption is done using a password. For information on using this application, see the section *Using the PDFSecure Application* later in this chapter.

PGP Decrypt and Verify Signature

Use this application when decrypting incoming messages using the private key of the intended recipient. If the message has been signed, this application will verify and remove the signature.

PGP Encrypt and Sign

This application is used to send a PGP encrypted and/or signed message.

PGP Harvest

Use this application to retrieve (harvest) the public key from incoming messages and update them to the Certificate Repository.

Registered Envelope

The incoming payload is encrypted using RC4 or AES and inserted into a HTML document. The document is then attached to an email and sent to the intended recipient. The envelope can be encrypted using plain text, MD5 and a SHA1 hash key. The IronPort Encryption appliance also provides different types of envelopes: Offline and Registered.

Registered Envelope Opener

Takes in the message, opens it and decrypts it, and then forwards the contents. This application type also provides support for Mobile Device Support (MDS).

Registered Envelope - CRES

Sends notifications and stores messages for Cisco Registered Envelope users.

Recipient Modifier

Use this application to add or remove SMTP or MIME recipients. SMTP and MIME can have different recipient lists. For example, this is how BCC works. The MIME document has only certain recipients listed in it, but the message is actually delivered to other users as well. The recipients who get the MIME doc do not know who else got the message via SMTP.

Remove Attachments

Removes attachments from messages.

Replace Message Body

Replaces the message body of an email with one that is templated.

Resend

Resends any message using original or new security credentials.

S/MIME Decrypt

Use this application when decrypting incoming messages using the private key of the intended recipient.

S/MIME Encrypt and Sign

This application is used to send an S/MIME encrypted and signed message.

S/MIME Harvest and Verify Signature

Use this application to retrieve (harvest) the public key from incoming signed messages and update them to the Certificate Repository. This application will optionally verify and optionally remove the signature.

SMTP Delivery

Sends email messages using SMTP.

Storage

Use to create an application that is a repository for storing messages.

User Mapper App

Use to change the domain of the email address of either the recipient(s) or sender of an email. It can convert an address from the form user@domain.com to the form user%domain.com@newdomain.com. It can also be used to revert and address of the form user%domain.com@newdomain.com to the original form user@domain.com.

This application was created to integrate the IronPort Encryption appliance with a TLS system, which requires that email domains be temporarily converted before routing through the MessagaeLabs TLS tower. But it could be useful in any case where you may need to temporarily change a Sender or Recipient's domain.

The User Mapper application allows a great deal of control over what kinds of addresses will be changed. The following configuration parameters are associated with this application type:

Domains to Change: A comma separated list of the domains to perform the conversion/reversion on. An address will be changed only if it's domain matches a domain on this list. In order to convert all domains use the wildcard '*'.

Target Domains: (This field is only used on a convert action.) A comma separated list that matches up to the Domains to Change list, and specifies what domain each of these domains to change should be converted to.

Delimiter: Specifies which string of characters to put before the saved original domain in a convert, and which string of characters to use to find the saved original domain in a revert.

Note — A revert will only work on an address that has been converted with the same delimiter. It is recommended that you use % for all cases.

User: Specify whether the Sender or Recipients' addresses should be checked for matches and have the action performed on them. An application with the action set to None does not perform any changes on email addresses.

Action: Specify whether the application performs the Convert or Revert action on matched emails addresses. An application with the action set to None does not perform any changes on email addresses.

Example:

The configuration parameter values:

Application Name: Convert Recipients

Matcher Name: All

Mailet Class: UserMapper

Domains to Change: zebra.com, chicken.com, *

Target Domains: zoo.com, food.com, animals.com

Delimiter: %

User: Recipient

Action: Convert

will take a message with the following recipients:

george@monkey.com, fried@chicken.com, charlotte@spider.com

and covert them to:

george%monkey.com@zoo.com, fried%chicken.com@food.com,
charlotte%spider.com@animals.com

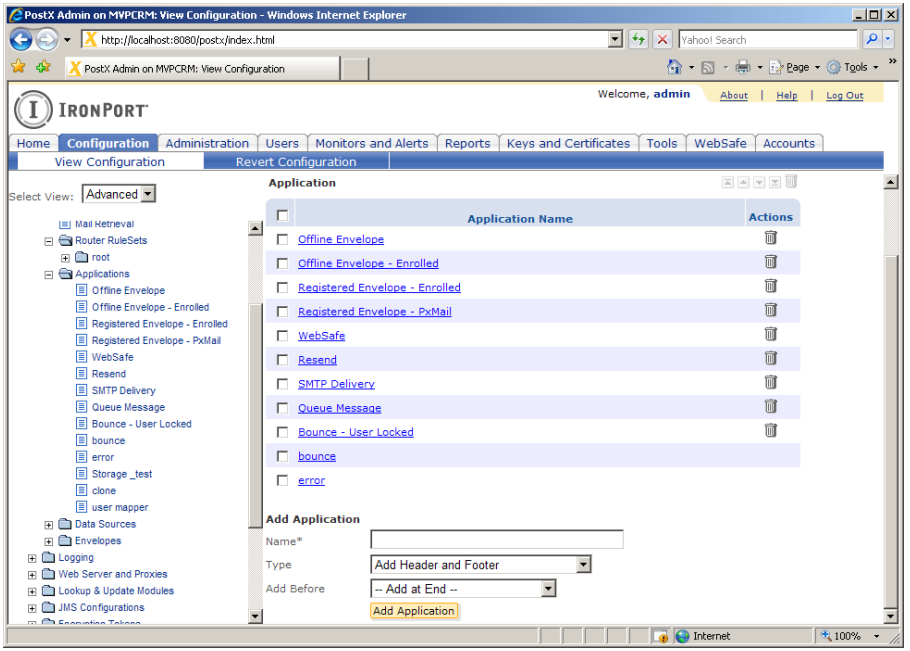
MANAGING APPLICATIONS

To view or edit application configurations, click the Configuration tab and navigate to Configuration > SMTP Adaptor > Applications. In the right pane, you can use the sub-tabs to configure the application (for example, you can use the Details and Message Personalization sub-tabs for the System Alerts Notification application). Application-specific configuration parameters are grouped by function. The sub-tabs vary by application.

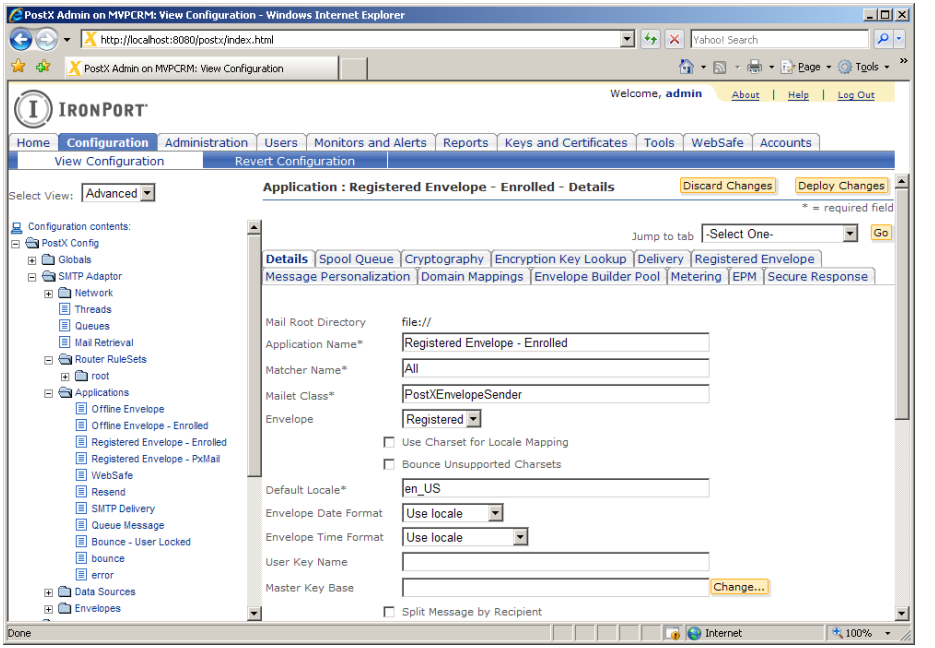
Viewing Applications

To view the applications available on the system:

1. Click the Configuration tab and click Configuration > SMTP Adaptor > Applications. You can either select the application you want to view from the tree or from the list of applications that appears in the right pane.



2. To view information about an application, click the application name.



Adding Applications

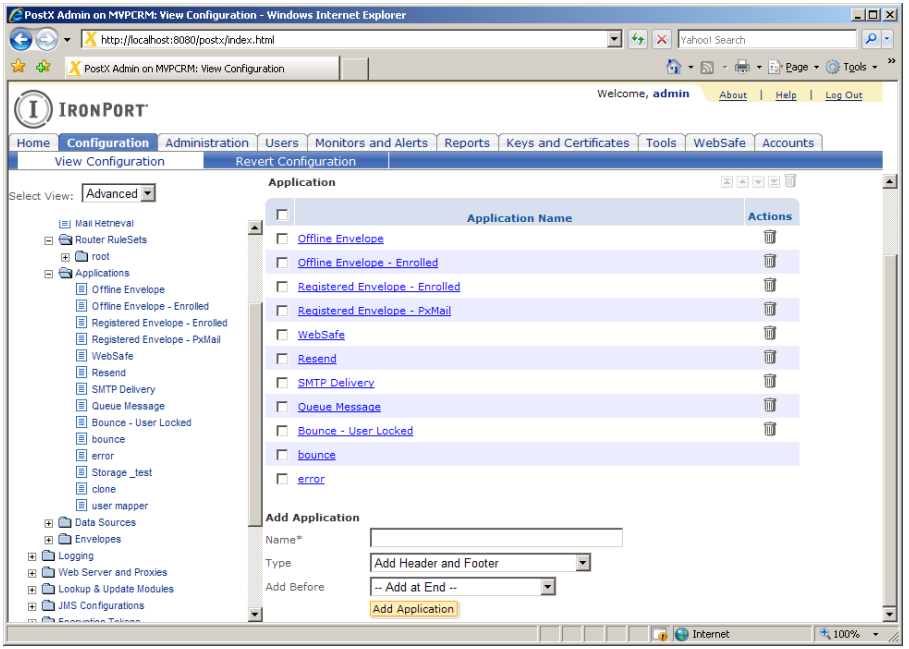
Before adding an application, review the pre-defined application configurations so that you can familiarize yourself with the parameters associated with the different application types. This will allow you to better determine the application you want to use and whether you need add an application.

Note: Typically, you will not need to add new applications, although it may be required to meet your specific needs (for example, multiple branding, etc.).

Via the Applications Node

To add an application, do the following:

1. Click the Configuration tab and click Configuration > SMTP Adaptor > Applications.



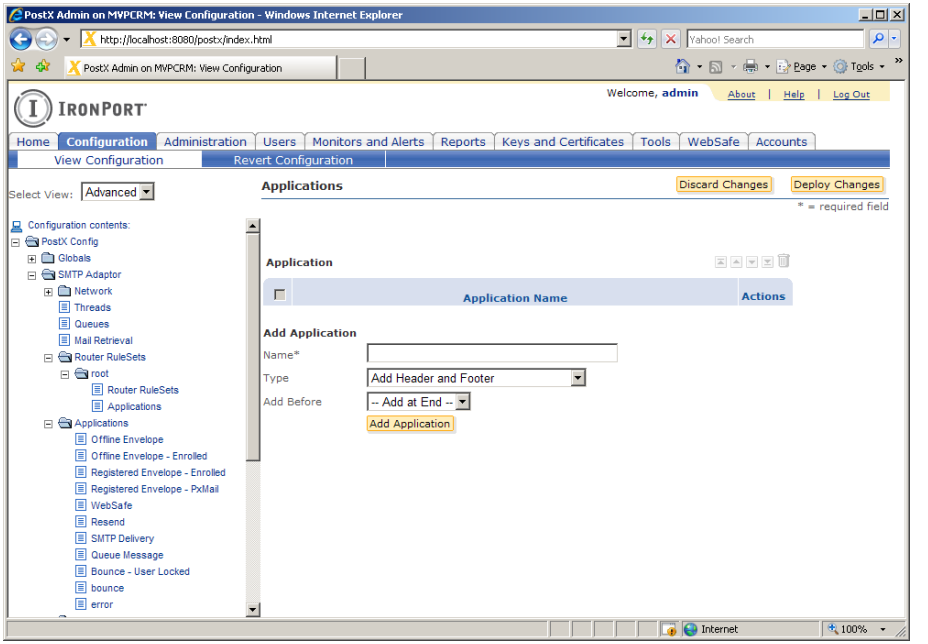
   The Add Application section appears at the bottom of the screen.

2. Type in an application name.
3. Enter a description for the new application. This field is not required.
4. Select a type from the drop-down. For a list of application types and descriptions, refer to the section *Application Types* in this chapter.
5. Use the Add Before drop-down to specify where the application appears in the list. The location of the application in the list does not affect the system. Add Before is available for organizational purposes only.
6. Click the **Add Application** button.
7. View the configurations for the new application either by navigating to the application in the configuration tree or clicking the name in the list of applications in the right pane. See *Appendix A: Configuration Parameters* in this manual for a complete list of configuration parameters associated with applications.

Via the Router RuleSets Node

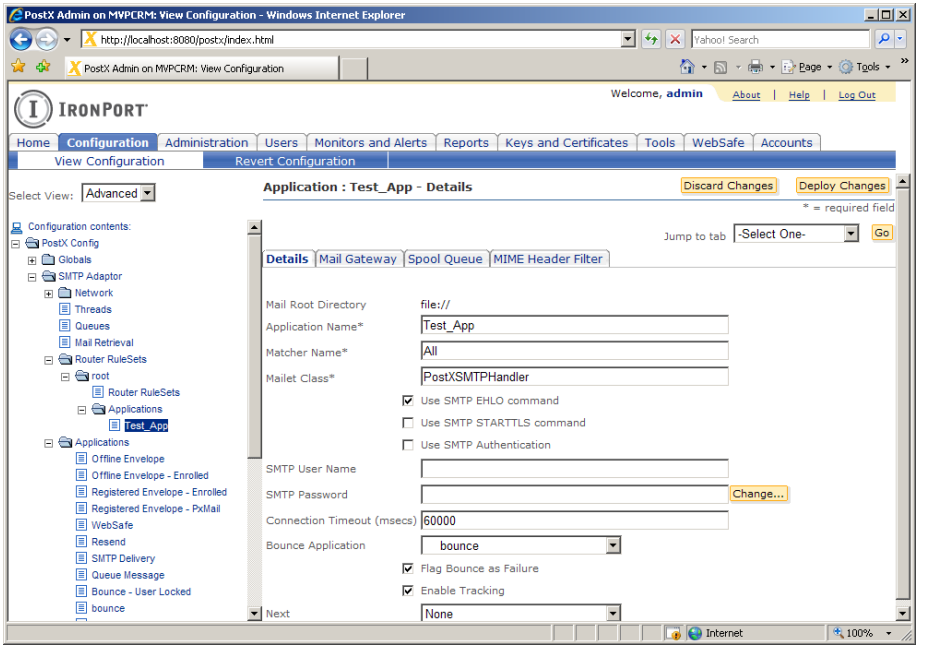
To add an application, do the following:

1. Click the Configuration tab and click Configuration > SMTP Adaptor >Router RuleSets > *Ruleset_name* (this example uses the 'root' RuleSet) > Applications.



2. Type in an application name.
3. Enter a description for the new application. This field is not required.
4. Use the **Add Before** drop-down to specify where the application appears in the list. The location of the application in the list does not affect the system. **Add Before** is available for organizational purposes only.
5. Click the **Add Application** button. The new application is added to the list.

6. To configure the application, click the application name. The tabs that support the application display.



Configuring Applications

Applications can be configured via the Administration Console. To do this, click the Configuration tab and click Configuration > SMTP Adaptor > Applications. Application specifics are grouped by function and are presented in a series of tabs. The following is a list of all of the subtabs associated with the various IronPort Encryption appliance applications.

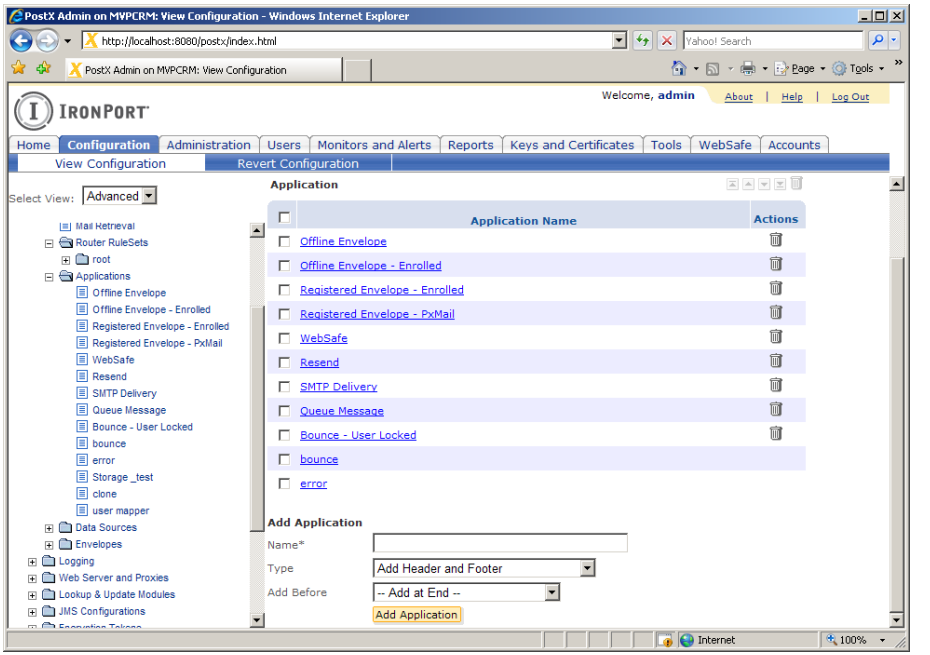
- Certificate Harvesting
- Cryptography
- Delivery
- Details
- Domain Mappings
- Encryption Key Lookup
- Envelope Builder Pool
- EPM
- Mailbox Quota

- Mail Gateway
- Message Personalization
- Message Unpacking
- Metering
- MIME Header Filter
- Registered Envelope
- Secure Response
- S/MIME Decryption
- Spool Queue

Deleting Applications

To delete an application, do the following:

1. Click the Configuration tab and click Configuration > SMTP Adaptor > Applications.

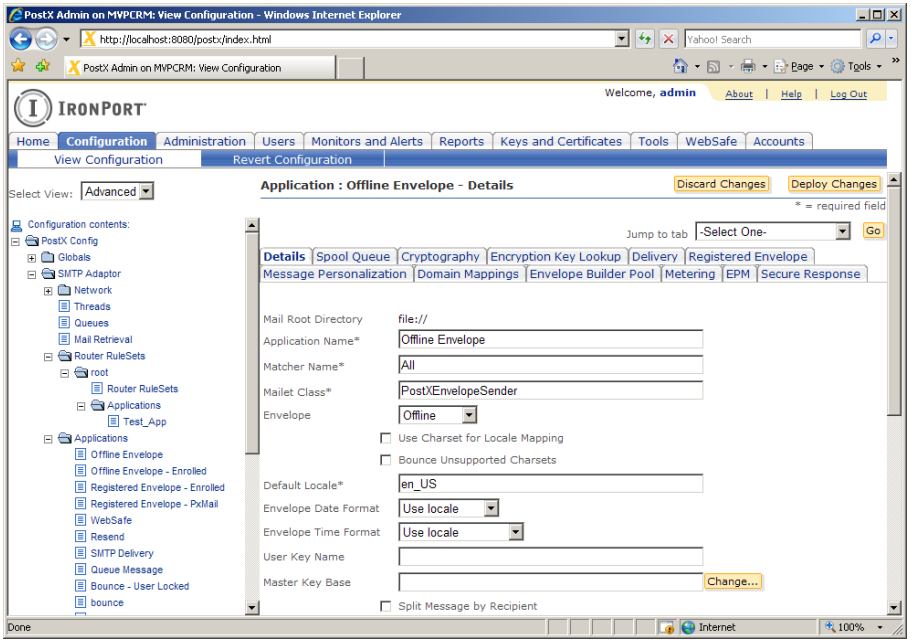


2. Click the trash can icon next to the application you want to delete. A dialog displays asking if you want to permanently delete the selected application. Click the **OK** button to delete the application or the **Cancel** button.

CHAINING

The IronPort Encryption appliance allows you to process mail through multiple applications or rulesets via chaining. To utilize this feature, do the following:

1. On the configuration tree navigate to the first application or ruleset you want to run the mail through. For example, click the Configuration tab and click Configuration > SMTP Adaptor > Applications > Offline Envelope**.**



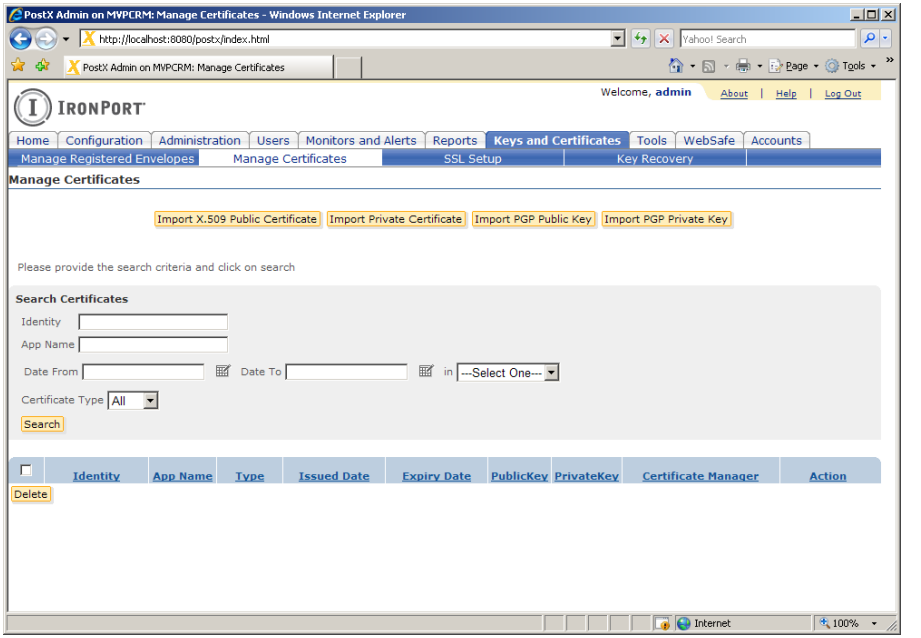
2. Scroll down the page and use the Next drop-down to specify which application or ruleset the mail will pass through once it is processed by the current application/ruleset. Click the **Deploy Changes** button to commit your changes.

Note — The last application/ruleset in the chain will have a value of "None" for the Next parameter.

USING THE PDFSECURE APPLICATION

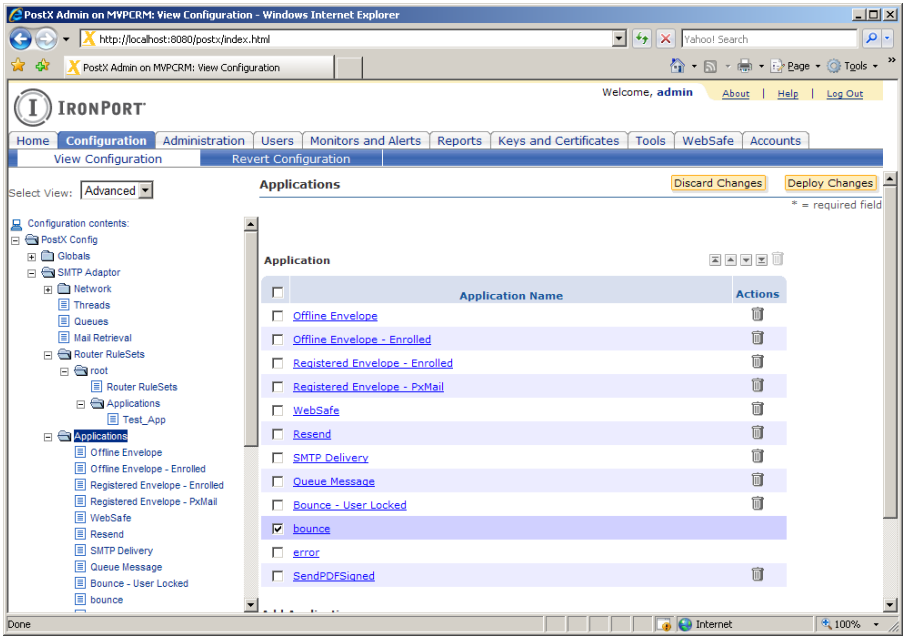
Use this application for signing and/or encrypting all of the PDF attachments present in a message, based on user configuration. The signing is done inline using a PKCS12 certificate and the encryption is done using a password. To configure this application, perform the following steps:

1. Click the Keys and Certificates tab and then the Manage Certificates subtab.



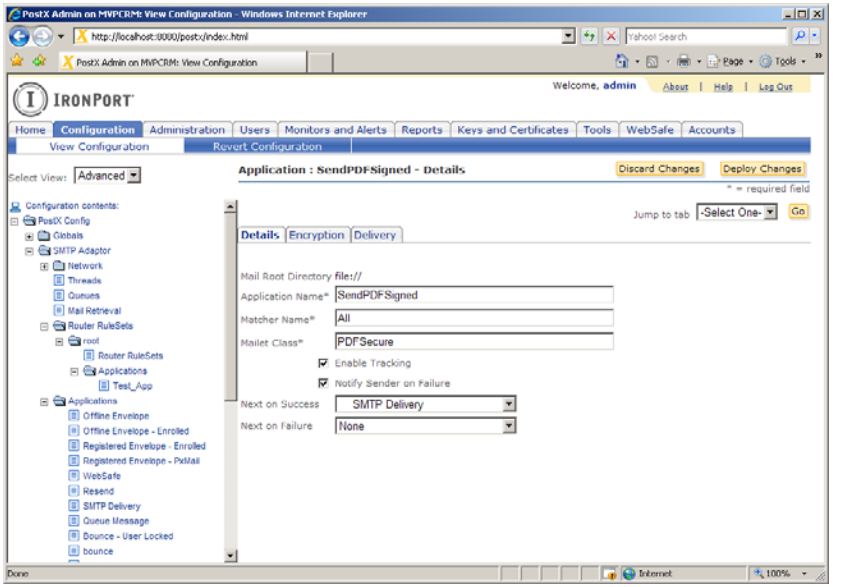
2. Click the **Import Private Certificate** button. Enter the requested information and click the **Import** button. This will install the private PKCS12 certificate for your sender email address.
3. Click the Manage Certificates tab and click the **Search** button. You should see your certificate in the list.
4. Click the Configuration tab. Note that you must be using the Advanced view. Click Configuration > SMTP Adaptor > Applications. In the Add Application section, enter the

name 'SendPDFSigned' and select 'PDF Secure' from the **Type** drop-down. Click the **Add** button.

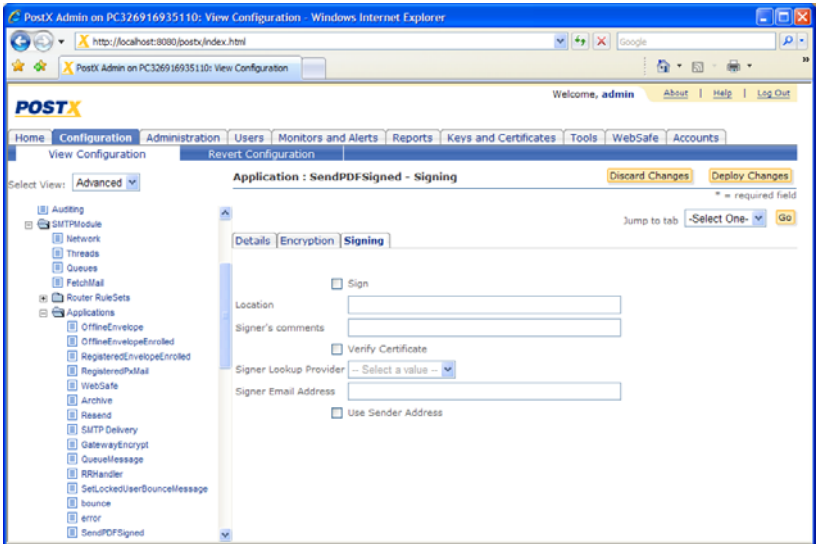


5. Repeat step 4 using the names SendPDFEncrypted and SendPDFBoth. When complete you should see the newly added SendPDFSigned, SendPDFEncrypted and SendPDFBoth applications at the bottom of the list.

6. Click SendPDFSigned in the Applications folder list to display the PDFSecure Application configuration page. Click the Details tab and select 'SMTP Delivery' from the Next Application drop down menu.



7. Click the Delivery subtab for the SendPDFSigned application.

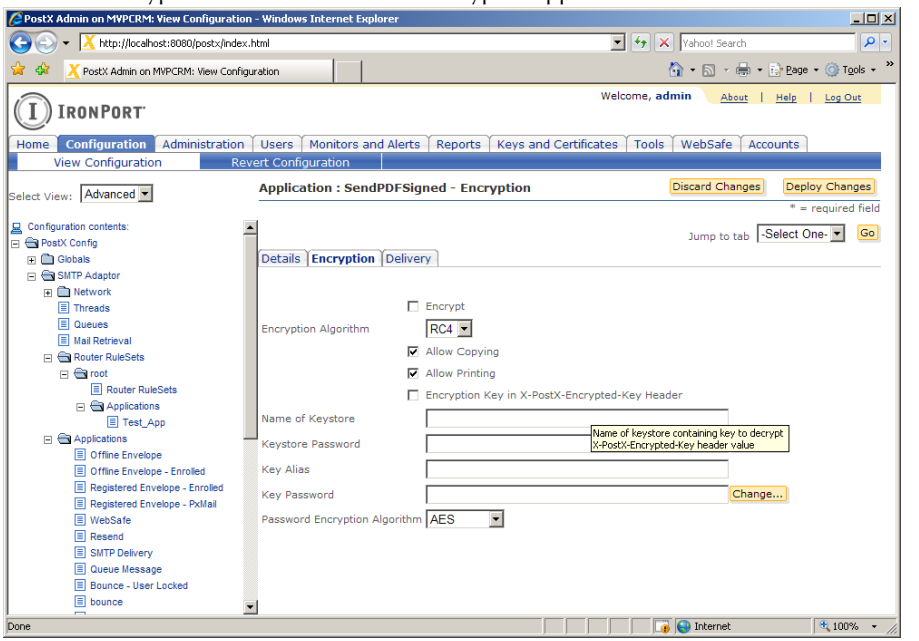


Configure the parameters:

- **Sign:** Check to enable signing.
- **Location**: Geographical name where the signing is being done.
- **Comments**: Comments that may be helpful to the recipient to understand the purpose of signing the document.
- **Verify Certificate**: Check to perform a certificate verification (CRL and Certificate chain verification) check. This parameter specifies that all of the PDF attachments of messages sent using this application would be inline signed using the certificate associated with either the sender's email address or the Signer Email Address specified.
- **Signer Lookup Provider**: Lookup Module to use when looking for the signing certificate.
- **Signer Email Address**: Email address of the person whose digital certificate is used for signing. (Used for PKI).
- **Use Sender Address**: Uses the email sender's address when looking for the signing certificate. If you want to use a common certificate to sign the PDF attachments in all of the messages, uncheck this parameter and specify the email address of the sender in Signer Email Address parameter.

Note — If Use Sender Address is unchecked and Signer Email Address is specified, the signer's private key will be loaded only once when the application is initialized. In the event you change the certificate associated with this identity, the SMTP Adapter needs to be restarted.

8. Click the Encryption tab for the SendPDFEncrypted application.

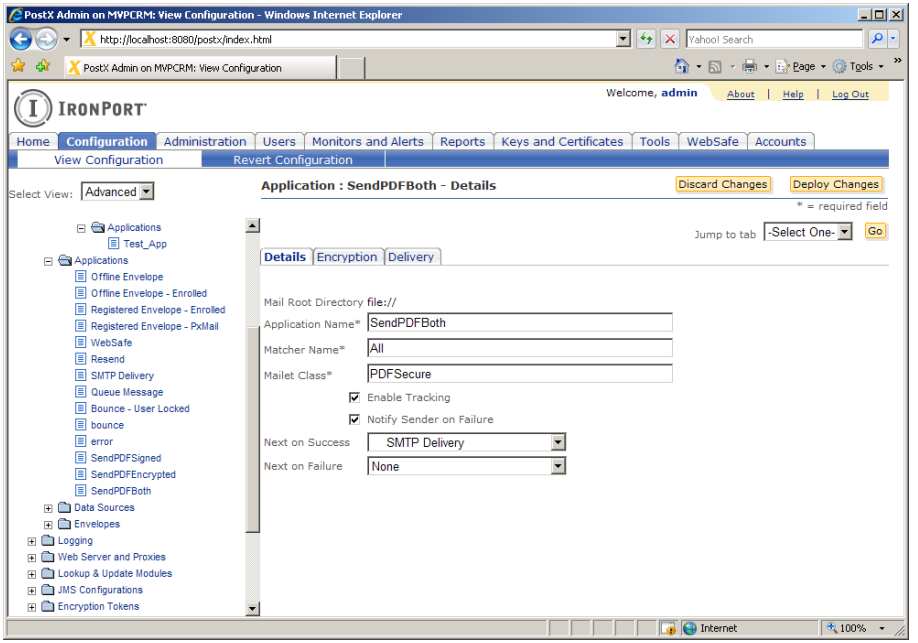


Configure the parameters:

- **Ecrypt:** Select to encrypt the PDF.
- **Encryption Algorithm:**
- **Allow Copying:** Permits the user to copy the content in the decrypted document.
- **Allow Printing**: Permits the user to print the decrypted document.
- **Encryption Key in X-PostX-Encrypted-Key Header**: If checked, PDF encryption key is value of X-PostX-Encrypted-Key header decrypted.
- **Name of Keystore:** Name of keystore containing key to decrypt X-PostX-Encrypted-Key header value.
- **Keystore Password:** Password for keystore.
- **Key Alias:** Alias of key in keystore.
- **Key Password:** Password for key in keystore.
- **Password Encryption Algorithm:** Algorithm used to decrypt X-PostX-Encrypted-Key header value.

  Alternatively, if the message contains an X-PostX-Key header, the value of this header will be used as the encryption password.

9. Click SendPDFBoth in the application's list to display the PDFSecure Application details page.



10. Follow steps 6 through 9 to configure the Details, Sign and Encrypt tabs for this application.

CHAPTER 2

Configuring Message Router Rules

This chapter discusses the concept of message routers and rules and how to configure them. Note that in previous releases of the software message routers were referred to as matchers and possessed slightly different functionality.

This chapter contains the following sections:

OVERVIEW

Email message routing is controlled by configuring and editing rulesets using the Administration Console for the IronPort Encryption appliance. Each ruleset consists of one or more rules. Each rule exercises tests against the message and then executes some action depending upon the results of that test. A rule can consist of multiple tests, AKA matchers or filters, combined using simple ALL OF/ANY OF operators. A matcher looks at a message without changing it, whereas a filter can look at a message and change it. For example, the Subject Filter matches the subject and can be configured to remove or replace portions of the subject.

The action carried out for a rule can be an application, another ruleset or discard message. In addition, a rule allows error handlers to be defined for messages that cause exceptions during the execution of the rule. rulesets can also have other rulesets as components, i.e., a ruleset within a ruleset.

The starting point for all messages is the ruleset called 'root'. Note that this corresponds to the 'Matchers' node in the previous versions of the product. New rules can be defined by the end user using whatever name he chooses, for example 'Outbound email'. In the Administration Console, rulesets appear in the configuration navigation tree under the Router RuleSets node (Configuration > SMTP Adaptor > Router RuleSets).

TESTS

A test is a matcher and an 'IF' or 'IF NOT' operator. The following tests are shipped with the system:

- Anti-Virus Command Line Matcher
- Basic Matcher
- BounceHandler Matcher
- ClamAV Anti-Virus Matcher
- Content Filter
- Custom Matcher or Filter
- Gateway Encrypt Matcher
- Is PGP Matcher
- Is S/MIME Matcher
- Is TLS Enabled Matcher
- Lookup Filter
- MIME Header Filter
- Registered Envelope Matcher
- Py Matcher or Filter
- Resend Matcher
- Subject Filter
- User Status Matcher

MATCHERS

The following sections contain information about specific matchers.

Anti-Virus Matchers

The IronPort Encryption appliance provides two anti-virus matcher types:

- Anti-Virus Command Line Matcher
- ClamAV Anti-Virus Matcher

Select the matcher type that corresponds to the anti-virus software you are planning to use with the system.

Basic Matcher

The Basic Matcher includes the following matcher types. Note: When RegEx is used, it must match the entire expression to be a valid match.

Matcher Type	Matcher Condition	Action Performed
All	None	Matches all recipients.
AttachmentFileNameIs	A comma or space delimited list of file names. File names may start with a wildcard '*'. Example: *.scr,*.bat,*.pif,*.pi,*.com,*.exe	Matches all recipients if the message has an attachment whose name matches that supplied in the Matcher Context.
CompareNumericHeaderValue	The headerName, a comparison operator and the numeric headerValue to compare with, space or tab delimited. The comparison operators are: <, <=, ==, >=, > Or: LT, LE, EQ, GE, GT. Example: "X-IsSpamProbability > 0.9"	Matches mails containing a header with a numeric value whose comparison with the specified value is true. If the header is missing in the message, there will be no match.
HasAttachment	None	Matches all recipients if the message has an attachment (if content type is multipart/mixed).
HasAttachmentName	Multiple names are separated by a comma.	Matches all recipients if the message has the specified attachment name.

Matcher Type	Matcher Condition	Action Performed
HasAttachmentType	Multiple types are separated by a comma.	Matches all recipients if the message has the specified attachment MIME type.
HasHabeasWarrantMark	None	Matches mails that have the Habeas Warrant (see http://www.habeas.com for details). All recipients are returned.
HasHeader	Name of header to match. For example, X-PostX-Secure	Matches all recipients if the message has the specified header.
HasMailAttribute	The attribute name.	This Matcher determines if the mail contains the attribute specified in the condition, and returns all recipients if it is the case.
HasMailAttributeWithValue	Value to compare against.	This Matcher determines if the mail contains the attribute specified in the condition and if the value is equal to the value specified in the condition.
HasMailAttributeWithValueRegex	Regular Expression	This Matcher determines if the mail contains the attribute specified in the condition and that the attribute matches the supplied regular expression, it returns all recipients if that is the case.
HeaderEquals	Multiple header/value pairs are separated by a comma.	Matches all recipients if the message has the specified header and value.
HeaderWithValueRegEx	Header = Perl5RegEx For example: Subject=** Secure.* Matches all emails with a subject that starts with "** Secure".	Matches all emails where the header matches the regular expression.
HostIs	Multiple hosts are separated by a comma.	Matches all recipients belonging to one of the specified hosts.

Matcher Type	Matcher Condition	Action Performed
HostIsFromFile	File name, where the file is expected to be a line-separated list of hosts.	Matches all recipients belonging to one of the specified hosts. The server will check for file modifications at runtime.
HostIsLocal	None	Check recipients's hosts against the list of host names set in configuration for mail server component.
InSpammerBlacklist	One of three strings - "blackholes.mail-abuse.org", "relays.mail-abuse.org", or "dialups.mail-abuse.org".	Checks the mail against one of a number of mail-abuse.org IP lists
IsDispositionNotification	None	Matches those messages whose content type indicates that they are disposition notification messages.
IsSingleRecipient	None	Matches those messages sent to only a single recipient. The single recipient is returned.
NESSpamCheck	None	A matcher derived from a Netscape Mail Server spam filter. If the matcher detects headers that indicate spam, the message is matched. All recipients are returned.
RecipientContains	Condition String	Matches the mails containing a specified string in the recipient email address.
RecipientIs	Multiple recipients are separated by a comma.	Match all recipients defined in condition.
RecipientIsLocal	Multiple recipients are separated by a comma.	Match all local recipients defined in condition.
RecipientIsRegex	Regular Expression	Matches recipients whose address matches a regular expression.

Matcher Type	Matcher Condition	Action Performed
RelayLimit	A positive integer that is the limit on the number of relays	Counts the number of Received headers in the mail (each of which represents a server in the relay chain). If the number equals or exceeds the specified limit, the mail is matched. All recipients are returned.
RemoteAddrInNetwork	Comma separated list of network addresses	Match all recipients if the message was received from an IP address that matches the comma separated list. Wildcards are supported. For example, 192.168.0.* is a valid option. Wildcard IP subnet of any class is supported.
RemoteAddrNotInNetwork	Comma separated list of network addresses	Match all recipients if the message was not received from an IP address that matches the comma separated list. Wildcards are supported. For example, 192.168.0.* is a valid option. Wildcard IP subnet of any class is supported.
SenderHostIs	List of domain names, comma separated	Checks the sender's domain name against the supplied list.
SenderHostIsFromFile	File name, where the file is expected to be a line-separated list of hosts.	Checks the sender's domain name against the supplied list. The server will check for file modifications at runtime.
SenderInFakeDomain	None	Matches messages where the host name in the address of the sender cannot be resolved. All recipients are returned
SenderIs	Comma separated list of addresses	Matches all recipients if sender is in the condition string, if not it matches none.
SenderIsRegex	Regular Expression	Matches mails that are sent by a sender whose address matches a regular expression.

Matcher Type	Matcher Condition	Action Performed
SizeGreaterThan	A positive integer followed by an 'm' or a 'k'. This is the maximum message size permitted specified in megabytes or kilobytes respectively.	Matches emails with a total message size (headers and body) greater than the specified limit. All recipients are returned
SMTPAuthSuccessful	None	Matches mails that are sent by an SMTP authenticated user.
SMTPAuthUserIs	A comma, tab or space separated list of users	Matches mails that are sent by an SMTP authenticated user present in a supplied list. If the sender was not authenticated, it will not match.
UserIs	A list of user names, comma or space delimited.	Matches mails that are sent to email addresses that have userids that are in the configuration list. Only matching recipients are returned

BounceHandler Matcher

This matcher detects messages that have bounced by checking the X-fetched-from header. It uses the HasHeader matcher to perform the check. All recipients are returned when the message matches.

- **Matcher Name** – This is preset to HasHeader and should not generally be changed.
- **Matcher Condition** – This is preset to X-fetched-from and should not generally be changed.

Content Filter Matcher

The Content Filter matcher allows you to make decisions based on the content of the email. You can configure a content filter to look for specific words or patterns in messages and make routing decisions based on them. For example, you can set up applications to secure only email that contains health care words or the pattern of a social security number. Another example could be using this to not allow emails that contain unprofessional language to go out. Each instance of a word or pattern increases the score for a particular message. You can also set different weights for different words and patterns. When the score exceeds or meets the maximum score the message is considered a match. Content Filter information is logged in the mail server log. For information on using and configuring the content filter, please see the *IronPort Encryption appliance Content Filter Manual*.

Custom Matcher or Filter

This matcher allows you to write a custom matcher. It is recommended that you have in-depth knowledge of the system before using this feature.

Gateway Encrypt Matcher

This matcher detects messages that were sent using Gateway Encrypt.

- **Matcher Name** – This is preset to HasAttachmentName and should generally not be changed.
- **Matcher Condition** – This is preset to px.secure.recips.txt and should generally not be changed.

Is PGP Matcher

This matcher detects messages that have been signed or encrypted using PGP. For a detailed discussion of this matcher, please see the *OpenPGP* chapter.

Is S/MIME Matcher

This matcher detects messages that have been signed or encrypted using S/MIME. For a detailed discussion of this matcher, please see the *S/MIME* chapter.

Is TLS Enabled Matcher

This matcher detects which recipients' servers support TLS and return those recipients.

Lookup Matcher

The lookup matcher can be used to match recipients based on properties obtained by using a lookup module. For more information on lookup modules, please see the *Configuring Lookup & Update Modules* .

- **Property Match** – The property to match, specified as <name>=<value>
- **Case Sensitive** – Whether or not the property match should be case sensitive.
- **Match If Property Not Found** – Whether or not to consider the recipient a match if the property is not found in addition to if the property matches.
- **Key Lookup is Domain** – Whether or not the key lookup should be done by domain.
- **Key Lookup Domain Prefix** – The prefix used when doing the domain lookup.
- **Lookup Provider** – The lookup module to use.
- **Lookup Identity** – The identity to lookup. This is preset to Message.Recipient (the address of the recipient) and does not typically need to be changed.

Registered Envelope Matcher

This matcher detects messages that have a Secure Envelope attachment. The envelope attachment can be detected if the envelope is simply an attachment of the message or if it is

an attachment of a message that is itself an attachment of the current message (such as when forwarding a message as an attachment). The configuration parameters can be used to restrict the search for envelope attachments but are not necessary. All recipients are returned when a match is found.

- **Attachment Name** – If specified, only attachments that match this name will be inspected. Wildcards are supported (For example, *.html).
- **Sender Domain** – If specified, only messages that were sent by a sender from the specified domain will be inspected.

Py Matcher or Filter

Py Matchers are another style of matcher available within the IronPort Encryption appliance standard library. A Py Matcher is a more robust and powerful matcher than a standard basic matcher. It gives you the ability to validate or manipulate messages passing through the IronPort Encryption appliance matchers. Py Matchers provide a way to write Jython code to provide this functionality. Py Matchers have full access to the Java libraries including MIME Messaging which is where a majority of your calls will be done. Py Matcher should be used only when the standard IronPort Encryption appliance matchers do not provide the functionality that is required by the request. As with all matchers, the Py Matchers return a Boolean.

Even though the matcher is called a Py Matcher; the code within the matcher is actually Jython. The reason for the name is that the code structure is still considered Python. Once you have learned the basic syntax of Python building Py Matchers to do extraordinary things will be easier.

What are Python and Jython?

Python is a very powerful high level language. Python is very similar to other high level programming languages such as C, C++ and Java. It has built in modules, it is object oriented and other functionality which makes it a great language to learn and know. Users should at least be familiar with Python before attempting to write a Py Matcher. Since Python is an interpreted language, it can be easily tested and deployed. Below is a very simple reference guide to Python within IronPort Encryption appliance, for more information on Python in general go to Dive into Python by Mark Pilgrim (`http://diveintopython.org`).

Jython is a complete re-implementation of the Python language written in Java. Jython gives you the ability to write Python code with full access to Java's extensive library. All of the syntax and style is the same as Python with the ability to utilize Java for functions. Jython provides the ability to prototype Java code and test it without having to compile and re-compile to debug. Jython, like Python, runs through an interpreter. This allows you to script code and test it almost immediately.

Jython Syntax and Tutorial

Jython syntax is the same as Python syntax in that it just instantiates the Java code in a different way. Here is the basic Jython syntax to get you started on building and deploying Py Matchers with the IronPort Encryption appliance.

The Structure

When you first deploy a Py Matcher on the IronPort Encryption appliance, you are presented a blank matcher template:

```
def match(mail):
return mail.getRecipients()
```

This is the basic structure for a Py Matcher. With these basic components you can start to create your own high powered Py Matchers. The first statement: def match(mail): is the beginning of the Py Matcher where the Mail Class (org.apache.mailet) is being instantiated. You now have access to all of the functionality available within the Mail Class. There is a list of all methods available in the section below or you can access the call information via the web at: James Java Docs (`http://james.apache.org/javadocs/index.html`). The last part, return mail.getRecipients(), is the end of the matcher where the Boolean is returned after the Py Matcher code has been written. In between these components is where the Py Matcher code lies.

Subject Contains

This is a useful Py Matcher that looks through the subject and determines if the value is contained anywhere within the subject. Sample:

```
def match(mail):
    search_string = '[:secure email:]'

    mime_message = mail.getMessage()
    subject = mime_message.getSubject()
print 'Current subject:', subject
    found_start = subject.lower().find(search_string)
    if found_start >= 0:
        found_end = found_start + len(search_string)
        print 'Found:', subject[found_start:found_end]
        subject = subject[:found_start] + subject[found_end:]
        print 'New subject:', subject
        mime_message.setSubject(subject)
        mime_message.setHeader('X-PostX-QPSC', 'T')
        mime_message.saveChanges()
        return mail.getRecipients()
    if mime_message.getHeader('X-PostX-QPSC'):
     return mail.getRecipients()
```

Resend Matcher

This matcher detects messages that have been resent from the archive. It is simply defined as a convenience and uses the HasHeader matcher to perform the check. All recipients are returned when the message matches.

- **Matcher Name** – This is preset to HasHeader and should not generally be changed.

- **Matcher Condition** – This is preset to X-PostX-Resend and should not generally be changed.

Subject Matcher

The Subject Matcher allows you to make decisions based on the subject of the email. You can configure the Subject matcher to match based upon the message subject, subject contains, subject starts with or subject ends with. The following configuration parameters are used to configure this matcher:

- **Match** - Specifies whether you want to match At Beginning of Subject, At End of Subject, Anywhere in Subject, and Entire Subject.
- **Search String**- The pattern you want to search against.
- **Case Sensitive** - Determines whether you are matching in a case sensitive manner.
- **Search String is Regular Expression** - Specifies whether the match pattern should be interpreted as a literal string or as a regular expression when comparing against the subject.
- **On Match** - Specifies whether you want to replace the matched part of the subject (with the replacement text), remove the matched part, or do nothing. Values are None, Remove Match, and Replace Match.
- **Replacement String** - If you choose Replace Match as your On Match action, the matched portion of the subject will be replaced with this string. If you choose Search String is Regular Expression the replacement string will also be treated as a regular expression.
- **Replaces All Matches** - If you choose this, all instances of the matched pattern will be replaced with the contents of Replacement String.

MIME Header Filter

The MIME Header Filter matcher removes any MIME headers, such as X-PostX-, from incoming email messages. The following configuration parameters are used to configure this matcher:

- **Allowed Network Addresses** - A comma separated list of network addresses specified in the same format as any other 'Net' matcher. Messages coming from clients in this list will NOT have the IronPort Encryption appliance headers removed from the email message.
- **Headers to Remove** - A comma separated list of regular expressions for the MIME header names that are to be removed. For example, X\-PostX\-.*
- **Headers to Keep** - A comma separated list of regular expressions for the MIME header names that are NOT removed, For example, X\-PostX\-Secure.*,X\-PostX\-Key,X\-PostX\-SHAedKey
- **Return Network Match Result** - Specifies whether the result from the 'allowed network address' test should be returned as the matcher results. This allows the matcher to be used as an network matcher as well as a MIME header filter. Generally this should be

deselected (false) so that the matcher acts as a filter and all messages are passed through it.

User Status Matcher

Checks the recipient of the message to determine if the user is in the `postx` database. If the user exists, then it will attempt to match the user status with the one configured in the matcher. The following configuration parameters are used to configure this matcher:

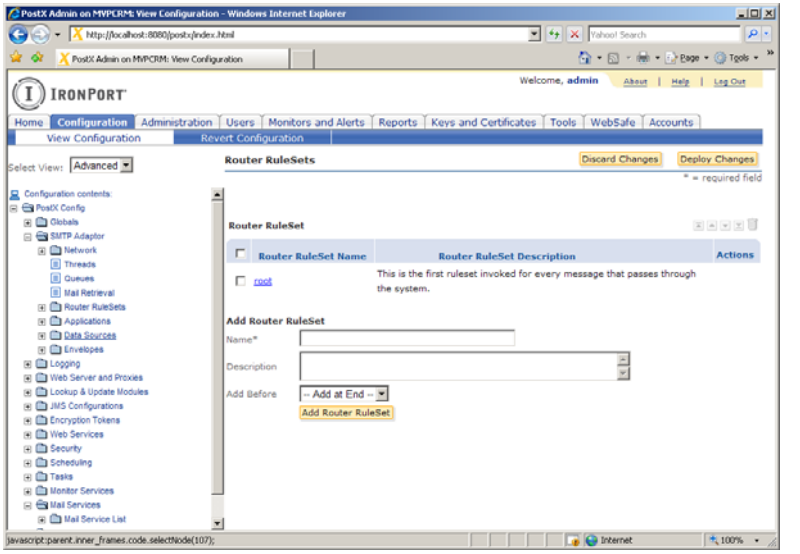
- **Matcher Name** – User specified matcher name.
- **User Status** – The user status to match against (New, Activated, Deleted, Blocked, Suspended, Pre-Enrolled, and Locked).

MANAGING RULESETS

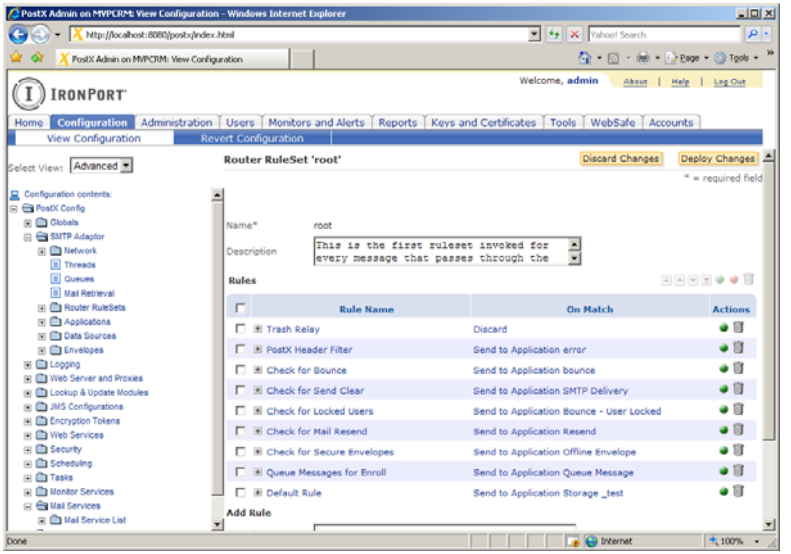
Viewing and Editing RuleSets

To view the rulesets currently available on your system, do the following:

1. Click the Configuration tab and navigate to Configuration > SMTP Adaptor > Router RuleSets. You can either select the rulesets you want to view from the tree or from the list that appears in the right pane.



2. To view the rules associated with a ruleset, click the ruleset name. For this example, click the 'root' ruleset.



A description of the ruleset is displayed, and the rules that comprise the ruleset are listed in a tabular format. For example, the following rules comprise the 'root' ruleset:

- Trash Relay
- Header Filter
- Check for Bounce
- Check for Send Clear
- Check for Locked Users
- Check for Mail Resend
- Check for Secure Envelopes
- Queue Messages for Enroll
- Default Rule

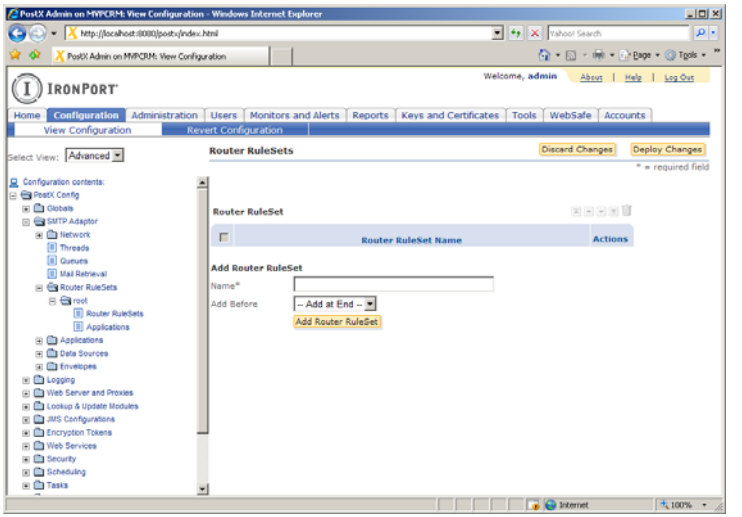
3. The following icons are used to help you manage rules and rulesets. Hover text allows you to see what each icon represents

Icon	Action
	Indicates that a rule or ruleset is disabled.
	Indicates that a rule or ruleset is enabled.
	Deletes a rule or ruleset.

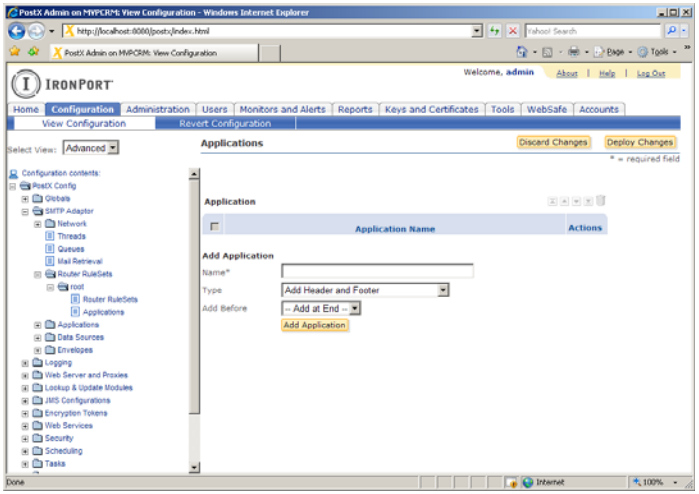
4. To disable a rule or ruleset, click the round green button in the Action column. The button will turn red. To enable it again, simply click the red button.
5. To delete a rule or ruleset, click the trash can icon in the Action column.

Note — Note that the 'root' ruleset does not have an of these icons in its Action column. This is because this is the default ruleset and cannot be deleted.

6. To see rulesets associated with a ruleset, navigate to Configuration > SMTP Adaptor > Router RuleSets > *Router RuleSet - This example uses 'root'* > Router RuleSets.



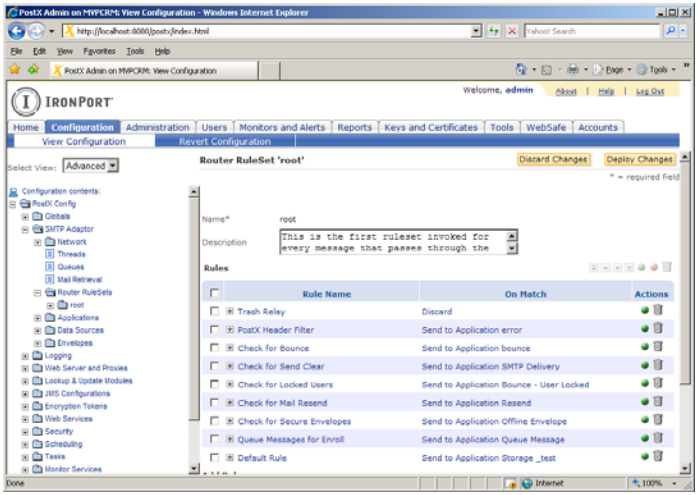
7. To see applications associated with the ruleset, navigate to Configuration > SMTP Adaptor > Router RuleSets > *Router RuleSet - This example uses 'root'* > Applications.



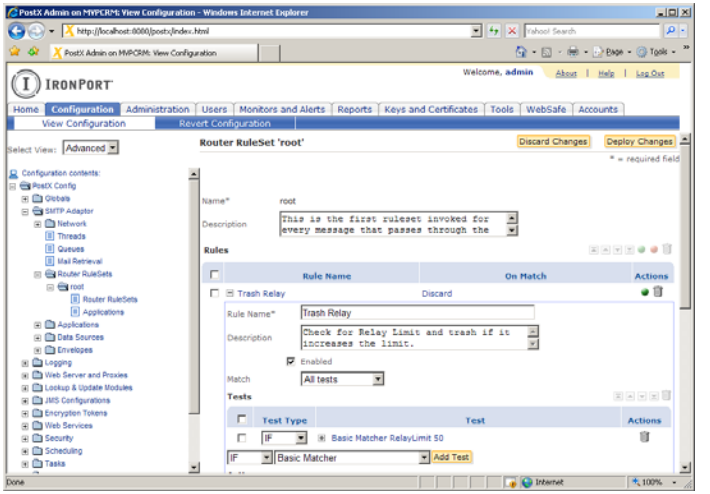
Viewing and Editing Rule Details

To view and edit rule details, do the following:

1. Click the Configuration tab and navigate to the location of the ruleset that contains the rules you want to view. For example > Configuration > SMTP Adaptor > Router RuleSets > root.



2. Click the '**+**' symbol next to the rule to expand the list of view the attributes associated with the rule.



The parameters associated with the rules display:

- **Rule Name -** The rule name.
- **Description -** A description of the rule.
- **Enabled** - Check this box to enable the rule.
- **Match -** Specifies how many tests to match. Values are All tests, Any test, Exactly one test.

The Tests section determines the tests that are associated with the rule. Tests are matchers and an 'IF' or 'IF NOT' operator.

- **Test -** The name of the test that the system will run on each message.
- **Test Type -** An operator that determines the action that the system will take. Valid test types are IF and IF NOT.

You can add a test by using the drop-downs to select the test name and test type, then clicking the **Add Test** button.

To reorder tests, click the check box next to the test name.The arrows at the top right of the screen will become active.

The order that tests appear is typically for organizational purposes only.

The **Actions** section determines what the system does when a message meets the test qualifications.

- **On Match -** Select the action you want the system to take. Valid values are:
    - **Send to Router RuleSet -** Send the message to a router ruleset. Select the ruleset you want to send the message to from the drop-down.
    - **Send to Application -** Send the message to an application. Select the application you want to send the message to from the drop-down.
    - **Store in Repository -** Store the message in the repository. Enter the repository where you want the message to be stored in the available field. You do not need to enter the full path since it will default to <install_dir>/apps/james/var/mail/. The new repository will appear on the Home page in the Spool Repositories box.
    - **Discard -** The message is discarded.
- **On Error -** Select the action you want the system to take. Valid values are:
    - **Send to Router RuleSet -** Send the message to a router ruleset. Select the router ruleset you want to send the message to from the drop-down.
    - **Send to Application -** Send the message to an application. Select the application you want to send the message to from the drop-down.
    - **Match All -** All recipients will be acted upon accordingly to On Match.
    - **Match None -** None of the recipients will be matched even if the error only applied to some.
    - **Discard -** The message is discarded.

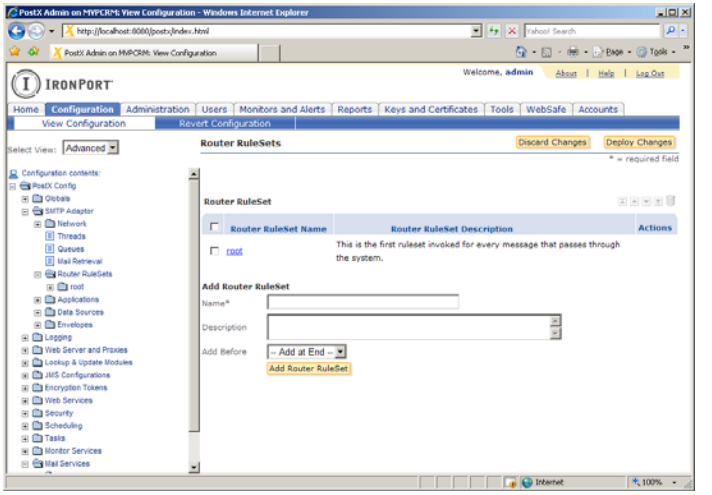
Adding Router RuleSets

RouterRuleSets allow you to organize system actions. There are two ways to add a router ruleset, at the top level of the tree or as a component of another ruleset. Note that there is no limit to the number of rulesets or hierarchy. For example, you can have a ruleset within a ruleset within a ruleset, etc.

Adding a Top-Level RuleSet

To add a router ruleset, do the following:

1. Click the Configuration tab and navigate to Configuration > SMTP Adaptor > Router RuleSets.



   The Add RouterRuleSet section appears at the bottom of the screen.

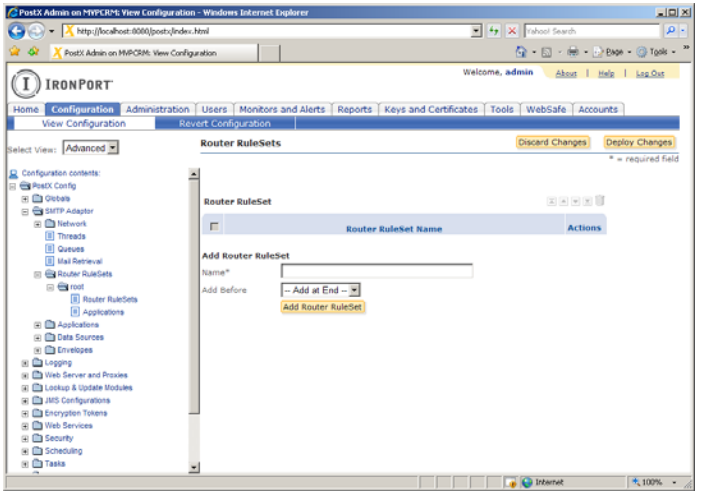
2. Type in a ruleset Name.
3. Enter a Description for the new ruleset. This field is not required.
4. Use the Add Before drop-down to specify where the ruleset appears in the list. The order that ruleset appear impacts the behavior of the system. For example, if a new ruleset is placed at the end of the list, the message may not utilize that ruleset as intended if an ruleset higher up on the list sends the message.
5. Click the **Add Router RuleSet** button.

   Each router ruleset has rules, rulesets and applications associated with it. To configure the new ruleset, see the following sections.

Adding a RuleSet within a Ruleset

To add a router ruleset as a component of a ruleset, do the following:

1. Click the Configuration tab and navigate to Configuration > SMTP Adaptor > Router RuleSets > *Router RuleSet - This example uses 'root'* > Router RuleSets.



   The Add RouterRuleSet section appears at the bottom of the screen.

2. Type in a ruleset Name.
3. Use the Add Before drop-down to specify where the ruleset appears in the list. The order that ruleset appear impacts the behavior of the system. For example, if a new ruleset is placed at the end of the list, the message may not utilize that ruleset as intended if an ruleset higher up on the list sends the message.
4. Click the **Add Router RuleSet** button.

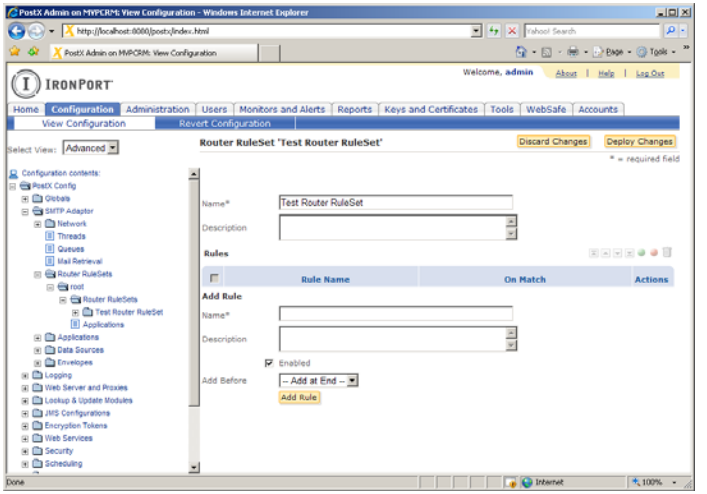
   Each router ruleset has rules, rulesets and applications associated with it. To configure the new ruleset, see the following sections.

Adding and Editing Rules

To add rules to a ruleset, do the following:

1. Click the Configuration tab and navigate to Configuration > SMTP Adaptor > Router RuleSets > *Router RuleSet - This example uses 'root'* or Configuration > SMTP Adaptor >

Router RuleSets > *RuleSet_Name* > Router RuleSets > *RuleSet_Name* depending upon the level of the ruleset.

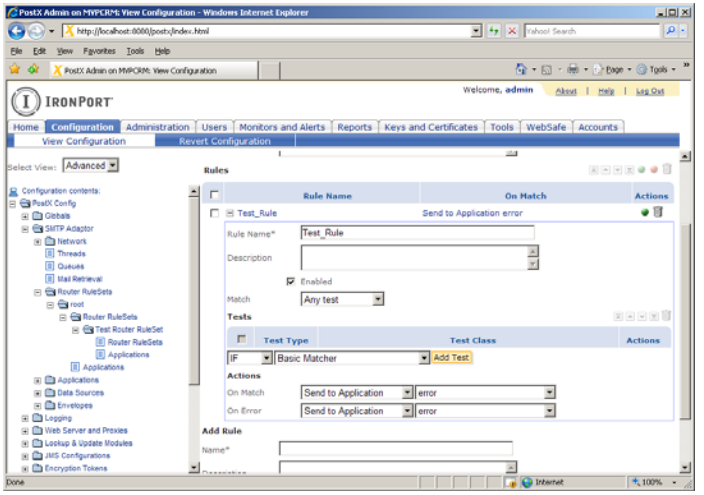


The Add Rule section appears at the bottom of the screen.

2. Type in a ruleset Name (For example, Test1).
3. Enter a Description for the new ruleset. This field is not required.
4. Make sure that the **Enabled** button is checked if you want to use this rule.
5. Use the Add Before drop-down to specify where the rule appears in the list. The order that rule appear impacts the behavior of the system. For example, if a new rule is placed at the end of the list, the message may not utilize that rule as intended if an rule higher up on the list sends the message.
6. Click the **Add Rule** button. The new rule will appear in the list.
7. Click on the rule you just added to select it. Using the arrows at the top right of the screen to change where the rule resides on the list.

New rulesets must appear after the root ruleset in the list.

8. Click the '**+**' symbol next to the rule you just added to expand the list of view the attributes associated with the rule.



9. In the Test section, select an option (for example, Basic Matcher) from the Test Class drop-down and click the **Add Test** button.

   The Actions section determines what the system does when a message meets the test qualifications.

   On Match - Select the action you want the system to take. Valid values are:

   - **Send to Router RuleSet -** Send the message to a router ruleset. Select the ruleset you want to send the message to from the drop-down.
   - **Send to Application -** Send the message to an application. Select the application you want to send the message to from the drop-down.
   - **Store in Repository -** Store the message in the repository. Enter the repository where you want the message to be stored in the available field. You do not need to enter the full path because it defaults to <home>/apps/james/var/mail/. The new repository will appear on the Home page in the Spool Repositories box.
   - **Discard -** The message is discarded.

   On Error - Select the action you want the system to take. Valid values are:

   - **Send to Router RuleSet-** Send the message to a router ruleset. Select the router ruleset you want to send the message to from the drop-down.
   - **Send to Application** - Send the message to an application. Select the application you want to send the message to from the drop-down.
   - **Match *All*** - *All* recipients will be acted upon accordingly to On Match.

- **Match None -** None of the recipients will be matched even if the error only applied to some.
- **Discard -** The message is discarded.

10. Click the '**+**' symbol next to the test class (for example, Basic Matcher) you just added to enter the attributes associated with the test class.
    - **Matcher Name -** Select the matcher name.
    - **Matcher Condition -** Enter the message condition.

CHAPTER 3

Configuring Authentication

This chapter contains the following sections:

WHY WOULD I CHANGE AUTHENTICATION DEFAULTS?

The IronPort Encryption appliance is configured with the most common authentication choices, however you may want to fine-tune the authentication mechanism to local needs. Specifically, to configure different authentication policies for different interfaces. For example, you can allow the use of persistent cookies for all logins except the Administration Console. Similarly, it is possible to perform a lookup in a corporate LDAP directory for WebSafe and to have a different policy for registered envelopes. However, the most common approach is to configure one set of policies for the Administration Console and a different set that applies to all other interfaces.

Note — You may not need to change the authentication defaults if they already meet your specific needs. For example, if you are not authenticating against LDAP or an Active Directory you can accept the default configurations.

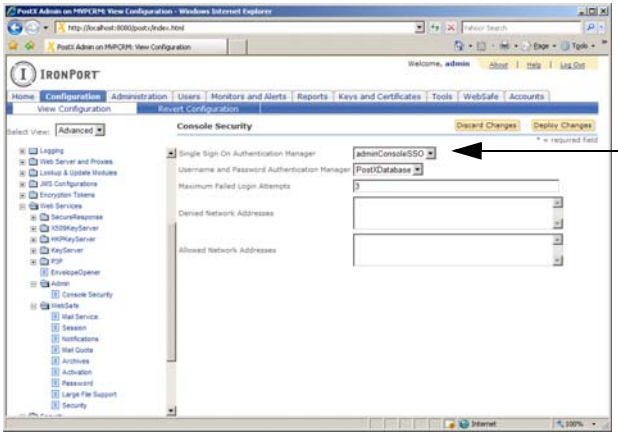
ABOUT USER AUTHENTICATION

The IronPort Encryption appliance has four interfaces where user authentication is required – Secure Mailbox, Registered Envelopes, Registered Envelope Management and the Administration Console. The default configuration follows that approach.

The basic building block is called an Authentication Provider. An example of an Authentication Provider is the `postx` database provider. This provider relies on user IDs and passwords stored in the user database. Other built-in Authentication Provider types rely on X.509 certificates, Kerberos (Active Directory), LDAP lookups, persistent cookies and other database lookups. In addition, it is possible to plug in custom Authentication Providers, such as third party single signon systems.

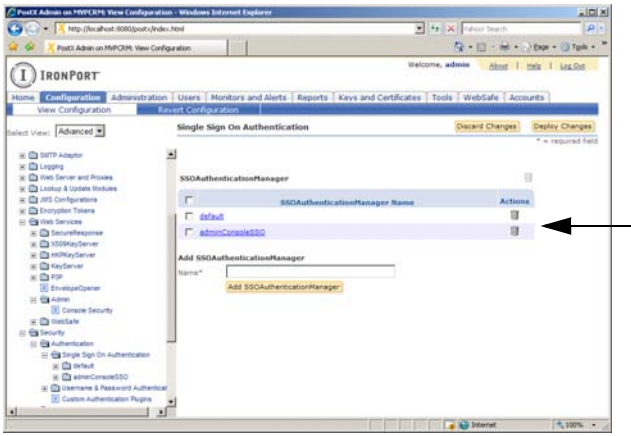
In effect, the IronPort Encryption appliance passes control of the authentication process to the Authentication Provider. That provider either rejects the authentication or approves it. In the case of approval the provider returns data that allows the IronPort Encryption appliance to manage the interface.

Authentication Providers can be chained together under an Authentication Manager. For example, click Web Services > Admin > Console Security.



This parameter is populated in the **Security > Authentication > Single Sign On Authentication** area of the configuration tree.

On that screen, you will see “Single Sign On Authentication Manager” and a pull-down menu. The names on the pull-down menu correspond to the Authentication Managers defined under Security > Authentication > Single Sign On Authentication.



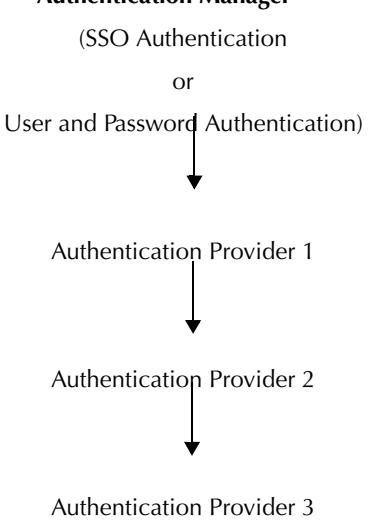
Managers added in this section populate the SSO Authentication Manager field shown on the previous screen example.

Registered Envelopes require additional configuration to support the message sensitivity feature. The basic presumption is that, on the same system, some messages contain low sensitivity information and some contain highly sensitive information. For optimal user acceptance, it is important that the level of authentication effort required be consistent with the user’s perception of the value of the information being protected. This is accomplished through the Trust Level of an authentication provider. In the default system, three levels of sensitivity are supported – low, medium, and high – and three corresponding levels of trust. The trust level to be associated with a particular Authentication Provider is set in the configuration screen for that provider.

AUTHENTICATION MANAGERS

Authentication Providers can be chained together under an Authentication Manager. Broadly the Authentication Managers are grouped as "Single Sign On Authentication" or "Username and Password Authentication" managers. The distinction is that SSO Authentication generally happens without the direct involvement of the application – it just receives a yes or no answer.

Note — For a given Authentication Manager, providers are executed in order. Success with any provider in the chain results in an authenticated user. In the example below, the system will attempt to authenticate the user by moving down the chain of authentication providers. If the user is successfully authenticated by Provider 2 then Provider 3 is not used.



Single Sign On Authentication Managers

Providers included in SSO Authentication Managers include "adminX509provider" and "adminCookieProvider". Custom providers written for third party single sign on authentication generally also are in this category. Each authentication manager of this type can be configured to filter which URLs it will authenticate. This option has very specialized uses and is a place-holder for a future feature. It should not be modified without explicit directions from IronPort Customer Support. Each interface requires that one manager of each

type be supplied. The SSO manager is always tried first, to minimize the number of contacts with the user. The following configuration parameter applies:

Parameter	Definition
URL	URL path for the sevlet request filter.

X509 Certificate Provider

This provider handles client certificate authentication (CCA) where the client certificate is provided by the browser making the request. The following configuration parameters apply:

Parameter	Description
Provider Type	Authentication provider type. Display-only field.
Authentication Provider Name	Authentication provider type. Display-only field.
Enabled	Select to enable the provider.
Trust Level	Sets the security trust level for authentications granted by this provider.
Load User from Database	Populate the user information from the database.
Proxy Support Enabled	Enabled if X509 Client Authentication is used behind a proxy.
Header Attribute Name	Name of the HTTP header where the X509 certificate is located.

Remember Me Cookie Provider

This provider looks for a persistent cookie that can be set at authentication time. Existence of this cookie authenticates the user. Using this provider enables each configured user interface to grant access if that cookie is set. This is a form of single sign-on among different interfaces that require user authentication. For example, if a user logs in to Secure Mailbox and selects the “Remember Me on this computer” option, a persistent cookie is set. That user can now open registered envelopes of the appropriate sensitivity without the need to re-enter his password. Cookies can be disabled for any interface, such as the administration console. It is important to note that sharing the cookie between the different encryption server web applications is optional.

The default cookies expiration is 525600 (365 days). The maximum value is 35791394 (about 68 years, 18 days). Any value larger than that will be set to the maximum. A negative value results in a session cookie (that is, not persistent), so the logged in user will remain authenticated until they close all instances of their browser. A value larger than

9223372036854775807, smaller than -9223372036854775808, or a non-integral value prevents the server from coming up. The following configuration parameters apply:

Parameter	Definition
Provider Type	Authentication provider type. Display-only field.
Authentication Provider Name	Authentication provider name. Display-only field.
Enabled	Select to enable the provider.
Trust Level	Sets the security trust level for authentications granted by this provider.
Cookie Name	The name of the cookie used to remember the user authentication details.
Token Validity	The duration of how long the token is valid for in minutes.
Case Sensitive Username	Determines if the username is case sensitive.

Default Configuration

Two SSO Authentication Managers, “default” and “adminConsoleSSO”, are pre-configured in the initial installation. Both these modules have the “adminX509provider” (disabled) and “adminCookieProvider” (enabled) in the chain of providers. The “default” authentication manager is intended to be used by all IronPort Encryption appliance user interfaces other than the Administration Console. The “adminConsoleSSO” authentication manager is used by the Administration Console, and has a different cookie that is not shared with other user interfaces.

Please review the default configuration prior to making any changes or adding an Authentication Manager.

Username and Password Authentication Managers

Username and Password Authentication managers generally require that the application redirect the users to a web page where they enter data which then is forwarded to the Authentication Provider.

IronPort Encryption Appliance Authentication Provider

The default provider that authenticates users registered through the IronPort Encryption appliance registration system. The following configuration parameters apply:

Parameter	Definition
Provider Type	Authentication provider type. Display-only field.

Parameter	Definition
Authentication Provider Name	Authentication provider name. Display-only field.
Enabled	Select to enable the provider.
Trust Level	Sets the security trust level for authentications granted by this provider.

Kerberos Authentication Provider

Use this authentication provider to authenticate with Microsoft Active Directory and other systems supporting Kerberos. The following configuration parameters apply:

Parameter	Definition
Provider Type	Authentication provider type. Display-only field.
Authentication Provider Name	Authentication provider name. Display-only field.
Enabled	Select to enable the provider.
Kerberos Configuration File	Full path to the Kerberos configuration file.
Add Kerberos Realm	Appends the Kerberos Name to the User ID to create a fully qualified User ID.
Kerberos Realm	Name of the Kerberos Realm.
Authentication DAO	Authentication DAO.
Lookup Name	Lookup name.
Identity Attribute	Attribute that contains the ID of the Kerberos user.
Trust Level	Sets the security trust level for authentications granted by this provider.

Lookup Authentication Provider

Use this authentication provider to create an authentication module that can wrap any lookup module to retrieve the password used for authentication. Lookups are a very important concept in the IronPort Encryption appliance system. For more information, see the Lookup chapter in this manual.

The following configuration parameters apply:

Parameter	Definition
Provider Type	Authentication provider type. Display-only field.
Authentication Provider Name	Authentication provider name. Display-only field.
Lookup Name	Lookup name.
Enabled	Select to enable the provider.
Encryption Type	Encryption type for this specific authentication provider.
Trust Level	Sets the security trust level for authentications granted by this provider.

LDAP Authentication Provider

Use this authentication provider to authenticate with LDAP compliant directories. The authentication provider uses the supplied user information to search the LDAP directory and then attempts to authenticate using an LDAP BIND operation or verify password using an LDAP COMPARE operation. The following configuration parameters apply:

Parameter	Definition
Provider Type	Authentication provider type. Display-only field.
Authentication Provider Name	Authentication provider name. Display-only field.
Enabled	Select to enable the provider.
Trust Level	Sets the security trust level for authentications granted by this provider.
Connect Securely	Select to allow a secure (i.e., SSL) connection to the LDAP server.
Server Name	Host name of the LDAP server.
Port Number	Port number that the LDAP server is listening on.
Logon to Server	Logon to the LDAP server to perform searches.
User Name	User name used to logon the server.
User Password	Password used to logon the server.

Parameter	Definition
RootDN	RootDN for the directory tree.
Subcontext	Subcontext that is appended to the RootDN for queries.
User Authentication Method	Method used for user authentication.
Query String	Query string that is used when searches are disabled.
Enable Subtree Search	Enables searches of the directory substring.
Login Attribute Name	Name of the attribute used to compare login names.
Time Out	The connection timeout in milliseconds.
Password Attribute	Schema name of the password attribute.
Authentication DAO	Authentication DAO.

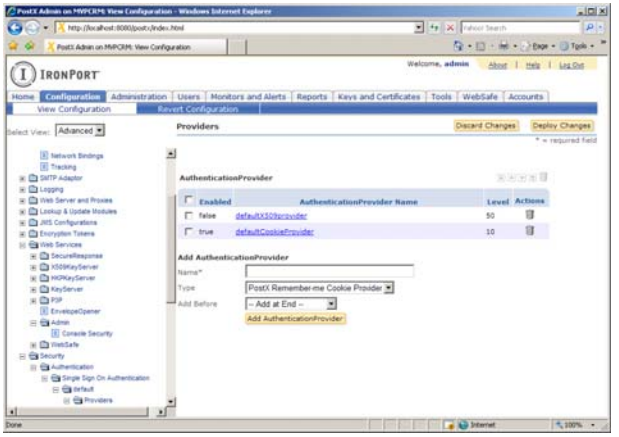
Default Configuration

A single authentication manager called “PostXDatabase” is configured in the default installation. This manager has “IronPort Encryption Database” as the single provider in its chain. All IronPort Encryption appliance user interfaces use “PostXDatabase” as the default username and password authentication manager.

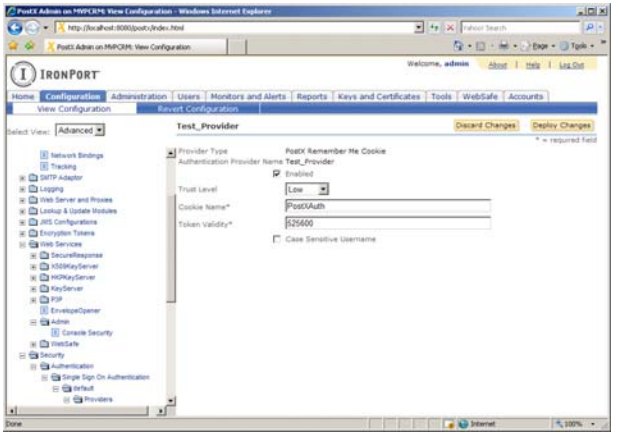
Note — Review the default configuration before making any changes or adding an Authentication Manager.

ADDING AN AUTHENTICATION PROVIDER

1. Click the Configuration tab and then in the left pane click Configuration > Security > Authentication. You can add a provider for any authentication manager. Navigate to the appropriate Providers folder.



2. Enter an authentication name in the Name field.
3. Use the Add Before drop-down menu to specify where the provider appears in the list. The order of providers affects the behavior of the system.
4. Click the **Add Authentication Provider** button.
5. Click Configuration > Security > Authentication, *Providers_Folder* > *New_Auth_Manager_Name* and configure the newly added authentication provider.



The configuration parameters on this tab vary depending on the type of authentication provider you are adding.

6. Click the **Deploy Configuration** button.

DELETING AN AUTHENTICATION PROVIDER

To delete an authentication provider, do the following:

1. Click on the Configuration tab and then click Configuration > Security > Authentication. Navigate to the appropriate Providers folder.
2. Click the trash can icon next to the authentication provider you want to delete. A confirmation dialog box verifies that you want to permanently delete the selected provider. Click the **OK** button to delete the provider, or click **Cancel**.

CHAPTER 4

Monitoring and Alerting

This chapter contains the following topics:

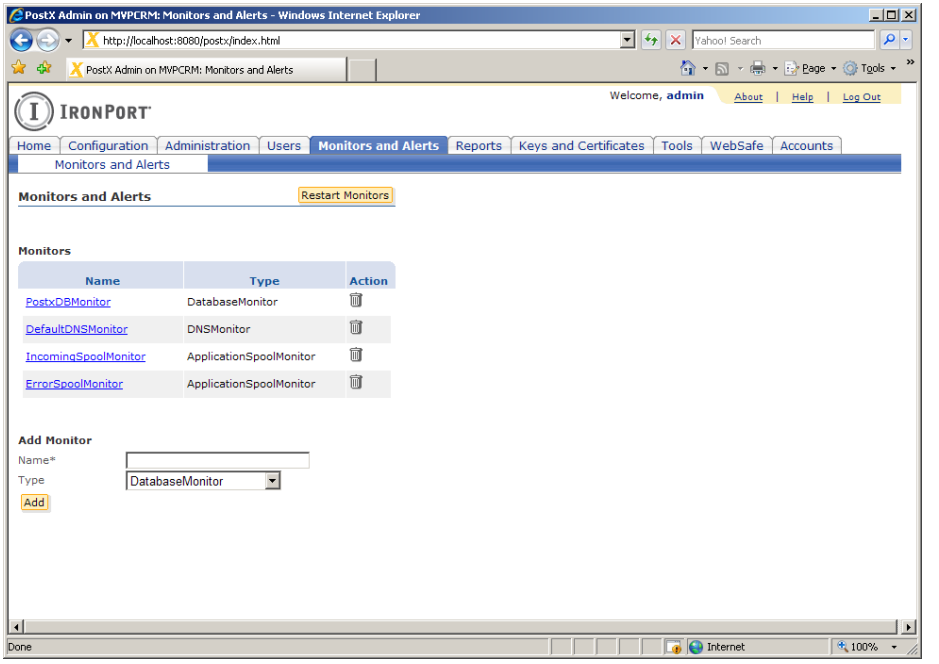
OVERVIEW

The *IronPort Encryption appliance* monitoring and alerting feature is designed to help you monitor your system and alert you in the event of a service interruption or change. These services include:

- Database connection status
- Spool size limits for different applications
- Disk partitions
- DNS connection status
- Gateway connection status

This Monitoring and Alerting mechanism will alert the authorized users by sending an email.

Click the Monitors and Alerts tab to display all monitors. Information includes monitor name and monitor type.



DEFAULT MONITORS

The IronPort Encryption appliance comes with a set of pre-configured default monitors. They are:

- **PostxDBMonitor -** Monitors the IronPort Encryption appliance database. An alert is raised if the database connection is lost.
- **DefaultDNSMonitor -** Monitors the default DNS server configured for the IronPort Encryption appliance. An alert is raised if the connection to the default DNS server is lost.
- **IncomingSpoolMonitor -** Monitors the incoming mail spool. An alert is raised if the incoming spool size exceeds 250 messages.
- **ErrorSpoolMonitor -** Monitors the mail error spool. An alert is raised if the size of the error spool exceeds 100 messages.

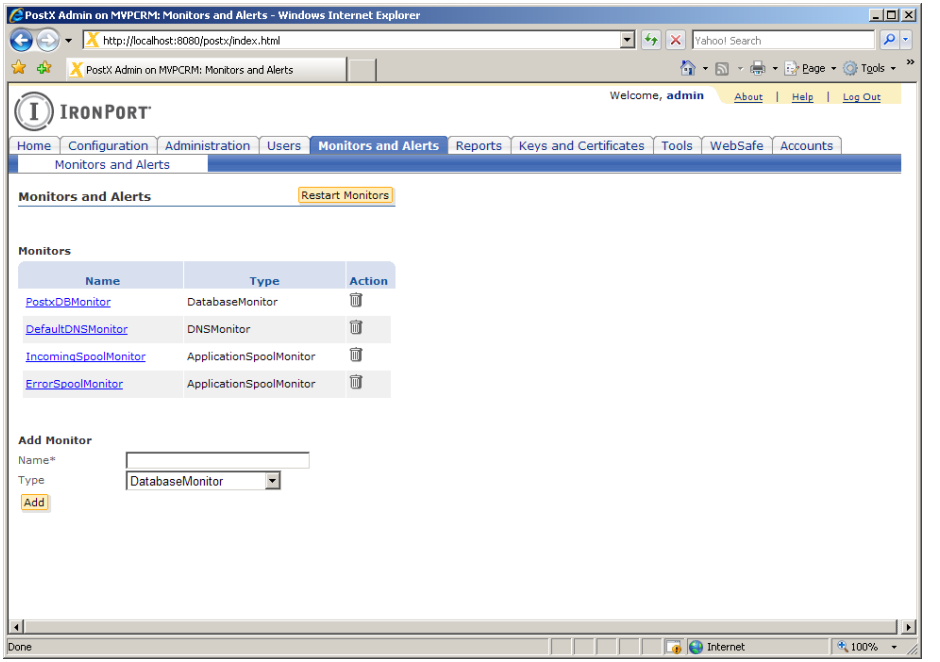
These monitors are configured to run at an interval of one hour and send out an alert to the postmaster via email. All of the above default monitors can also be modified. For more information, see “Configuring and Editing a Monitor” on page 68.

MANAGING MONITORS

Adding a Monitor

To add a monitor, do the following:

1. Click the Monitors and Alerts tab**.**



   The Add Monitor section appears at the bottom of the screen.

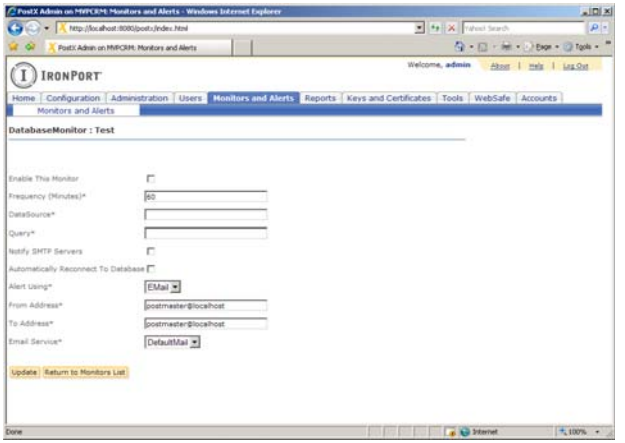
2. Type in a monitor Name.
3. Select a Type from the drop-down. Valid types are: DatabaseMonitor, DNSMonitor, GatewayMonitor, DiskMonitor, ApplicationSpoolMonitor.
4. Click the **Add** button.

Configuring and Editing a Monitor

To view the configuration associated with the new monitor, or to edit an existing monitor:

1. Click the Monitors and Alerts tab**.**
2. Click on the name of the monitor you want to configure or edit.

3. Configure or edit the monitor parameters.



Note that the configuration parameters vary according to monitor type.

- **Enable this Monitor -** Select to enable the monitor.
- **Frequency (Minutes) -** Specify the monitoring frequency in minutes. Additionally, if you have opted to automatically reconnect to the database, this parameter determines how frequently the system attempts to reconnect to the database .
- **Datasource -** Datasource used to connect to the database to check for database connectivity.
- **Query -** Sample query that is run to verify that the database connectivity is on.
- **Notify SMTP Servers -** If this check box is selected, the SMTP server is notified if the database connectivity is lost.
- **Automatically Reconnect to Database -** Select to automatically reconnect to database if connectivity is lost. The Frequency parameter additionally determines the frequency with which the system will try to reconnect to the database in the event of a lost connection.
- **Alert Using -** Select an alert type from the drop-down list. The Alerting feature uses email for sending alerts, and the default value is Email.
- **From Address -** Email address of the alert sender.
- **To Address -** Email address of the alert receiver.
- **Email Service -** Select an Email Service from the drop-down list. The Email Service drop-down list lists are configured mail services on the IronPort Encryption appliance. By default, the Alerting feature uses the default IronPort Encryption appliance mail service for sending alerts.
- **IP Address -** IP address of the DNS server or gateway to monitor.

- **Port -** Port of the gateway to monitor. The default is 25 for mail gateways.
- **SpoolSize Threshold -** Threshold for the number of messages in a spool queue that will trigger an alert to be sent.
- **Application Name -** Name of the spool queue to monitor, selected from the list of all available spool queues.
- **Free Threshold (MB) -** Threshold for the amount of free space left on the disk that will trigger an alert, measured in MB.
- **Reset Threshold (MB) -** Threshold for reset.
- **Drive Name -** Name of the drive to monitor.

4. Click the **Update** button to commit your changes. Click the **Return to Monitors List** to exit from this page without making any changes.

Deleting Monitors

To delete a monitor, do the following:

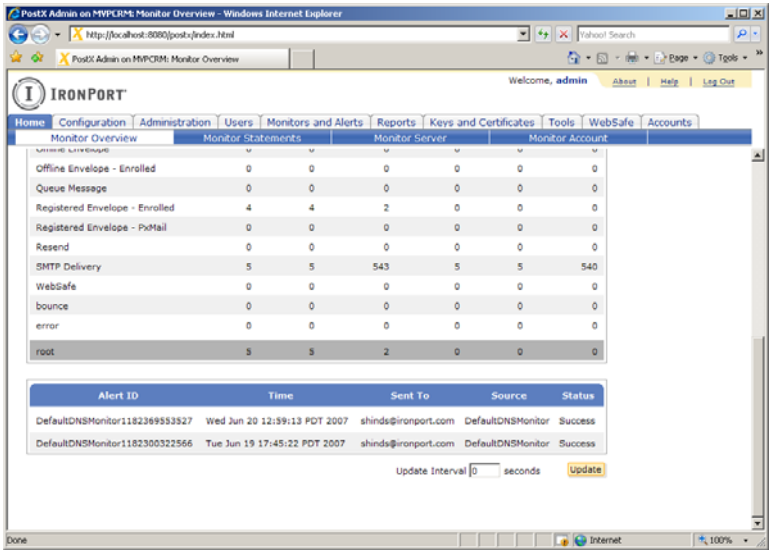
1. Click the Monitors and Alerts tab to display a list of monitors.
2. Click the trash can icon next to the monitor you want to delete. A dialog displays asking if you want to permanently delete the selected monitor. Click the **OK** button to delete the monitor or the **Cancel** button.

Restarting Monitors

Any modification to the monitor list (Add/Delete/Modify) requires restarting all the monitors. Click the **Restart Monitors** button on the Monitors page to restart all of the monitors. A confirmation message is displayed after all of the monitors are successfully restarted.

ALERTS

The Home page of the Administration Console displays a dashboard of recent alerts that have been sent successfully.



This dashboard lists the five most recent alerts that have been sent. The Alert ID, Time, Sent To, Source and Status displays for each alert.

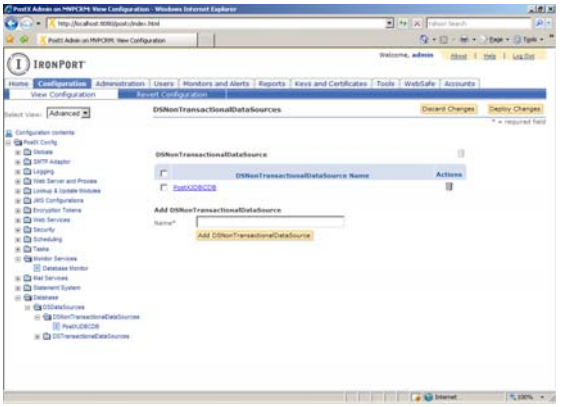
CHAPTER 5

Database Management

This chapter contains the following sections:

DATASOURCES

The IronPort Encryption appliance is pre-configured with the datasources required by the IronPort Encryption appliance applications so you rarely need to add or remove datasources. To view the datasources used by the IronPort Encryption appliance, click the Configuration tab and then in the left pane click Configuration > Database > DSDataSources > *DSNonTransactionalDatasources* or *DSTransactionalDatasources*. Please refer to *Appendix A, Configuration Parameters* in this manual for a list of associated parameters.



The datasources used by the IronPort Encryption appliance are:

Non-Transactional

- PostXJDBCDB - Used for basic JDBC access.

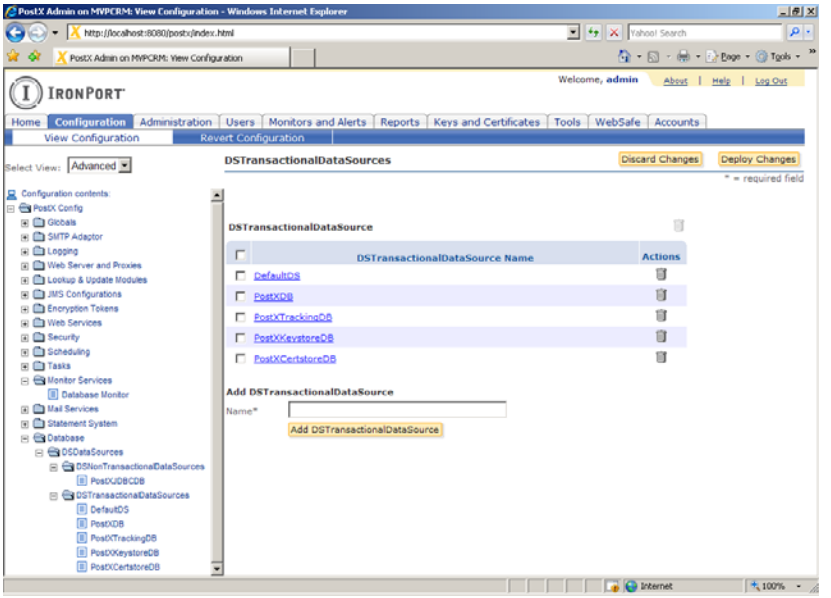
Transactional

- DefaultDS - Datasource used to access miscellaneous system tables.
- PostXDB - Datasource used to access primary the IronPort Encryption appliance database used for users, roles, WebSafe, and so forth.
- PostXTrackingDB - Datasource used to access message tracking and response history database.
- PostXKeystoreDB - Datasource used to access key server database.
- PostXCertstoreDB - Datasource used to access certificate store database.

ADDING A DATASOURCE

To add a datasource, do the following:

1. Click the Configuration tab and then click Configuration > Database > DSDataSources > *DSNonTransactionalDatasources* or *DSTransactionalDatasources*, depending on the type of datasource you want to add.



   The Add DSTransactionalDatasources or Add DSNonTransactionalDatasources section appears after the list of existing datasources.

2. Type in a datasource name.
3. Click the **Add DSTransactionalDataSource** or **Add DSNonTransactionalDataSource** button.
4. View the configurations for the new datasource either by navigating to the datasource in the configuration tree or clicking the name in the list of datasource in the right pane. See *Appendix A: Configuration Parameters* in this manual for a complete list of configuration parameters associated with datasources.

Changing the IronPort Encryption Appliance Database After Installation

The following steps allow you to change the IronPort Encryption appliance database after installation.

1. Stop the encryption server.

2. Create a new database along with the IronPort Encryption appliance specific tables using the scripts installed in:

   `<install_dir>/bin/<database_specific_directory>`

   You can optionally use the rundll script in the `<Install Dir>/bin` directory to create the tables.

3. Edit the pxeconf.xml file:

   `<install_dir>/conf/pxeconf.xml`

   In this file, you must change two sections for each datasource, the first is the security realm and the second is the datasource definition. Each datasource has its own security realm:

DataSource	SecurityRealm	Comments
DefaultDS	DefaultDSRealm	You should not need to edit this one.
PostXDB	PostXDBRealm	
PostXJDBCDB	PostXJDBCDBRealm	
PostXTrackingDB	PostXTrackingDBRealm	
PostXKeystoreDB	PostXKeystoreDBRealm	
PostXCertstoreDB	PostXCertstoreDBRealm	

4. For each datasource that you are relocating, change the following entries:

- "JDBC_URL"
- "JDBC_Driver"

The JDBC URL must be changed according to the database you want to connect to as shown below. Replace `<server>` with the hostname of the machine where the database server is installed and `<dbname>` with the name of the database.

Hypersonic

`"jdbc:hsqldb:hsql://localhost:1701"`

MySQL

`"jdbc:mysql://<server>/"`

Oracle - JBoss

Note: That you must have the Oracle client installed prior to restarting the server.

`"jd jdbc:oracle:oci:@myhost:1521:inst1"`

MSSQL

"jdbc:microsoft:sqlserver://<*server*>:1433;
DatabaseName=<*dbname*>"

MSSQL (If using the jtds driver)

"jdbc:jtds:sqlserver://<*server*>/<*dbname*>"

PostgreSQL

"jdbc:postgresql://<*server*>:5432/<*dbname*>"

DB2

"jdbc:db2://<*server*>/<*dbname*>"

The JDBC Driver must be changed according to the database you want to connect to as follows:

Hypersonic

"org.hsqldb.jdbcDriver"

MySQL

"com.mysql.jdbc.Driver"

Oracle - JBoss

"oracle.jdbc.driver.OracleDriver"

PostgreSQL

"org.postgresql.Driver"

MSSQL

"com.microsoft.jdbc.sqlserver.SQLServerDriver"

MSSQL (if using the jtds driver)

"net.sourceforge.jtds.jdbc.Driver"

DB2

"COM.ibm.db2.jdbc.net.DB2Driver"

5. For each security realm that you are relocating, change the following entries:
   - JDBC_Username
   - JDBC_Password

   Change the user ID and password to the one that has read/write access to the database pointed to by the above URL. To edit the security realms, click Configuration > Security > DatabaseSecurity > SecurityRealms > *realm_name*
6. Select the database you want to use by clicking Configuration > Database. In the Database Type field, select the database using the drop-down menu.

7. Copy the relevant JDBC driver JAR files into the appropriate locations on the application server.

   If you are using JBoss as your application server, copy the relevant JDBC JAR files to the `<Install_Dir>/jboss/server/postx/lib` directory. For other application servers, such as WebSphere, refer to the application server documentation for the locations of the JDBC driver JAR files.

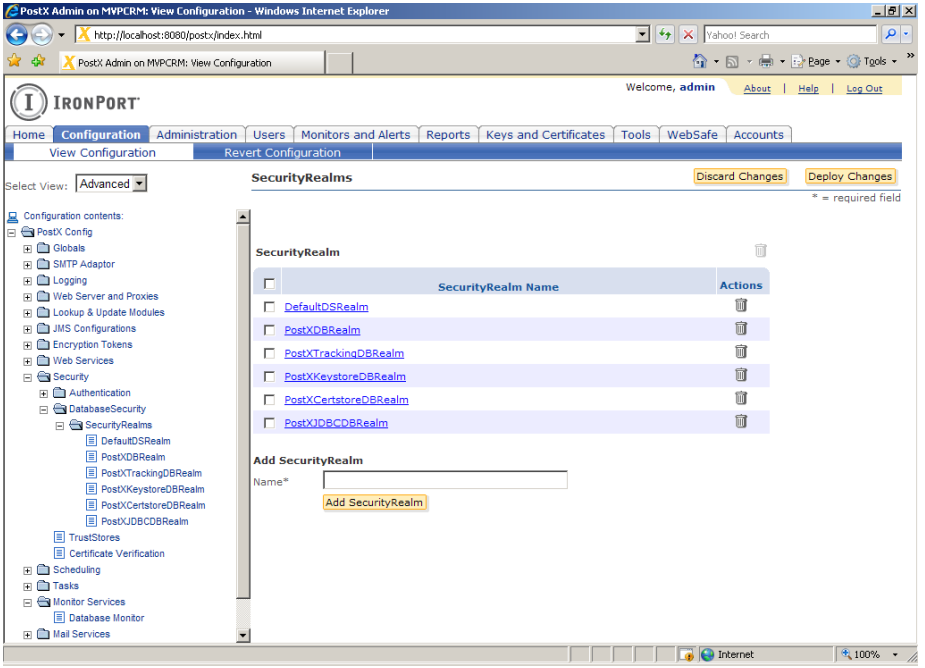
USING SECURITY REALMS

The Security Realm feature is used to manage the security credentials (i.e., username and password) needed to log in to a database.

Adding a Security Realm

To add a security realm, perform the following steps:

1. Log on to the IronPort Encryption appliance. Click the Configuration tab and then click Configuration > Security > DatabaseSecurity > SecurityRealms.



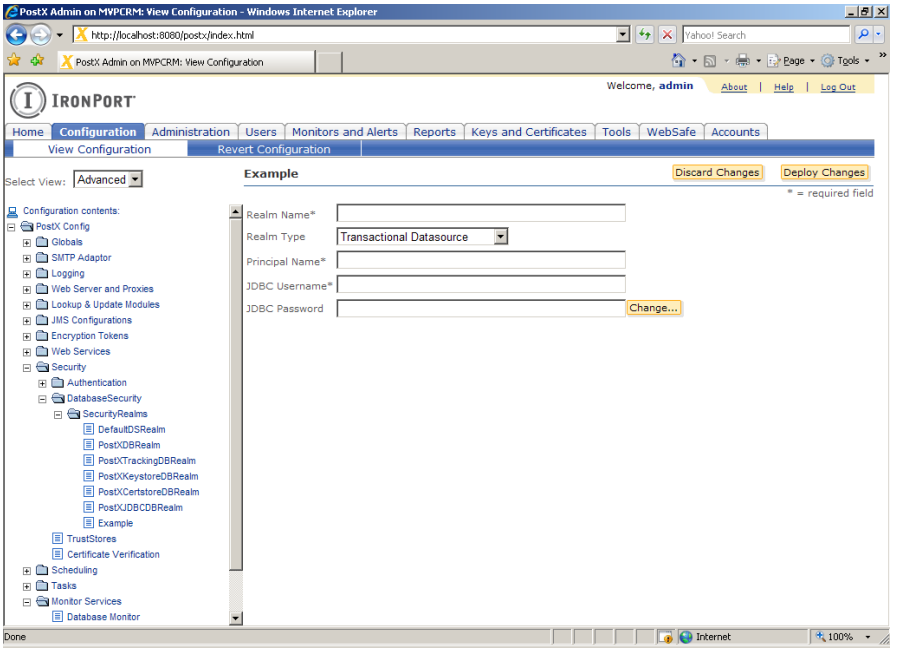
   The Add SecurityRealm section appears below the list of realms.

2. Type in a name for the security realm.
3. Click the **Add SecurityRealm** button.

Configuring a Security Realm

To configure a newly added security realm, or edit a realm, do the following:

1. Navigate down the tree to Configuration > Security > DatabaseSecurity > Security Realms and the name of the realm you want to configure or edit.



2. Enter values for the following fields:

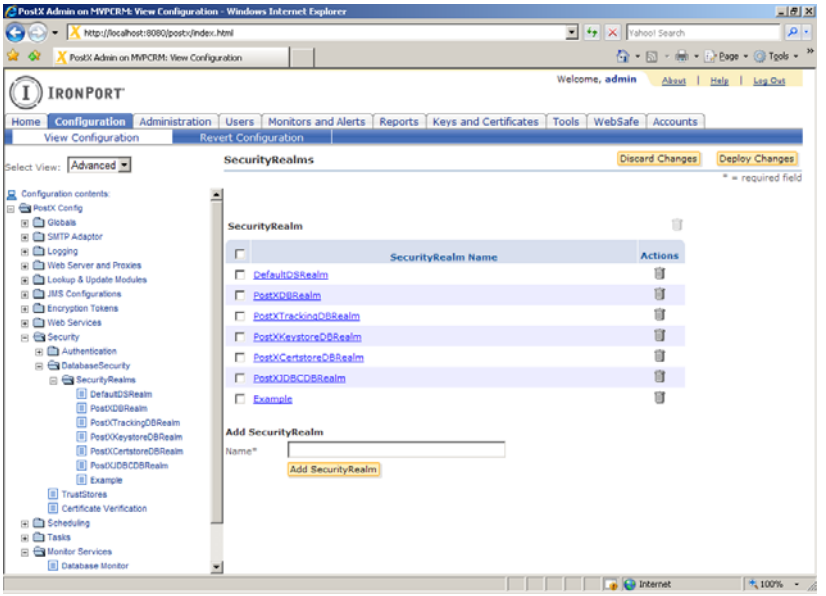
- **Realm Name -** Name of the security realm.
- **Realm Type -** Specifies whether the realm is used by a transactional or non-transactional datasource.
- **Principal Name -** Name of the object that will be accessed using this security realm; for example, a database table name.
- **JDBC Username -** Username that is used when you connect using this security realm.
- **JDBC Password -** Password to use when connecting using this security realm.

3. Click the **Deploy Changes** button.

Deleting a Security Realm

To delete a security realm, perform the following steps:

1. Navigate down the tree to Configuration > Security > DatabaseSecurity > SecurityRealms.



2. Click the trash can icon next to the security realm you want to delete. A dialog box asks if you want to permanently delete the selected security realm. Click the **OK** button to delete or the **Cancel** button.

   Alternatively, check the check boxes next to security realm names and then click the trash can icon above the Actions column.

CHAPTER 6

Configuring Multi-Server

This chapter contains information on configuring the IronPort Encryption appliance in a multi-server environment.

This chapter contains the following sections:

USING A MULTI-SERVER ARCHITECTURE

The IronPort Encryption appliance can be installed and configured to operate in a multi-server environment. You may choose to select a multi-server architecture for the following reasons:

- Must load balance between multiple machines running the encryption server
- To split the functionality of the encryption server between two machines (for example, Web Components and Mail Components)
- A combination of the above two reasons

The configuration options for a multi-server setup depend on which reason you select. These options are described in detail below.

LOAD-BALANCED MULTI-SERVER

This type of setup typically involves running identical encryption server configurations on multiple machines. An SMTP load balancer is used at the gateway end to route mail messages to the farm of IronPort Encryption appliances. At the web service end, a HTTP load balancer can be used to load share http connections between the servers. It is necessary to set the "use sticky sessions" option for the HTTP load balancer. It is also recommended that the encryption server running on each of these multiple machines talk to a shared database. This enables any machine to service any email or user by accessing the data from the central database. Having a multi-server configuration without a shared database is not recommended. Consult with an IronPort Sales Engineer to ensure that such a configuration will work for the feature set you plan to deploy.

A load balanced multi-server setup running the encryption server needs an identical configuration for each server. You can synchronize the configuration manually by following these steps:

1. Edit the configuration through the Administration Console of the IronPort Encryption appliance by connecting to one of the machines running the encryption server.
2. Restart this server to reload the new configuration.
3. Synchronize the conf directory folder among the other machines by copying the conf folder from the machine that was modified to the other machines, overwriting the existing configuration files.
4. Restart the other server(s) as well to load the new configuration.

You can do the synchronization automatically by designating one machine as the Master and configuring for the "Multi-server File Sharing" mode. Details on how to configure this is explained in a separate section below.

FUNCTIONAL SPLIT MULTI-SERVER

This setup is required when you split the encryption server by function. A typical use case is to have one machine running the Mail Server components of the encryption server and the other one running the Web Components of the encryption server. In this case, the configuration on both machines will be different. At install time you select whether you want a “Complete Server Install” or just a “Web Components Only” installation. The complete installation is what will be used for the Mail Server components of the encryption server.

It is possible to have multiple servers running each component.Each functional group of servers can be configured similarly to the “Load Balanced” multi-server setup.

The servers running the “Web Components Only” configuration can access the database in two different ways:

1. Share the database externally

   To configure it to work in this mode select the "Web Components only" option at install time. Do not select the “create” database option and keep the “JNDI URL” empty. In this mode, the “Web Components only” server will access the database directly over the network using the appropriate drivers.

2. Share EJBs

   In this mode the “Web Components Only” server accesses the database indirectly using EJBs (Enterprise Java Beans) running on the application server for the “Complete Server Install”. If you have concerns regarding accessing the database directly from the network hosting this server, you should choose this option.

   This mode also requires the complete server installation to allow connection from the “Web Components Only” server access by adding it to Allowed Network Address. This is configured by navigating to Configuration > SMTP Adaptor > Router RuleSets > root. Expand the Header Filter by clicking the + symbol. Then expand the Mime Header Filter by clicking the + symbol. In the Allowed Network Addresses field, add the addresses of the “Web Components Only” servers separated by commas, instead of the default `127.0.0.1`.

   To enable communication between the complete server and remote server machines, perform the following steps:

   a. On all server machines, go to the Configuration tab and click Configuration > Globals > Network Bindings. Then, change the following values to the physical IP address of the machine:

      - Naming Service Binding Address
      - Naming Service RMI Binding Address
      - RMI Invoker Binding Address
      - JMS RMI Adaptor Binding Address

      Then, click the **Deploy Changes** button.

b. On all server machines, go to the Configuration tab and click Configuration > Globals > Local Server Group. Then, add the machine name for the machine running the complete server and click **Add Group Member**. Next, click the link for the machine name, and change the IP address to the physical IP address of the machine. Leave the port number as 1099. Next add the machine names and update the physical IP addresses for all remote servers in the server group. Click **Deploy Changes** when you are finished.

c. On all server machines, go to the Configuration tab and click Configuration > Globals > Multi Server. In the Remote Server field, select the name of the machine running the complete server, and then click **Deploy Changes.** Perform this step on *all* machines, including the machine running the remote server.

To configure it to work in this mode at install time, specify the "Remote Hostname" and "Remote JNDI Port" pointing to the server running the complete encryption server setup.

MULTI-SERVER FILE SHARING CONFIGURATION

Overview

The multi-server file sharing mode in the encryption server consists of the ability to share configuration files (namely, pxeconf.xml, pxkeystore, and so forth) between several machines. The machines are configured to be publishers and subscribers with the ability of subscribers to subscribe to configuration file changes from publishers.

Configuration

Configuring the IronPort Encryption appliance for multi-server file sharing mode consists of the following steps.

1. Creating JMS Topics

   IronPort Encryption appliance uses the JMS "topic" technology to distribute configuration files between machines. In a typical Master slave configuration for such distribution, all modifications are done to the Master with the slaves receiving the changes as they get deployed on the Master. A minimum of 2 topics must be created in the Master with each of the other machines having a minimum of 1 topic created. For example, the Master will have 2 topics named Publisher and Subscriber. The rest will have a single topic called Subscriber.

   To add a JMS topic, click the Configuration tab and navigate to JMS Configurations > JMS Topics > TopicList.

   Care should be taken configuring the topics since once the machines are connected to each other, all of them end up sharing a single configuration file. Also, the configuration file should be carefully analyzed before deployment for any machine specific dependencies. All URLs that need the action executing on a local machine should be changed to localhost, and all URLs that require a particular machine for execution should have its machine name clearly entered with all prefix/domain qualifications.

2. Configuring the JMS Topics

   The topics in the Master machine must be configured such that there is at least one topic with a topic configuration element "Type" specified as "Subscriber" and one with the "Type" specified as "Publisher". The Provider URL for both topics needs to be set to <*Machine Name*>:<*Local Naming Port*>. Typically the naming port is at 1099. The <*Machine Name*> should be a name/IP accessible over the entire network to identify that machine and should not be localhost or 127.0.0.1.

   All the remaining machines must be configured so that there is at least one topic with Topic Configuration element "Type" as "Subscriber". The provider URL for the topic should be set to:

   <*Master Machine Name*>:<*Master Naming Port*>, where the Master machine specifies the machine to connect to for retrieving the configuration file.

Also a “FileCatalog” location needs to be specified. This is a text file that contains all of the files that the publisher and subscriber are planning to share.

If the topic requires a username/password to access it, the necessary information can be entered in the topic element.

The following parameters are used to configure a JMS topic:

Parameter	Definition
Topic Connection Factory	Connection Factory used to get connection to the topic. Required field.
Name	Name of the topic. Required field.
Provider URL	URL connecting to the JNDI service of the file sharing machine (namely, Master).
File Catalog	Location of file that contains a list of files to be shared between the machines. The Current Working Directory (CWD) for the path locations in this catalog is `$postx.home/conf` Required field.
User Name	User Name if necessary for creating a topic connection
Password	Password if necessary for creating a topic connection.
Initial Context Factory	Initial Context Factory for topic Lookup.
Type	Topic Type. Valid values are Subscriber, Publisher. Required field.

3. Restarting the encryption servers on all machines

   All of the encryption servers that have been changed should be manually restarted (the Administration Console will prompt you to do this). Care should be taken to have the Master up and running before the rest of the servers are started up so they can find the Master Naming Service.

Advantages

The basic advantage obtained using multi-server file sharing is the ability to deploy a single change to several machines running encryption servers over the network. Also, actions such as server restarts are propagated over the network once the mechanism is in place. For example, restarting the Master through the Administration Console results in all machines subscribed to it being restarted.

MANAGING ENCRYPTION TOKENS IN A MULTI-SERVER ENVIRONMENT

The encryption server has the ability to optionally encrypt messages stored in WebSafe using an encryption token. The system is installed with a default encryption token which seeds off the install license key. However, you can add more encryption tokens through the Administration Console and use them to encrypt messages in WebSafe. In a multi-server configuration the database is shared across the different machines and therefore care should be taken to make sure the encryption tokens are synchronized between the machines. If you use the “Multi-server File Sharing” mode the system will take care of this for you. However, if you are planning to manually synchronize the configuration between the two machines you must ensure that the encryption tokens which are placed in the “pxkeystore” file in the conf directory are definitely the same on all the machines. Any addition or deletion of an encryption token will result in you having to bring down all servers, copy the file from the modified machine to the rest of the machines and then restart the entire server farm. Failure to do so will lead to some messages being stored in the WebSafe database that cannot be read.

CHAPTER 7

Customizing the IronPort Encryption Appliance

This chapter addresses the steps required to customize the IronPort Encryption appliance to meet your organization's specific needs.

This chapter contains the following sections:

OVERVIEW

The IronPort Encryption appliance is designed to support full customization of system messages, including notification and registration, the Registered Envelope and the registration web presence. In addition, you can brand the user interface with your logo.

The following text and HTML files are available for customizing. These files are located in the `<install_dir>/conf` directory with the exception of the messagebar.html file which is located in `<install_dir>/conf/messagebar` directory.

- **AccountStatusNotify.txt -** This file is used to send a notification email to an account's administrator and support contacts when the status of the account is changed. A copy of the email is also sent to the PxMail Administration Team as specified in pxmail.properties.
- **ActivationNotification.txt -** This file contains the message text sent to recipients after they register to receive messages.
- **ActivationReminder.txt -** This file contains the message text sent to recipients to remind them that they have a specific number of days left to register their account before it expires. This file is used when you are running the ActivationReminder task.
- **AlertEmailTemplate.txt -** This file contains the message text sent to the administrator when an alert occurs. this is a consolidated template that includes all of the alerts that the system can generate. The system will select the correct of the template to use depending upon the alert type.
- **CancelNotification.txt -** This file is used to send an email to the recipient when activation for the recipient has been cancelled. This is to inform the recipient that his account was not activated and has been removed from the system.
- **ChangePasswordBody.txt -** This file contains the message text sent to recipients when their password is reset/changed.
- **CharsetLocaleMap.txt -** This file maps the incoming email charset to a locale which is used to read the corresponding localized template file.
- **EmailBody.txt -** This file contains the message text sent with a WebSafe message.
- **EnrollBody.txt -** This file contains the message text sent to recipients to inform them that they have been sent a message encrypted using IronPort PXE technology.
- **EnrollSuccess.txt -** This file contains the message text sent to recipients they have enrolled successfully.
- **ExpireNotification.txt -** This file contains the text used in the notification emails telling people that their accounts have expired without being activated.
- **FileCatalog.txt -** This file contains a list of files which will be replicated from the master server to other configurations.
- **keyservernotify.txt -** This file contains the text that is used when the message sent to the recipient has not been opened with a specified period of time.

- **KeyserverRecipientEnrollBody.txt -** This file contains the message text sent with a registration notification message to recipients who are not already enrolled. By default, this is only used by DesktopEncrypt.
- **KeyserverSenderEnrollBody.txt -** This file contains the message text sent with an registration notification message to senders.
- **LicenseReminder.txt -** This file contains the text that is sent in the reminder message when the license is up due for renewal. It is configured in Configuration > Scheduling > Scheduled Tasks > Send License Notifications.
- **MDS_Notify.txt -** The file that contains the text that is sent in the notification message when using Mobile Device Support.
- **MessageDisplayNotification.txt -** This file contains the text that is used when a Return Receipt is sent to a sender.
- **Mixed Enroll.txt -** This file is needed only if you have a setup where your encrypted email sent to recipients can be either S/MIME, PGP or Envelopes. This template is specified as the notification message template for QueueMessage and will instruct the recipient to provide appropriate credentials to receive the encrypted email. For instance, this email might ask the recipient to provide his X.509 certificate or PGP key and if none available the recipient is provided the enrollment link to enroll with the Enrollment system and provide an encryption password.
- **PGPRecipientTemplate.txt -** This file contains the message text that is sent to a recipient to notify them that a PGP key has been generated on their behalf and to follow the instructions to install the key.
- **PGPSenderTemplate.txt -** This file contains the message text that is sent to the sender notifying them that a PGP key was generated for a recipient of a message they sent. This contains the PIN that the recipient must install the key.
- **PinTemplate.txt -** This file contains the message text that is sent to the certificate requestor informing them of the PIN required to obtain the digital certificate.
- **PostmasterActivationNotification.txt -** This file contains the message text for the activation email sent to the individual you specify via the WebSafe activation configuration.
- **PostXMessage.txt -** This file contains the message text sent to recipients when they receive a Registered Envelope.
- **ProvisionAccountNotify.txt -** This file is used to send a notification email to the PxMail Administration Team when a new account has been provisioned via the 'Provision Account' screen in Websafe. The notification email includes all the information that was entered by the user to provision a new account.
- **QueueMessageBounce.txt -** This file contains the text sent to a sender as a bounced message when the original message from the sender did not reach the intended recipient.

- **QuotaExceededEmail.txt -** This file contains the message text sent to recipients when they exceed their WebSafe mailbox quota.
- **QuotaWarningEmail.txt -** This file contains the message text sent to recipients when they approach their WebSafe mailbox quota.
- **RecipientTemplate.txt -** This file contains the message text that is sent to a recipient to notify them that a SMIME certificate has been generated on their behalf and to follow the instructions to install the certificate.
- **ScheduledReportEmail.txt -** The IronPort Encryption appliance has the ability to schedule a task that will run the specified report and email the contents of the report to the configured administrator email address(es). This file is used as the body of this email.
- **SenderActivationNotification.txt -** This file contains the message text for the activation email sent to the sender.
- **SenderTemplate.txt -** This file contains the message text that is sent to the sender notifying them that a SMIME Certificate was generated for a recipient of a message they sent. This contains the PIN that the recipient must install the certificate.
- **SendRegEnvBody.txt -** This file contains the text that is sent in the notification message when a user has successfully registered for secure messaging.
- **SuccessNotification.txt -** This file is used to send an email to the recipient when activation for the recipient is complete. This is to inform the recipient that his account has been activated.
- **TempPswdNotification.txt -** This file contains the message text that is sent to the user when he has clicked the "Forgot Password" link and the system is configured to send a new temporary, random password to the user. It is configured in Configuration > Web Services > WebSafe > Password.
- **AccountStatusNotify.html -** This file is used to send a notification email to an account's administrator and support contacts when the status of the account is changed. A copy of the email is also sent to the PxMail Administration Team as specified in pxmail.properties.
- **ActivationNotification.html -** This file contains the message HTML sent to recipients after they register to receive messages.
- **ActivationReminder.html -** This file contains the message HTML sent to recipients to remind them that they have a specific number of days left to register their account before it expires. This file is used when you are running the ActivationReminder task.
- **attachmenttemplate.html -** This file contains the message HTML that is sent when a message exceeds the large file support trigger size. The message contains a button that directs the recipient to the server to download the attachment.
- **CancelNotification.html -** This file is used to send an email to the recipient when activation for the recipient has been cancelled. This is to inform the recipient that his account was not activated and has been removed from the system.

- **EmailBody.html -** This file contains the message HTML sent with a WebSafe message.
- **EnrollBody.html -** This file contains the message HTML sent with an registration notification message.
- **ExpireNotification.txt -** This file contains the text used in the notification emails telling people that their accounts have expired without being activated
- **KeyserverRecipientEnrollBody.htm -** This file contains the message HTML sent with an registration notification message to recipients who are not already enrolled. By default, this is only used by DesktopEncrypt.
- **KeyserverSenderEnrollBody.html -** This file contains the message HTML sent with an registration notification message to senders.
- **MDS_Notify.html -** The file that contains the text that is sent in the notification message when using Mobile Device Support.
- **messagebar.html -** This file contains the HTML that is displayed in the envelope message bar.
- **MixedEnroll.html -** This file is needed only if you have a setup where your encrypted email sent to recipients can be either S/MIME, PGP or Envelopes. This template is specified as the notification message template for QueueMessage and will instruct the recipient to provide appropriate credentials to receive the encrypted email. For instance, this email might ask the recipient to provide his X.509 certificate or PGP key and if none available the recipient is provided the enrollment link to enroll with the Enrollment system and provide an encryption password.
- **PostmasterActivationNotification.html -** This file contains the message HTML for the activation email sent to the individual you specify via the WebSafe activation configuration.
- **PostXMessage.html -** This file contains the message HTML sent to recipients when they receive a Registered Envelope.
- **ProvisionAccountNotify.html -** This file is used to send a notification email to the PxMail Administration Team when a new account has been provisioned via the 'Provision Account' screen in Websafe. The notification email includes all the information that was entered by the user to provision a new account.
- **SenderActivationNotification.html -** This file contains the message HTML for the activation email sent to the sender.
- **SendRegEnvBody -** This file contains the text that is sent in the notification message when a user has successfully registered for secure messaging.
- **SuccessNotification.html -** This file is used to send an email to the recipient when activation for the recipient is complete. This is to inform the recipient that his account has been activated.

- **TempPswdNotification.html -** This file contains the message HTML that is sent to the user when he has clicked the "Forgot Password" link and the system is configured to send a new temporary, random password to the user. The option is configured in Web Services > WebSafe > Password.
- **textbodytemplate.html -** This file contains the email body for IronPort PXE messages. Because these are template files you can modify the look-and-feel of the messages and add additional message information for display as needed.

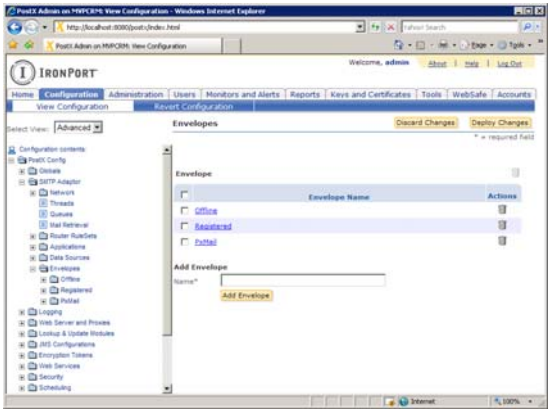
CUSTOMIZING THE REGISTERED ENVELOPE

The Registered Envelope "look-and-feel" is customizable, allowing you to edit it to reflect your enterprise's specific requirements. The following elements can be customized: logos, graphics, buttons, and fields. In addition you can customize the envelope behavior.

The following sections contains instructions for adding and editing an envelope.

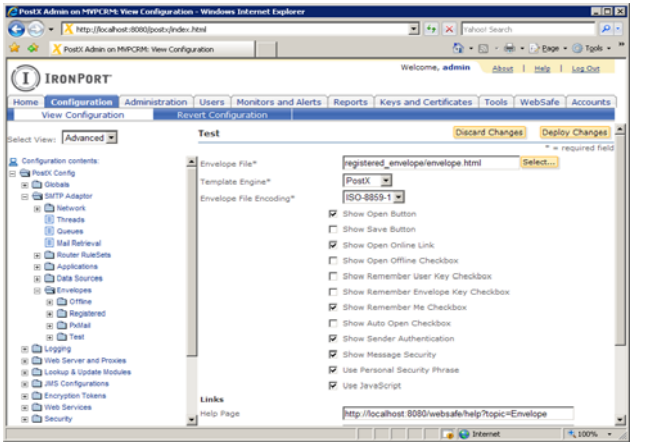
Adding a Registered Envelope

1. Click the Configuration tab and navigate to Configuration > SMTP Module > Envelopes.



The Add Envelope section appears at the bottom of the screen.

2. Type in an envelope name.
3. Use the Add Before drop-down to specify where the envelope appears in the list. The order that envelopes appear impacts the behavior of the system. For example, if a new envelope is placed at the end of the list, the message may not utilize that envelope.
4. Click the **Add Envelope** button.
5. Navigate to Configuration > SMTPModule > Envelopes > *New_Envelope_Name* to edit the new envelope.



6. Edit the following configuration parameters as needed:

- **Envelope File –** Envelope file path. Use the **Select** button to navigate to the file.
- **Template Engine –** Name of the template engine used by this envelope. Options are: postx, velocity, xmlc and xslt.
- **Envelope File Encoding –** Specifies the file encoding for envelope files in the envelope directory. Options are UTF-8, UTF-16, Big5, Shift-JIS and iso-8859-1.

  The following options allow you to specify the buttons and check boxes that appear on the envelope.

- **Show Open Button –** Include an Open button on the Envelope, allowing it to be opened locally.
- **Show Save Button –** Includes a Save button on the Envelope, allowing saving of the payload to disk.
- **Show Open Online Link –** Include an Open Online link on the Envelope, allowing opening the Envelope using the online opener. The online opener is always used if JavaScript isn't available, whether the Open Online link is shown or not.

- **Show Open Offline Checkbox –** Include a checkbox on the envelope which, when checked, causes the envelope to encrypt the session key with the user's key and save it in a cookie, allowing a registered envelope to be opened offline.
- **Show Remember User Key Checkbox –** Includes a checkbox on the envelope which, when checked, causes the envelope to save the user's key to a cookie. The name is based upon the User Key Name settings from the Details tab of the application. This enables all envelopes with the same User Key Name to be opened without entering credentials once one is opened. This setting should only be checked if a User Key Name is set.
- **Show Remember Envelope Key Checkbox –** Include a checkbox on the envelope which, when checked, causes the envelope to save the session key in a cookie unique to each envelope, allowing the envelope to be opened without entering credentials.
- **Show Remember Me Checkbox –** Include a checkbox on the envelope which, when checked, causes the envelope to request that the server store the user's address and key in a cookie so that future envelopes can be opened automatically.
- **Show Auto Open Checkbox –** Include a checkbox on the envelope which, when checked, causes the envelope to open automatically the next time it's opened if the session key is available in a cookie. This setting should only be checked if Show Remember Envelope Key Checkbox is checked.
- **Show Sender Authentication –** Display the sender.
- **Show Message Security –** Display the message security on the envelope.
- **Use Personal Security Phrase –** Include a phrase on the envelope which, when checked, further validates that the envelope is being sent from the IronPort Encryption appliance. The phrase is recipient specific. If you elect to use this option, the recipient will enter a phrase during the registration process.
- **Use JavaScript –** Use JavaScript to enhance the user experience for the envelope and, when possible, to decrypt the message.

  In the Links section, provide the following information:

- **Help Page –** URL for the envelope's help page.
- **Address Not Listed Page –** URL for this envelope's page explaining that the user's address may not have been in the displayed recipient's list.
- **Personal Security Phrase Info Page –** URL for the web page that explains why the user's passphrase is not being displayed.
- **Forgot Password Page –** URL for this envelope's forgot password page.

  In the Key section, complete the following fields:

- **Field *Separator*** – *Separator* placed between each input field to form the key.
- **Case Sensitive** – Select if the key is case sensitive.

7. Click the **Deploy Changes** button.

Adding and Editing Envelope Graphics

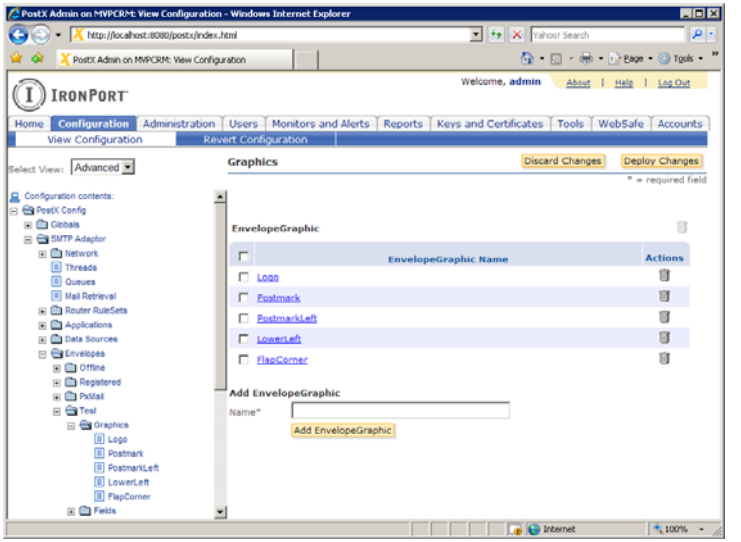
Logo, Postmark and PostmarkLeft are graphical elements of the envelope shipped with the IronPort Encryption appliance. In addition to the graphics already on the envelope, a graphic can be added in the lower left corner of the envelope by creating a new graphic named LowerLeft.

You can add and edit graphics by navigating to Configuration > SMTPModule > Envelopes > *New_Envelope_Name* > Graphics.

Adding a Graphic

To add a graphic:

1. Navigate to Configuration > SMTP Adaptor > Envelopes > *New_Envelope_Name* > Graphics. Use the Add Envelope Graphic section that appears at the bottom of the right pane.

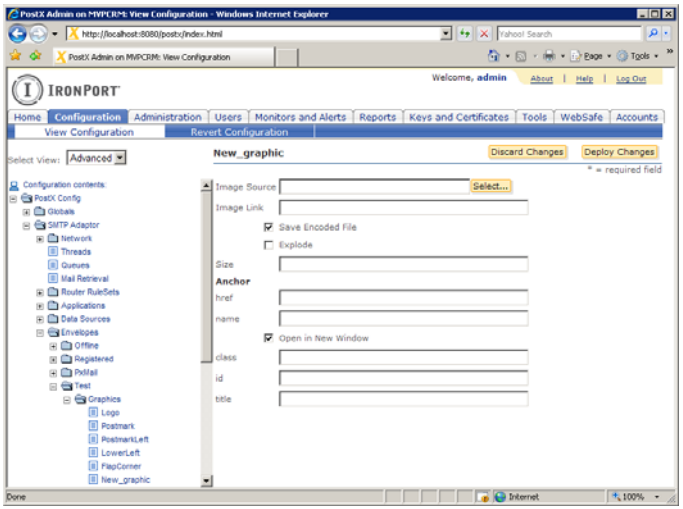


2. Type in a graphic **Name**.
3. Use the **List Location** drop-down to specify where the graphic appears in the list. The order that graphic appear impacts the behavior of the system. For example, if a new graphic is placed at the end of the list, the message may not utilize that graphic.
4. Click the **Add Envelope Graphic** button.

Configuring/Editing a Graphic

The following steps illustrate how to configure a new graphic or edit an existing one.

1. Navigate to Configuration > SMTP Adaptor > Envelopes > *new_envelope_name* > Graphics > *New_Graphic*. The following screen is displayed:



2. Configure the Logo configuration parameters for your specific graphic.

   Image Source – Image file path.

   Image Link – Link to online image.

   Save Encoded File – Specifies whether to save a copy of the encoded file for future use.

   Explode – Check to draw a blank line between every constant-color rectangle in the image. For demonstration only; not supported on all browsers.

   Size – Size of each pixel in image. For demonstration only; not supported on all browsers.

   href – Destination URL if the image is clicked. Leave blank for a non-clickable image.

   name – Anchor name attribute. Leave blank for none.

   Open in New Window – Check to open destination URL (if any) in new window.

   class – Anchor class attribute. Leave blank for none.

   id – Anchor id attribute. Leave blank for none.

   title – Anchor title attribute. Leave blank for none.

3. Click the **Deploy Changes** button.

Adding and Editing Fields on an Envelope

You can add and edit the text associated with an Envelope. To do this navigate to Configuration > SMTP Adaptor > Envelopes > *New_Envelope_Name* > Fields. The “Password”

element is shipped with the IronPort Encryption appliance. You can also add other fields as desired.

Envelope Configuration Parameters

For a complete list of the configuration parameters associated with the Envelope feature, see Appendix A, “Configuration Parameters,” on page 239.

USING A CUSTOM LOGO FOR WEBSAFE AND SECURE REPLY

All WebSafe web pages display a logo in the header part of the page. This is also the logo that is displayed on the secure reply pages. The logo file is named `customer-logo.gif`. The default logo file is located in the websafe.war file in the "`images`" directory. To override this logo with a new image do the following:

1. Locate the `<install_dir>/conf` directory.
2. Inside the conf directory create the following directory path:

   `custom/websafe/branding`
3. Copy the new image file to the images directory and rename it customer-logo.gif. This file must be a valid GIF file.
4. Restart the encryption server.

If the new logo is not a valid GIF file then you must also do the following before restarting the encryption server.

1. Locate the `<install_dir>/conf/custom/websafe` directory.
2. Inside the websafe directory locate the file named `standard.properties` file. If this file does not exist then create it.
3. Open standard.properties in a text editor and add the following line:

   `page.top-logo.url = images/<file-name>`

   Replace `<file-name>` with the name of the new logo file; for example, `company_logo.jpg`.
4. Save the file. If you are using Microsoft Word or another word processor be sure to save the file as "text-only with line breaks".
5. Restart the encryption server.

CHANGING WEBSAFE LINK URLS

The standard WebSafe page layout includes Contact and About links in the page footers and also associates a URL with the logo in the header. Each can be configured to point to appropriate pages on your company's web site; for example, clicking on the logo takes the user to your company's home page, About points to the "About" page of your company's web site and Contact points to the contact info web site page. To change any of these links do the following:

1. Locate the `<install_dir>/conf` directory.
2. Inside the conf directory create the following directory path:

   `custom/websafe`
3. Inside the websafe directory locate the file named "standard.properties". If this file does not exist then create it.
4. Open standard.properties in a text editor and add the following lines:

   ```
   page.top-logo.href=http://your-company.com
   reference.contact-us.href=http://your-company.com/contact
   reference.contact-us.name=contact
   reference.about.href =http://your-company.com/about
   ```

   Replace the URLs with the appropriate URLs for your company.
5. Save the file. If you are using Microsoft Word or another word processor be sure to save the file as "text-only with line breaks".
6. Restart the encryption server.

You can also change the display text of the Contact Us and About links and provide appropriate tooltip messages. To do so, add these additional lines to the standard.properties file:

```
page.top-logo.tooltip = The logo tooltip text here.
reference.contact-us.tooltip = The Contact Us link tooltip text
here.
reference.contact-us.name = New display text for the Contact Us link
reference.about.tooltip = The About link tooltip text here.
reference.about.name = New display text for the About link
```

Your specific tooltip text should only contain letters and punctuation. Do not use special symbols like less-than or greater-than symbols.

To hide either the "Contact Us" or "Abort" links, set their display names to _hide. For example:

```
reference.contact-us.name=_hide
reference.about.name=_hide
```

CUSTOMIZING THE REGISTRATION PAGE

The registration page is fully customizable allowing you to edit it to meet your specific requirements. The registration page is a WebSafe page; therefore, before discussing customizing the registration page, review the following section to understand the overall layout of WebSafe pages.

Customizing WebSafe Pages

All WebSafe pages are generated from HTML "skins" and custom content generated using eXtensible Stylesheet Language (XSL) technology. The custom XSL-generated content is placed into the specific page's HTML based on instructions contained in the HTML skin. By modifying the skin you can modify the look-and-feel of WebSafe pages. For example, by adding additional information beneath the footer or between the header and the main body portion of each page.

WebSafe uses the following four skins:

- **login –** Used during login (before the user has been authenticated by the IronPort Encryption appliance). Contained in skin-login.xhtml.
- **search-page –** Used when the user is doing Basic or Advanced searches. Contained in skin-search.xhtml.
- **print –** Used when the user prints email messages. Contained in skin-print.xhtml.
- **standard –** Used for all other pages. Contained in skin-standard.xhtml.

Each of these skins are contained in a separate xhtml file as noted above. This is to remind you that while the files contain standard HTML, the HTML must also be valid XML. HTML tags such as <P> or
 that do not require closing tags in standard HTML files must be associated with closing tags in these skin files. An easy way to do this is to use <P/> in place of <P> and
 in place of
, and so on.

The easiest way to modify a skin is to use a copy of the skin that was installed with the kit. The skins are contained in a file called websafe.war in the "templates" directory. To locate the skin files do the following:

1. Use your OS search tool to locate the postx.ear file. This is a standard ZIP file and can be opened with any standard ZIP file viewer.
2. Locate the websafe.war file within postx.ear and extract the file.
3. Unzip the websafe.war file and locate the skin file you want to modify and extract a copy.
4. Edit the skin file using a standard text editor. Note that if you use Microsoft Word or another word processor you must save the updated file as "text-only with line breaks".

Once you have modified a copy of the skin file do the following to install it into WebSafe:

1. Locate the `<install_dir>/conf` directory.
2. Inside the conf directory create the following directory path:

```
custom/websafe/templates/skins
```

3. Copy the modified skin file to the skins directory.
4. Restart the encryption server.

You can also include new images in your modified skin file by adding the appropriate IMG tag; for example:

```
<IMG SRC="http://company.com/data/myimage.jpg"/>
```

Note that the IMG tag contains a closing "/" character so that the tag is properly closed. You could have also done the following:

```
<IMG SRC="http://company.com/data/myimage.jpg"></IMG>
```

You may reference image source files from an external web site such as your corporate site. If this is not possible, you can use the IronPort Encryption appliance to serve the image files. For example, if the image source file is named "myimage.jpg" then do the following to have IronPort Encryption serve the image file:

1. Locate the `<install_dir>/conf` directory.
2. Inside the conf directory create the following directory path:

   ```
   custom/websafe/images
   ```

3. Copy the image file to the images directory.
4. Format the IMG tag like this:

   ```
   <IMG SRC="./images/myimage.jpg"/>
   ```

5. Restart the encryption server.

Editing the Registration Page

When a new user clicks on the registration link contained in the registration notification email, an registration form is displayed. The contents and layout of this form are configurable, including changing text labels, field formatting and overall layout. Included in this overall layout are numerous content areas that can vary depending on the state of the user's session (for example, logged in versus logged out) or the command that was executed (for example, "view folders" versus "compose email"). Each of these content areas is called a pane. The standard skin contains four panes: header, footer, navigation bar and body (the main content area.) Within the skin file these panes are defined by <postx-ws:xslt> tags. Each <postx-ws:xslt> tag corresponds to a separate named pane, with the name defined by the "pane" attribute of the tag.

WebSafe uses XSLT technology to generate the display contents for each pane. By modifying the XSL stylesheet (not to be confused with a Cascading Stylesheets or CSS stylesheet) that defines the layout of a pane you can change what is displayed to the user. Although you can modify the XSL stylesheets associated with any pane on the page, we are only concerned here with the stylesheet that is used to create the "body" pane of the Registration page. WebSafe provides two types of registration pages. The standard page displays the user's ID and prompts

for her first and last name, password, forgot password challenge question and forgot-password challenge answer. The alternative page also displays the user's mailbox ID and notification address. This discussion focuses on changing the former only but the same approach is used to change the latter.

The look-and-feel of the registration form is defined by the "`client-pxenroll.xsl`" XSL stylesheet. Any changes you make to this file will be reflected in the form. client-pxenroll.xsl is contained in a file called websafe.war, in the "templates" directory.

To locate the client-pxenroll.xsl file do the following:

1. Use your OS search tool to locate the `postx.ear` file. This is a standard ZIP file and can be opened with any standard ZIP file viewer.
2. Locate the websafe.war file within postx.ear and extract the file.
3. Unzip the websafe.war file and locate the client-pxenroll.xsl file and extract a copy.
4. Edit the file using a standard text editor. Note that if you use Microsoft Word or another word processor you must save the updated file as "text-only with line breaks".

   This file is an XSL stylesheet file and so contains both XSL tags and HTML tags. Add, modify and remove HTML as appropriate but be sure to preserve the XSL tags as is. Also, This entire file must be a valid XML file so be sure that any changes you make are both valid HTML and valid XML (for example, <P/> instead of <P> with no closing </P> tag).

Once you have modified client-pxenroll.xsl do the following to install it into WebSafe:

1. Inside the conf directory create the following directory path:

   `custom/websafe/templates/`
2. Copy the modified skin file to the templates directory.
3. Restart the encryption server.

CHAPTER 8

Configuring the Appliance to Use CRES

This chapter contains the following sections:

OVERVIEW

If you do not want to use the IronPort Encryption appliance as a local key server, you can configure the appliance to use the hosted key service, Cisco Registered Envelope Service (CRES). When you use the hosted key service, encryption keys for each message are stored on a remote Cisco server and retrieved from that server when recipients open Secure Envelopes.

The process for setting up an IronPort Encryption appliance to use Cisco Registered Envelope Service involves the following steps:

1. **Retrieve an account token.** You need a token for the Cisco Registered Envelope Service account to enable communication between the service and the IronPort Encryption appliance. For more information, see "Retrieving the Account Token" on page 111.
2. **Upload the token to the appliance.** After you download and save the token from Cisco Registered Envelope Service, you upload it to the IronPort Encryption appliance. For more information, see "Uploading the Token to the Appliance" on page 113.
3. **Configure the SMTP Adaptor.** You need to configure the SMTP Adaptor to use Cisco Registered Envelope Service as the encryption key server. For more information, see "Modifying the SMTP Adaptor Configuration" on page 114.

After you complete these steps, you store encryption keys for Secure Envelopes on the hosted key service, Cisco Registered Envelope Service. You no longer use the IronPort Encryption appliance as a local key server.

RETRIEVING THE ACCOUNT TOKEN

To use the hosted key service with an IronPort Encryption appliance, you need an account token from Cisco Registered Envelope Service. There are two ways to obtain an account token:

- Contact IronPort Customer Support to request a token. For information about contacting Customer Support, see the following web page:

  `http://www.ironport.com/support/contact_support.html`

- *If you have a Cisco Registered Envelope Service administrator account,* you can download the token directly from Cisco Registered Envelope Service.

This section describes the procedure for downloading the token from the Cisco Registered Envelope Service web site. You must have an *administrator* account to download the token. Otherwise, contact IronPort Customer Support for assistance.

To download an account token:

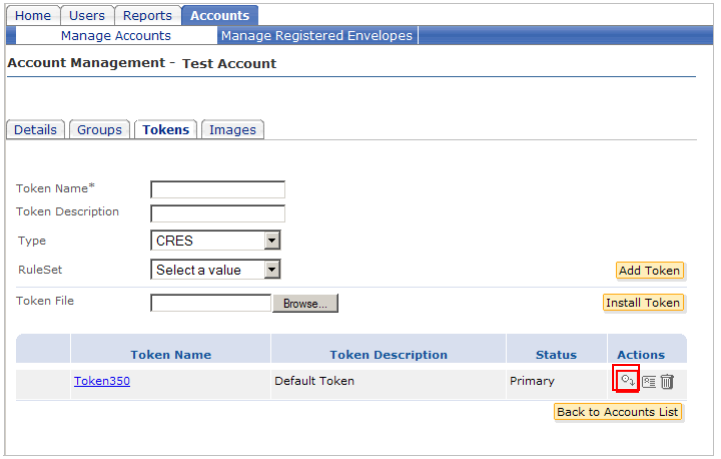
1. Log in to your Cisco Registered Envelope Service administrator account at the following address:

   `https://res.cisco.com/admin/`

2. Click Accounts > Manage Accounts.
3. On the Account Management page, click the link for your account number.

   Note — By default, only one account number appears in the list of accounts.

4. Click the Tokens subtab for your account. The following page is displayed.



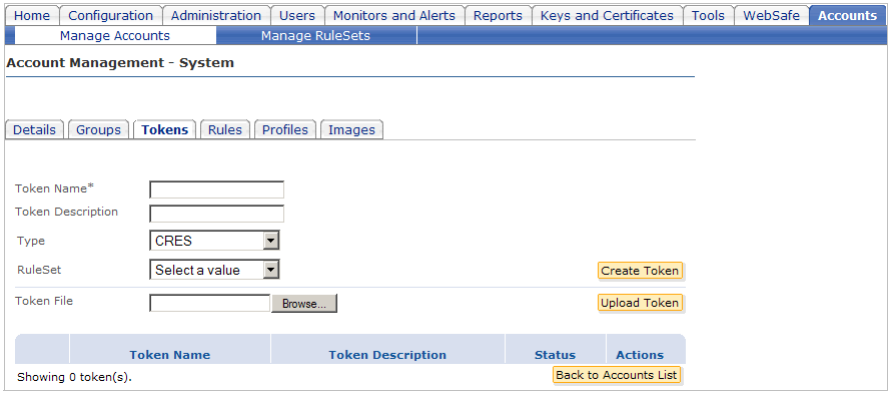
5. Click the Save Token icon  for the default token.
6. Save the token file to your hard disk.

UPLOADING THE TOKEN TO THE APPLIANCE

After you download an account token from Cisco Registered Envelope Service—or after you receive the token file from IronPort Customer Support—you need to upload the token to your IronPort Encryption appliance.

To upload the token to the IronPort Encryption appliance:

1. In the Administration Console, click the Accounts tab and then click the Account Management subtab.
2. On the Account Management page, click the link for the System account.
3. On the Account Management – System page, click the Tokens subtab for the System account.



4. Click the **Browse** button, and navigate to the token.jar file on your hard drive.
5. Click **Upload Token.**

   A message appears on the Tokens tab if the token is successfully installed.
6. Click the **Back to Accounts List** button.

   The account number for the Cisco Registered Envelope Service account appears below the System account in the list of accounts.

MODIFYING THE SMTP ADAPTOR CONFIGURATION

After you upload the Cisco Registered Envelope Service account token to the IronPort Encryption appliance, you need to modify the SMTP Adaptor configuration for the following two applications:

- Registered Envelope
- Registered Envelope Throttled

Configuring the Registered Envelope Application

First, modify the SMTP Adaptor configuration for the Registered Envelope application, and then repeat the steps for the Registered Envelope Throttled application.

To modify the SMTP Adaptor configuration for the Registered Envelope application:

1. In the Administration Console, click the Configuration tab and select the Expert view in the drop-down menu.
2. Navigate to Configuration > SMTP Adaptor > Router RuleSets > encrypt > Applications.
3. Click the link for the Registered Envelope application.
4. On the Details tab, select CRES in the Envelope drop-down menu.

   When you select CRES, you change the envelope profile that is used to generate Registered Envelopes.
5. In the Opener Host field, change the opener host to the following value:

   `res.cisco.com`
6. In the GPT URL field, change the Get Payload Transport URL to the following value:

   `https://res.cisco.com`
7. In the GPT Token drop-down menu, select the token that you uploaded to the appliance. The token name has the following format:

   token<*account_number*>:<*token_ID*>

   If you have only uploaded one token file to the appliance, the uploaded token appears below the Default:1 token in the drop-down menu.
8. In the "Jump to tab" drop-down menu, select Registered Envelope, and click **Go.**
9. On the Registered Envelope subtab, change the Key Server Host field to the following value:

   `res.cisco.com`
10. In the Key Server Internal URL field, delete the existing value, and leave the field blank.
11. In the Authentication Token drop-down menu, select the token that you uploaded to the appliance.

12. In the "Jump to tab" drop-down menu, select Secure Response, and click **Go.**
13. On the Secure Response subtab, change the host to the following value:

    `res.cisco.com`
14. (Optional) Select check boxes for Secure Reply, Secure Reply to All, and Secure Forward to enable these features for the Cisco Registered Envelope Service account.
15. In the Encryption Token drop-down menu, select the token that you uploaded to the appliance, but *do not* select the "Use Token for Registered Envelopes" check box.
16. Click **Deploy Changes.**

Configuring the Registered Envelope Throttled Application

After you change the configuration for the Registered Envelope application, you need to make the same changes to the Registered Envelope Throttled application.

To modify the SMTP Adaptor configuration for the Registered Envelope Throttled application:

1. In the Administration Console, click the Configuration tab and select Expert view in the drop-down menu.
2. Navigate to Configuration > SMTP Adaptor > Router RuleSets > encrypt > Applications.
3. Click the link for the Registered Envelope Throttled application.
4. On the Details tab, select CRES in the Envelope drop-down menu.

   When you select CRES, you change the encryption profile that is used to generate Registered Envelopes.
5. In the Opener Host field, change the opener host to the following value:

   `res.cisco.com`
6. In the GPT URL field, change the Get Payload Transport URL to the following value:

   `https://res.cisco.com`
7. In the GPT Token drop-down menu, select the token that you uploaded to the appliance. The token name has the following format:

   token<*account_number*>:<*token_ID*>

   If you have uploaded only one token file to the appliance, the uploaded token appears below the Default:1 token in the drop-down menu.
8. In the "Jump to tab" drop-down menu, select Registered Envelope, and click **Go.**
9. On the Registered Envelope subtab, change the Key Server Host field to the following value:

   `res.cisco.com`
10. In the Key Server Internal URL field, delete the existing value, and leave the field blank.

11. In the Authentication Token drop-down menu, select the token that you uploaded to the appliance.
12. In the "Jump to tab" drop-down menu, select Secure Response, and click **Go.**
13. On the Secure Response subtab, change the host to the following value:

    `res.cisco.com`
14. (Optional) Select the check boxes for Secure Reply, Secure Reply to All, and Secure Forward to enable these features for the Cisco Registered Envelope Service account.
15. In the Encryption Token drop-down menu, select the token that you uploaded to the appliance, but *do not* select the "Use Token for Registered Envelopes" check box.
16. Click **Deploy Changes.**

CHAPTER 9

Configuring Mobile Device Support

This chapter contains the following sections:

OVERVIEW

If you use the IronPort Encryption appliance to generate envelopes—for example, Secure Reply envelopes—then you might want to configure the appliance to support envelopes received on mobile devices.

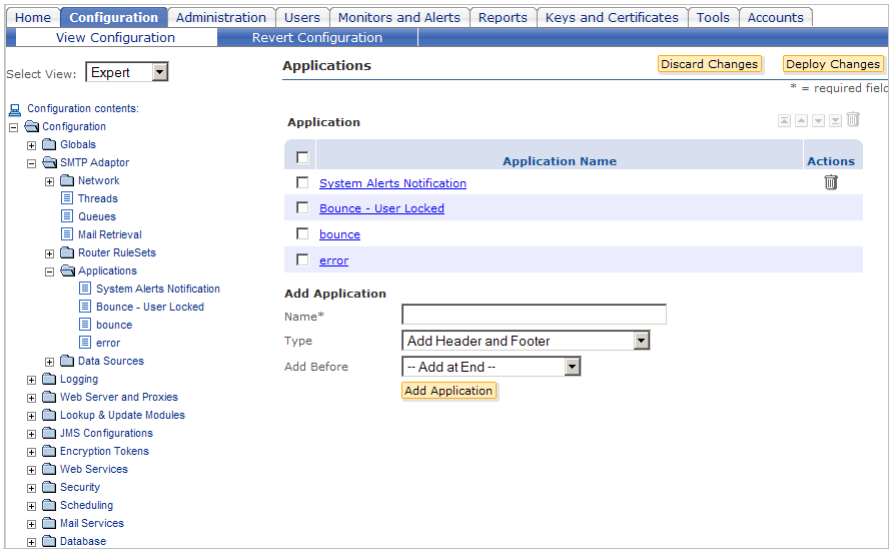
Configuring mobile device support involves the following tasks:

- **Create a Mobile Device Support application.** You create an application to support opening envelopes on mobile devices. For more information, see "Creating the Mobile Device Support Application" on page 119.
- **Create a Mobile Device Support rule.** You create a rule to route messages to the Mobile Device Support application when recipients forward messages to a specified email address (for example, `mobile@domain.com`). For more information, see "Creating the Mobile Device Support Rule" on page 121.
- **Modify the branding.template.properties file.** You modify the properties file to change the mobile device support email address that appears in notification messages sent to recipients. For more information, see "Modifying the branding.template.properties File" on page 123.

CREATING THE MOBILE DEVICE SUPPORT APPLICATION

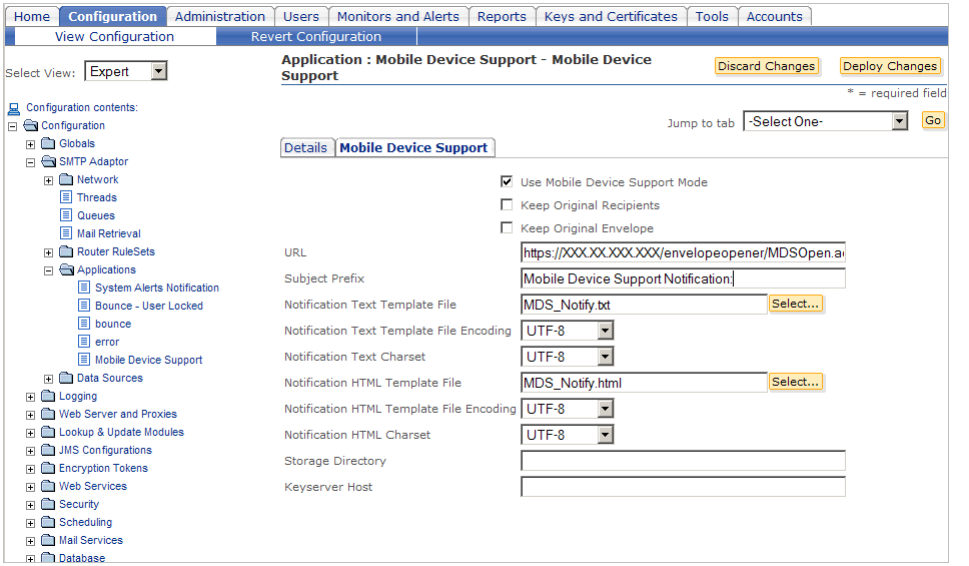
To create the Mobile Device Support application:

1. In the Administration Console, click the Configuration tab and select Expert view.
2. Click SMTP Adaptor > Applications.



3. In the Add Application area, enter `Mobile Device Support` in the Name field.
4. Select Envelope Opener as the application type, and click **Add Application.**

5. In the list of applications, click the link for the Mobile Device Support application, and then select the Mobile Device Support tab.

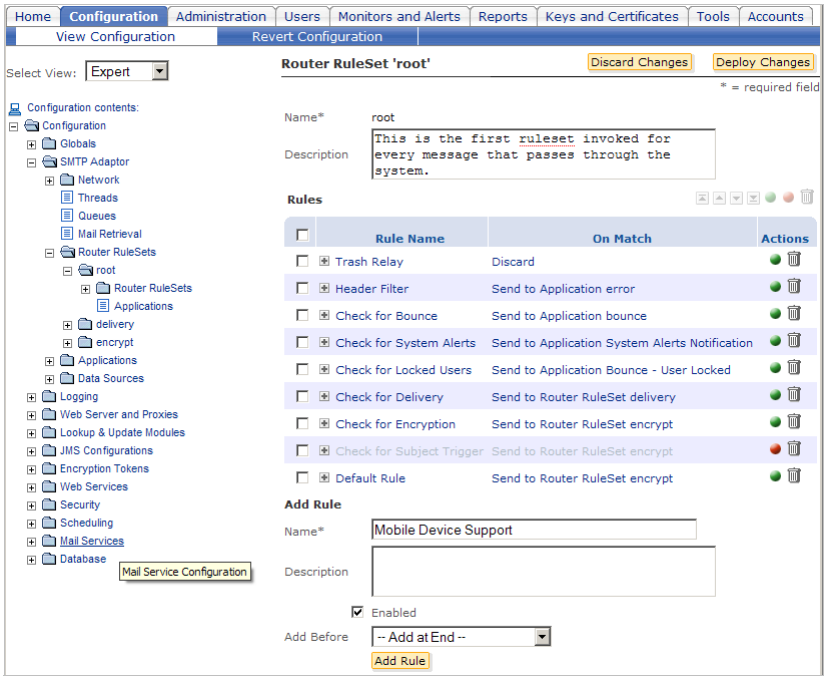


6. Select the check box labeled “Use Mobile Device Support Mode.”
7. In the Subject Prefix field, enter descriptive text for the subject line; for example: `Mobile Device Support Notification:`
8. Click **Deploy Changes** and then click **Restart SMTP Adaptor.**

CREATING THE MOBILE DEVICE SUPPORT RULE

To create the Mobile Device Support rule:

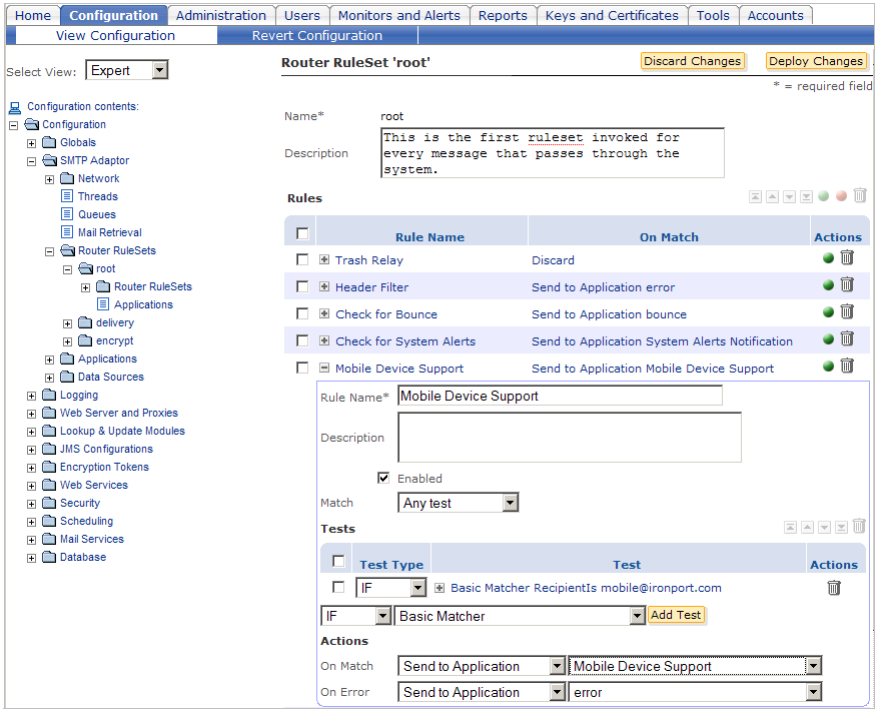
1. In the Administration Console, click the Configuration tab and select Expert view.
2. Click SMTP Adaptor > Router RuleSets > root.



3. In the Add Rule section, enter `Mobile Device Support` as the name.
4. In the Add Before drop-down list, select "Check for Locked Users."
5. Click **Add Rule.**
6. In the list of rules, click the plus sign (**+**) for the Mobile Device Support rule.
7. Click **Add Test.**
8. Click the plus sign (**+**) for the Basic Matcher All test.

9. Configure the test as follows:
   a. Select RecipientIs for the matcher name.
   b. For the matcher condition, enter the following string:
      `mobile@your_domain.com`

      When recipients forward messages to this address, the rule is triggered.



10. In the Actions area, configure the On Match action so that the left-hand drop down list displays “Send to Application” and the right-hand drop-down list displays “Mobile Device Support.”
11. Click **Deploy Changes** and then click **Restart SMTP Adaptor.**

MODIFYING THE BRANDING.TEMPLATE.PROPERTIES FILE

After you create the Mobile Device Support application and the Mobile Device Support rule, you need to modify the branding.template.properties file on the appliance. You modify the properties file to specify the Mobile Device Support email address that appears in notification messages. When you specify the email address that appears in notification messages, you use the same address that you used in the matcher condition of the Mobile Device Support rule.

To modify the branding.template.properties file:

1. Log in to the appliance as the admin user.
2. At the main menu, enter `x` to exit the shell.
3. Enter the following command to change the directory:
   `cd /usr/local/postx/server/conf/`
4. Enter the following command to edit the branding.template.properties file:
   `vi branding.template.properties`
5. Change the `mobile.email` variable to match the email address you entered in step 9 of the preceding procedure. (The default value is mobile@res.cisco.com.)
6. Save the branding.template.properties file.

CHAPTER 10

EJBCA Support for the IronPort Encryption Appliance

This chapter contains information on configuring Enterprise Java Bean Certificate Authority (EJBCA) support for the IronPort Encryption appliance.

This chapter contains the following sections:

ABOUT EJBCA

Enterprise Java Bean Certificate Authority (EJBCA) is a fully functional certificate authority based on J2EE technology. It constitutes a robust, high performance and component based Certificate Authority (CA). Flexible and platform independent, EJBCA can be used as a standalone or can be integrated in any J2EE application.

EJBCA is an enterprise class Public Key Infrastructure (PKI); it can be used to build a complete PKI infrastructure for organizations.

PROXY CERTIFICATE GENERATION

EJBCA integrated with the IronPort Encryption appliance is a solution for proxy certificate generation without the hassles of using an external CA. The IronPort Encryption appliance uses proxy certificates. If a policy needs a certificate either for signing or for encryption and the sender/recipient does not have a digital certificate, the IronPort Encryption appliance can use an external certificate authority to generate a proxy certificate for them. The proxy certificate configuration of the IronPort Encryption appliance has been tested with Microsoft Certificate Server (MSCA).

CONFIGURING THE IRONPORT ENCRYPTION APPLIANCE WITH EJBCA SUPPORT

EJBCA integration with the IronPort Encryption appliance is passive and does not interfere in any workflow related to the IronPort Encryption appliance. The presence of EJBCA is transparent (invisible) to administrators and users unless it is deployed and installed. EJBCA is currently only supported on JBOSS application server deployments.

Deploying

To deploy the EJBCA integration for the IronPort Encryption appliance:

1. Navigate to the folder `<home>/bin/ejbca/` and locate the file ejbca.properties in this directory.
2. Customize the properties in this file. The comments in the properties file explain the usage of each property along with the list of acceptable values. The default values for the database properties generate the database configuration for a Hypersonic database. The following is a list of properties in the file:
    - **ca.name –** Common Name of the CA.
    - **ca.dn –** Subject DN of the CA certificate.
    - **ca.keysize –** Key size (in bits) of the CA Key.
    - **ca.validity –** Validity period (in days) of the CA certificate.
    - **ca.policy –** Policy OID of the CA (if any); 'null' if none exists.
    - **database.name –** Name of the database to be used. Supported values are hsqldb, mysql, postgresql, sqlserver2000 and Oracle. The default value is hsqldb.
    - **datasource.mapping –** The data source mapping selected for the deployment. Supported values are Hypersonic SQL, mySQL, PostgreSQL 8.0, MS SQLSERVER2000 and Oracle9i. The default value is Hypersonic SQL.
    - **database.url –** Database connection URL. The default value is: `jdbc:hsqldb:hsql://localhost:1701`
    - **database.driver –** Database driver class name. The default value is: `org.hsqldb.jdbcDriver`
    - **security.realm –** Security realm that needs to be used for connecting to the database. The default value is PostXJDBCDBRealm.
    - **superadmin.dn –** Subject DN of the CA administrator certificate.
    - **superadmin.password –** Password for the CA administrator certificate.
    - **httpsserver.hostname –** Host name of the server on which EJBCA runs.
3. Stop encryption server if it is already running.
4. Run the script ejbcadeploy.sh (ejbcadeploy.bat in Windows). This will reconfigure the .ear file.
5. Copy the reconfigured .ear and the database descriptor to the JBoss deployment directory.

Installing

The installation process creates a root CA certificate and a private key for the CA administrator. To install do the following:

1. Start the encryption server.

   Note — Root (administrator) privileges are required to run the installation script. If root privileges are not available, the JRE keystore fails to get updated.

   Note — Make sure that Unlimited Strength Java (TM) Cryptography Extension Policy Files are available in JRE. If they are not available download the package from Sun Java web site at http://java.sun.com/j2se/1.4.2/download.html. Replace your current local_policy.jar and US_export_policy.jar files in `JAVA_HOME/jre/lib/security` with the downloaded files.

2. Run the script ejbcainstall.sh (ejbcainstall.bat in Windows).
3. This script takes the JRE keystore password as a parameter. (The default keystore password for Sun JRE is "*changeit*".) For example, run the script as:

   ```
   $ sh ejbcainstall.sh changeit
   ```

4. This script generates the rootca certificate and the superadmin private key in `<home>/conf/ejbca/p12/`. It also imports the root CA certificate to the JRE keystore.
5. Restart the encryption server.
6. Import the superadmin.p12 file to the browser from where the EJBCA administration screen will be accessed. The password for this p12 file can be configured in ejbca.properties file.

Testing the Deployment and Installation

To test the deployment and installation:

1. Open the URL `http://localhost:8080/ejbca/` (Substitute localhost by your hostname). This displays the EJBCA home page.
2. Click the administration link. This uses the imported superadmin.p12 file for logging into EJBCA.

DATABASE CREATION

The EJBCA packaged with the IronPort Encryption appliance supports the following databases:

- Hypersonic (HSQLDB)
- MySQL
- PostgreSQL 7.4
- Microsoft SQL Server
- Oracle 9
- Oracle 10

Creating Database Tables

EJBCA automatically creates the tables required for its operation provided sufficient privileges (Table creation privileges) are given to the Database Realm in which it operates (PostXJDBCDBRealm).

You can also create database tables manually. Run the script `<home>/bin/ejbca/runejbcaddl.sh` (`runejbcaddl.bat` in Windows) for creating and dropping database tables. You should provide the script with arguments that specify the required command (create/drop), database connection URL, username, password and database name.

Note — Currently, creation script are provided for only MySQL and PostgreSQL databases.

UNINSTALLING EJBCA

Uninstalling EJBCA from the IronPort Encryption appliance is a two-step process: deleting the files created during EJBCA installation, and cleaning up the database tables created by EJBCA. The following sections describe them in detail.

Deleting EJBCA Related Files

A shell script - ejbcacleanup.sh (ejbcacleanup.bat in Windows) is available at `<home>/bin/ejbca/`. Run this script after stopping the encryption server. It deletes all the files which EJBCA creates during installation.

The files are:

- `<home>/jboss/server/postx/deploy/ejbca.ear`
- `<home>/jboss/server/postx/deploy/ejbca-ds.xml`
- `<home>/conf/ejbca/`

Cleaning Up the Database

A database cleanup script, runejbcaddl.sh (runejbcaddl.bat in Windows), is available for deleting the tables which EJBCA creates. Locate this script at `<home>/bin/ejbca/.` Provide the script with the arguments that specify the required command (create/drop), database connection URL, username, password and database name.

Note: Currently the deletion script supports only MySQL and PostgreSQL databases.

CHAPTER 11

Internationalization Support

This chapter contains the following sections:

OVERVIEW

The IronPort Encryption appliance can be configured to read I18N data and send emails with different charsets through the Administration Console. Secure Envelopes and related message template files can be internationalized by creating internationalization versions of these files in corresponding local directories.

The encryption server includes a CharsetLocaleMap.txt file located in the conf directory. This file can be used to map the incoming email charset to a specific locale. Each record of the file has the following format:

```
Charset         LanguageCode CountryCode      Variant      FileCodeSet

iso-2022-jp     ja           JP               -              -
```

Note — FileCodeSet is not used currently and is for future use only.

For each application, the parent directory for envelope files is the one specified in the EnvelopeDir config entry. The directory for I18N envelope files is constructed as "<EnvelopeDir>/<LanguageCode>/<CountryCode>/<Variant>", where these values are read from applicable locale information. If the relevant locale directory does not contain the files, the system will go up the directory hierarchy till it finds the files. Using the above example, the envelope files will be read from the directory "default_envelope/ja/JP" or "default_envelope/ja". The root directory "EnvelopeDir" will continue to have US-ASCII files requiring no change for the english (non-I18N) version.

CONFIGURING FOR I18N

To configure the IronPort Encryption appliance to support I18N, you must do the following steps:

- Add/Change Envelope Files
- Add/Change Message Template Files
- Add Entries to CharsetLocalMap.txt
- Edit configurations parameters

Adding/Changing Envelope Files

Per the previously mentioned directory structure, you can add locale directories and localize envelopes in the envelope directory (for example, samples/registered_envelope). It is recommended that these files be in the UTF-8 encoding format.

Adding/Changing Message Template Files

Per the previously mentioned directory structure, you can add locale directories and localize message template files into the conf directory. The files that must be modified are: PostXMessage.txt, PostXMessage.html, and textbodytemplate.html, and messagebar/messagebar.html. If adding a new directory, for example ja, copy these files and modify them for that locale. It is recommended that these files be in the UTF-8 encoding format.

Adding entries to CharsetLocaleMap.txt File

Edit the CharsetLocaleMap.txt file to include entries for all of the charset encodings that you want to support. Please ensure that the locale entries have their corresponding directories and localized files as listed above.

CONFIGURATION PARAMETERS FOR I18N

The following configuration parameters are I18N specific.

Application Level

Click the Configuration tab and then click Configuration > SMTP Adaptor > Applications > *Application_Name* > Details tab. The following configuration parameters are I18N specific.

Parameter	Definition
Use Charset For Locale Mapping	Check this option if you want to select the locale and corresponding envelope and message template files based on the charset of the incoming email. The encryption server will use the mapping file to select entries corresponding to the email charset. For example, the encryption server supports English and Japanese locales. By enabling this option, if the incoming email is in English it will map to the English locale. Conversely, if the incoming email has the charset as Shift-JIS (or ISO-2022-JP) it will map the Japanese locale. Both these entries have to exist in the CharsetLocaleMap.txt file.
Bounce Unsupported Charsets	If selected, this option results in incoming emails with unsupported charsets (no corresponding entry in the map file) to be bounced back instead of using the DefaultLocale. This entry is valid only if UseCharsetToLocaleMapping is selected. Using the above example, if you get an email with the charset as "ks_c_5601-1987" with this option enabled the email will be bounced back to the sender with appropriate messages.
Default Locale	Specifies the default locale to be used in selecting envelope and related template files. The default value is "en_US" and can be changed to any supported locale by the server. If UseCharsetToLocaleMapping is not selected above, the default locale will represent the locale for all incoming emails. Similarly if that option is selected, and BounceUnsupportedCharsets is not selected, then the default locale will be used for all incoming emails that don't map to any specific locale in the mapping file.
Envelope Date Format	This parameter allows you to choose the format for the date stamp shown on the Secure Envelope. It could be selected as one of the standard four formats ("dd-mm-yyyy", "mm-dd-yyyy", "yyyy-mm-dd" or "yyyy-dd-mm") or "Use locale" which allows the date formatting to be based on the locale selected for each incoming email.

Parameter	Definition
Envelope Time Format	This parameter allows you to choose the format for the time stamp shown on the Secure Envelope. It could be selected as one of the different hour, minute and second combinations or "Use locale" which allows the time formatting to be based on the locale selected for each incoming email.

Message Personalization

Click the Configuration tab and then click Configuration > SMTP Adaptor > Applications > *Application_Name* > Message Personalization. The following configuration parameters are I18N specific.

Parameter	Definition
Outgoing Text Body File Encoding	Specifies the file encoding for the Message Template File entry. The default is "ISO-8859-1". Similar to the EnvelopeFileEncoding parameter above, if you want to use I18N data for the email message, it is recommended that the file be saved in UTF-8 file encoding format and that you select UTF-8 for this parameter.
Outgoing Text Body Charset	Character set of text part of outgoing message body.
Outgoing Text Body Content-Transfer-Encoding	Content-Transfer-Encoding of text part of outgoing message body.
Outgoing HTML Body File Encoding	Character encoding to use when reading Outgoing HTML Body File.
Outgoing HTML Body Charset	Character set of HTML part of outgoing message body.
Outgoing HTML Body Content-Transfer-Encoding	Content-Transfer-Encoding of HTML part of outgoing message body.
Envelope Message Template File Encoding	The character encoding used for the template file.
Attachment Encoding	Content transfer encoding of the outgoing attachment. Values are 7bit, 8bit, base64, and quoted-printable. It is strongly recommended that you leave this value as the default, which is base64.

Envelope Level

Click the Configuration tab and then click Configuration > SMTP Adaptor > Envelopes > *Envelope_You_Are_Using*. The following configuration parameter is I18N specific.

Parameter	Definition
Envelope File Encoding	Specifies the file encoding for envelope files pointed to by the EnvelopeDir directory. The default for this parameter is "ISO-8859-1." If the envelope files contain I18N data, it is recommended that these files be saved in UTF-8 file encoding format and that you select UTF-8 for this parameter.

Reply-Message

Click the Configuration tab and then click Configuration > Web Services > SecureResponse > Response-Message. The following configuration parameters are I18N specific.

Parameter	Definition
Email Charset	Specifies the charset to be used for the body of the secure reply email.
Email Content Encoding	Specifies the content-transfer-encoding to be used for the secure reply email body. I18N data typically requires using a content-transfer-encoding other than 7-bit. It is recommended that you use Base64.
Attachment Content Encoding	Specifies the content-transfer-encoding to be used for the attachment file included in the secure reply email. It is recommended that you use Base64 or Base on Content.
Convert SingleByte Kana to DoubleByte Kana	Applies only if the I18N data under consideration is Japanese data with the charset of "ISO-2022-JP". With this option selected, the secure-reply web service will convert the reply email data entered from single byte kana to double byte kana before it is sent as an email.

Return Receipt

Click the Configuration tab and then click Configuration > Web Services > KeyServer > Return Receipt. The following configuration parameter is I18N specific.

Parameter	Definition
Mail Body Charset	Specifies the charset to be used for the return receipt that is sent for registered envelopes. The default is “ISO-8859-1.”

CHAPTER 12

Configuring the Key Server

This chapter contains the following sections:

OVERVIEW

The key server provides an additional way to deliver Secure Envelopes. The symmetric key used for encryption is stored in a server repository. When a recipient opens a Secure Envelope sent with this delivery option, the recipient enters a password, which is then used to retrieve the encryption key from the key server. This delivery method provides greater security and more control for the sender at the enterprise level. It also provides a return receipt functionality so the sender can see when a recipient opens the envelope.

The key server can also be configured to authenticate the sender with the registration database. This option is specified as an additional URL parameter in the requests sent to generate and open envelopes. If specified, the sender is authenticated with the registration database. This is typically used in conjunction with the Desktop Solution products, which support generation and automatic opening of Registered Envelopes. This feature is not used when the encryption server generates Registered Envelopes or when recipients open Registered Envelopes in a web browser.

KEY SERVER DATABASE

You must configure the system to point to the key server source to use. To specify the key server source:

1. Click the Configurations tab and navigate to Configuration > Web Services > KeyServer > KeyServerDB.
2. Edit the configuration parameters to specify the Java Naming and Directory Interface (JNDI) provider and factory used to look up the key server database.

Parameter	Definition
DataSource Prefix	JNDI namespace prefix used to look up the DataSource.
DataSource Name	Name of the DataSource used for the keystore database (This is a drop down combo box of all the DataSources that are configured under DSDataSources).
DataSource User Name	Not currently used.
Database Password	Not currently used.
Database Table Name	Database tablename where the keystore is stored.
Factory	JNDI Factory Class. This Factory Class is used for JNDI lookup and should correspond to the Provider URL specified below.
Provider	The URL that points to the JNDI Provider to use for JNDI lookup.

3. Click the **Deploy Changes** button.

LOOKUP

Use the Lookup node to specify the following parameters:

Parameter	Definition
Sender Lookup Provider	Specifies the lookup module used to verify whether the sender is enrolled when a Registered Envelope is sent.
Recipient Lookup Provider	Specifies the lookup module used for verifying whether the recipient is enrolled when a Registered Envelope is sent.

MAIL SERVER

Use the Mail Server node define the mail server configuration. Applications and services that send mail, such Secure Mailbox, use a mail service. You can define multiple mail services for use by different applications. For example:

SecureMailboxMail = localhost:25

BillingMail = mail.xyz.com:25

The Mail Service Name drop-down list is populated when you add a mail service (click the Configurations tab and navigate to Configuration > Mail Services > Mail Service List). For a list of parameters, see Appendix A, “Configuration Parameters,” on page 239.

RETURN RECEIPTS

You can configure the system to send a return receipt when a Registered Envelope is opened. To do this, modify the Mail Body Charset, Email Subject, and Template File configuration parameters.

SENDER AUTHENTICATION

Use the Sender Authentication node (Configuration > Web Services > KeyServer > Sender Authentication) to set the parameters for authenticating the client to the key server.

Parameter	Definition
Session Timeout	Idle timeout value for the authentication session if used in context of the key server. (Default = 1200)
Single Sign On Authentication Manager	Authentication provider to use for certificates, cookie and single sign-on. This parameter is only relevant when using Desktop Solutions.
Username and Password Authentication Manager	Authentication provider to use for username/password authentication.
Max Password Retries	Maximum number of times the sender is allowed to retry entering their password until they are locked out.
Denied Network Addresses	A comma separated list of network addresses that will be denied access to the application.
Allowed Network Addresses	A comma separated list of network addresses that will be denied access to the application.

RECIPIENT AUTHENTICATION

Use the Recipient Authentication node (Configuration > Web Services > KeyServer > Recipient Authentication) to set the parameters for authenticating the recipient to the key server. The value configured here is a default. It is overridden by the value configured on the Registered Envelope tab of an IronPort Encryption appliance application. It generally will only be used by Desktop Solution, and even then it can be overridden (in the plug-in configuration).

ENVELOPE

Use the Envelope node (Configuration > Web Services > KeyServer > Envelope) to set the parameters for the envelope, including poll parameters.

Parameter	Definition
Check Access Rules	Check access rules using a key server token.
Access PostX Registration Data	Is user registration information stored in the IronPort Encryption appliance database.
Enable Traffic Encryption	Enable encryption of data passing between the key server and the envelope using a random key.
Validate Email Addresses	When checked, the key server validates all email addresses it receives before using them. When unchecked, it trusts the email addresses to be legitimate. The default is checked.
Maximum Open Attempts	Maximum attempts a user can make to open a registered envelope before it is locked. Note that some authentication providers have a similar configuration.
Minimum Message Security	Lowest message security level that will be allowed. Any message with a message level lower than this value will be rejected and either spooled or bounced.
Envelope Poll Parameters	
Keyserver Wait Interval	Number of milliseconds the server will wait for results before closing the connection.
Minimum Poll Interval	Minimum number of milliseconds the envelope will wait between poll requests.
Maximum Poll Interval	Maximum number of milliseconds the envelope will wait between poll requests.
Total Wait Time	Total Number of milliseconds the envelope will wait for a valid response from the key server.

NOTIFICATION

Use the Notification node to set the parameters that define whether notifications are sent to non-enrolled recipients and senders. Use this node to further define the notification template file, notification URL, and so forth. To configure notification, click the Configuration tab and navigate to Configuration > Web Services > KeyServer >Notification. Configuration parameters include:

Parameter	Definition
Registration URL	Registration URL that is provided in the register notification email. The value can be overridden on a per-application basis by changing the corresponding value under the Registered Envelope tab of the Registered Envelope application. The default value is: `https://<encryption_server>/websafe/register`
Change Expired Password URL	URL of the page to which the key server directs a user whose password has expired. If password expirations are not enforced, then this will have no effect. The value can be overridden on a per-application basis by changing the corresponding value under the Registered Envelope tab of the Registered Envelope application. The default value is: `https://<encryption_server>/websafe/custom.action?cmd=changeExpiredPassword`

MASTER KEYS

This feature allows you to have a global master key or a master key for each recipient domain.

Configuring a Global Master Key

To enable this feature, select the "Enable Master Keys" option and then enter a global master key. Subsequently, any recipient from any domain can open a Registered Envelope with the global master key.

Configuring a Domain-Specific Master Key

You can also enter a master key for each domain (for example, one for "Yahoo.com" and a separate one for "aol.com"). To do this, perform the following steps:

1. Click on the Configuration tab and navigate to Configuration > Web Services > KeyServer > MasterKeys > Domain Master Keys.
2. Enter a name to designate the new domain/master key combination and click the **Add DomainMasterKeys** button.
3. Navigate to the newly added domain master key and enter the Domain Name and Master Key value for that domain.

Subsequently any recipient from that domain (for example, yahoo.com) can open a Registered Envelope using the entered master key for the "Yahoo.com" domain.

This feature is best if you are using gateway-level decryption of Registered Envelopes. For example, XYZCorp could have an encryption server that receives all inbound envelopes for XYZCorp recipients. Using the configured Registered Envelope Opener application, it can decrypt all envelopes using the specified master key. The key specific to this application should match the domain master key or global master key used by the sending encryption server. This eliminates the necessity for the gateway server to have access to individual recipient passwords.

An important point is that this works in conjunction with decrypting the message with a per recipient password. So a Registered Envelope sent with the master key enabled for a domain will open using the recipient's personal password as well as the domain or global master key.

CHAPTER 13

Configuring Lookup and Update Modules

This chapter contains the following sections:

OVERVIEW OF LOOKUP AND UPDATE REPOSITORIES

Lookup repositories allow you to access data in external datasources, while update repositories allow you to update data in external datasources. You can choose to use the pre-defined lookup or update repositories and simply configure them to your specific requirements, or you can elect to add new repositories.

The IronPort Encryption appliance includes the following predefined lookup repositories:

- LDAP
- User
- Database
- Chained
- PK3I
- CMP
- PKCS10
- MSCA
- PGP
- HKP
- Custom

The IronPort Encryption appliance includes the following predefined update repositories:

- LDAP
- User
- Database
- Chained
- PGP

For information about specific lookup and update repositories, see the following sections.

WHY WOULD I WANT TO ADD MULTIPLE REPOSITORIES OF THE SAME TYPE?

Typically, you add multiple lookup repositories if you are using multiple instances of the same lookup and need to configure them individually. For example, if you are retrieving information from two LDAP compliant directories, you would need to create two new lookup repositories. The same holds true for adding new update modules.

LOOKUP REPOSITORIES

This section describes the various lookup repositories and their parameters. To view and edit look up repositories, click the Configuration tab and then navigate to Configuration > Lookup Update Modules > Lookup Modules.

LDAP Lookup Repository

The IronPort Encryption appliance can be configured to retrieve an encryption key or certificate for a recipient from any LDAP-compliant directory. To configure the LDAP-compliant directory as a lookup provider, a LDAP lookup repository containing the LDAP lookup information is needed. If a LDAP lookup repository does not currently exist, you must add one.

Parameter	Definition
Name	Name of the LDAP Lookup Repository.
Connect Securely	Select to allow a secure (that is, SSL) connection to the LDAP server.
Server Name	Name of the LDAP server.
Port Number	TCP/IP port of the LDAP server.
Logon to Server	If checked, the LDAP server requires logging on to perform reads and updates.
User Name	User account used to log in to the LDAP server.
User Password	User password used to log in to the LDAP server.
RootDN	The base distinguished name (DN) against which all lookups and searches are carried out, for example “dc=ironnport,dc=com” or “o=IronPort,c=US”.
Query String	A simple expression that yields the query string used to identify a user in LDAP lookup requests. This parameter is only used in lookups, it is *not* used in searches. For example “cn=${identity}”, where ${identity} is the value the application obtains from the MIME message using the application’s Key Lookup Identity configuration parameter.

Parameter	Definition
Enable Directory Search	Enables the use of LDAP searches instead of using lookups. Lookups are better, but can only be used when the users can be identified by their distinguished name. When you want to use the user's email address in order to identify them, you must use a search by selecting this and setting the Search String value appropriately.
Enable Subtree Search	Enables the use of LDAP subtree scope while searching for a user.
Enable Proxy Certificate Search	Enables the use of proxy certificate searches.
Search String	A simple expression that yields the query string used to search the LDAP directory. This parameter is only used in searches, it is not used in lookups. For example "mail=${identity}", where ${identity} is the value the application obtains from the MIME message using the application's Key Lookup Identity configuration parameter.

Attribute Names

Parameter	Definition
Certificate Type	The type of certificate that is stored in the LDAP field.
Password Attribute	The LDAP schema name of the password attribute that is returned by the LDAP server in response to lookup requests and searches. For example "userPassword".
Password Attribute Alias	LDAP subtype or alias name that is the attribute name actually returned by the LDAP server when a Password Attribute is requested.
PKCS7 Certificate Attribute	LDAP schema name of the attribute used to hold the user's PKCS #7 public key certificate.
PKCS12 Certificate Attribute	LDAP schema name of the attribute used to hold the user's PKCS #12 private key certificate.
PKCS12 Certificate Password Attribute	LDAP schema name of the attribute used to store the password value that was used to encrypt the PKCS #12 certificate.
PGP Certificate Attribute	LDAP schema name of the attribute used to hold the user's PGP public key certificate.

Sender Policies

Parameter	Definition
Check Sender Policy	Determines whether to check the policy for the email sender or not.
Sender Role Attribute	The LDAP sender attribute that contains its role.
Sender Role Attribute Alias	LDAP sender attribute alias that contains its role.
Sender Query String	LDAP query to perform to lookup the sender's role.
Enable Search for Sender	Determines whether to perform a search for the sender's role attribute or just a lookup.
Sender Search String	LDAP attribute used to perform a search for the sender's identity.

Parameter	Definition
Role Value for SendAll Permission	The value for the sender's role for SendAll type permission.
Allow Partial Match for SendAll	Determines whether a sub-string match or exact match is required to compare the send all value to the sender's role.
Role Value for SendRestricted Permission	The value for the sender's role for SendRestricted type permission.
Allow SendRestricted Partial Match	Determines whether a sub-string match or exact match is required to compare the send restricted value to the sender's role.
Enable Search sender domain	Determines whether to perform a search for the sender's restrict domain attribute or just a lookup.
Domain List Attribute	The attribute that contains a list of domains that the sender is restricted to be able to send or not send to.
Domain List Attribute Alias	The alias for the domain list attribute.
Action for Restricted Send	The action to perform (Send or NoSend) if the recipient's destination host address matches an address on the restricted domain list.
Role Value for SendNone Permission	The value for the sender's role for SendNone type permission.
Allow Partial Match for SendNone	Determines whether a sub-string match or exact match is required to compare the send none value to the sender's role.
Default Sender Role	If the sender's role cannot be found in the LDAP server, the default policy value. This is either SendAll, SendRestricted, or SendNone.
Certificate is PEM Encoded	Flag that says that the public cert in the LDAP directory is PEM encoded.

Database Lookup Repository

The database can be used to look up the encryption key for the recipient. In order to configure the database as a lookup provider, a database lookup repository containing the

database lookup information is needed. If a database lookup repository does not currently exist you must add one.

Parameter	Definition
Name	Name of the database repository.
DB Datasource JNDI Name	JNDI Name of the datasource used to connect to the DBLookup database.
DB Table Name	Name of the table to be looked up in the database lookup.
DB Key Separator	The separator for multiple password fields.
DB Primary Column	The column used as the db key to obtain the encryption key.
Key Column1	One or more password fields stored in the database.
Key Column2	One or more password fields stored in the database.
Key Column3	One or more password fields stored in the database.
Key Column4	One or more password fields stored in the database.
Enroll Column1	Name of the database field that contains registered status.
Enroll Value1	Value in Enroll Column 1 indicating the recipient is enrolled.
Enroll Column2	Name of the database field that contains registered status.
Enroll Value2	Value in Enroll Column 2 indicating the recipient is enrolled.
Enroll if Password Exists	Determines whether or not to set the registration state to true if the password exists (override the check for the register column and value). Default is checked.
Case Insensitive Lookup	Specifies whether case insensitive lookups are used. Default is not checked.

Chained Lookup Repository

The IronPort Encryption appliance can be configured to use multiple sources to look up the encryption key for the recipient. To use the chained lookup provider, two or more lookup repositories (any combination of LDAP, Database, or User Lookups) must be configured.

Parameter	Definition
Name	Name of the chained repository.

PK3I Lookup Repository

The IronPort Encryption appliance can be configured to request a certificate from a certificate authority on behalf of a recipient who does not already possess one. The request is made via the CMP protocol to a certificate server that supports certificate generation.

Parameter	Definition
Name	Name of the PK3I lookup module.
URL Protocol	Protocol used to access the PK3I server.
URL Host	Host name of the PK3I server.
URL Port	PK3I server port that listens for PK3I requests.
Request Path	Path used to submit request to RSA Server.
Request Token	Request token.
Version	Version number.

Email Attributes

Parameter	Definition
Email Pin To Sender	Select to send an email to the certificate requester.
Encrypt Pin Email	Select to encrypt the PIN email.
Email Subject	Subject of the PIN email.
Email Template File	Template file for the body of the PIN email.
Email Sender Template File Encoding	Encoding used to read the template file.
Email Sender Template Charset	Charset used for the email that the file becomes.
Mail Service Name	Mail service for sending the email period.
PostMaster Email Address	Sender of the email period.

CMP Lookup Repository

The IronPort Encryption appliance can be configured to request a certificate from a certificate authority on behalf of a recipient who does not already possess one. The request is made via the CMP protocol to a certificate server that supports certificate generation.

Parameter	Definition
Name	Name of the CMP lookup module.
Protocol	Protocol used to access the CMP server.
Host	Host name of the CMP server.
Port	Server port that listens for CMP requests.
Certificate Pickup URL	URL for picking up the certificate.
Shared Secret Key	Name of the secret used for making a valid CMP request.
Shared Secret Value	The value of the secret used for making a valid CMP request.
Shared Secret Salt	Salt value for encrypting the secret.
Shared Secret Encoding Iterations	Number of iterations used to encrypt the secret.

Parameter	Definition
KeyUpdateProvider	Update Module used to store the requested certificate.

Email Attributes

Parameter	Definition
Email Pin To Sender	Select to send an email to the certificate requester.
Encrypt Pin Email	Select to encrypt the requester's email.
Email Sender Subject	Subject of the PIN email.
Email Sender Template File	Template file for the body of the requester's email.
Email Sender Template File Encoding	Encoding used to read the template file.
Email Sender Template Charset	Charset used for the email that the file becomes.
Email To Recipient	Allows email notification of certificate request to be turned off for recipient.
Email Recipient Subject	Subject for the certificate request email
Email Recipient Template File	Template file for the certificate request email
Email Recipient Template File Encoding	Encoding used to read the template file.
Email Recipient Template Charset	Charset used for the email that the file becomes.
Mail Service Name	Mail service for sending the email.
PostMaster Email Address	Sender of the email.

Certificate Attributes

Parameter	Definition
Organization	Certificate owner's organization.
Organizational Unit	Certificate owner's organizational unit.
City	Certificate owner's city.
State	Certificate owner's state.
Country	Certificate owner's country.

PKCS10 Lookup Repository

The IronPort Encryption appliance can be configured to request a certificate from a certificate authority on behalf of a recipient who does not already possess one. The request is made via the PKCS10 protocol to a certificate server that supports certificate generation.

Parameter	Definition
Name	Name of the lookup module.
URL Protocol	Protocol used to access the server.
URL Host	Host name of the server.
URL Port	Server port that listens for requests.
Certificate Pickup URL	URL for picking up the certificate.
Request Path	Path used to submit request to Server.

PKCS10 Request Parameter Name	Parameter values necessary to submit the request to the Server.
	`The default value is:`
	`domainID=8a12d649003200e9224ae0cb003de2175daac43b,CA=41df114e79bbebb0321b4cd35035d3a6,PRO=No Extensions,ManHidden=,ExtHidden=`
	The `domainID` value needs to be changed to match the "Issuing Jurisdiction ID" of the Certificate Authority.
	The `CA` value needs to be changed to match the "Certificate ID" of the Certificate Authority.

Other Request Parameters	Other parameter values necessary to submit the request to the server.
Key Update Provider	Update module used to store the requested certificate.
Key Lookup Provider	Specifies user lookup or certificate lookup.
Use Public Certificate Lookup Provider	Click to enable the use of a lookup to retrieve the public certificate.
Public Certificate Lookup Provider	The lookup used to pickup the public cert that was requested by the lookup itself.

Email Attributes

Parameter	Definition
Email Pin To Sender	Select to send an email to the certificate requester.
Encrypt Pin Email	Select to encrypt the requester's email.
Email Subject	Subject for the PIN email.
Email Sender Template File	Template file for the body of the requester's email.
Email Sender Template File Encoding	Encoding used to read the template file.
Email Sender Template Charset	Charset used for the email that the file becomes.
Email To Recipient	Allows email notification of certificate request to be turned off for recipient.
Email Recipient Subject	Subject for the certificate request email.
Email Recipient Template File	Template file for the certificate request email.
Email Recipient Template File Encoding	Encoding used to read the template file.
Email Recipient Template Charset	Charset used for the email that the file becomes.
Mail Service Name	Mail service for sending the email.
PostMaster Email Address	Sender of the email.

Certificate Attributes

Parameter	Definition
Organization	Certificate owner's organization.
Organizational Unit	Certificate owner's organizational unit.
City	Certificate owner's city.
State	Certificate owner's state.
Country	Certificate owner's country.

MSCA Lookup Repository

Using the MSCA Lookup, you can configure the encryption server to retrieve certificates from

a Microsoft Certificate Authority. MSCA is supported on Windows operating systems only. The recommended way to configure the MSCA Lookup is to first create a new MSCA Lookup. Aside from setting the server, email, and certificate attributes, the KeyUpdateProvider is set to point to certupdate so that certificates retrieved from the MS CA are stored in certupdate. Next a new Chained Lookup should be created with two links. The first link in the chain should point to certlookup so any certificates previously retrieved from the MS CA and the second link should point to the MSCA Lookup that was created and configured. Any applications that wish to use the MSCA Lookup should point to the Chained Lookup for accessing certificates.

Parameter	Definition
Name	Name of the lookup module.
MS CA Server	Server where the MS CA is located including repository in the form host\repository.
Certificate Template OID	The OID of the Certificate Template to use.
MSCert.dll location	Path to the MSCert.dll which contains JNI functions so the IronPort Encryption appliance can call the MS CA Server.
KeyUpdateProvider	Update module used to store the requested certificate, typically certupdate.
Certificate Pickup URL	URL for picking up the certificate.

Email Attributes

Parameter	Definition
Email Pin To Sender	Select to send an email to the certificate requester.
Encrypt Pin Email	Select to encrypt the requester's email.
Email Subject	Subject for the PIN email.
Email Sender Template File	Template file for the body of the requester's email.
Email Sender Template File Encoding	Encoding used to read the template file.
Email Sender Template Charset	Charset used for the email that the file becomes.
Email To Recipient	Allows email notification of certificate request to be turned off for recipient.
Email Recipient Subject	Subject for the certificate request email
Email Recipient Template File	Template file for the certificate request email
Email Recipient Template File Encoding	Encoding used to read the template file.
Email Recipient Template Charset	Charset used for the email that the file becomes.
Mail Service Name	Mail service for sending the email.
PostMaster Email Address	Sender of the email.

Certificate Attributes

Parameter	Definition
Organization	Certificate owner's organization.
Organizational Unit	Certificate owner's organizational unit.
City	Certificate owner's city.
State	Certificate owner's state.
Country	Certificate owner's country.

PGP Lookup Repository

The IronPort Encryption appliance has the ability to look up PGP keys for recipients and

senders. PGP keys can be read from the Certificate Database using a PGP Lookup Repository. You can also use other lookup repository types like “LDAP” and “Database” to lookup PGP keys.

Parameter	Definition
Name	Name of the lookup module.
Lookup Service Name	Name of the EJB service to bind the lookup to.
Key Update Provider	Update module used to store the requested certificate, typically pgpupdate.
Certificate Pickup URL	URL for picking up the certificate.

Email Attributes

Parameter	Definition
Email Pin To Sender	Select to send an email to the certificate requester.
Encrypt Pin Email	Select to encrypt the requester's email.
Email Sender Subject	Subject for the PIN email.
Email Sender Template File	Template file for the body of the sender's email.
Email Sender Template File Encoding	Encoding used to read the template file.
Email Sender Template Charset	Charset used for the email that the file becomes.
Email To Recipient	Allows email notification of certificate request to be turned off for recipient.
Email Recipient Subject	Subject for the certificate request email
Email Recipient Template File	Template file for the email
Email Recipient Template File Encoding	**Encoding that the file is given when it is stored.**
Email Recipient Template Charset	Charset used for the email that the file becomes.
Mail Service Name	Mail service for sending the email
Postmaster Email Address	Sender of the email

Proxy PGP Key Generation

Parameter	Definition
Generate PGP proxy key	If this check box is selected and a particular identity does not have a PGP key registered with the IronPort Encryption appliance, then a proxy PGP key generated.
Renew expired PGP proxy keys	If this check box is selected and an expired proxy PGP key is found, then the IronPort Encryption appliance renews that key. The key pair does not change as a result of the renewal process.

Parameter	Definition
Proxy PGP keys generated are valid forever	If this check box is selected, then the proxy PGP keys generated by the IronPort Encryption appliance have no expiry time. They are valid indefinitely. Note: If 'Proxy PGP keys generated are valid forever' is selected, then 'Validity (in days)' has no effect. If 'Proxy PGP keys generated are valid forever' is *not* selected and 'Validity (in days)' is *not* specified, then a default value of 365 days is used.
Validity (in days)	This positive integer value specifies the validity of proxy PGP certificates generated by the IronPort Encryption appliance.

HKP Lookup Repository

HKP Lookup can be used to lookup PGP public keys from a PGP Public key server. Once a HKP Lookup is configured, it can be used anywhere a PGP Public key is required. Before using a HKP Lookup with an envelope application to send PGP encrypted messages, make sure that the recipient's PGP Public key is uploaded to the PGP key server from which the HKP Lookup is configured to retrieve the keys.

Parameter	Definition
HKP Lookup Name	Name of the HKP Lookup repository.
Base HKPUrl	Base URL of the public key server.
Additional Parameters	Any additional parameters that need to be passed to the key server. These parameters should be in URL Encoded form. The parameters will be appended to the Base URL and a HTTP GET request will be sent to the key server.
Identity Parameter Name	Name of the search parameter that is used by the key server. Typically, this will be 'search'.
Proxy to access HKP Server	Proxy configuration to be used to access the key server.

Custom Lookup Repositories

The custom lookup repository can be used to create customized lookups.

Parameter	Definition
Custom Lookup Name	Name of the lookup repository.
Class Name	Fully qualified name of the custom lookup class.
Config File	Explicit path of the configuration file.

User Lookup Repository

Parameter	Definition
Name	Name of the user repository.
Class	Name of the class that implements the type of lookup. Use com.postx.james.lookup.UserLookup for Secure Mailbox lookup.
Lookup Service Name	Name of the EJB service to which the lookup is bound.
Application Name	Used to identify the AppName, a method for grouping the lookup. Used to group identities in CertLookup.

Note — Generally, you should not change default settings for user lookup unless a Customer Support engineer instructs you to do so.

Adding a Lookup Repository

To add a lookup repository:

1. Click the Configuration tab and then click Configuration > Lookup & Update Modules > Lookup Modules and navigate to the type of repository you want to add.
2. Enter a new repository name and click the **Add Repository** button.
3. Click PostX Config, Lookup & Update Modules > Lookup Modules > *Repository Type* > *New repository name* and configure the newly added repository. Please refer to *Appendix A, Configuration Parameters* for a list of the lookup repository parameters.
4. Click **Deploy Configuration**.

Deleting a Lookup Repository

To delete a lookup repository:

1. Click the Configuration tab, navigate to Configuration > Lookup & Update Modules > Lookup Modules, and select the type of repository you want to delete.
2. Click the trash can icon next to the repository you want to delete.
3. Click **Deploy Configuration**.

Configuring Sender Policy Using LDAP

The IronPort Encryption appliance can be configured to look up sender permissions using the LDAP server. You need an LDAP lookup repository configuration to use an LDAP server as a lookup provider. If the appropriate LDAP lookup repository configuration does not exist, then add one. For more information see, “Adding a Lookup Repository” on page 172. The LDAP Lookup Repository configuration also has a Sender Policies tab that you can use to set permissions based on the email sender address. The sender can have one of the following policies: SendAll, SendRestricted, or SendNone.

- SendAll

  Permission to send to anyone

- SendRestricted

  Restricted permissions to send (depends on the recipient’s domain.)

- SendNone

  No permissions to send to anyone

For SendRestricted, if a domain listed in the domain list starts with @, then an exact match is required. Otherwise, a sub-string match is done.

UPDATE MODULES

This section describes the update modules. To view and edit update modules, click the Configuration tab and then navigate to Configuration > Lookup & Update Modules > Update Modules.

LDAP Update Repository

The IronPort Encryption appliance can be configured to update certificates in an LDAP directory.

You need an LDAP update repository configuration to configure an LDAP server as an update provider. If an LDAP update repository does not exist, you must add one. An LDAP update repository has the following parameters.

Parameter	Definition
Name	Name of the LDAP update Repository.
Connect Securely	Use to specify whether you want to connect securely via LDAPS.
Server Name	Name of the LDAP server.
Port Number	TCP/IP port of the LDAP server.
Logon to Server	If checked, the LDAP server requires logging on to perform updates.
User Name	User account used to log in to the LDAP server.
User Password	User password used to log in to the LDAP server.
RootDN	The base distinguished name (DN) against which all lookups and searches are carried out, for example “dc=postx,dc=com” or “o=PostX,c=US”.
Query String	A simple expression that yields the query string used to identify a user in LDAP lookup requests. This parameter is only used in lookups, it is **not** used in searches. For example “cn=${identity}”, where ${identity} is the value the application obtains from the MIME message using the application’s Key Lookup Identity configuration parameter.
Enable Directory Search	Enables the use of LDAP searches instead of using lookups. Lookups are better, but can only be used when the users can be identified by their common name. When you want to use the user’s email address in order to identify them, you must use a search by selecting this and setting the Search String value appropriately.

Parameter	Definition
Search String	A simple expression that yields the query string used to search the LDAP directory. This parameter is only used in searches, it is not used in lookups. For example "mail=${identity}", where ${identity} is the value the application obtains from the MIME message using the applications Key Lookup Identity configuration parameter.
Retry Count	The maximum number of times to retry after communication failure.

Attribute Names

Parameter	Definition
PKCS7 Certificate Attribute	LDAP schema name of the attribute used to hold the users PKCS #7 public key certificate.
PKCS12 Certificate Attribute	LDAP schema name of the attribute used to hold the users PKCS #12 private key certificate.
PKCS12 Certificate Password Attribute	LDAP schema name of the attribute used to store the password value that was used to encrypt the PKCS #12 certificate.

Database Update Repository

A database update repository is used to update an encryption key for a recipient in a database. For example, if you store the keystore in a database. In order to configure the database for updating, a database update repository containing the database lookup information is needed. If a database update repository does not exist, you must add one. A database update repository has the following parameters.

Parameter	Definition
Name	Database update repository.
DB DataSource JNDI Name	JNDI Name of the datasource used to connect to the DBLookup database.
DB Table Name	Name of the table to be looked up in the database lookup.
DB Key Separator	The separator for multiple password fields.
DB Primary Column	The recipient's email address which is used as the db key to obtain the encryption key.

Parameter	Definition
Key Column1	One or more password fields stored in the database.
Key Column2	One or more password fields stored in the database.
Key Column3	One or more password fields stored in the database.
Key Column4	One or more password fields stored in the database.
Register Column1	Name of the database field that contains registered status.
Register Value1	Value in Register Column 1 indicating the recipient is registered.
Register Column2	Name of the db field that contains registered status.
Register Value2	Value in Register Column 2 indicating the recipient is registered.
Enroll If Password Exists	Whether or not to set the registration state to true if the password exists (override the check for the register column and value).
Case Insensitive Update	Specifies whether case insensitive lookups are used Default is not checked.

Chained Update Repository

The IronPort Encryption appliance can be configured to use multiple sources to update the encryption key for a user. In order to use the chained update provider 2 or more update repositories (any combination of LDAP, Database, or User Lookups) should be configured.

Parameter	Definition
Name	Name of the chained repository.

<Name of Added Chained Lookup>

Parameter	Definition
Name	Name of the item in the chained lookup.
Update Name	Name of the update module associated with this item in the chain.

PGP Update Repository

The IronPort Encryption appliance has the ability to generate PGP keys for recipients and senders. The generated PGP keys can be updated to the PostX Certificate Database using a PGP Update Repository. You must add an update module of this type in order to generate and store PGP keys.

Parameter	Definition
Name	Name of the repository.
Class	Name of the class that implements this repository.
Update Service Name	Name of the EJB service to bind the update to.
Application Name	Used to identify the Application Name, a method for grouping the update. Used to group identities in CertLookup.

User Update Repository

The IronPort Encryption appliance can be configured to update certificates in the certificate store. You need a user update repository configuration to use the certificate store as an update provider. If a user update repository does not exist, you must add one. A user update repository has the following parameters.

Parameter	Definition
Name	Name of the user repository.
Class	Name of the class that implements the type of lookup. Use com.postx.lookup.UserUpdate for websafe updates.
Update Service Name	Name of the EJB service to bind the update to.
App Name	Used to identify the Application Name, a method for grouping the update. Used to group identities in CertLookup.

Adding an Update Repository

To add an update repository:

1. Click the Configuration tab and then navigate to Configuration > Lookup & Update Modules > Update Modules, and select the type of repository you want to add.
2. Enter a new update repository name, and click the **Add Update Repository** button. Click **Deploy Configuration**.
3. Click Configuration > Lookup & Update Modules > Lookup Modules > *Repository Type* > *New repository name* and configure the newly added repository. For a list of the lookup repository parameter, see Appendix A, "Configuration Parameters," on page 239.
4. Click **Deploy Configuration**.

Deleting an Update Repository

To delete an update repository:

1. Click the Configuration tab, navigate to Configuration > Lookup & Update Modules > Update Modules, and then select to the type of repository you want to delete.
2. Click the trash can icon next to the repository you want to delete.
3. Click **Deploy Configuration**.

CHAPTER 14

OpenPGP

This chapter discusses the OpenPGP functionality that the IronPort Encryption appliance provides.

This chapter contains the following sections

OVERVIEW

The OpenPGP functionality can be used by organizations to encrypt outgoing email and decrypt incoming email at the gateway level. On the IronPort Encryption appliance, PGP support is based on the OpenPGP specifications. It has been fully tested for interoperability with standard PGP. To facilitate these and other OpenPGP applications, the IronPort Encryption appliance provides the following PGP related features:

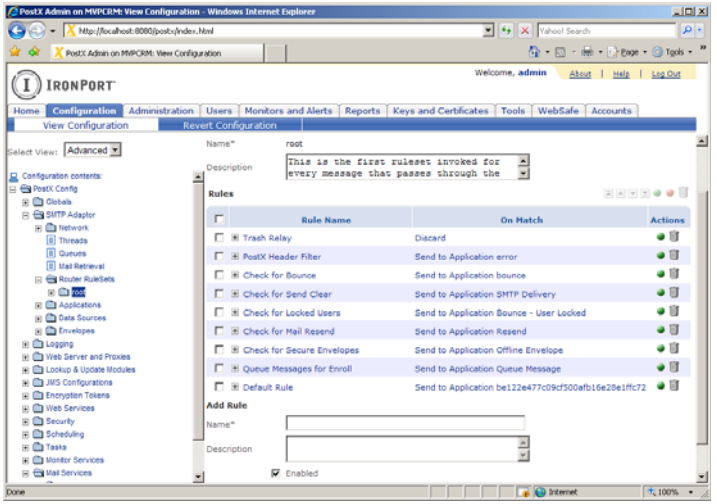
- PGP Matcher
- PGP Key Harvesting
- PGP Decryption
- PGP Lookup
- PGP Update

The following sections describe these features.

OPENPGP RULES

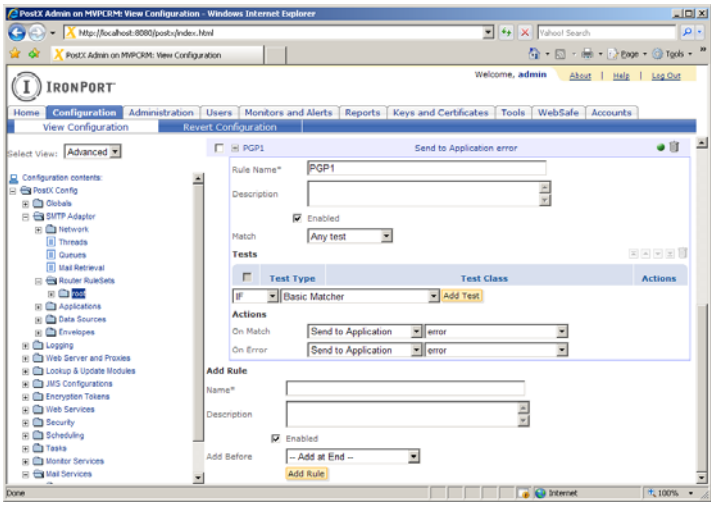
This component allows the OpenPGP gateway to recognize standard PGP messages that are signed or signed/encrypted. It then routes them to an IronPort Encryption appliance application for processing and delivery via the appropriate mechanism.

1. Click the Configuration tab and then navigate to Configuration > SMTP Adaptor > Router RuleSets > root.



2. Enter a new rule name (e.g., PGP1) and a description at the bottom of the page. Click the **Add Rule** button. The new rule is added to the list of rules.

3. Click the '**+**' symbol next to the rule you just added to expand the list of attributes associated with the rule.



4. In the Tests section, select 'Is PGP Matcher' from the Test Class drop-down and click the **Add Test** button.

- **Match -** Select the criteria for the matcher. Options are:
    - **Any –** Matches either signed or encrypted messages and public keys
    - **Signed Only –** Matches only signed messages
    - **Encrypted –** Matches only encrypted messages
    - **Public Key –** Matches only messages that contain PGP public keys
- **Sender Host List -** Enter any specific hosts to match. This is a comma separated list of hosts that should be checked. If the email is from a host that is not in the list, the email will not be checked.

  The Actions section determines what the system does when a message meets the test qualifications.

- **On Match -** Select the action you want the system to take. Valid values are:

    - **Send to Router RuleSet -** Select the router ruleset you want to send the message to from the drop-down.
    - **Send to Application -** Select the application you want to send the message to from the drop-down. If you wish to use certificate harvesting or decryption, you must configure a PGP Handler application as described in the PGP Handler section below.
    - **Store in repository -** Enter the repository where you want the message to be stored. You do not need to enter the full path since it will default to <install_dir>/apps/james/var/mail/. The new repository will appear on the Home page in the Spool Repositories box.
    - **Discard -** The message is discarded.
- **On Error -** Select the action you want the system to take. Valid values are:
    - **Send to Router RuleSet -** Select the router ruleset you want to send the message to from the drop-down.
    - **Send to Application -** Select the application you want to send the message to from the drop-down.
    - **Match All** - All recipients will be acted on according to On Match.
    - **Match None** - None of the recipients will be matched, even if the error applied to only some of the recipients.
    - **Discard -** The message is discarded.

CONFIGURING PGP

There are several application types that work in conjunction with the PGP matcher to provide additional PGP functionality:

- **PGP Decrypt and Verify Signature -** Use this application when decrypting incoming messages using the private key of the intended recipient. This application will optionally verify the PGP signature.
- **PGP Encrypt and Sign -** Use this application to send a PGP encrypted and signed message.
- **PGP Harvest -** Use this application to retrieve (harvest) the public key from incoming messages and update them in the Certificate Repository.

PGP Harvesting

The system can be configured to retrieve (harvest) the public key from incoming messages and update them in the Certificate Repository. Once harvested, a key may be used to send standard OpenPGP encrypted messages to the owner of the harvested key from the OpenPGP gateway.

The PGP harvesting configuration parameters can be accessed by adding an application with a type of PGP Harvest. Configure the application by navigating to Configuration > SMTP Adaptor > Applications > *PGP Harvest_Application_Name* and then clicking the PGP Key Harvesting tab.

Parameter	Definition
Key Update Provider	Specifies the update module used to store the harvested certificates.
Store Updated Certificates	Updates an existing certificate with a new certificate. The update occurs only if the new certificate has a later expiration date than the existing certificate. If this check box is cleared, existing certificates are not updated.
Import for All IDs	Imports the PGP key for all user IDs associated with the PGP key. If this check box is cleared, the PGP Harvest application imports the key for the sender identity only. By default, the check box is selected.
Treat Unsigned as Success	Treats the mail as if harvesting is successful when no public key is found. If the option is disabled, mail is treated as a harvest failure when no public key is found.
Next on Success	Application or ruleset the email passes through once the certificate is harvested.

Parameter	Definition
Next on Failure	Application or ruleset the email passes through if harvesting fails.

OpenPGP Decryption

The system can be configured to decrypt incoming messages using the private key of the intended recipient which is stored in the Certificate Repository. The decryption can be optionally done using domain keys or even an enterprise wide common key as specified in the "Encryption Key Lookup" tab. Once unencrypted, the message may be forwarded to the intended recipient in its original PGP format, unencrypted, or via an alternate delivery mechanism such as Registered Envelope, Secure Mailbox, or other IronPort Encryption appliance applications.

The decryption configuration parameters can be accessed by navigating to Configuration > SMTP Adaptor > Applications > *PGP Decrypt and Verify Signature _Application_Name* and then clicking on the PGP Decryption and Signature Verification tab.

Parameter	Definition
Verify Signature	If selected, and the input message is either signed or signed and encrypted, the system will verify the signature before storing it in the update module. If the harvested certificate is not valid, then it is not stored in the update module. If this option is not selected, signature verification is not done.
Public Key Lookup Provider	Name of the lookup to use when the signer's public key is to be retrieved for signature verification.
Subject Prefix on Success	The subject to prepend when signature verification is successful.
Subject Prefix on Failure	The subject to prepend when signature verification fails.
Next On Success	Application or ruleset the email will pass through if decryption is successful.
Next On Failure	Application or ruleset the email will pass through if decryption fails.

PGP LOOKUP

The IronPort Encryption appliance has the ability to look up PGP keys for recipients and senders. PGP keys can be read from the Certificate Database using a PGP Lookup Repository. You can also use other lookup repository types such as “LDAP” and “Database” to lookup PGP keys. For more information, see Chapter 13, “Configuring Lookup and Update Modules,” on page 153.

PGP UPDATE

The IronPort Encryption appliance has the ability to generate OpenPGP keys for recipients and senders. The generated OpenPGP keys can be updated to the Certificate Database using a PGP Update Repository. You must add an update module of this type in order to generate and store OpenPGP keys.

For more information refer to the *Configuring Lookup and Update Modules* chapter in this manual.

LOOKING UP PGP PUBLIC CERTIFICATES

The PGP public certificates stored in the IronPort Encryption appliance repository can be looked up over HTTP via the HKP certificate server. Access the server at:

```
http://localhost:8080/pks
```

To retrieve a certificate, provide the user-id (email address for which the PGP public key is required) in the Identity field and click the **Retrieve Key** button. If a PGP public key exists for the identity provided, it is retrieved.

The key can also be looked up without using the form. The base URL for the HKP server is:

```
http://localhost:8080/pks/lookup
```

The mandatory `search` parameter specifies the identity for which the PGP Public key needs to be looked up. For example, to look up user@ironport.com, you use the following URL:

```
http://localhost:8080/pks/lookup?search=user@ironport.com
```

If the requested identity's key is not available in the key store, an Error page is displayed. Click the Back link in the browser to try a different lookup.

CHAPTER 15

S/MIME

This chapter contains the following sections:

OVERVIEW

You can use the S/MIME functionality of the IronPort Encryption appliance to communicate with recipients who have email clients that support the standard S/MIME implementation. It can also be used by organizations to decrypt email at the gateway level. To facilitate these and other S/MIME applications the IronPort Encryption appliance provides the following S/MIME-related features:

- S/MIME Matcher
- Certificate Harvesting
- S/MIME Decryption

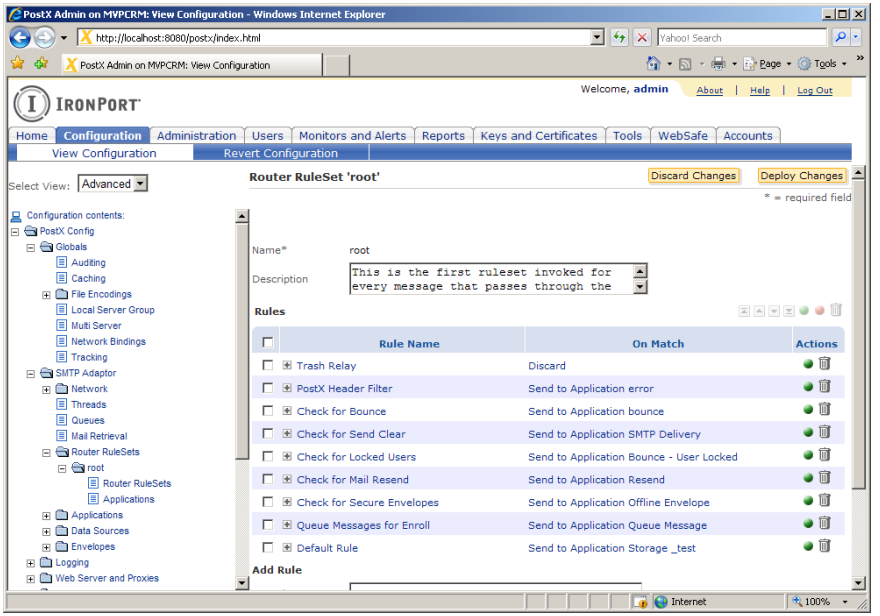
This chapter also includes information on accessing X.509 certificates.

CONFIGURING THE S/MIME RULE

You need to configure a router rule that enables the IronPort Encryption appliance to recognize standard S/MIME messages that are signed or signed/encrypted. It then routes them to the appropriate application for processing and delivery.

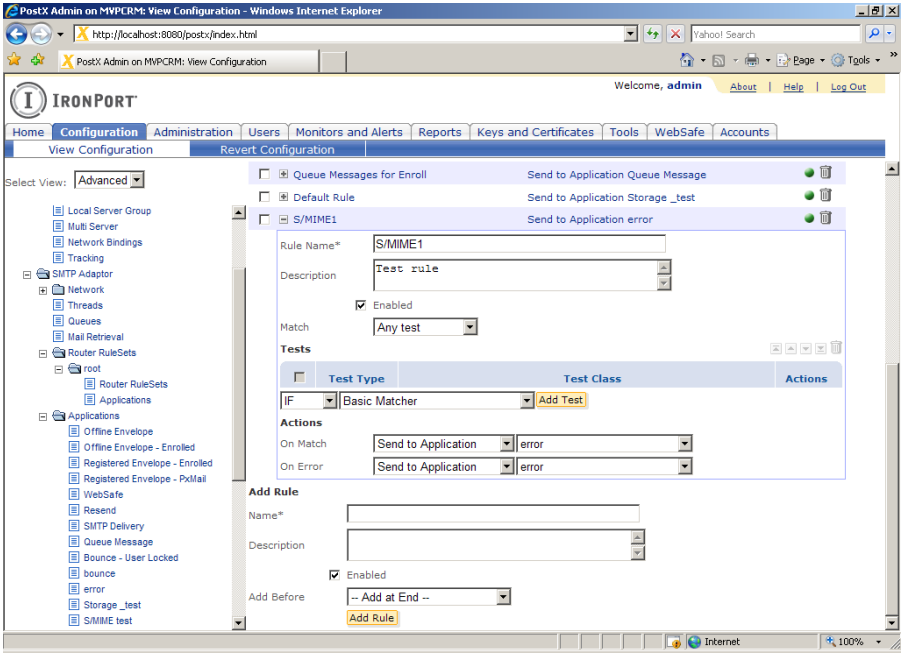
To configure a new rule that directs messages to the S/MIME application.

1. Click the Configuration tab and navigate to Configuration > SMTP Adaptor > Router RuleSets > root.



2. In the Add Rule section at the bottom of the page, enter a new rule name (for example, S/MIME1) and description. Verify that the **Enabled** check box is selected.
3. Click the **Add Rule** button. The new rule is displayed in the list.
4. Select the new rule in the list, and click the up arrow to move it above the default rule.

5. Click the plus sign (+) next to the new rule to expand the rule.



6. In the Tests section, select 'Is S/MIME Matcher' from the Test Class drop-down and click the **Add Test** button. Click the '**+**' symbol next to the test you just added to expand test.

- **Match -** Select the criteria for the matcher. Options are:
  - **Any –** Matches either signed or encrypted messages
  - **Signed Only –** Matches only signed messages
  - **Encrypted –** Matches only encrypted messages
- **Sender Host List -** Enter any specific hosts to match. This is a comma separated list of hosts that should be checked. If the email is from a host that is not in the list, the email will not match.

  The Actions section determines what the system does when a message meets the test qualifications.

- **On Match -** Select the action you want the system to take. Valid values are:
  - **Send to Router RuleSet -** Select the router ruleset you want to send the message to from the drop-down.
  - **Send to Application -** Select the application you want to send the message to from the drop-down.

    - **Store in Repository -** Enter the repository where you want the message to be stored. You do not need to enter the full path since it will default to `<install_dir>/apps/james/var/mail/.` The new repository will appear on the Home page in the Spool Repositories box.
    - **Discard -** The message is discarded.
- **On Error -** Select the action you want the system to take. Valid values are:
    - **Send to Router RuleSet -** Select the router ruleset you want to send the message to from the drop-down.
    - **Send to Application -** Select the application you want to send the message to from the drop-down.
    - **Match All -** All recipients will be acted on according to On Match.
    - **Match None -** None of the recipients will be matched, even if the error applied to only some of the recipients.
    - **Discard -** The message is discarded.

CONFIGURING S/MIME

There are several application types that work in conjunction with the S/MIME matcher to provide additional S/MIME functionality.

- S/MIME Decrypt

  Use this application when decrypting incoming messages using the private key of the intended recipient.

- S/MIME Encrypt and Sign

  This application is used to send an S/MIME encrypted and signed message.

- S/MIME Harvest and Verify Signature

  Use this application to retrieve (harvest) the public key from incoming signed messages and update them in the Certificate Repository. This application will optionally verify and optionally remove the signature.

Certificate Harvesting

The system can be configured to retrieve (harvest) the public key certificate from incoming digitally signed or signed/encrypted messages and update them in the Certificate Repository. Once harvested, a certificate may be used to send standard S/MIME encrypted messages to the owner of the harvested certificate from the IronPort Encryption appliance S/MIME gateway.

When a certificate is harvested, it can optionally be verified. One part of verification is checking that the certificate has not expired. The other part is to verify that there is a root certificate and that it has not expired. The root certificate must be loaded into the system using the process described in the *Managing Certificates* in the *IronPort Encryption Appliance Operation's Manual*.

The certificate harvesting configuration parameters can be accessed by clicking the Configuration tab and navigating to Configuration > SMTP Adaptor > Applications. Add an application using the S/MIME Harvest and Verify Signature application type. Next navigate to the newly added application and click the Certificate Harvesting and Signature Verification tab.

Parameter	Definition
Harvest Certificates	Turns certificate harvesting on and off.
Harvest on Signature Verification Failure	If checked, the certificate is harvested even if signature verification fails.
Key Update Provider	Update module used to store the harvested certificates.

Parameter	Definition
Verify Certificates	If this option is checked, the harvested certificate is verified until a trusted root certificate. If this option is not checked then only an expiry check is made on the harvested certificate.
Store Updated Certificates	If checked, existing certificates are replaced by newer certificates.
Verify Signature	Determines if the system should verify the certificate before storing it in the update module. If Verify Signature is selected and the harvested certificate is not valid, then it is not stored in the update module.
Subject Prefix on Success	The subject to prepend when signature verification is successful.
Subject Prefix on Failure	The subject to prepend when signature verification fails.
Next on Success	Application or ruleset the email passes through once the certificate is harvested.
Next on Failure	Application or ruleset the email passes through if harvesting fails.
Treat Unsigned as Success	If no public key is found, the mail is treated as if harvesting is successful if this is turned on. If turned off, mail is treated as harvest failure if no public key is found.
Remove Signature	Remove signature part of signed message.

S/MIME Decryption

The system can be configured to decrypt incoming messages using the private key of the intended recipient which is stored in the Certificate Repository. The decryption can be optionally done using domain certificates or even an enterprise wide common certificate as specified in the "Encryption Key Lookup" tab. Once unencrypted, the message may be forwarded to the intended recipient in its original S/MIME format, unencrypted, or via an alternate delivery mechanism such as Registered Envelope, Secure Mailbox, or other applications on the IronPort Encryption appliance.

The decryption configuration parameters can be accessed by clicking the Configuration tab and navigating to Configuration > SMTP Adaptor > Applications. Add an application using

the S/MIME Decrypt application type. Next navigate to the newly added application and click the S/MIME Decryption tab.

Parameter	Definition
Remove Signature	Remove signature part of signed message.
Next On Success	Application or ruleset the email will pass through if decryption is successful.
Next On Failure	Application or ruleset the email will pass through if decryption fails.

LOOKING UP X.509 PUBLIC CERTIFICATES

You can look up the IronPort Encryption appliance X.509 public certificates stored in the Certificate Repository over HTTP via the X.509 certificate server. Access the server at:

`http://<appliance_hostname>/pks/X509lookup.jsp`

To retrieve a certificate, provide the user ID (that is, the email address for which the X.509 public certificate is required) in the Identity field and click the **Retrieve Certificate** button. The certificate server displays an X.509 public certificate for the identity one exists.

X.509 public certificates can also be looked up without using the form. The base URL for the X.509 certificate server is:

`http://<appliance_hostname>/pks/X509lookup`

Use the mandatory `search` parameter to specify the identity for which you want to look up the X.509 public certificate. For example, to look up user@ironport.com, use the following URL:

`http://<appliance_hostname>/pks/X509lookup?search=user@ironport.com`

If the requested identity's certificate is not available in the certificate store, an Error page is displayed. Click the Back link to try a different lookup.

CHAPTER 16

Port Numbers

This chapter contains information about using the Network Bindings feature to bind JBoss services to specific IP addresses and port numbers.

This chapter contains the following section:

NETWORK BINDINGS AND PORT NUMBERS

The Network Bindings configuration node lets you bind various JBoss services to specific port IP addresses. If the BindAddresses are left empty, by default it binds the service to all of the interfaces.

To access the Network Bindings node, click the Configuration tab and then navigate to Configuration > Globals > Network Bindings.

Parameter	Settings	Port Number/ Default Value
Naming Service Binding Address	Network adaptor that the naming service will bind to	127.0.0.1
Naming Service Port	Network port that the naming service will bind to. Used by the Java Naming and Directory Interface (JNDI). This is used to allow clients to look up services by name, e.g., EJBs, LDAP etc.	1099
Naming Service RMI Binding Address	Network adaptor that the naming RMI service will bind to	127.0.0.1
Naming Service RMI Port	Network port that the naming RMI service will bind to	1098
Web Services Binding Address	Network adaptor that the web services will bind to	127.0.0.1
Web Services Port	Network port that the web service will bind to. This port number is used to download file from the JBoss server configuration directory, e.g., the login-config.xml. It is used to enable dynamic download of .class files to RMI/EJB clients.	8083
RMI Invoker Binding Address	Network adaptor that the RMI invoker will bind to	127.0.0.1
RMI Invoker Port	Network port that the RMI server objects listen on using the JRMP protocol.	4444
JMX RMI Adaptor Binding Address	Network adaptor that the JMX RMI adaptor will bind to	127.0.0.1
JMX RMI Adaptor Port	Network port that the JMX RMI adaptor will bind to	19001

Parameter	Settings	Port Number/ Default Value
Web Server Binding Address	Network adaptor that the web server will bind to	0.0.0.0
Web Server Port	Network port that the web server will bind to	8080
Web Server SSL Port	Network port that the web server will bind to for SSL	443
Web Server AJP13 Port	Network port that the web server AJP13 listener will bind to	8009
JMS OIL Listener Binding Address	Network adaptor that the JMS OIL listener will bind to	127.0.0.1
JMS OIL Listener Port	Network port that the JMS OIL listener will bind to	8090
JMS OIL2 Listener Binding Address	Network adaptor that the JMS OIL2 listener will bind to	127.0.0.1
JMS OIL2 Listener Port	Network port that the JMS UIL2 listener will bind to	8092
JMS UIL2 Listener Binding Address	Network adaptor that the JMS UIL2 listener will bind to	127.0.0.1
JMS UIL2 Listener Port	Network port that the JMS UIL2 listener will bind to. Used by Hypersonic.	8093
Hypersonic DB Binding Address	Network adaptor that the Hypersonic DB server will bind to	127.0.0.1
Hypersonic DB Port	Network port that the Hypersonic DB server will bind to	1701
Cache Listener Binding Address	IP address of network adaptor the distributed Cache binds to.	127.0.0.1
Cache Listener Port	Port the Cache listener binds to.	40001
Mail Server Remote Manager Enabled	Enable or disable the mail server remote manager. Used by the James Remote Manager. This is a command interface that allows you to manage James users using Telnet.	Default is Enabled.

Parameter	Settings	Port Number/ Default Value
Mail Server Remote Manager Binding Address	Network adaptor that the mail server remote manager will bind to	127.0.0.1
Mail Server Remote Manager Port	Network port that the mail server remote manager will bind to	4555
Mail Server SMTP Service Enabled	Enable or disable the mail server SMTP service	Default is Enabled.
Mail Server SMTP Binding Address	Network adaptor that the mail server SMTP service will bind to	0.0.0.0
Mail Server SMTP Port	Network port that the mail server SMTP service will bind to	25
Mail Server SMTP TLS Service Enabled	Enable or disable the mail server SMTP TLS service	Default is Disabled.
Mail Server SMTP TLS Binding Address	Network adaptor that the mail server SMTP TLS service will bind to	0.0.0.0
Mail Server SMTP TLS Port	Network port that the mail server SMTP TLS service will bind to	465
Mail Server SMTP TLS Keystore Path	Mail server SMTP TLS keystore path	../../conf/keystore
Mail Server SMTP TLS Keystore Password	Mail server SMTP TLS keystore password	N/A

CHAPTER 17

SSL for the IronPort Encryption Appliance

This chapter contains the following sections:

OVERVIEW

This is an overview of how to configure Secure Socket Layer (SSL) for the IronPort Encryption appliance using Sun's reference implementation for the Java Secure Sockets Extension (JSSE).

THE BASICS

The following steps are required to configure the IronPort Encryption appliance for SSL:

1. Generate a public/private key pair and a certificate request.
2. Optionally obtain a certificate from a known certificate authority (CA).
3. Load the certificate obtained from the CAs into the JSSE Keystore.
4. Configure the JsseListener to use the keystore setup in the previous step.

For detailed instructions, refer to the sections below.

Step 1: Generate Key Pair and Certificate Request

The simplest way to generate keys and certificates is using the Get Certificate Request feature available within the IronPort Encryption appliance. To use this feature, click the Keys and Certificates tab, then click the SSL Setup subtab.

The OpenSSL tools can also be used to generate keys and certificates or to convert ones that have been used with Apache or other servers.

Note — If you already have keys and certificates, please skip to step 3 to load them into a JSSE key store.

Click the **Get Certificate Request** button then use the following configuration parameters to enter the information required to generate the key pair and certificate request.

Parameter	Definition
Keystore	The temporary file in which the generated public and private keys will be stored. Note, any previous file of the same name will be renamed to avoid conflict. Select a file name that is different.
Host	The URL for your website. This is the name by which the generated public and private keys will be indexed.
Organization	Name of your organization
Organizational Unit	Name of your organizational unit
City	City name
State	State name. You must use the full state name instead of the abbreviation.
Country	Country name
Password	Pick a password that is at least six characters long.

Parameter	Definition
Validity Period	The number of days for which this certificate will be valid.

Click the **Generate Keys and Certificate Request** button and the "certificate signing request" or CSR will be generated and display in the last field.

Note that the generated key pair will be stored in a new keystore file called as "enterprise.keystore" in the `<Install_Dir>/conf` directory.

You now have the minimal requirements to run an SSL connection and can proceed directly to step 4 to configure an SSL listener. However, the certificate you have generated will not be trusted by the browser and the user will be prompted to this effect. This is often sufficient for testing, but for most public sites you will need step 2 to obtain a certificate trusted by most popular clients.

Step 2: Request a Trusted Certificate

The keys and certificates generated in Step1 are sufficient to run an SSL listener. However, the certificate you have generated will not be trusted by the browser and the user will be prompted to this effect.

To obtain a certificate that will be trusted by most common browsers, you must request a well known certificate authority (CA) to sign your key/certificate. The Certificate Signing Request (CSR) generated in step1 will be used during this process. Such trusted certificate authorities include: AddTrust, Entrust, GeoTrust, RSA Data Security, Thawte, VISA, ValiCert, Verisign, and beTRUSTed among others.

When requesting an SSL cert from your Certificate Authority (for example, Verisign), they typically ask what type of web server the cert is for. It is recommended that you select Apache for the web server type.

Step 3: Load Trusted Certificate into the Keystore

Once a CA has sent you a certificate, it must be loaded into the JSSE keystore. Refer to instructions from your CA on how you can copy the signed certificate into a file. The preferred format for the certificate is PEM and you should select the option if provided to include all certificates in the certificate chain.

A certificate in PEM form may be directly loaded into the keystore using the "Import CA Certificate" option in the "SSL Setup" configuration in the Administration Console.

To directly load a certificate in PEM format into the keystore, use the Import CA Certificate feature. To use this feature, click the Keys and Certificates tab, SSL Setup subtab and then click

the **Import CA Certificate** button. The following configuration parameters are associated with importing a certificate.

Parameter	Definition
Keystore	The temporary file in which the generated public and private keys will be stored. Note, any previous file of the same name will be renamed to avoid conflict. Display only field.
Host	The URL for your website. This is the name by which the generated public and private keys will be indexed.
Certificate	Provide the full path to the certificate that you wish to import.
Password	This password corresponds to the actual generated keys as well as the keystore. Note that the password host entry specified here should match the password and host entry entered in step1 above.
Trust CA Certs	Select this checkbox.

Click the **Import Certificate** button load the certificate into the keystore.

PEM Format

The PEM format is a text encoding of certificates and an example PEM file is:

```
-------------------------------------------------------------
# more webserver.crt
-----BEGIN CERTIFICATE-----
MIICSDCCAfKgAwIBAgIBADANBgkqhkiG9w0BAQQFADBUMSYwJAYDVQQKEx1Nb3J0
IEJheSBDb25zdWx0aW5nIFB0eS4gTHRkLjEOMAwGA1UECxMFSmV0dHkxGjAYBgNV
BAMTEWpldHR5Lm1vcnRiYXkub3JnMB4XDTAzMDQwNjEzMTk1MFoXDTAzMDUwNjEz
MTk1MFowVDEmMCQGA1UEChMdTW9ydCBCYXkgQ29uc3VsdGluZyBQdHkuIEx0ZC4x
DjAMBgNVBAsTBUpldHR5MRowGAYDVQQDExFqZXR0eS5tb3J0YmF5Lm9yZzBcMA0G
CSqGSIb3DQEBAQUAA0sAMEgCQQC5V4oZeVdhdhHqa9L2/ZnKySPWUqqy81riNfAJ
7uALW0kEv/LtlG34dOOcVVt/PK8/bU4dlolnJx1SpiMZbKsFAgMBAAGjga4wgasw
HQYDVR0OBBYEFFV1gbB1XRvUx1UofmifQJS/MCYwMHwGA1UdIwR1MHOAFFV1gbB1
XRvUx1UofmifQJS/MCYwoVikVjBUMSYwJAYDVQQKEx1Nb3J0IEJheSBDb25zdWx0
aW5nIFB0eS4gTHRkLjEOMAwGA1UECxMFSmV0dHkxGjAYBgNVBAMTEWpldHR5Lm1v
cnRiYXkub3JnggEAMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEEBQADQQA6NkaV
OtXzP4ayzBcgK/qSCmF44jdcARmrXhiXUcXzjxsLjSJeYPJojhUdC2LQKy+p4ki8
Rcz6oCRvCGCe5kDB
-----END CERTIFICATE-----
```

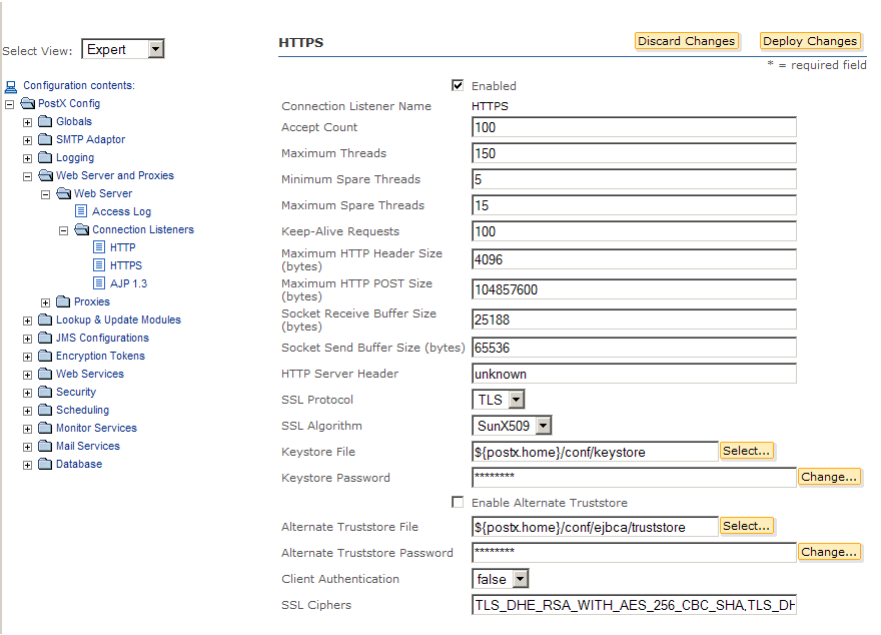
If the certificate you receive from the CA is not in the above format, then use openssl to convert to this format.

```
# openssl x509 -in webserver.der -inform DER -outform
        PEM -out webserver.crt
```

If you generated your own certificate without going through the Administration Console you must load the certificate and private key into the keystore using keytool commands. Refer to the Sun Microsystems documentation for more information about using the keytool.

Step 4: Configuring the Server to Use the New Certificate

This last step is to configure the encryption server to use SSL. Click the Configuration tab and navigate to Configuration > Web Servers and Proxies > Web Server > Connection Listeners > HTTPS.



Use the following parameters to configure the encryption server to start an SSL listener and use the new generated certificate from the enterprise.keystore file.

Parameter	Definition
Enabled	Click to enable.
Connection Listener Name	Display-only field.

Parameter	Definition
Accept Count	The maximum queue length for incoming connection requests.
Maximum Threads	The maximum number of request processing threads to be created by this Connector.
Minimum Spare Threads	The number of request processing threads that will be created when this Connector is first started.
Maximum Spare Threads	The maximum number of unused request processing threads that will be allowed to exist until the thread pool starts stopping the unnecessary threads.
Keep-Alive Requests	The maximum number of HTTP requests which can be pipelined until the connection is closed by the server.
Maximum HTTP Header Size (bytes)	The maximum size of the request and response HHTP header, specified in bytes.
Maximum HTTP POST Size (bytes)	The maximum size of FORM POSTs which will be handled by the web server, specified in bytes.
HTTP Server Header	Value of server header in HTTP responses.
SSL Protocol	Select the SSL protocol from the drop-down. Valid values are TLS and SSL.
SSL Algorithm	Select the SSL algorithm from the drop-down. Valid values are SunX509 and IBMX509.
Keystore File	The file in which the generated public and private keys were stored. Select a file name that is different.
Keystore Password	This password corresponds to the actual generated keys as well as the keystore.
Enable Alternate Truststore	Click to enable the use of alternate trust stores.
Alternate Truststore File	Contains the root certificates used to verify the SSL certificate imported into the keystore file.
Alternate Truststore Password	The password for the alternate trust store file.
Client Authentication	Set this value to true if you want Tomcat to require all SSL clients to present a client Certificate in order to use this socket. This is an optional parameter.
SSL Ciphers	A list of the encryption ciphers that may be used. (Comma separated)

Restart the IronPort Encryption appliance and test the configuration by using the Administration Console at the following URL:

`https://<appliance_hostname/admin/`

CONFIGURING SSL FOR WEBSPHERE

The IronPort Encryption appliance setup on WebSphere can be configured to use the http server bundled with these application servers. In this case you should follow instructions from the respective products on how to perform steps 1 to 4 above.

RENEWING SSL CERTIFICATES

To renew an SSL certificate, you essentially follow the same steps you performed when requesting a new certificate with the exceptions noted below:

Step 1: Generate Key Pair and Certificate Request

You must select a keystore file name different from the existing one. A recommended option is to append the year to the keystore file name, for example, enterprise.keystore.2007.

Step 2: Request a Trusted Certificate

Follow the instructions from your Certificate Authority for certificate renewal including submitting the certificate signing request (CSR) as generated in step (1).

Step 3: Load Trusted Certificate into the Keystore

There are no exceptions for this step.

Step 4: Configure the Server to Use the New Certificate

Remember to select the same keystore file that you specified in step 1.

CONFIGURING SMTP TLS TO USE THE NEW SERVER CERTIFICATE

The certificate and key pair generated in the above steps can also be used to provide SMTP-TLS capability through the encryption server. The same keystore file (enterprise.keystore) and password needs to be specified in the SMTP TLS configuration in the Network Bindings section of PostXConfig. The default setup uses a pre-installed "keystore" file which carries a self-signed test certificate.

CHAPTER 18

Configuring WebSafe

This chapter contains the following sections:

CONFIGURING THE WEBSAFE RULE

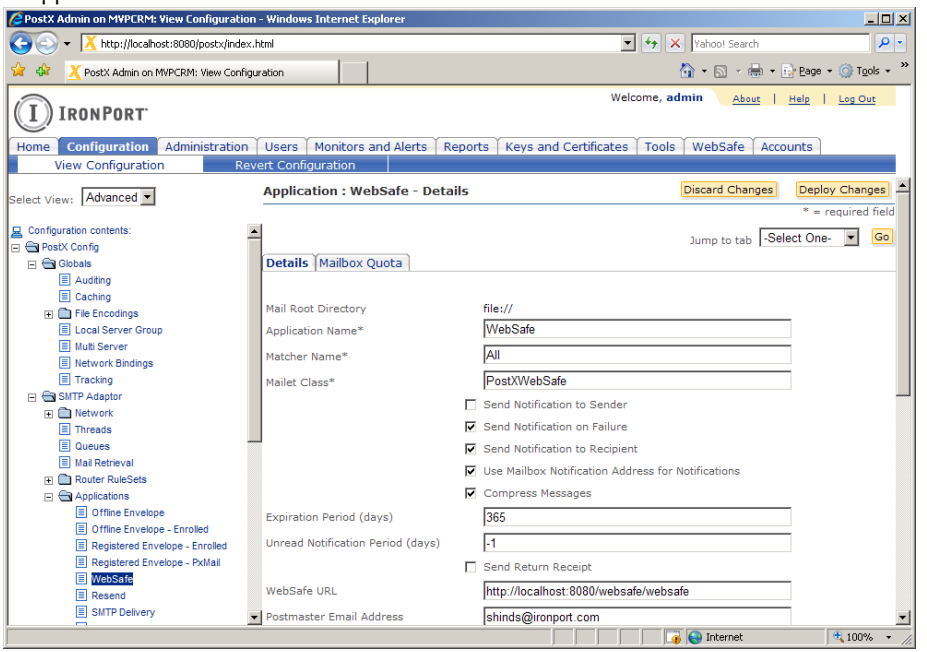
To use WebSafe, you need to configure a rule that will send messages to the WebSafe application according to the criteria you select. Please refer to the *IronPort Encryption Appliance Operation's Manual* for information on using and configuring Router RuleSets.

CONFIGURING THE WEBSAFE APPLICATION

The standard WebSafe application configuration is similar to the other applications configured within the *encryption server*. The following configuration parameters are specific to WebSafe and are configured on a per application basis. Please note that you must deploy the new configuration and restart the SMTP Adapter from the Administration Console to have these parameters take affect.

To configure the WebSafe application do the following.

1. Click the Configuration tab and then in the left pane click Configuration > SMTP Adaptor > Applications > WebSafe.



2. Enter/edit the following values:

- **Send Notification to Sender –** If enabled a notification email is sent to the sender for each email that WebSafe receives. The notification is in the form of a "Message Disposition Notification" as per RFC 2298.
- **Send Notification on Failure –** If enabled a notification email is sent to the sender for each incoming email that WebSafe is unable to process. The notification is in the form of a "Message Disposition Notification" as per RFC 2298. If WebSafe is not able to find the mailbox for the specified recipient (which means recipient is not enrolled with WebSafe) then the recipient email address will be listed in the failure notification send to the sender.

- **Send Notification to Recipient –** If enabled a notification email is sent to the recipient for each email received indicating that the recipient has a new email in his WebSafe account. This notification email also includes the URL to login to WebSafe. If this URL is used to logon to WebSafe the recipient will see the new emails received in his mailbox.
- **Use Mailbox Notification Address for Notifications –** This box is checked by default. If checked, then all notifications go to the mailbox notification address that was specified during registration. If unchecked, then all notifications go to the recipient address of incoming email overriding the mailbox notification address.
- **Compress Message –** Compresses all messages stored in WebSafe mailboxes before storage.
- **Expiration Period (days) –** WebSafe supports aging feature for all the messages it stores in its content database. This parameter specifies the default number of days the email (content) will be held in the content database before it is marked for deletion. Once the email is marked for deletion it remains in the database but is not seen by the recipient. In order to disable this feature and not have a default expiry limit for all messages specify the parameter as –1. This application global value can be changed on a per content basis by specifying the value for each incoming email.
- **Unread Notification Period (days) –** WebSafe supports sending return receipts when the recipient reads a new email and this can be enabled by a separate configuration parameter. In addition if the email is not read within a specified duration, especially for time-sensitive communications, the sender can be informed in order to take further action. This parameter specifies the number of days counting from the sent-date by which the recipient should have read his email. If the email is not read within the time limit a notification email is send to the sender to that effect. The notification is in the form of a "Message Disposition Notification" as per RFC 2298. The default value is –1 indicating that this notification feature is not enabled. This application global value can be changed on a per content basis by specifying the value for each incoming email.
- **Send Return Receipt –** If enabled, this parameter applies to all emails composed from WebSafe email client and the outgoing emails contain standard SMTP header information requesting return receipt. A return receipt notification email is sent to the WebSafe sender mailbox for each new email opened by the recipient. The notification is in the form of a "Message Disposition Notification" as per RFC 2298. Please note that not all external email clients will respect this SMTP header for Return Receipt and hence RR is not guaranteed for emails sent out to the external world.
- **WebSafe URL –** This URL is specified in the notification emails sent to the recipient as explained above. The format of the URL is `http://<host name>:8080/WebSafe/WebSafe`

  Here host name is the machine running the webserver/appserver where the WebSafe web mail client is deployed.
- **Postmaster Email Address –** This is the email address of the administrator of WebSafe who gets notified on any specific WebSafe errors.

- **Encryption Algorithm –** This parameter specifies the encryption algorithm to be used for encrypting the email content when storing in the database. The current version of the server does not support encryption of the content and hence this option will not have any significant effect. In future this parameter will allow the administrator to choose the encryption algorithm from values like ARC4, AES etc.
- **Encryption Token –** The encryption token to use when encrypting messages stored in the database. This drop-down is populated when you add encryption tokens by clicking the Configuration tab and navigating to Configuration > Encryption Tokens >Token List.
- **Recipient Destination –** The recipient notification sent from WebSafe includes the WebSafe URL, which lets the user login to WebSafe, and access his mailbox. This parameter is used to choose between three different notification types which deal with the type of data shown after login. The three values are "Inbox" which shows the recipient his complete inbox on login, "Single Message" which shows the recipient a single email message which generated this notification and "Unread Messages" which shows the recipient all the unread emails from the mailbox.
- **Notification Text Template File –** This parameter specifies the file, which contains the text part of the recipient notification email sent out from WebSafe. The file can be changed to reflect the new text or a new file can be specified. You can use the **Select** button to browse for the file.
- **Notification Text Template File Encoding –** The encoding that the file is given when it is stored.
- **Notification Text Charset –** The charset used for the email that the file becomes.
- **Notification HTML Template File –** This parameter specifies the file, which contains the HTML part of the recipient notification email sent out from WebSafe. The file can be changed to reflect the new text or a new file can be specified. You can use the **Select** button to browse for the file. If this field is empty, the notifications will only have a text part.
- **Notification HTML Template File Encoding –** The encoding that the file is given when it is stored.
- **Notification HTML Charset –** The charset used for the email that the file becomes.
- **Use Incoming Subject As Outgoing Subject –** Check to use the subject of the incoming message as the subject if the outgoing message.
- **Notification Subject –** Notification email subject.
- **Notification Sender –** The email address that displays in the From field of notification emails.
- **Notification Reply-To** – The email address that is used when recipients reply to the notification email.
- **Use Variable Substitution –** Check to enable personalization of the text message that is sent with each email.

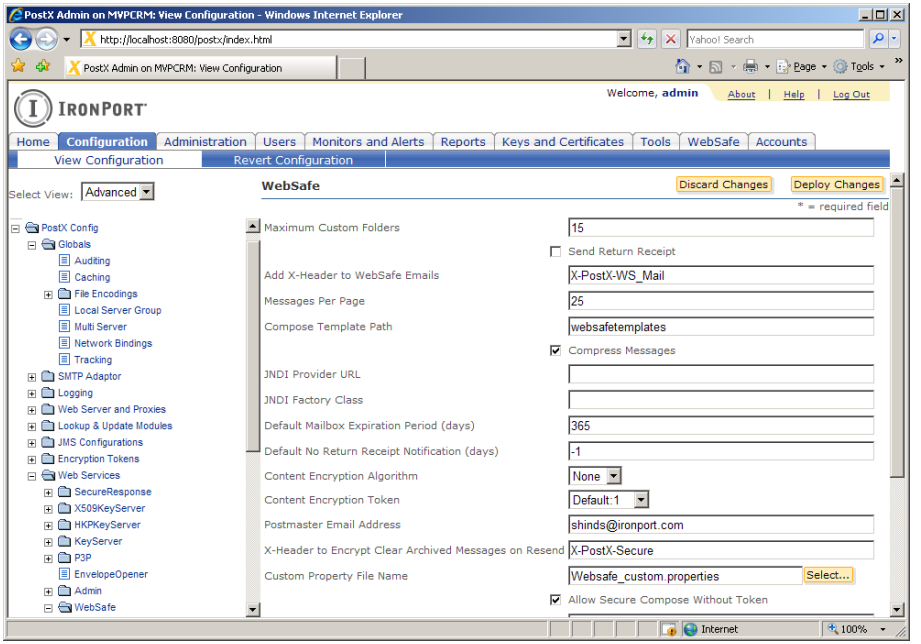
- **Notification Variable Map File –** Java properties file containing the variables mapping. The default value is variablemap.properties.
- **Bounce Application –** Application to send bounced messages to.
- **Delivery Application –** Application to use for delivering messages.
- **Enable Tracking –** Select to enable tracking of outgoing emails for the application.
- **Next –** Used to specify which application or ruleset that the mail will pass through once it is processed. See the *Chaining* section in the *Applications* chapter in this manual.

3. Click the **Deploy Changes** button to commit your configuration.
4. Click the Administration tab then the **Restart SMTP Adaptor** button. Wait about 15 seconds and the system will be restarted.

CONFIGURING THE WEBSAFE WEB MAIL USER INTERFACE

To configure the WebSafe Web Mail user interface do the following.

1. Click the Configuration tab and then in the left pane click Configuration > Web Services > WebSafe.



2. Enter/edit the following values:

- **Maximum Custom Folders –** A WebSafe client user cannot create more customer folders than this specified value.
- **Send Return Receipt –** If enabled this parameter applies to all emails composed from WebSafe email client and the outgoing emails contain standard SMTP header information requesting return receipt. A return receipt notification email is sent to the WebSafe sender mailbox for each new email opened by the recipient. The notification is in the form of a "Message Disposition Notification" as per RFC 2298. Please note that not all external email clients will respect this SMTP header for Return Receipt and hence RR is not guaranteed for emails sent out to the external world.
- **Add X-Header to WebSafe Emails –** The SMTP X-header that gets added to all outgoing emails from WebSafe.
- **Messages Per Page –** Specifies the number of emails to be listed on each page of the web mail user interface. If the number of emails exceeds this limit the remaining emails are

listed on a new page and you can navigate between pages using the “Prev” and “Next” buttons.

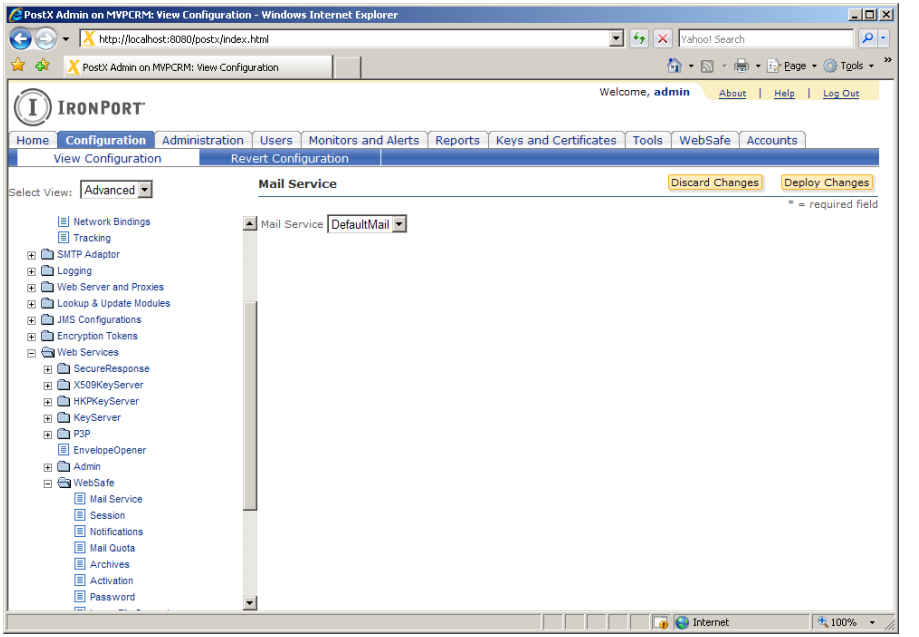
- **Compose Template Path –** WebSafe supports templates to be used when composing a new email. These templates are designed by the enterprise and specifies each new composed email to have certain pre-filled values, restrict certain parameters like cc or attachments, specify custom parameters, list allowable or restricted attachments, max limit for attachment size etc. These templates are defined in XML format and this parameter specifies the path where these templates are present. The default is “WebSafetemplates” which is a relative path within the encryption server configuration directory.
- **Compress Messages –** Compresses all messages stored in WebSafe mailboxes before storage.
- **JNDI Provider URL –** The JNDI Provider location that needs to be specified especially if the WebSafe Client is running on a separate system other than the WebSafe Server component. This URL points to the JNDI Provider to use for JNDI lookup.
- **JNDI Factory Class –** The JNDI Factory Class that needs to be specified especially if the WebSafe Client is running on a separate system other than the WebSafe Server component. This Factory Class is used for JNDI lookup and should correspond to the Provider URL specified above.
- **Default Mailbox Expiration Period (days)** – WebSafe supports aging feature for all the messages it stores in its content database. This parameter specifies the default value of the expiry duration for each new mailbox that is created by the administrator. The value is used to form the expiry date for all emails composed from WebSafe. However this value will be useful to detect expiry only if the email is sent within the WebSafe domain to another WebSafe mailbox. This mailbox global value can be changed on a per email basis in future releases.
- **Default No Return Receipt Notification (days) –** WebSafe supports requesting return receipts for emails sent out from its webmail client. In addition if the email is not read within a specified duration, especially for time-sensitive communications, the sender can be informed in order to take further action. If the email is not read within the specified days a notification email is send to the sender to that effect. The notification is in the form of a “Message Disposition Notification” as per RFC 2298. However this value will be useful for no RR notifications only if the email is sent within the WebSafe domain to another WebSafe mailbox. This mailbox global value can be changed on a per email basis in future releases. The default value is -1, which means the feature is disabled.
- **Content Encryption Algorithm –** Specifies the encryption algorithm to be used for encrypting the email content when storing in the database for emails composed through WebSafe email client.
- **Content Encryption Token –** Specifies the content encryption algorithm to be used for encrypting the email content.

- **Postmaster Email Address –** The email address of the administrator of WebSafe Client. The administrator address is the from address for all activation notification emails that get sent from WebSafe.
- **X-Header to Encrypt Clear Archived Messages on Resend –** Header added to resent messages that were archived unencrypted and are resent in "As Is" mode. For example, X-PostX-Secure.
- **Custom Property File Name –** The property file that contains configuration values that are customer specific. You can use the **Select** button to browse for the file.
- **Allow Secure Compose Without Token –** Select to allow secure compose without the use of a token.
- **Attachment Template Type –** Name of the template engine.
- **Attachment Template File –** File containing the attachment template.
- **Maximum Post Size (in KB) –** This parameter limits the maximum size of data posted to WebSafe from the recipient's client machine. This parameter directly affects the maximum size of allowed attachments and should match the size accordingly.
- **Password Challenge Question –** The password challenge feature allows for the system to store a challenge question and corresponding answer for future use if the user forgets his/her password. This will allow the user to select the challenge question you want to use from the drop-down.
- **Registration Cleanup Time –** Number of days before unused registration messages expire.
- **Enable CAPTCHA –** Display the CAPTCHA image that the user must type.
- **Enable X509 certificate enrollment –** Check to enable X509 certificate enrollment. When this parameter is checked, users will see an option to upload an X509 certificate on their enrollment page. Uploading of X509 certificates is optional; users can continue the registration process normally even if they don't have X509 certificates. The system will not accept expired X509 certificates. The email address in the X509 certificate should match the email address for which the certificate is being registered.
- **Enable PGP certificate enrollment –** Check to enable PGP certificate enrollment. When this parameter is checked, users will see an option to upload a PGP certificate on their enrollment page. Uploading of PGP certificates is optional; users can continue the registration process normally even if they don't have PGP certificates. The system will not accept expired PGP certificates.

3. Click the **Deploy Changes** button to commit your configuration.
4. Click the Administration tab and then the **Restart SMTP Adaptor** button. Wait about 15 seconds and the system will be restarted.

Mail Service

1. Click the Configuration tab and then in the left pane click Configuration > Web Services > WebSafe > Mail Service.



2. Enter/edit the following values:

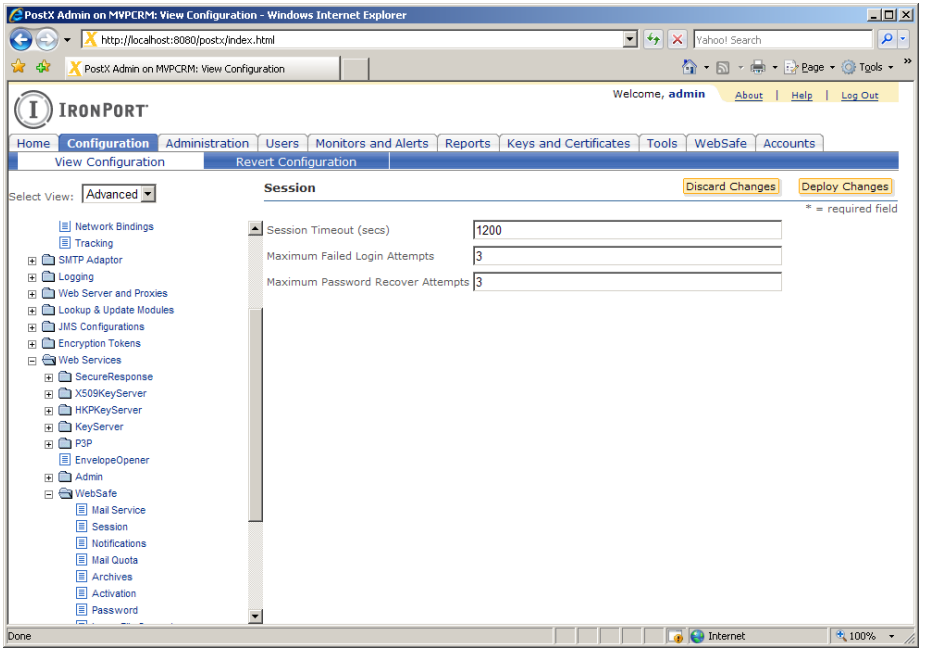
   Mail Service – Used to send return receipt notification emails and emails composed from within WebSafe. The default mail service is "DefaultMail," which is usually the machine that hosts the mail server for the IronPort Encryption appliance. You configure the mail server on the Mail Service node of the Administration Console (in the configuration tab, navigate to Configuration > Mail Services > Mail Service List).

3. Click the **Deploy Changes** button to commit the configuration.

4. Click the Administration tab and then the **Restart SMTP Adaptor** button. The system restarts after approximately 15 seconds.

Session

1. Click the Configuration tab and then in the left pane click Configuration > Web Services > WebSafe > Session.



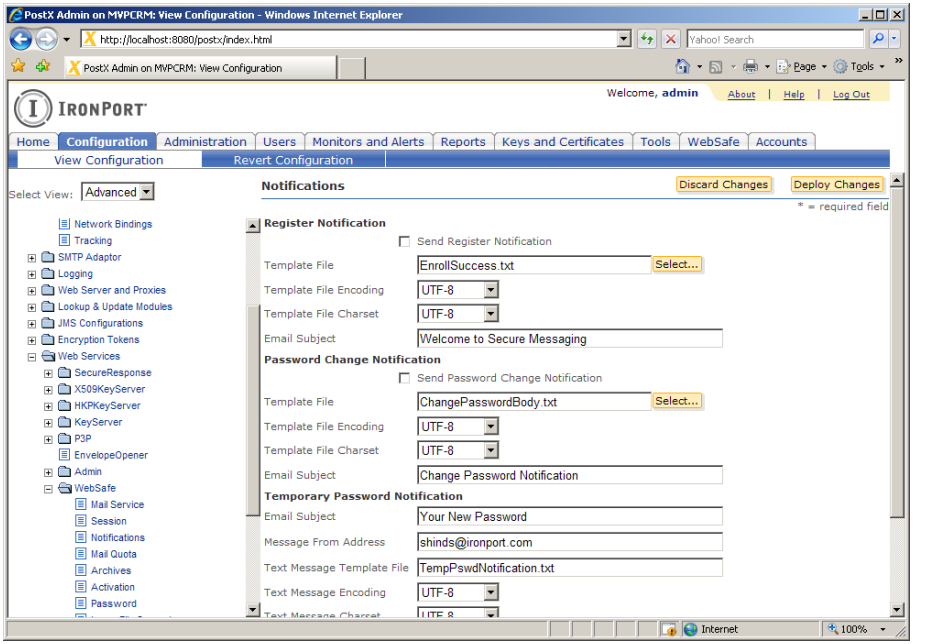
2. Enter/edit the following values:

- **Session Timeout (secs) –** The session logic of WebSafe will automatically logout any recipient when no action is detected for specific duration of time. This duration in seconds is specified here.
- **Maximum Failed Login Attempts –** Specifies the maximum number of password attempts before the user is blocked from further access. A blocked user needs to be enabled by the administrator before he can successfully login to this account.
- **Maximum Password Recover Attempts –** Specifies the number of failed attempts after which the user's status will change to SUSPENDED when the user goes through the Forgot Password link.

3. Click the **Deploy Changes** button to commit your configuration.
4. Click the Administration tab and then the **Restart SMTP Adaptor** button. Wait about 15 seconds and the system will be restarted.

Notifications

1. Click the Configuration tab and then in the left pane click Configuration > Web Services > WebSafe > Notifications.



2. Enter/edit the following values:

   Register Notification:

- **Send Register Notification –** Select to enable the use of registration notifications.
- **Template file –** The name of the template file that contains the notification message text. Click the **Select** button to browse to the location of the file.
- **Template File Encoding –** Encoding that the file is given when it is stored.
- **Template File Charset –** Charset used for the email that the file becomes.
- **Email Subject –** The subject of the registration notification message.

  Password Change Notification:

- **Send Password Change Notification –** Select to send a notification message when a password is changed.
- **Template File –** The name of the template file that contains the password change message text.
- **Template File Encoding –** Encoding that the file is given when it is stored.

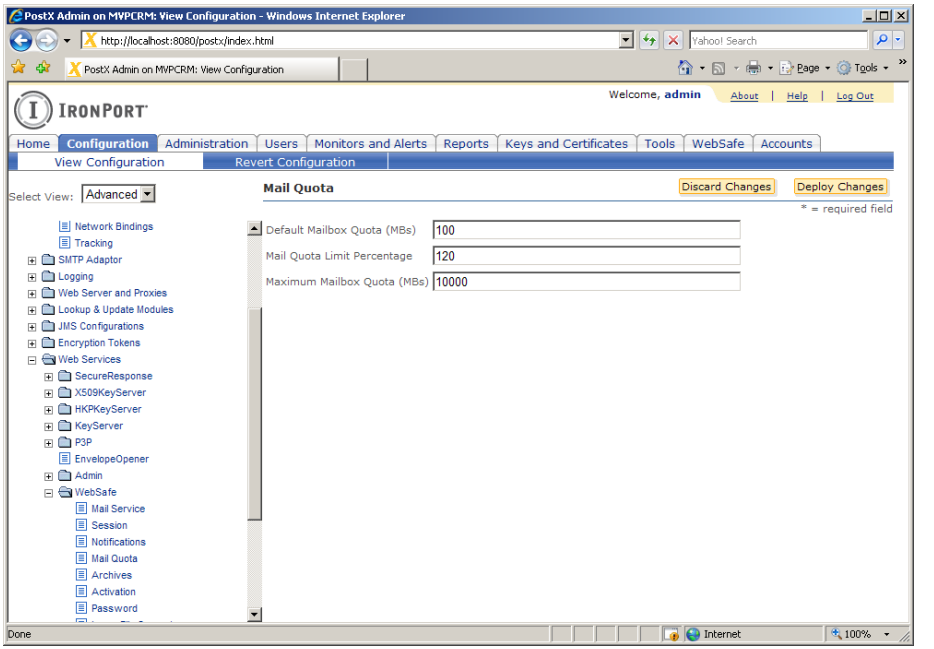
- **Template File Charset –** Charset used for the email that the file becomes.
- **Email Subject** – The subject of the password change notification message.

  Temporary Password Notification:
- **Email Subject** –The subject of the temporary password notification message.
- **Message From Address** – The temporary password email will be from this email address.
- **Text Message Template File –** The name of the text template file that contains the temporary password message.
- **Text Message Encoding –** Encoding that the file is given when it is stored.
- **Text Message Charset –** Charset used for the email that the file becomes.
- **HTML Message Template File –** The name of the HTML template file that contains the temporary password message.
- **HTML Message Encoding –** Encoding that the file is given when it is stored.
- **HTML Message Charset –** Charset used for the email that the file becomes.
- **Change Password URL** – The URL used in the notification email to allow the user to change their temporary password.

3. Click the **Deploy Changes** button to commit your configuration.
4. Click the Administration tab and then the **Restart SMTP Adaptor** button. Wait about 15 seconds and the system will be restarted.

Mail Quota

1. Click the Configuration tab and then in the left pane click Configuration > Web Services > WebSafe > Mail Quota.



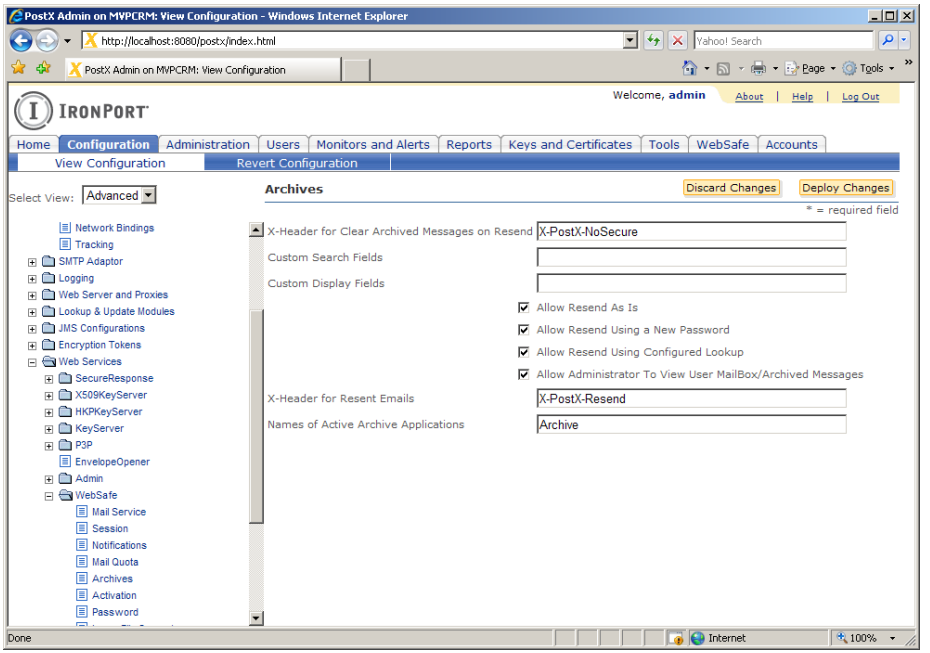
2. Enter/edit the following values:

- **Default Mail Box Quota (MBs) –** The default disk quota or space allocated for each mailbox when created by the admin. (Default = 100MBs)
- **Mail Quota Limit Percentage** – The % limit for the mailbox quota that when reached WebSafe will give an error on the Compose screen and not allow the user to send any email. (Default = 120%)
- **Maximum Mailbox Quota (MBs)** – The size of the mailbox space that can be used before a warning message is sent. (Default = 10000 MBs)

3. Click the **Deploy Changes** button to commit your configuration.
4. Click the Administration tab and then the **Restart SMTP Adaptor** button. Wait about 15 seconds and the system will be restarted.

Archives

1. Click the Configuration tab and then in the left pane click Configuration > Web Services > WebSafe > Archives.



2. Enter/edit the following values:

- **X-Header for Clear Archived Messages on Resend –** Header added to resent messages which were archived unencrypted and are resend in "As Is" mode. For example, X-PostX-NoSecure
- **Custom Search Fields –** A list of custom property fields associated with archived messages which are allowed in the archival search. For example, CustomerID,PlanID,JobID.
- **Custom Display Fields –** A list of names for the custom property fields associated with archived messages which are allowed in the archival search. These display names match 1:1 with the search fields used in Archival. For example, Customer ID,Plan ID,Job ID
- **Allow Resend As Is –** Send messages as they currently are without a new password.
- **Allow Resend Using a New Password –** Send messages with a new password.
- **Allow Resend Using Configured Lookup –** Send Messages encrypted using a configured lookup.
- **Allow Administrator To View User MailBox/Archived Messages –** Determines whether the WebSafe or archive administrator will get the ability to view all messages. If this

parameter is not checked, the administrator can still search and manage or resend all messages, but he cannot view them.

- **X-Header for Resent Emails –** Header added to resent messages which were archived unencrypted and are resend in "As Is" mode. For example, X-PostX-NoSecure.
- **Names of Active Archive Applications –** A comma-separated list of applications that are actively being used for archive purposes.

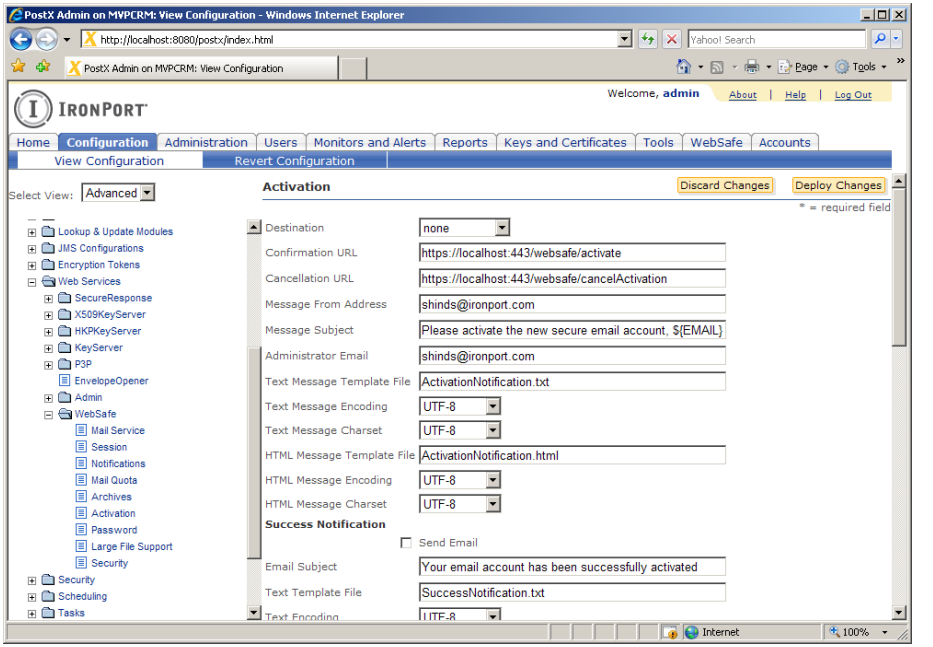
3. Click the **Deploy Changes** button to commit your configuration.
4. Click the Administration tab and then the **Restart SMTP Adaptor** button. Wait about 15 seconds and the system will be restarted.

Please refer to *Chapter 4: Archive System* for more information.

Activation

Use this area to customize the activation email message.

1. Click the Configuration tab and then in the left pane click Configuration > Web Services > WebSafe > Activation.



2. Enter/edit the following values:

- **Destination –** Activation destination. Valid values are recipient, sender, and administrator.
- **Confirmation URL –** URL used in the activation email to confirm the registration.

- **Cancellation URL –** URL used in the activation email to cancel the registration.
- **Message From Address –** The email address the activation is from.
- **Message Subject –** The activation email subject.
- **Administrator Email –** If administrator is selected above, then this is the message destination.
- **Text Message Template File –** Text file containing the email body used for the activation email.
- **Text Message Encoding –** Encoding used for the text message.
- **Text Message Charset –** Charset used for the text message.
- **HTML Message Template File –** HTML file containing the email body used for the activation email.
- **HTML Message Encoding –** Encoding used for the HTML message.
- **HTML Message Charset –** Charset used for the HTML message.

Success Notification:

- **Send Email –** Select to inform users when their accounts have been successfully activated.
- **Email Subject –** The subject of the successful activation email.
- **Text Template File** – The text template of the successful activation email.
- **Text Encoding** – Encoding used for the text version of the successful activation email.
- **Text Charset** – Charset used for the text version of the successful activation email.
- **HTML Template File –** The HTML template of the successful activation email.
- **HTML Encoding** – Encoding used for the successful activation email.
- **HTML Charset** – Charset used for the successful activation email.

Cancel Notification:

- **Send Email** – Select to inform users when their account activation has been canceled.
- **Email Subject** – The subject of the canceled activation email.
- **HTML Template File** – The HTML template of the canceled activation email.
- **HTML Encoding** – Encoding used for the canceled activation email.
- **HTML Charset** – Charset used for the canceled activation email.
- **Text Template File** – The text template of the canceled activation email.
- **Text Encoding** – Encoding used for the text version of the canceled activation email.
- **Text Charset** – Charset used for the text version of the canceled activation email.

Expire Notification:

- **Expiration Period** – Number of days before activation requests expire. A zero value indicates they will never expire.
- **Activation Email Subject** – The subject of the expired activation email.
- **HTML Template File** – The HTML template of the expired activation email.
- **HTML Encoding** – Encoding used for the expired activation email.
- **HTML Charset** – Charset used for the expired activation email.
- **Text Template File** – The text template of the expired activation email.
- **Text Encoding** – Encoding used for the text version of the expired activation email.
- **Text Charset** – Charset used for the text version of the expired activation email.

  Activation Reminder:
- **Email Subject** – The subject of the activation reminder email.
- **HTML Template File** – The HTML template of the expired activation email.
- **HTML Encoding** – Encoding used for the expired activation email.
- **HTML Charset** – Charset used for the expired activation email.
- **Text Template File** – The text template of the expired activation email.
- **Text Encoding** – Encoding used for the text version of the expired activation email.
- **Text Charset** – Charset used for the text version of the expired activation email.

3. Click the **Deploy Changes** button to commit your configuration.
4. Click the Administration tab and then the **Restart SMTP Adaptor** button. Wait about 15 seconds and the system will be restarted.

Password

Forgotten Passwords

When users forget their password they can click the "Forgot Password" link. The system can be configured to either use a password challenge question or to provide a temporary password. The default is to use a temporary password. The forgot password link only works if the account is in a valid state (active or blocked).

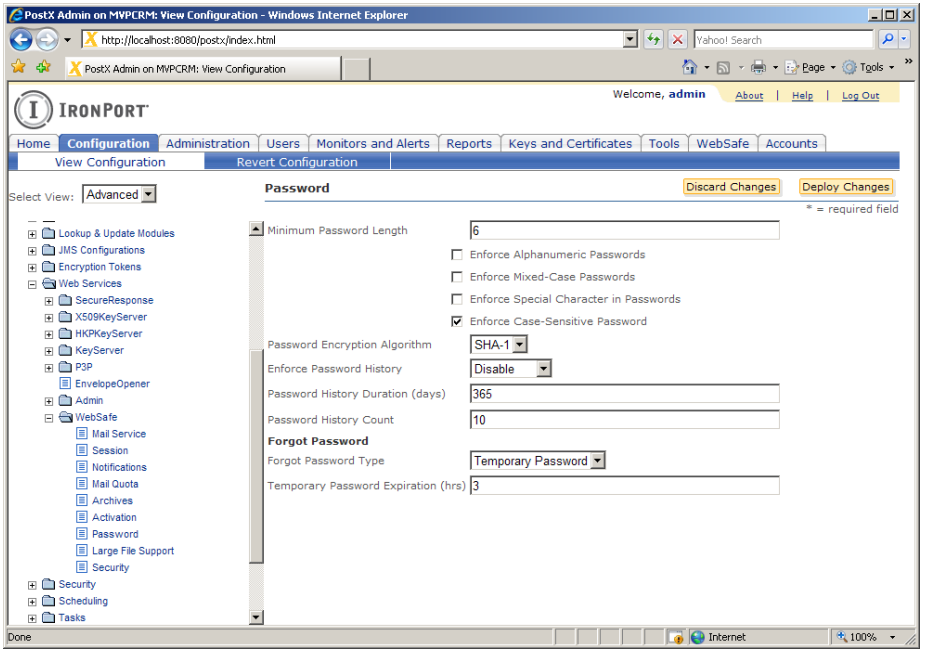
- Temporary Passwords Method

  If you elect to use a temporary password, the user will be asked to enter their email address and a new, temporary, random password will be emailed to them. The password is for one-time use and will only last a specified number of hours. Their old password will continue to work. If the user logs in with a valid, unexpired temporary password, they will immediately be prompted for a new password. When they set a valid password, the temporary password will be expired.
- Password Challenge Question

If you elect to use the password challenge question method, the user will be prompted to answer a previously specified question. If they answer the question correctly, they will immediately be prompted to change their password.

Configuring Passwords

1. Click the Configuration tab and then in the left pane click Configuration > Web Services > WebSafe > Password.



2. Enter or update the following values:

- **Minimum Password Length** – The password management system within WebSafe uses this value to enforce minimum password length.
- **Enforce Alphanumeric Passwords** – If checked, the password management system within WebSafe will enforce all passwords to be alphanumeric.
- **Enforce Mixed-Case Passwords** – If checked, the password management system within WebSafe will enforce all passwords to be mixed case.
- **Enforce Special Character in Passwords** – If checked, the password management system within WebSafe will enforce all passwords to contain special characters.
- **Enforce Case-Sensitive Password** – If this parameter is set checked, then passwords will be case sensitive. Since the database for pxenroll and WebSafe are the same, the sensitivity set in one affects the other. Therefore it is recommended that you set both to either sensitive or not.

- **Password Encryption Algorithm** – The administrator can select the password-hashing algorithm used by WebSafe before storing the passwords to the DataStore. The values available for selection are "SHA-1" and "Plain".
- **Enforce Password History** – Password History allows you to specify frequency with which a password can be reused. This configuration parameter determines how you are going to use this feature. Options are:

  Disable – Do not use the password history feature

  ByDuration – Enforce the password history by duration

  ByCount – Enforce the password history by count
- **Password History Duration (days)** – The number of days that must pass prior to a password being reused.
- **Password History Count** – The number of times that a password can be changed prior to allowing its reuse.

  Forgot Password:
- **Forgot Password Type** – Specifies the action to take when a forgotten password occurs. Values are:
  - **Temporary Password** - If selected, the user will be asked to enter their email address and a new, temporary, random password will be emailed to them.
  - **User-Reset** - If selected, the system will reset the user's password and they will be prompted to change their password immediately.
- **Temporary Password Expiration (hrs)** – Number of hours until temporary password expires.

3. Click the **Deploy Changes** button to commit your configuration.
4. Click the Administration tab and then the **Restart SMTP Adaptor** button. Wait about 15 seconds and the system will be restarted.

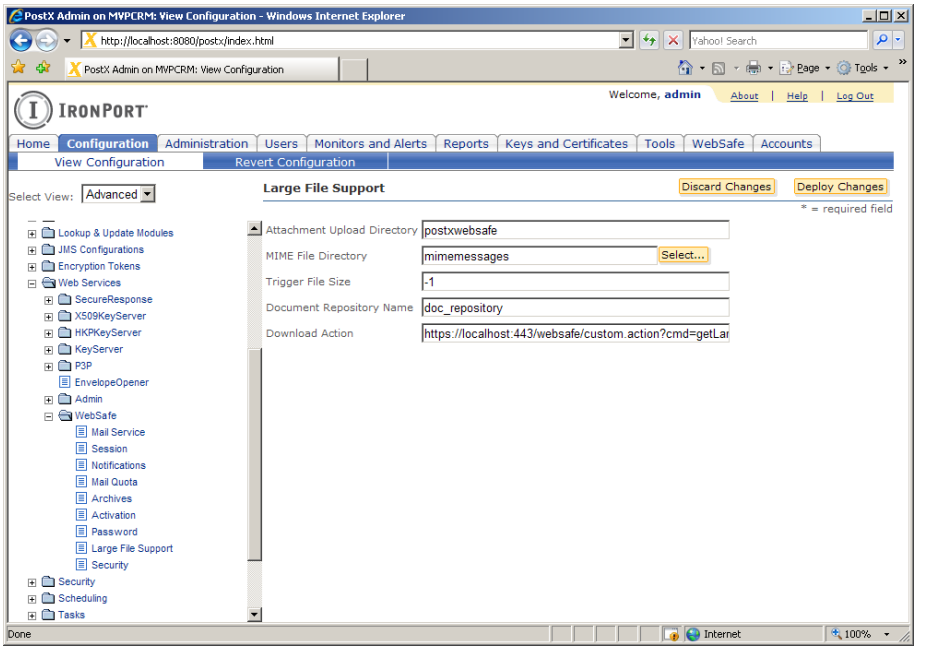
Large File Support

The default WebSafe installation is configured to save sent and received emails in the database. When an email contains one or more attachments the entire email, including the attachments, it is stored in the database. If your users frequently send or receive emails that contain large attachments you can configure WebSafe to save these large files to the hard drive and not in the database.

To enable large file support, enter a maximum file size (in KB) in the Trigger File Size field. When the size of an email and its attachments exceeds this maximum size WebSafe will automatically save the attachments on the hard drive. When the email is viewed (in WebSafe or an external email application) the attachment will still appear as a link. When the user clicks this link, WebSafe will download the attachment to the browser. If the user is not

currently logged into WebSafe then WebSafe will prompt for a valid username and password before permitting the download.

1. Click the Configuration tab and then in the left pane click Configuration > Web Services > WebSafe > Large File Support.



2. Enter/edit the following values:

- **Attachment Upload Directory** – Specifies the directory used to temporarily store attachments that a user has added to an email. The IronPort Encryption appliance creates a unique subdirectory for each user. Any files in a user's subdirectory are deleted when:

    a. the user navigates to the **Compose Message** page to start writing an email,

    b. the email is sent,

    c. the user removes an attachment from the email being composed or

    d. the user logs out of WebSafe.

    In addition, all contents of the Attachment Upload Directories (all users' subdirectories) are deleted when the encryption server is restarted. A user's temporary files are not deleted when the user's session times out (that is, the user does not explicitly log out of WebSafe) but will be deleted when the user next logs in and composes an email or explicitly logs out of WebSafe.

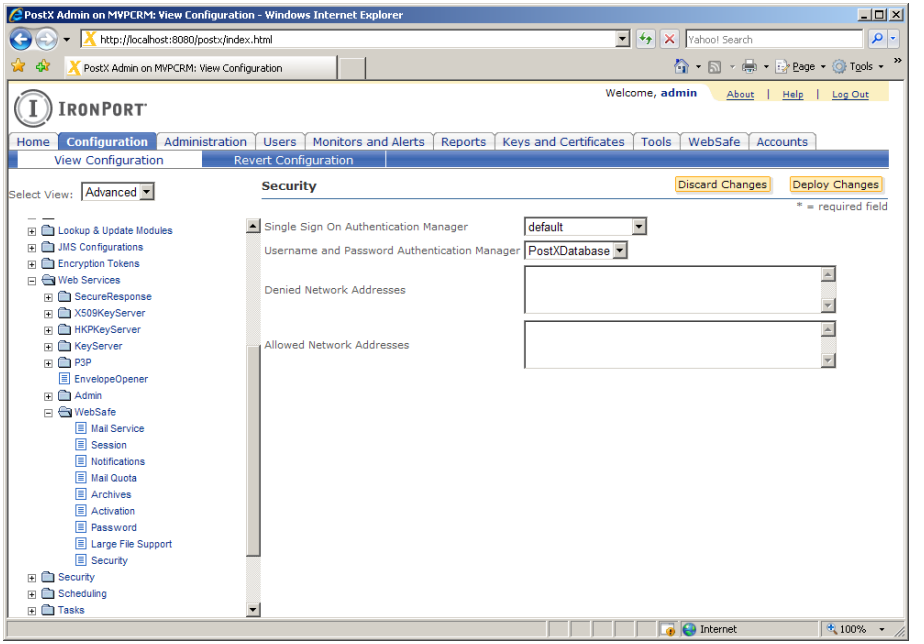
If you change the value of the **A**ttachment Upload Directory field so that a different directory path is used any temporary files stored in the previous directory path (and all user subdirectories) will not be deleted; for example, files that were uploaded as part of an email that was not sent before the user's session timed out. When you change this value you will have to manually delete the files in the previous directory using OS file management tools. Since some of the files in this previous directory may be associated with an email that a user is currently composing, we recommend that you do not delete the contents of the previous directory until the encryption server has been restarted.

- **MIME File Directory** – Directory to save the MIME message in when file save is triggered. You can use the **Select** button to browse for the file.
- **Trigger File Size** – File size that triggers files to be saved to disk. If -1, there is no file size trigger.
- **Document Repository Name** – Name of the document repository.
- **Download Action** – The location of the download repository. The default is https://<*Server_Name*>/websafe/custom.action?cmd=getLargeFile

3. Click the **Deploy Changes** button to commit your configuration.
4. Click the Administration tab and then the **Restart SMTP Adaptor** button. Wait about 15 seconds and the system will be restarted.

Security

1. Click the Configuration tab and then in the left pane click Configuration > Web Services > WebSafe > Security.



2. Enter/edit the following values:

- **Single Sign On Authentication Manager** – Used for authentication that is using providers that DO NOT require a username and password to be entered by the user. This includes X509 certificates, remember me cookie and single sign on.
- **Username and Password Authentication Manager** – Used for authentication that is using providers that DO require a username and password to be entered by the user. This includes the default database, Kerberos, Lookup, and LDAP.
- **Denied Network Address** – List of network addresses that are denied access to the application. (Comma separated)
- **Allowed Network Address** – List of network addresses that are allowed access to the application. (Comma separated)

3. Click the **Deploy Changes** button to commit your configuration.
4. Click the Administration tab and then the **Restart SMTP Adaptor** button. Wait about 15 seconds and the system will be restarted.

APPENDIX A

Configuration Parameters

This appendix contains a complete list of configuration parameters for the Configuration node, which you access on the Configuration tab.

Note — The nodes that you can access depend on the view you select. Select Expert view to display all nodes, or select Standard view to display only basic nodes. For more information, see the chapter called "Administration Console Basics" in the *IronPort Encryption Appliance Operations Manual*.

This appendix contains the following sections:

CONFIGURATION

Globals

Parameter	Definition
Mail Server Domain Name	Name of the mail server for the IronPort Encryption appliance. This domain name is used when you connect to the mail server, and it responds with a fully-qualified mail server name.
Mail Root Directory	Root folder for the mail spool queues and mail folders.
Crypto Provider	Select the crypto provider you want to use from the drop-down list. Valid values are PostX and RSA JsafeJCEFIPS. To use a crypto provider other than PostX, you must download and install the JCE Unlimited Strength Jurisdiction Policy Files from `http://java.sun.com/products/jce/index-14.html` To use AES encryption with the RSA JCE provider, Unlimited Strength Jurisdiction Policy Files 1.4.2 must be downloaded and installed from `http://java.sun.com/j2se/1.4.2/download.html#docs`
Always Set Secure Cookies	If checked, any cookies created are marked secure.
Customer Support Email	Email Address to contact customer support.

Auditing

For definitions of individual audit components, please refer to the "Auditing" chapter in the *IronPort Encryption Appliance Operation's Manual*.

Parameter	Definition
Audit Service	JNDI lookup name for the auditor service.
Audit Queue Processing Interval (secs)	The interval in seconds for writing auditing to the database. A - 0 value indicates synchronous writes after creation of each auditing record.
Record Unknown Events	If checked, events not listed above are recorded, otherwise they are ignored.

Caching

Parameter	Definition
Automatic Discovery Options	
Automatically Discover Cache Peers	If checked, cache peers in this cluster are discovered automatically.
Multicast Group Address	Multicast group address for auto-discovery of cache peers.
Multicast Group Port	Multicast group port for auto-discovery of cache peers.
Time To Live	Specifies how fare the multicast packets will propagate.
Manual Discovery Options	
Cache Cluster Servers	Comma-separated list of cache cluster server host names or IP addresses.

File Encodings

Parameter	Definition
File Encodings	This area allows you to select the values that populate the file encoding fields that appear throughout the UI. It also allows you to add a new encoding with the caveat that it has to be a valid Java character encoding. Current values are: • ISO-8859-1 • UTF-8 • UTF-16 • Shift-JIS|SJIS • Big5

Local Server Group

Parameter	Definition
Group Member Name	Group member name (display only).
JNDI Provider URL	This group member's JNDI provider URL.
Initial Context Factory	This group member's initial context factory.
JNDI Principal	Principal (user) used to access this group member.

Parameter	Definition
JNDI Credentials	Credentials (passwords) used to access this group member.

Multi Server

Parameter	Definition
Remote Server	The server in the local server group that provides the remote services for this server.

Network Bindings

Parameter	Settings
Naming Service Binding Address	Network adaptor that the naming service will bind to
Naming Service Port	Network port that the naming service will bind to
Naming Service RMI Binding Address	Network adaptor that the naming RMI service will bind to
Naming Service RMI Port	Network port that the naming RMI service will bind to
Web Services Binding Address	Network adaptor that the web services will bind to
Web Services Port	Network port that the web service will bind to
RMI Invoker Binding Address	Network adaptor that the RMI invoker will bind to
RMI Invoker Port	Network port that the RMI invoker will bind to
JMX RMI Adaptor Binding Address	Network adaptor that the JMX RMI adaptor will bind to
JMX RMI Adaptor Port	Network port that the JMX RMI adaptor will bind to
Web Server Binding Address	Network adaptor that the web server will bind to
Web Server Port	Network port that the web server will bind to
Web Server SSL Port	Network port that the web server will bind to for SSL
Web Server AJP13 Port	Network port that the web server AJP13 listener will bind to
JMS OIL Listener Binding Address	Network adaptor that the JMS OIL listener will bind to
JMS OIL Listener Port	Network port that the JMS OIL listener will bind to
JMS OIL2 Listener Binding Address	Network adaptor that the JMS OIL2 listener will bind to

Parameter	Settings
JMS OIL2 Listener Port	Network port that the JMS UIL2 listener will bind to
JMS UIL2 Listener Binding Address	Network adaptor that the JMS UIL2 listener will bind to
JMS UIL2 Listener Port	Network port that the JMS UIL2 listener will bind to
Hypersonic DB Binding Address	Network adaptor that the Hypersonic DB server will bind to
Hypersonic DB Port	Network port that the Hypersonic DB server will bind to
Cache Listener Binding Address	IP address of network adaptor the distributed Cache binds to.
Cache Listener Port	Port the Cache listener binds to.
Mail Server Remote Manager Enabled	Enable or disable the mail server remote manager
Mail Server Remote Manager Binding Address	Network adaptor that the mail server remote manager will bind to
Mail Server Remote Manager Port	Network port that the mail server remote manager will bind to
Mail Server SMTP Service Enabled	Enable or disable the mail server SMTP service
Mail Server SMTP Binding Address	Network adaptor that the mail server SMTP service will bind to
Mail Server SMTP Port	Network port that the mail server SMTP service will bind to
Mail Server SMTP TLS Service Enabled	Enable or disable the mail server SMTP TLS service
Mail Server SMTP TLS Service Binding Address	Network adaptor that the mail server SMTP TLS service will bind to
Mail Server SMTP TLS Service Port	Network port that the mail server SMTP TLS service will bind to
Mail Server SMTP TLS Service Keystore Path	Path where the mail server TLS keystore is located.
Mail Server SMTP TLS Service Keystore Password	Password to open the keystore.

Tracking

Parameter	Definition
Tracking Level	Governs the amount of detail that is written to the tracking database for each email message. Levels are: • None • Errors Only • Deliveries and Errors
Tracking Service	Name of the tracking service.
Tracking Queue Length	How many tracking steps to queue before writing to the database. When the number of messages in the queue exceed Tracking Queue Length they are written to the database.

Templates

Parameter	Definition
WebServer URL	Specifies the base URL to use when the appliance sends out notifications. For example, the base URL appears in the Help and About links on the notification message that is sent to recipients of Secure Envelopes. The WebServer URL field is initially populated with the public hostname that you specify during installation.

SMTP ADAPTOR

Network

Parameter	Definition
DNS Server	Primary DNS server to use for address lookup. If you change this value, you will also need to go to the Monitors and Alerts tab and change the "DefaultDNSMonitor" to point to your new DNS Server address.
Secondary DNS Server	An optional secondary DNS server to use for address lookup.
Mail Server Domain Name	Display-only field.
Auto Detect Server Name	Select if you want to auto detect the server name.
Auto Detect Server IP	Select if you want to auto detect the server IP address.
PostMaster Email Address	The email address users will send mail to when they encounter problems. You should change this value to an address that can receive incoming messages.
Keep Message in Memory	Stores the messages in memory.
Enable Block Read	Read SMTP requests in blocks instead of a character at a time.
SMTP Authorization Required	SMTP Authorization required.
SMTP Pre-Authenticated Addresses	Comma separated list of Authorization Addresses for SMTP authorization.
Auto Detect Hello Name	Auto detect the hostname to identify itself in the SMTP protocol.
SMTP Adaptor Hello Name	SMTP server host name. Display-only field.
Maximum Recipients per Message	Maximum number if recipients accepted per email.
Maximum Message Size (KBs)	Maximum SMTP message sixe in Kilobytes, set to 0 for unspecified.
Maximum Loop Count	Maximum number of times a message is seen before being considered in a loop.
Require Client TLS	Require all clients to connect using TLS.

SSL Authentication

Parameter	Definition
Require TLS Certificates	If checked, TLS connections are only allowed with servers presenting TLS server certificates.
Accept Untrusted Certificates	If checked, TLS connections are allowed even with servers presenting TLS certificates from an unknown CA.
Accept Self Signed Certificates	If checked, TLS connections are allowed even with servers presenting self-signed TLS certificates.
Accept Expired Certificates	If checked, TLS connections are allowed even with servers presenting expired TLS certificates.
Accept Not yet Valid Certificate	If checked, TLS connections are allowed even with servers presenting not yet valid TLS certificates.

Threads

Parameter	Definition
Number of Spool Threads	Number of threads processing messages from the spool queue

Queues

Parameter	Definition
Mail Root Directory	Root folder for the mail spool queues and mail folders
Mail Storage Type	Storage type for the spool queues and mail folders
Inbox Folder	Path where mail inboxes are stored
Outgoing Queue	Base path name where outgoing messages are queued for delivery
Error Folder	Path where messages that could not be delivered are stored
Spool Queue	Path where incoming messages are queued for processing
Bounce Queue	Path where messages that must be bounced are queued for processing
Mailing List Folder	Path where mailing lists are stored
Users Account Folder	Path where user account information is stored
User Repository Class	Name of the repository class used for storing user account information to files. For file queue, this value should be org.apache.james.userrepository.UsersFileRepository.
Enable JMS Receiver	Enables the SMTP adaptor service to read messages from a JMS queue
JMS Queue Name	Name of the JMS queue that the SMTP adaptor reads MIME messages from
Encryption Algorithm	Specifies the encryption algorithm to use when encrypting files in the James Spool and Queues. Valid values are: None, ARC41 and AES.
Encryption Token	Encryption token.

Mail Retrieval

Parameter	Definition
Mail Retriever Name	
Host	Name of mail server host to pop mail from.
User Name	Name of account holder.
Password	Password for the account.
Start Time:	
Hour	Hour field for start time
Minute	Minute field for start time
Second	Second field for start time
Stop Time:	
Hour	Hour field for start time
Minute	Minute field for start time
Second	Second field for start time
Interval (msecs)	Fetch interval (Default 60000= fetch runs every minute).
Protocol	Mail Provider Name. Can be either pop3 or imap.
Folder	Folder From which mail will be fetched.
Leave Message On Server	Specifies if messages must be left on the server.

Router RuleSets

Parameter	Definition
Rule Name	The rule name.
Description	A description of the rule.
Enabled	Check this box to enable the rule.
Test	The name of the test that the system will run on each message.

Parameter	Definition
Test Type	An operator that determines the action that the system will take. Valid test types are IF and IF NOT.
Actions	Determines what the system does when a message meets the test qualifications.
On Match	Select the action you want the system to take. Valid values are: • **Send to Router RuleSet**- Select the router ruleset you want to send the message to from the drop-down. • **Send to Application** - Select the application you want to send the message to from the drop-down. • **Store in Repository** - Enter the repository where you want the message to be stored. You do not need to enter the full path because it defaults to <home>/apps/james/var/mail/. The new repository will appear on the Home page in the Spool Repositories box. • **Discard** - The message is discarded.
On Error	Select the action you want the system to take. Valid values are: • **Send to Router RuleSet**- Select the router ruleset you want to send the message to from the drop-down. • **Send to Application** - Select the application you want to send the message to from the drop-down. • **Match All** - A message must pass all tests for the rule action to be invoked. • **Match None** - A message only needs to pass any one of the tests for the rule action to be invoked. • **Discard** - The message is discarded.

Basic, Gateway Encrypt, Archive, Resend, BounceHandler

Note: Please note that the above matchers share the same configuration parameters.

Parameter	Definition
Match Name	Name of the matcher.
Matcher Condition	Condition that the matcher will check for.

Content Filter

Please refer to the *IronPort Encryption Appliance Content Filter* manual for information on using and configuring the content filter.

Subject Filter

Parameter	Definition
Name	Name of the matcher.
Match	Specifies the type of match. Values are At Beginning of Subject, At End of Subject, Anywhere in Subject, and Entire Subject.
Search String	The pattern you want to match against.
Case Sensitive	Determines whether you are matching based on case sensitive.
Search String is Regular Expression	Specifies whether the match pattern should be interpreted as a literal string or as a regular expression when comparing against the subject.
On Match	Specifies whether you want to replace the matched part of the subject (with the replacement text), remove the matched part, or do nothing.
Replacement String	If you choose replaceMatch as your action, the matched portion of the subject will be replaced with this string. If use regex, is selected regex style replacement will be used.
Replace All Matches	Modify all instances of match found.

Is S/MIME Matcher, Is PGP Matcher

Parameter	Definition
Match	Specifies whether you want to match Signed Only and Encrypted.
Sender Host List	Sender host list.

Lookup Matcher

Parameter	Definition
Property Match	Property match.
Case Sensitive	Specifies whether it is case sensitive.

Parameter	Definition
Match If Property Not Found	Match to use if the property is not found.
Key Lookup is Domain	If checked, indicates the key lookup should be done by domain.
Key Lookup Domain Prefix	The prefix used when doing the domain lookup.
Lookup Provider	Lookup provider.
Lookup Identity	Lookup identity.

Registered Envelope Matcher

Parameter	Definition
Attachment Name	Attachment name.
Sender Domain	From domain.

Anti-Virus Command Line Matcher

Parameter	Definition
Anti-virus Scanner	The full path to the anti-virus command line scanner executable.
Command Line Parameters	Option command line parameters that are passed to the anti-virus scanner.
Scan Always	Scan the email even if there are no attachments.
Exit Codes	Comma separated list of exit codes indicating that a virus was found.

ClamAV Anti-Virus Matcher

Parameter	Definition
ClamAV Server	The host name or IP address where CLAMD is running.
ClamAV Port	The port on which CLAMD is listening.
Maximum Startup Pings	The maximum number of connection retries during startup, 0 = no startup test will be done.

Parameter	Definition
Ping Intervals (msecs)	The interval between each connection retry during startup.
Buffer Size	The buffer size used when writing to the CLAMD daemon.
Connection Timeout (msecs)	The connection time (ms) when making the main connections (not for the initialization pings).
Debug	Enables debug log messages.

MIME Header Filter Matcher

Parameter	Definition
Allowed Network Addresses	A comma separated list of network addresses specified in the same format as any other 'Net' matcher. Messages coming from clients in this list will NOT have the IronPort Encryption appliance headers removed from the email message.
Headers to Remove	A comma separated list of regular expressions for the MIME header names that are to be removed. For example: `X\-PostX\-.*`
Headers to Keep	A comma separated list of regular expressions for the MIME header names that are NOT to be removed. For example: `X\-PostX\-Secure.*,X\-PostX\-Key,X\-PostX\-SHAedKey`
Return Network Match Result	Specifies whether the result from the 'allowed network address' test should be returned as the matcher results. This allows the matcher to be used as an network matcher as well as a MIME header filter. Generally this should be deselected (false) so that the matcher acts as a filter and all messages are passed through it.

TLS Enabled Matcher

Parameter	Definition
Connect Timeout	Time in milliseconds for connecting to a remote SMTP server.
Read/Write Timeout	Time in milliseconds for reading and writing messages to a remote SMTP server.

Parameter	Definition
Cache Size	Size of the cache used to store information read from a remote SMTP server.
Cache Timeout (mins)	Amount of time in minutes that information read from a remote SMTP server will remain in the cache.

PY Matcher or Filter

Parameter	Definition
Code	Jython code used to validate or manipulate messages passing through the IronPort Encryption appliance matchers.

PY Matcher or Filter

Parameter	Definition
Code	Jython code used to validate or manipulate messages passing through the IronPort Encryption appliance matchers.

User Status Matcher

Parameter	Definition
User Status	User status value to match against.

Applications

There may be multiple applications associated with an installation of the encryption server. The configuration parameters vary depending upon the application type.

Offline Envelope, Offline Envelope - Enrolled, Registered Envelope - Enrolled, and Registered Envelope - PxMail - Details Tab

Note: Please note that the above applications share the same configuration parameters on the Details tab.

Parameter	Definition
Mail Root Directory	The root path that the application will use for spool queues. This value is configured in the Globals section and shown here for convenience.
Application Name	Name of the application.
Matcher Name	Name of the matcher.
Mailet Class	Action taken when a message matches the rule specified in the matcher. This is the name of a Java class that implements the required functionality and should not normally be changed.
Envelope	Envelope type you want to use for this application.
Use Charset for Locale Mapping	Check this option if you want to select the locale and corresponding envelope and message template files based on the charset of the incoming email. The encryption server will use the mapping file to select entries corresponding to the email charset. For example, the encryption server supports English and Japanese locales. By enabling this option, if the incoming email is in English it will map to the English locale. Conversely, if the incoming email has the charset as Shift-JIS (or iso-2022-jp) it will map the Japanese locale. Both these entries have to exist in the CharsetLocaleMap.txt file.
Bounce Unsupported Charsets	If selected, this option results in incoming emails with unsupported charsets (no corresponding entry in the map file) to be bounced back instead of using the DefaultLocale. This entry is valid only if "Use Charset for Locale Mapping" is selected. Using the above example, if you get an email with the charset as “ks_c_5601-1987” with this option enabled the email will be bounced back to the sender with appropriate messages.

Parameter	Definition
Default Locale	Default locale to be used in selecting envelope and related template files. The default value is “en_US” and can be changed to any supported locale by the server. If UseCharsetToLocaleMapping is not selected above, the default locale will represent the locale for all incoming emails. Similarly if that option is selected, and Bounce Unsupported Charsets is not selected, then the default locale will be used for all incoming emails that don’t map to any specific locale in the mapping file.
Envelope Date Format	Format for the date stamp shown on the Registered Envelope. It could be selected as one of the standard four formats (“dd-mm-yyyy”, “mm-dd-yyyy”, “yyyy-mm-dd” or “yyyy-dd-mm”) or “Use locale” which allows the date formatting to be based on the locale selected for each incoming email.
Envelope Time Format	Format for the time stamp shown on the Registered Envelope. It could be selected as one of the different hour, minute and second combinations or “Use locale” which allows the time formatting to be based on the locale selected for each incoming email.
User Key Name	If set, the user's key is cached in their browser using this name as the cookie name.
Master Key Base	Used in Fallback Key Retrieval to generate the fallback key.
Split Message by Recipient	Separate the incoming message into one per recipient and process them individually
Secure Email From	The email address that displays in the From field.
Secure Email Reply-To	The email address that is used when recipient’s reply to the message.
Cache Session Key	If checked, generated envelopes cache the session key in a cookie when the user initially opens the envelope. If Encrypt Cached Session Key isn't set, the user won't have to enter a password to open the envelope.
Encrypt Cached Session Key	If checked, and the session key is cached, the cached session key is first encrypted with the user's key.
Open Automatically (when possible)	If checked, and the key is available at startup, the envelope will open automatically.

Parameter	Definition
Suppress Applet for Open	If checked, the IronPort Encryption appliance tools applet won't be used to open multi-file payloads.
Open in Same Window (less secure)	If checked, multi-file payloads open in the same window as the envelope. This will leave decrypted files on disk but doesn't trigger pop-up blockers.
Maximum Open Attempts	Maximum number of times a recipient can attempt to open an offline envelope before he is locked out. Leave blank for no limit. For Registered Envelopes, configure the maximum open attempts in the Max Database Retries configuration parameter located in Web Services, Key Retrieval, Keystore Database.
Opener Host	Hostname and port of the online envelope opener service.
Use GET Payload Transport (GPT)	If checked, envelopes use an alternate payload transport method (that is compatible with Outlook Web Access) when JavaScript isn't available. The envelope needs to be specially constructed to take advantage of this method.
GPT URL	The URL the payload is sent to when GET Payload Transport is checked. This need not be secure as the payload is encrypted. The user's credentials are sent and the envelope contents are received over an SSL connection to the host specified in Opener Host.
GPT Token	The token used when generating GET Payload Transport payload fragments.
Enable Tracking	Select to enable tracking of outgoing emails for the application.
Notify Sender on Failure	Notify the sender that the message failed
Next	Determines which application the mail will pass through once it is processed by the current application.

WebSafe - Details Tab

Parameter	Definition
Mail Root Directory	The root path that the application will use for spool queues. This value is configured in the Globals section and shown here for convenience.
Application Name	Name of the application.

Parameter	Definition
Matcher Name	Message matching rule. See matcher parameters for more information.
Mailet Class	Action taken when a message matches the rule specified in Match. This is the name of a Java class that implements the required functionality and should not normally be changed.
Send Notification to Sender	If enabled, a notification email is sent to the sender for each email that WebSafe receives. The notification is in the form of a "Message Disposition Notification" as per RFC 2298.
Send Notification on Failure	Sends a notification email to the sender for each incoming email that WebSafe is unable to process. The notification is in the form of a "Message Disposition Notification" as per RFC 2298. If WebSafe is not able to find the mailbox for the specified recipient (which means recipient is not enrolled with WebSafe) then the recipient email address will be listed in the failure notification send to the sender.
Send Notification to Recipient	Sends a notification email to the recipient for each email received indicating that the recipient has a new email in his WebSafe account. This notification email also includes the URL to login to WebSafe. If this URL is used to logon to WebSafe the recipient will see the new emails received in his mailbox
Use Mailbox Notification Address for Notifications	Sends a notification email to the mailbox notification address for each email received indicating that the recipient has a new email in his WebSafe account.
Compress Messages	Compresses all messages stored in WebSafe mailboxes before storage.
Expiration Period (days)	WebSafe supports aging feature for all the messages it stores in its content database. This parameter specifies the default number of days the email (content) will be held in the content database before it is marked for deletion. Once the email is marked for deletion it remains in the database but is not seen by the recipient. In order to disable this feature and not have a default expiry limit for all messages specify the parameter as –1. This application global value can be changed on a per content basis by specifying the value for each incoming email.

Parameter	Definition
Unread Notification Period (days)	WebSafe supports sending return receipts when the recipient reads a new email and this can be enabled by a separate configuration parameter. In addition if the email is not read within a specified duration, especially for time-sensitive communications, the sender can be informed in order to take further action. This parameter specifies the number of days counting from the sent-date by which the recipient should have read his email. If the email is not read within the time limit a notification email is send to the sender to that effect. The notification is in the form of a "Message Disposition Notification" as per RFC 2298. The default value is –1 indicating that this notification feature is not enabled. This application global value can be changed on a per content basis by specifying the value for each incoming email.
Send Return Receipt	If enabled, this parameter applies to all emails composed from WebSafe email client and the outgoing emails contain standard SMTP header information requesting return receipt. A return receipt notification email is sent to the WebSafe sender mailbox for each new email opened by the recipient. The notification is in the form of a "Message Disposition Notification" as per RFC 2298. Please note that not all external email clients will respect this SMTP header for Return Receipt and hence RR is not guaranteed for emails sent out to the external world.
WebSafe URL	This URL is specified in the notification emails sent to the recipient as explained above. The format of the URL is `http://<host name>:8080/WebSafe/login.jsp.` Here host name is the machine running the webserver/appserver where the WebSafe web mail client is deployed.
Postmaster Email Address	Email address of the WebSafe administrator.
Encryption Algorithm	Encryption algorithm to be used for encrypting the email content when storing in the database. Options are: None, ARC4 and AES.
Encryption Token	The encryption token to use when encrypting messages stored in the database. This drop-down is populated when you add encryption tokens via Configuration > Encryption Tokens > Token List.

Parameter	Definition
Recipient Destination	Defines the type of data shown after login. The three values are “Inbox” which shows the recipient his complete inbox on login, “SingleMessage” which shows the recipient a single email message which generated this notification and “UnreadMessages” which shows the recipient all the unread emails from the mailbox. The recipient notification sent from WebSafe includes the WebSafeURL, which lets the user login to WebSafe, and access his mailbox.
Notification Text Template File	File which contains the email message text for the recipient notification email sent from WebSafe. The file can be changed to reflect the new text or a new file can be specified. You can use the **Select** button to browse for the file.
Notification Text Template File Encoding	The encoding that the file is given when it is stored.
Notification Text Charset	The charset used for the email that the file becomes.
Notification HTML Template File	File which contains the email message HTML for the recipient notification email sent from WebSafe. The file can be changed to reflect the new HTML or a new file can be specified. You can use the **Select** button to browse for the file.
Notification HTML Template File Encoding	The encoding that the file is given when it is stored.
Notification HTML Charset	The charset used for the email that the file becomes.
Use Incoming Subject As Outgoing Subject	If checked, the subject of the new email notification mail will be the same as that of the message delivered. By default this parameter is not checked.
Notification Subject	Notification email subject.
Notification Sender	The email address that displays in the From field of notification emails.
Notification Reply-To	The email address that is used when recipient’s reply to the notification email.
Use Variable Substitution	Enables personalization of the text message that is sent with each email.
Notification Variable Map File	Java properties file containing the variables mapping. The default value is variablemap.properties.

Parameter	Definition
Bounce Application	Name of the application used to process bounced messages.
Delivery Application	Name of the application used to deliver messages.
Enable Tracking	Select to enable tracking of outgoing emails for the application.
Next	Specifies which application or ruleset the mail will pass through once it is processed by the current application or ruleset.

Archive - Details Tab

Parameter	Definition
Mail Root Directory	The root path that the application will use for spool queues. This value is configured in the Globals section and shown here for convenience.
Application Name	Name of the application.
Matcher Name	Message matching rule. See matcher parameters for more information.
Mailet Class	Action taken when a message matches the rule specified in Match. This is the name of a Java class that implements the required functionality and should not normally be changed.
Compress Messages	If enabled, all messages stored in WebSafe mailboxes are compressed before storage.
Create Mailbox	If checked, a mailbox is created using the To address of the archived email if the mailbox does not exist.
Mailbox Prefix	This value of this parameter is prepended to the archived email address before creating the mailbox. The prefix would be useful if you want to keep the official mailbox for a user different from his archived mailbox. So if the prefix is “archive-“, an incoming email to user@enterprisedomain.com will result in a mailbox created as “archive-user@enterprisedomain.com”.

Parameter	Definition
Archive Folder	The default archive folder for messages would be the Inbox for the respective mailboxes. However you can optionally archive the messages to a separate folder in each mailbox. The intent is to logically separate messages, if desired, into separate archived folders as “Statements” and “Confirms” etc.
Encryption Period (days)	Number of days after which the mail in the archive folder will be discarded.
Encryption Algorithm	Specifies the encryption algorithm to be used for encrypting the email content when storing in the database. The current version of the server does not support encryption of the content and hence this option will not have any significant effect. In the future, this parameter will allow the administrator to choose the encryption algorithm from values like RC4, 3DES etc.
Encryption Token	The encryption token to use when encrypting messages stored in the database. This drop-down is populated when you add encryption tokens via Configuration > Encryption Tokens > Token List.
Enable Tracking	Select to enable tracking of outgoing emails for the application.
Next	Specifies which application or ruleset the mail will pass through once it is processed by the current application or ruleset.

Resend - Details Tab

Parameter	Definition
Mail Root Directory	The root path that the application will use for spool queues. This value is configured in the Globals section and shown here for convenience.
Application Name	Name of the application.
Matcher Name	Message matching rule. See matcher parameters for more information.
Mailet Class	Action taken when a message matches the rule specified in Match. This is the name of a Java class that implements the required functionality and should not normally be changed.

Parameter	Definition
Enable Tracking	Select to enable tracking of outgoing emails for the application.
Next	Specifies which application or ruleset the mail will pass through once it is processed by the current application or ruleset.

SMTP Delivery - Details Tab

Parameter	Definition
Mail Root Directory	The root path that the application will use for spool queues. This value is configured in the Globals section and shown here for convenience.
Application Name	Name of the application.
Matcher Name	Message matching rule. See matcher parameters for more information.
Mailet Class	Action taken when a message matches the rule specified in Match. This is the name of a Java class that implements the required functionality and should not normally be changed.
Use SMTP EHLO command	If checked, the SMTP EHLO command is used instead of HELO.
Use SMTP STARTTLS command	If checked, the SMTP STARTTLS command is used to enable TLS.
Use SMTP Authentication	If checked, authenticate with the mail server or gateway with the username and password.
SMTP User Name	Username used to authenticate with the mail server or gateway.
SMTP Password	Password used to authenticate with the mail server or gateway
Connection Timeout (msecs)	Number, in milliseconds, that the system will try to connect to a remote SMTP server. (Default = 60000)
Bounce Application	Specifies the bounce application.

Parameter	Definition
Flag Bounce As Failure	This flag is only used if the "Bounce Application" is specified. If this flag is set, the bounced email will be flagged as a delivery failure. If this flag is not set, the bounce email will be sent unmodified.
Enable Tracking	Select to enable tracking of outgoing emails for the application.
Next	Specifies which application or ruleset the mail will pass through once it is processed by the current application or ruleset.

Gateway Encrypt - Details Tab

Parameter	Definition
Mail Root Directory	The root path that the application will use for spool queues. This value is configured in the Globals section and shown here for convenience.
Application Name	Name of the application.
Matcher Name	Message matching rule. See matcher parameters for more information.
Mailet Class	Action taken when a message matches the rule specified in Match. This is the name of a Java class that implements the require functionality and should not normally be changed.
Enable Tracking	Select to enable tracking of outgoing emails for the application.

Queue Message - Details Tab

Parameter	Definition
Mail Root Directory	The root path that the application will use for spool queues. This value is configured in the Globals section and shown here for convenience.
Application Name	Name of the application.
Matcher Name	Message matching rule. See matcher parameters for more information.

Parameter	Definition
Mailet Class	Action taken when a message matches the rule specified in Match. This is the name of a Java class that implements the require functionality and should not normally be changed.
Notification URL	URL to which \notification messages will be sent.
Notification Text Template File	Path to the file that contains the text part of notifications.
Notification Text Template File Encoding	The encoding that the file is given when it is stored.
Notification Text Charset	The charset used for the email that the file becomes.
Notification HTML Template File	Optional path to the template file for the HTML part of notifications. If empty, notifications will only have a text part.
Notification HTML Template File Encoding	The encoding that the file is given when it is stored.
Notification HTML Charset	The charset used for the email that the file becomes.
Notification Subject	Notification email subject.
Notification Sender	The email address that displays in the From field of notification emails.
Notification Reply-To	The email address that is used when recipient's reply to the notification email.
Use Variable Substitution	Enables personalization of the text message that is sent with each email.
Notification Variable Map File	Java properties file containing the variables mapping.
Bounce Application	Defines the application that will handle bounced emails.
Bounce Notification Template File	File which contains the email message text for bounced email.
Bounce Notification Template File Encoding	The encoding that the file is given when it is stored.
Bounce Notification Charset	The charset used for the email that the file becomes.
Bounce Notification Subject	Subject of the email for bounced message. If left blank, it will default to the original subject.
Encryption Algorithm	List of algorithms that can be used to encrypt the reply headers. The default value is ARC4.

Parameter	Definition
Encryption Token	Specifies a list of encryption tokens. The key for the chosen token will be used for encryption
Require Certificate	Select to require that the recipient has a certificate as well as being enrolled. If selected, the recipient must be enrolled and have a certificate or the message is queued. If not selected, the recipient need only be enrolled.
Enable Tracking	Select to enable tracking of outgoing emails for the application.
Next	Specifies which application or ruleset the mail will pass through once it is processed by the current application or ruleset.

Bounce - Details Tab

Parameter	Definition
Application Name	Name of the application.
Delivery Application	Name of the application used to deliver messages.
Sender Source	Determines how to set up the sender email address.
Specified Sender	The sender email address to use when the Sender Source parameter is set to 'Specified Sender'.
Subject Prefix	Text that is prefixed to the original subject for the notification email.
Attach Original Message	Whether to attach the original email to the notification message.
Debug	Enables debug log messages.
Bounce Message Charset	Character set used for the bounce email.
Bounce Message	The body text of the bounce email message.

error - Details Tab

Parameter	Definition
Application Name	Name of the application.

Parameter	Definition
Repository Name	Name of the storage repository to use.
Next	Application or ruleset to handle error messages.

Storage- Details Tab

Parameter	Definition

Application Parameters

The following nodes are configurable on a per-application basis. Note that the nodes and fields within those notes vary depending upon the application type.

Certificate Harvesting and Signature Verification

Parameter	Definition
Harvest Certificates	Turns certificate harvesting on and off.
Harvest on Signature Verification Failure	If checked, the certificate is harvested even if the signature verification fails.
Key Update Provider	Update module used to store the harvested certificates
Verify Certificates	If this option is checked, the user's certificate is verified until a trusted root certificate. If this option is not checked then only an expiry check is made on the user's certificate.
Store Updated Certificates	If checked, existing certificates are replaced by newer certificates.
Verify Signature	Determines if the system should verify the certificate before storing it in the update module. If Verify Signature is selected and the harvested certificate is not valid, then it is not stored in the update module.
Subject Prefix on Success	The subject to prepend when signature verification is successful.

Parameter	Definition
Subject Prefix on Failure	The subject to prepend when signature verification fails.
Next on Success	Application or ruleset the email passes through once the certificate is harvested.
Next on Failure	Application or ruleset the email passes through if harvesting fails.
Treat Unsigned as Success	If no public key is found, the mail is treated as if harvesting is successful if this is turned on. If turned off, mail is treated as harvest failure if no public key is found.
Remove Signature	Remove signature part of signed message

Cryptography

Parameter	Definition
Salt Generation	Algorithm used to generate the salt appended to keys used in ARC4 encryption
IV Generation	Algorithm used to generate the initialization vector used by AES encryption (only used if AES encryption is used).
Session Key Generation	Algorithm used to generate the session key.
Session Key Encryption	Algorithm used to encrypt the session key.
Session Key Verification	Algorithm used to verify the session key after decryption.
Payload Encryption	Algorithm used to encrypt the secure portion of the payload
Payload Verification	Algorithm used to verify the secure portion of the payload after decryption

Delivery

Parameter	Definition
Encryption	Determines level of encryption. Options include None, Envelope, SMIME and OpenPGP. If set to “OpenPGP”, encryption will be done using the recipient’s PGP public key. The encryption can be done either as PGP Inline or as PGP/MIME.

Parameter	Definition
Signature	Specifies the various signature modes to choose from. Options are: • None – No signature • Envelope – The envelope carries the signature. This is used for encryption types Envelope and InlineEnvelope. • SMIME – S/MIME signature. This should be used only when the encryption mode is SMIME or None. • OpenPGP - If this is set to "OpenPGP", signing will be done using the sender's PGP public key. The signing can be done either as PGP Inline or as PGP/MIME.
Verify Certificate	If this option is checked, the user's certificate is verified until a trusted root certificate. If this option is not checked then only an expiry check is made on the user's certificate.
Signer Lookup Provider	Lookup Module to use when looking for the signing certificate.
Signer Email Address	Email address of the person whose digital certificate is used for signing. (Used for PKI)
Use Sender Address	Uses the email sender's address when looking for the signing certificate.
Application Key Store	Store name for the recipient's key information for the application.
Signer Key Store	Store name for the signer's key information.

Domain Mappings

Parameter	Definition
Name	Name of the domain you want to map.

<Name of the domain you added>

Parameter	Definition
Domain Name Regular Expression	Pattern/character search used to match the specified domain. For example, aol\..*
Content-Type	Type of content the IronPort Encryption appliance is sending to the specified domain. For example, text/html.

Encryption Key Lookup

Parameter	Definition
User Key Lookup	Select to use a plug-in module for looking up encryption keys for each message recipient
Key Lookup Provider	Class name of the lookup module. This class must implement the interface com.postx.james.api.Lookup.
Key Lookup Identity	The identity value the application obtains from the MIME message.
Key Lookup Is SHA1	If checked, indicates that the key returned by the lookup module has been encoded using the SHA-1 algorithm.
Key Lookup Is Domain	If checked, indicates that the key lookup should be done by domain.
Key Lookup Domain Prefix	The prefix to use when doing the domain lookup.
Embed Key in Envelope	If checked, the key will be embedded in the envelope such that the recipient will not have to enter a password to open the envelope.
Use Random Key	If checked, generate a random key to embed in the envelope. This option has no effect if the Embed Key option is not enabled.

Envelope Builder Pool

Parameter	Definition
Envelope Builder Pool Size	Number of envelope builder instances to allocate at startup.
Envelope Builder Pool Timeout (msecs)	Duration (in mseconds) each instance is held until it is discarded.

EPM

Parameter	Definition
Postmark Envelopes	Determines whether envelopes are postmarked.
EPM Server Address	IP address of the primary EPM server.
EPM Server Port	Port on which the primary EPM server is running.

Footer Options

Parameter	Definition
Insert at End	Select to insert the footer at the end of the email. If unchecked, it will use the parameters below to determine the position.
Search String Separators	The footer will be placed in the message immediately before the first instance of any one of these strings.
Search Strings	The footer will be placed in the message immediately before the first instance of any one of these strings.
Always Insert	If no search strings are found, checking this option will ensure that the footer is still inserted at the end of the message.

Header and Footer Text

Parameter	Definition
Header Text	Text to prepend to the incoming message body to create the outgoing message body.
Footer Text	Text to append to the incoming message body to create the outgoing message body..

Mailbox Quota

Parameter	Definition
Quota Approaching:	
Send Warning when Mailbox Approaching Quota	Select to send warning notification emails.
Warning Percentage	The percentage that the mailbox reaches at which point a warning notification is sent to the user.
Warning Subject	Subject of the notification email warning the user that their mailbox is almost full.
Warning Template File	Use the **Select** button to navigate to the .txt file containing quota approaching warning template.

Parameter	Definition
Warning Template File Encoding	Character encoding used to read the Warning Template File.
Warning Charset	Warning's content-type header charset attribute value.
Quota Exceeded:	
Send Warning When Mailbox Exceeds Quota	Select to send warning notification emails when a mailbox exceeds its quota.
Mailbox Percentage	The percentage that the mailbox reaches at which point a warning notification is sent to the user stating that the user may cease to receive emails.
Notification Subject	Subject of the notification email warning the user that their mailbox is full and they may cease to receive emails.
Notification Template File	Use the **Select** button to navigate to the .txt file containing the notification text.
Notification Template File Encoding	Character encoding used to read the Notification Template File.
Notification Charset	Notification's content-type header charset attribute value.

Mail Gateway

Parameter	Definition
Use Gateway	Select to use a relay mail server.
Gateway	Hostname of the gateway server.
Gateway Port	SMTP port of the gateway server. Default = 25.
Gateway TLS Port	The port number of the SMTP server that will accept TLS. This is only used if "Use SMTP STARTTLS command" is enabled. When the "Gateway TLS Port" and the "Use SMTP STARTTLS Command" are specified, mail will be sent using the "Gateway TLS Port" using TLS. If this fails, "Gateway Port" using non-TLS will be used.
Keep Gateway Alive	Use to keep the sender from hanging up between messages. Valid values are YES, TRUE, 1, NO, FALSE or 0.
Require TLS	If checked, only connect to gateway server if it's using TLS.

Message Personalization

Parameter	Definition
Use Incoming Body as Outgoing Body	Select to use the first MIME part of each incoming e-mail message to become the first MIME part of each outgoing e-mail message, and removes that part from the payload. The only change made to the incoming MIME part is to remove any name attribute that appears in the Content-Type header in the part. This allows the body of the outgoing e-mail (the first MIME part) to be specified exactly in the incoming e-mail, including alternatives, etc.
Outgoing Body Action	Turns personalization of outgoing message bodies on and off.
Outgoing Body Source	Source of the body of outgoing messages
Outgoing Text Body File	Path to the template file for the text part of the outgoing message bodies; only used if Outgoing Body Source is 'File'.
Outgoing Text Body File Encoding	Character encoding to use when reading Outgoing Text Body File.
Outgoing Text Body Template Type	Template engine type to use to template Outgoing Text Body File.
Outgoing Text Body Content-Type	Content-Type of text part of outgoing message body.
Outgoing Text Body Charset	Character set of text part of outgoing message body.
Outgoing Text Body Content-Transfer-Encoding	Content-Transfer-Encoding of text part of outgoing message body.
Outgoing HTML Body File	Optional path to template file for HTML part of outgoing message bodies. This is only used if Outdoing Body Source field is "File". If empty, outgoing message bodies only have text part.
Outgoing HTML Body File Encoding	Character encoding to use when reading Outgoing HTML Body File.
Outgoing HTML Body File Template Type	Template engine type to use to template Outgoing HTML Body File.
Outgoing HTML Body Content-Type	Template engine type to use to template Outgoing HTML Body File.
Outgoing HTML Body Charset	Character set of HTML part of outgoing message body.

Parameter	Definition
Outgoing HTML Body Content-Transfer-Encoding	Content-Transfer-Encoding of HTML part of outgoing message body.
Message Bar Personalization	Select the message bar HTML personalization file.
Message Bar File	Select the message bar HTML file.
Message Bar File Encoding	Specifies the encoding of the message bar template file.
Envelope Message Personalization	Turns email message personalization on or off. Permissible values are: None - Turns personalization off. Use Template - Turns personalization on.
Envelope Message Source	Specifies where the source of the email message text is read from. Permissible values are: None - No source, this effectively disables personalization. Mime - Body of the message text from the body part of the incoming Mime message is added to the variable set, which is then applied to the template file identified in Message Text File and the resulting document used as the email message text.
Envelope Message Template File	Name of the template file.
Envelope Message Template File Encoding	The character encoding used for the template file.
Envelope Message MIME Type	The MIME type of the message text after the template has been executed with the variable set. This is used to set the MIME type of the envelope message text within the payload of the outgoing IronPort Encryption appliance envelope. This is usually “text/html” to ensure that the message is opened using the recipient’s default web browser and that the attachment files can be accessed as links from the main message window.
Attachment Encoding	Content transfer encoding of the outgoing attachment. Values are 7bit, 8bit, base64 and quoted-printable.
Attachment Name	Name to use for the IronPort Encryption appliance envelope attachment file. The name must end in .html.
Use Variable Substitution	Java properties file containing the variable mapping.
Variable Map File	Enables personalization of the plain text message that is sent with each email.

Message Unpacking

Parameter	Definition
Use Headers	If checked, message header values are used to construct the outgoing message.
Check Attachment Type	Select to use the attachment content type match to identify the IronPort Encryption appliance Secure Direct mail bodypart.
Attachment Type	Content type which identifies the IronPort Encryption appliance Secure Direct mail bodypart.
Check Attachment Name	Select to use the Attachment name match to identify the IronPort Encryption appliance Secure Direct mail bodypart.
Attachment Name	Attachment name that identifies the IronPort Encryption appliance Secure Direct mail bodypart.
Alternative MIME Subtype	Specifies the subtype from the multipart/alternative part for the secure mail body.

Metering

Parameter	Definition
Billing Service Name	Name of the billing service.
Billing Update Frequency	Not editable. Used by metering to indicate the number of messages between updates to the metering service database.
Billing Wakeup Interval (secs)	Not editable. Wake up interval used by metering to flush any outstanding counts when no messages are being processed.

MIME Header Filter

Parameter	Definition
Headers to Remove	Comma separated list of regular expressions for header names to remove.
Headers to Keep	Comma separated list of regular expressions for header names to keep.

Mobile Device Support

Parameter	Definition
Use Mobile Device Support Mode	Select to use Mobile Device Support.
Keep Original Recipients	When checked, the application will process the message and then send it as is without changing the recipients at all. By default this setting is false, which means that the application will switch the To and From values when creating the new message.
Keep Original Envelope	Normally MDS removes the attachment and sends the recipient a link because the assumption is that they already have the envelope attachment. However, when this check box is selected, the application processes the message and keeps the envelope as an attachment to the notification message.
URL	The base URL used by mobile device to retrieve the message.
Subject Prefix	The prefix that is preprended to the subject of the original message.
Notification Text Template File	Template file for the notification text email.
Notification Text Template File Encoding	Encoding that the file is given when it is stored.
Notification Text Charset	Charset used for the notification text template file.
Notification HTML Template File	Template file for the notification HTML email.
Notification HTML Template File Encoding	Encoding that the file is given when it is stored.
Notification HTML Charset	Charset used for the notification HTML template file.
Storage Directory	Temporary storage directory used when storing MDS files (UNC paths supported).
Keyserver Host	The key server host for which to allow messages. If blank, the application will process all envelope regardless of their origination server. Otherwise, if the host for the envelope does not match the configured host, the message will be routed to the failure application.

PGP Decryption and Signature Verification

Parameter	Definition
Verify Signature	If selected ,and the input message is either signed or signed and encrypted, the system will verify the signature before storing it in the update module. If the harvested certificate is not valid, then it is not stored in the update module. If this option is not selected, signature verification is not done.
Public Key Lookup Provider	Name of the lookup to use when the signer's public key is to be retrieved for signature verification.
Subject Prefix on Success	The subject to prepend when signature verification is successful.
Subject Prefix on Failure	The subject to prepend when signature verification fails.
Next On Success	Application or ruleset the email will pass through if decryption is successful.
Next On Failure	Application or ruleset the email will pass through if decryption fails.

PGP Key Harvesting

Parameter	Definition
Treat messages without Public key as success	If no public key is found, the mail is treated as if harvesting is successful if this is turned on. If turned off, mail is treated as harvest failure if no public key is found.
Key Update Provider	Update module used to store the harvested certificates
Key Update Identity	Identifies the certificate owner.
Verify Certificate	When checked, the options in the global certificate verification will be used to determine what type of certificate verification will be done.
Update Certificate if New	Determines if the certificate should be updated if new.
Next on Success	Application or ruleset the email will pass through if decryption is successful.
Next on Failure	Application or ruleset the email will pass through if decryption fails.

Registered Envelope

Parameter	Definition
Use Registered Envelopes	Check to send Registered Envelopes.
Authentication Provider	Authentication provider.
Key Server Host	The domain name, and optionally port, used by Registered Envelopes to contact the key server.
Key Server Proxy	The key server proxy configuration to use. This field is populated with settings specified on the Configuration > Proxy > HTTP Proxy page.
Key Server Internal URL	The URL used by other components of the encryption server to contact the key server. Leave blank to use the key server host.
Hash Key	Check to have the envelope hash the user's credentials when sending them to the key server. In the main tab of an envelope application you can set up a User Key Name that is used to cache users' keys on their computers. When that form of key caching is used the key is always hashed and the state this checkbox is ignored.
Authentication Token	Select the authentication token from the drop-down.
Send Return Receipt	Select to send return receipts.
Use Repository	Select to use a database keystore repository
Expiration Period (days)	The number of days envelopes are held in the key server database before being marked for deletion.
Unread Notification Period (days)	The number of days before senders are notified of unopened envelopes.
Registration URL	The URL of the page to which the envelope should send an unregistered user. By default this value is blank, which means that the value configured under Web Services > KeyServer > Notification > Registration URL will be used. This configuration simply provides a way to override the key server value on a per-application basis (primarily for multi-branding).

Parameter	Definition
Password Expired URL	The URL of the page to which the envelope should send a user whose password has expired. By default this value is blank, which means that the value configured under Web Services > KeyServer > Notification > Change Expired Password URL will be used. This configuration simply provides a way to override the key server value on a per-application basis (primarily for multi-branding).
Authentication Frame URL	URL of authentication page embedded in envelope used when personal security phrase is enabled.
Message Security	Select the message sensitivity level. Valid values are Low, Medium and High.

Secure Response

Parameter	Definition
Secure Response Host	Hostname and port for the secure reply service.
Allow Secure Reply	Enables the Secure Reply button on the envelope. The reply is sent to the sender only.
Allow Secure Reply to All	Enables the Secure Reply All button on the envelope. The reply is sent to the sender and all of the recipients in the To list.
Allow Secure Forward	Enables the Secure Forward button on the envelope which allows the recipient to forward the message to other users. Note: Attachments are not currently forwarded.
Reply Web Service	Determines how the Secure Reply page (shown when a user clicks "Secure Reply", "Secure Reply All" or "Secure Forward" in an envelope) is displayed. The default value "/websafe/securereply" shows a page which can be customized with the company's logo or other look-and-feel changes. This form requires that the user's browser permits JavaScript. If the company does not allow JavaScript in user's browsers then set this entry to "/securereply/index.jsp".
Encrypt Response Headers	Determines whether the reply headers are encrypted. The default value is true
Encryption Algorithm	List of algorithms that can be used to encrypt the reply headers. The default value is ARC4.

Parameter	Definition
Encryption Token	Specifies a list of encryption tokens. The key for the chosen token will be used for encryption
Use Token for Registered Envelopes	If checked, the specified token (instead of a random key) is used to encrypt response parameters.

SMIME Decryption

Parameter	Definition
Remove Signature	Remove signature part of signed message
Next On Success	Application or ruleset the email will pass through if decryption is successful.
Next On Failure	Application or ruleset the email will pass through if decryption fails.

Spool Queue

Parameter	Definition
Delivery Threads	Number of threads used for message processing and delivery.
Outgoing Repository	Directory used to store outgoing messages for retries, etc.
Retry Interval (msecs)	Retry delay time in milliseconds.
Maximum Retries	Maximum number of times to retry sending the message. After this the message is errored and returned to its sender.

Datasources

Parameter	Definition
Datasource Prefix	JNDI namespace prefix used to look up the DataSource.
Datasource Name	Name of the DataSource used for the keystore database (This is a drop down combo box of all the DataSources that are configured under DSDataSources).
DataSource Class	Class for this datasource.
Datasource Username	Username for this datasource.
Datasource Password	Password for this datasource.

Envelopes

Parameter	Definition
Envelope File	Envelope file path. Use the **Select** button to navigate to the file.
Template Engine	Name of the template engine used by this envelope. Options are: postx, velocity, xmlc and xslt.
Envelope File Encoding	Specifies the file encoding for envelope files in the Envelope Directory. Options are UTF-8, Big5 and iso-8859-1.
Show Open Button	Include an Open button on the envelope, allowing opening the envelope locally.
Show Save Button	Include a Save button on the envelope allowing saving the payload to disk.
Show Open Online Link	Include a Open Online link on the envelope allowing opening the envelope using the online opener. The online opener is always used if JavaScript isn't available, whether the Open Online button is shown or not.
Show Open Offline Checkbox	Include a checkbox on the envelope which, when checked, causes the envelope to encrypt the session key with the user's key and save it in a cookie, allowing a registered envelope to be opened offline.

Show Remember User Key Checkbox	Include a checkbox on the envelope which, when checked, causes the envelope to save the user's key to a cookie with a name based upon the User Key Name settings from the Details tab of the application using this envelope allowing all envelopes with the same User Key Name to be opened without entering credentials once one is opened. This setting should only be checked if a User Key Name is set.
Show Remember Envelope Key Checkbox	Include a checkbox on the envelope which, when checked, causes the envelope to save the session key in a cookie unique to each envelope, allowing the envelope to be opened without entering credentials.
Show Remember Me Checkbox	Include a checkbox on the envelope which, when checked, causes the envelope to request that the server store the user's request and key in a cookie so that future envelopes can be stored automatically.
Show Auto Open Checkbox	Include a checkbox on the envelope which, when checked, causes the envelope to open automatically the next time it's opened if the session key is available in a cookie. This setting should only be checked if Show Remember Envelope Key Checkbox is checked.
Show Sender Authentication	Display the sender authentication (either Sender or Gateway) on the envelope.
Show Message Security	Display the message sensitivity on the envelope.
Use Personal Security Phrase	Use a two-way personal security phrase on the envelope to fight phishing by providing the user with assurance that the server with which he is authenticating is legitimate.
Use JavaScript	Use JavaScript to enhance the user experience for the envelope and, when possible, to decrypt the message.
Links:	
Help Page	URL for this envelope's help page.
Address Not Listed Page	URL for this envelopes page explaining why the user's address may not have been in the displayed recipient list.
Personal Security Phrase Info Page	URL for this envelopes page explaining why the user's passphrase is not displayed.
Forgot Password Phrase	URL for this envelopes forgot password page.
Key:	
Field Separator	Separator placed between each input field to form the key.

Case Sensitive	Select if the key is case sensitive.

Graphics

Logo

Parameter	Definition
Image Source	Image file path.
Image Link	Link to online image
Save Encoded File	Specifies whether to save a copy of the encoded file for future use.
Explode	Check to draw a blank line between every constant-color rectangle in the image. For demonstration only; not supported on all browsers.
Size	Size of each pixel in image. For demonstration only; not supported on all browsers.
Anchor:	
href	Destination URL if the image is clicked. Leave blank for a non-clickable image.
name	Anchor name attribute. Leave blank for none.
Open in New Window	Check to open destination URL (if any) in new window.
class	Anchor class attribute. Leave blank for none.
id	Anchor id attribute. Leave blank for none.
title	Anchor title attribute. Leave blank for none.

Postmark, PostmarkLeft and LowerLeft

Parameter	Definition
Image Source	Image file path.
Image Link	Link to online image
Save Encoded File	Specifies whether to save a copy of the encoded file for future use.

Explode	Check to draw a blank line between every constant-color rectangle in the image. For demonstration only; not supported on all browsers.
Size	Size of each pixel in image. For demonstration only; not supported on all browsers.
Anchor:	
href	Destination URL if the image is clicked. Leave blank for a non-clickable image.
name	Anchor name attribute. Leave blank for none.
Open in New Window	Check to open destination URL (if any) in new window.
class	Anchor class attribute. Leave blank for none.
id	Anchor id attribute. Leave blank for none.
title	Anchor title attribute. Leave blank for none.

Fields

Parameter	**Definition**
Label Position	The position of the title in relationship to the field. Options are Left of Input Field, Above Input Field, Right of Input Field, and Below Input Field.
Label:	
Text	Text to display as the title of the field.
id	Title text id attribute. Leave blank for none.
class	Title text class attribute. Leave blank for none.
Input Field:	
Size	Visual size (in characters) of the input field.
Maximum Length	Maximum number of characters that can be entered in the input field.
Obscure Input	Check to display typed characters as asterisks or bullets.
id	Input field id attribute. Leave blank for none.

class	Input field class attribute. Leave blank for none.
title	Input field title attribute. Leave blank for none.

LOGGING

Destinations

Parameter	Definition
Destination Name	Displays the name of the destination. Display-field only.
Enabled	Select this box to enable or disable the destination.
Log Level	Overall logging threshold. Determines the priority of the messages going to the platform log file. Valid values are DEBUG, INFO, WARN, ERROR or FATAL.
Log File Name	The name of the log file for this destination.
Append	Append or create a new file when the server starts up.
Maximum File Size	The maximum file size before log file rotation occurs.
Number of Backup Files	Number of backup log files to keep when log file rotation occurs.
Conversion Pattern	Formatting pattern used to write messages to log file.

Filters

Parameter	Definition
Filter Name	Name of the filter category.
Description	Log filter description.
Log Level	Threshold for logging to syslog. This needs to be a higher priority than the Threshold parameter to be logged. Valid values are DEBUG, INFO, WARN, ERROR or FATAL_ERROR.
Log Destination	Destination of the filter. This drop-down is populated in the Destinations area of Logging. There are two Log Destination fields since you may want to log to two different places.

WEB SERVERS AND PROXIES

Web Server Configuration

Access Log

Parameter	Definition
Enabled	Select this box to enable or disable the destination.
Log File Directory	Log file directory.
Log File Name Prefix	Log file name prefix.
Log File Name Suffix	Log file name suffix.
Format	Formatting pattern used to write messages to log file.

Connection Listeners

Connection Listeners - HTTP

Parameter	Definition
Enabled	Click to enable.
Connection Listener Name	Connector name. Display-only field.
Accept count	The maximum queue length for incoming connection requests.
Maximum Threads	The maximum number of request processing threads to be created by this Connector.
Minimum Spare Threads	The number of request processing threads that will be created when this Connector is first started.
Maximum Spare Threads	The maximum number of unused request processing threads that will be allowed to exist until the thread pool starts stopping the unnecessary threads.
Keep-Alive Requests	The maximum number of HTTP requests which can be pipelined until the connection is closer by the server.
Maximum HTTP Header Size (bytes)	The maximum size of the request and response HHTP header, specified in bytes.
Maximum HTTP POST Size (bytes)	The maximum size in bytes of HTTP POST requests handled by this connection listener.

Parameter	Definition
HTTP Server Header	Value of server header in HTTP responses.

Connection Listeners - HTTPS (SSL)

Parameter	Definition
Enabled	Click to enable.
Connection Listener Name	Connector name. Display-only field.
Accept count	The maxima queue length for incoming connection requests.
Maximum Threads	The maximum number of request processing threads to be created by this Connector.
Minimum Spare Threads	The number of request processing threads that will be created when this Connector is first started.
Maximum Spare Threads	The maximum number of unused request processing threads that will be allowed to exist until the thread pool starts stopping the unnecessary threads.
Keep-Alive Requests	The maximum number of HTTP requests which can be pipelined until the connection is closer by the server.
Maximum HTTP Header Size (bytes)	The maximum size of the request and response HHTP header, specified in bytes.
Maximum HTTP POST Size (bytes)	The maximum size of FORM POSTs which will be handled by the web server, specified in bytes.
HTTP Server Header	Value of server header in HTTP responses.
SSL Protocol	Select the SSL protocol from the drop-down. Valid values are TLS and SSL.
SSL Algorithm	Select the SSL algorithm from the drop-down. Valid values are SunX509 and IBMX509.
Keystore File	The file in which the generated public and private keys were stored. Select a file name that is different.
Keystore Password	This password corresponds to the actual generated keys as well as the keystore.
Enable Alternate Truststore	Click to enable the use of alternate trust stores.

Parameter	Definition
Alternate Truststore File	Contains the root certificates used to verify the SSL certificate imported into the keystore file.
Alternate Truststore Password	The password for the alternate trust store file.
Client Authentication	Set this value to true if you want Tomcat to require all SSL clients to present a client Certificate in order to use this socket. This is an optional parameter.
SSL Ciphers	Comma separated list of encryption ciphers that may be used.

Connection Listeners - HTTP AJP 1.3

Parameter	Definition
Enabled	Click to enable.
Connector Listener Name	Connector name. Display-only field.
Maximum HTTP POST Size (bytes)	The maximum size of FORM POSTs which will be handled by the web server, specified in bytes.

Proxies

Proxy Configurations

Parameter	Definition
Proxy Name	Name given to this proxy configuration.
Description	Description of the proxy server.
Host Name	Host name of the proxy server.
Port Number	Port number the proxy server is listening on.
User Name	User name to access the proxy server.
Password	Password to access the proxy server. This field displays if it is a Web proxy server or Socks5 proxy server. This field does NOT display if it is a Socks4 proxy server.

LOOKUP & UPDATE MODULES

LDAPLookupRepository

Parameter	Definition
Name	Name of the LDAP Lookup Repository.

<Name of LDAP Lookup Module you added> - Details Tab

Parameter	Definition
Name	Name of the LDAP Lookup Repository.
Connect Securely	Select to allow a secure (i.e., SSL) connection to the LDAP server.
Server Name	Name of the LDAP server.
Port Number	TCP/IP port of the LDAP server.
Logon to Server	Logon to the LDAP server in order to perform searches.
User Name	User account used to log in to the LDAP server.
User Password	User password used to log in to the LDAP server.
RootDN	The base distinguished name (DN) against which all lookups and searches are carried out, for example "dc=ironport,dc=com" or "o=IronPort,c=US".
Query String	A simple expression that yields the query string used to identify a user in LDAP lookup requests. This parameter is only used in lookups, it is **not** used in searches. For example "cn=${identity}", where ${identity} is the value the application obtains from the Mime message using the applications Key Lookup Identity configuration parameter.
Enable Directory Search	Enables the use of LDAP searches instead of using lookups. Lookups are better, but can only be used when the users can be identified by their common name. When you want to use the user's email address in order to identify them, you must use a search by selecting this and setting the Search Query value appropriately.
Enable Subtree Search	Enables the use of LDAP subtree scope while searching for a user.
Enable Proxy Certificate Search	Enables the search of proxy certificates.

Parameter	Definition
Search String	A simple expression that yields the query string used to search the LDAP directory. This parameter is only used in searchers, it is not used in lookups. For example “mail=${identity}”, where ${identity} is the value the application obtains from the Mime message using the applications Key Lookup Identity configuration parameter.

Attribute Names

Parameter	Definition
Certificate Type	The type of certificate that is stored in the LDAP field.
Password Attribute	The LDAP schema name of the password attribute that is returned by the LDAP server in response to lookup requests and searchers. For example “userPassword”.
Password Attribute Alias	LDAP subtype or alias name that is the attribute name actually returned by LDAP server when a Password Attribute is requested.
PKCS7 Certificate Attribute	LDAP schema name of the attribute used to hold the users PKCS7 public key certificate.
PKCS12 Certificate Attribute	LDAP schema name of the attribute used to hold the users PKCS12 private key certificate.
PKCS12 Certificate Password Attribute	LDAP schema name of the attribute used to store the password value that was used to encrypt the PKCS12 certificate.
PGP Certificate Attribute	Schema name of attribute used for the PGP public key certificate.

Sender Policies

Parameter	Definition
Check Sender Policy	Determines whether to check the policy for the email sender or not.
Sender Role Attribute	The LDAP sender attribute that contains its role.
Sender Role Attribute Alias	LDAP sender attribute alias that contains its role.

Parameter	Definition
Sender Query String	LDAP query to perform to lookup the sender's role.
Enable Search for Sender	Determines whether to perform a search for the sender's role attribute or just a lookup.
Sender Search String	LDAP attribute used to perform a search for the sender's identity.
Role Value for SendAll Permission	The value for the sender's role for SendAll type permission.
Allow Partial Match for SendAll	Determines whether a sub-string match or exact match is required to compare the send all value to the sender's role.
Role Value for SendRestricted Permission	The value for the sender's role for SendRestricted type permission.
Allow SendRestricted Partial Match	Determines whether a sub-string match or exact match is required to compare the send restricted value to the sender's role.
Enable Search sender domain	Determines whether to perform a search for the sender's restrict domain attribute or just a lookup.
Domain List Attribute	The attribute that contains a list of domains that the sender is restricted to be able to send or not send to.
Domain List Attribute Alias	The alias for the domain list attribute.
Action for Restricted Send	The action to perform (Send or NoSend) if the recipient's destination host address matches an address on the restricted domain list.
Role Value for SendNone Permission	The value for the sender's role for SendNone type permission.
Allow Partial Match for SendNone	Determines whether a sub-string match or exact match is required to compare the send none value to the sender's role.
Default Sender Role	If the sender's role cannot be found in the LDAP server, the default policy value. This is either SendAll, SendRestricted, or SendNone.
Certificate is PEM Encoded	Flag that says that the public cert in the LDAP directory is PEM encoded.

User Lookup Repository

Parameter	Definition
Name	Name of the user repository.

<Name of User Lookup Repository you added>

Parameter	Definition
Name	Name of the user repository.
Class	Name of the class that implements the type of lookup. Use com.postx.james.lookup.UserLookup for websafe lookup. Use com.postx.james.lookup.CertLookup for certificate store lookup.
Lookup Service Name	Name of the EJB service to bind the lookup to.
App Name	Used to identify the AppName, a method for grouping the lookup. Used to group identities in CertLookup.

Database Lookup Repository

Parameter	Definition
Name	Name of the database repository.

<Name of Database Repository you added>

Parameter	Definition
Name	Name of the database repository.
DB Datasource JNDI Name	JNDI Name of the datasource used to connect to the DBLookup database.
DB Table Name	Name of the table to be looked up in the database lookup.
DB Key Separator	The separator for multiple password fields.
DB Primary Column	The recipient's email address which is used as the db key to obtain the encryption key.
Key Column 1	One or more password fields stored in the database.

Parameter	Definition
Key Column 2	One or more password fields stored in the database.
Key Column 3	One or more password fields stored in the database.
Key Column 4	One or more password fields stored in the database.
Enroll Column 1	Name of the database field that contains register status.
Enroll Value 1	Value for the database register field to signify that the recipient is enrolled.
Enroll Column 2	Name of the database field that contains register status.
Enroll Value 2	Value for the database register field to signify that the recipient is enrolled.
Enroll if Password Exists	Determines whether or not to set the registration state to true if the password exists (override the check for the register column and value). Default is checked.
Case Insensitive Lookup	Specifies whether case insensitive lookups are allowed. Default is not checked.

Chained Lookup Repository

Parameter	Definition
Name	Name of the chained repository.

PK3I Lookup Repository

Parameter	Definition
Name	Name of the PK3I repository.

<Name of PK3I Lookup Item you added>

Parameter	Definition
Name	Name of the CMP lookup module.
URL Protocol	Protocol used to access the PK3I server.

Parameter	Definition
URL Host	Host name of the CMP server.
URL Port	CMP server port that listens for CMP requests.
Request Path	Path used to submit request to RSA Server.
Request Token	Request token.
Version	Version number.

Chained Lookup Repository - Details Tab

CMP Lookup Repository

Parameter	Definition
Name	Name of the chained repository.

<Name of CMP Lookup Item you added> - Details Tab

Parameter	Definition
Name	Name of the CMP lookup module.
Protocol	Protocol used to access the CMP server.
Host	Host name of the CMP server.
Port	CMP server port that listens for CMP requests.
Certificate Pickup URL	URL for picking up the certificate.
Shared Secret Key	Name of the secret used for making a valid CMP request.
Shared Secret Value	The value of the secret used for making a valid CMP request.
Shared Secret Salt	Salt value for encrypting the secret.
Shared Secret Encoding Iterations	Numb7er of iterations used to encrypt the secret.
KeyUpdateProvider	Update Module used to store the requested certificate.

PKCS10 Lookup Repository

Parameter	Definition
Name	Name of the chained repository.

<Name of PKCS10 Lookup Item you added>

Parameter	Definition
Name	Name of the lookup module.
URL Protocol	Protocol used to access the server.
URL Host	Host name of the server.
URL Port	Server port that listens for requests.
Certificate Pickup URL	URL for picking up the certificate.
Request Path	Path used to submit request to RSA Server.
PKCS10 Request Parameter Name	Parameter values necessary to submit the request to the RSA Server. The default value is: domainID=8a12d649003200e9224ae0cb003de2175daac43b,CA=41df114e79bbebb0321b4cd35035d3a6,PRO=NoExtensions,ManHidden=,ExtHidden= The domainID value needs to be changed to match the "Issuing Jurisdiction ID" of the Certificate Authority. The CA value needs to be changed to match the "Certificate ID" of the Certificate Authority.
Other Request Parameters	Other parameter values necessary to submit the request to the RSA Server.
Key Update Provider	Update module used to store the requested certificate.
Key Lookup Provider	Specifies user lookup or certificate lookup.
Use Public Certificate Lookup Provider	Click to enable the use of a lookup to retrieve the public certificate.
Public Certificate Lookup Provider	The lookup used to pickup the public cert that was requested by the lookup itself.

MSCA Lookup Repository

Parameter	Definition
Name	Name of the MSCA repository.

<Name of MSCA Lookup Item you added>

Parameter	Definition
Name	Name of the lookup module.
MS CA Server	Server where the MS CA is located including repository in the form host\repository.
Certificate Template OID	The OID of the Certificate Template to use.
MSCert.dll location	Path to the MSCert.dll which contains JNI functions so encryption server can call the MS CA Server.
KeyUpdateProvider	Update module used to store the requested certificate, typically certupdate.
Certificate Pickup URL	URL for picking up the certificate.

PGP Lookup Repository

Parameter	Definition
Name	Name of the PGP repository.

<Name of PGP Lookup Item you added>

Parameter	Definition
Name	Name of the lookup module.
Lookup Service Name	Name of the EJB service to bind the lookup to.
KeyUpdateProvider	Update module used to store the requested certificate, typically certupdate.
Certificate Pickup URL	URL for picking up the certificate.
Create Certificate	Select to create the certificate.

HKP Lookup Repository

Parameter	Definition
Name	Name of the HKP repository.

<Name of HKP Lookup Item you added>

Parameter	Definition
HKP Lookup name	Name of the HKP lookup module.
Base HKPUrl	Base HKPIUrl.
Additional Parameters	Additional parameters.
Identity Parameter Name	Identity Parameter Name
Proxy to access HKP Server	Process to access HKP Server.

PK3I, CMP, PKCS10, MSCA and PGP Email Attributes

Parameter	Definition
Email Pin To Sender	Select to send an email to the certificate requester.
Encrypt Pin Email	Select to encrypt the requester's email.
Email Subject	Subject for the PIN email.
Email Sender Template File	Template file for the body of the sender's email.
Email Sender Template File Encoding	Encoding that the file is given when it is stored.
Email Sender Template Charset	Charset used for the email that the file becomes.
Email To Recipient	Allows email notification of certificate request to be turned off for recipient.
Email Recipient Subject	Subject for the certificate request email
Email Recipient Template File	Template file for the body of the recipient's email
Email Recipient Template File Encoding	Encoding that the file is given when it is stored.
Email Recipient Template Charset	Charset used for the email that the file becomes.

Parameter	Definition
Mail Service Name	Mail service for sending the email
PostMaster Email Address	Sender of the email

CMP, PKCS10 and MSCA Certificate Attributes

Parameter	Definition
Organization	Certificate owner's organization
Organizational Unit	Certificate owner's organizational unit
City	Certificate owner's city
State	Certificate owner's state
Country	Certificate owner's country

UpdateModules

LDAPUpdateRepository

Parameter	Definition
Name	Name of the LDAP Lookup Repository.

<Name of LDAP Update Module you added>

Parameter	Definition
Name	Name of the LDAP Lookup Repository.
Connect Securely	Use to specify whether you want to connect securely via LDAPS.
Server Name	Name of the LDAP server.
Port Number	TCP/IP port of the LDAP server.
Logon to Server	Logon to the LDAP server in order to perform searches.
User Name	User account used to log in to the LDAP server.
User Password	User password used to log in to the LDAP server.
RootDN	The base distinguished name (DN) against which all lookups and searches are carried out, for example “dc=ironport,dc=com” or “o=IronPort,c=US”.
Query String	A simple expression that yields the query string used to identify a user in LDAP lookup requests. This parameter is only used in lookups, it is **not** used in searches. For example “cn=${identity}”, where ${identity} is the value the application obtains from the Mime message using the applications Key Lookup Identity configuration parameter.
Enable Directory Search	Enables the use of LDAP searches instead of using lookups. Lookups are better, but can only be used when the users can be identified by their common name. When you want to use the user’s email address in order to identify them, you must use a search by selecting this and setting the Search Query value appropriately.

Parameter	Definition
Search String	A simple expression that yields the query string used to search the LDAP directory. This parameter is only used in searchers, it is not used in lookups. For example "mail=${identity}", where ${identity} is the value the application obtains from the Mime message using the applications Key Lookup Identity configuration parameter.
Retry Count	The maximum number of times to retry after communication failure.

Attribute Names

Parameter	Definition
PKCS7 Certificate Attribute	LDAP schema name of the attribute used to hold the users PKCS7 public key certificate.
PKCS12 Certificate Attribute	LDAP schema name of the attribute used to hold the users PKCS12 private key certificate.
PKCS12 Certificate Password Attribute	LDAP schema name of the attribute used to store the password value that was used to encrypt the PKCS12 certificate.

UserUpdateRepository

Parameter	Definition
Name	Name of the user repository.

<Name of User Lookup Repository you added>

Parameter	Definition
Name	Name of the user repository.
Class	Name of the class that implements the type of lookup. Use com.postx.james.lookup.UserLookup for websafe lookup. Use com.postx.james.lookup.CertLookup for certificate store lookup.
Update Service Name	Name of the EJB service to bind the update to.

App Name	Used to identify the Application Name, a method for grouping the lookup. Used to group identities in CertLookup.

DatabaseUpdateRepository

Parameter	Definition
Name	Name of the database repository.

<Name of Database Repository you added>

Parameter	Definition
Name	Name of the datasource.
DB Datasource JNDI Name	JNDI Name of the datasource used to connect to the DBLookup database.
DB Table Name	Name of the table to be looked up in the database lookup.
DB Key Separator	The separator for multiple password fields.
DB Primary Column	The recipient's email address which is used as the db key to obtain the encryption key.
Key Column 1	One or more password fields stored in the database.
Key Column 2	One or more password fields stored in the database.
Key Column 3	One or more password fields stored in the database.
Key Column 4	One or more password fields stored in the database.
Enroll Column 1	Name of the database field that contains register status.
Enroll Value 1	The value for the database register field to signify that the recipient is enrolled.
Enroll Column 2	Name of the db field that contains register status.
Enroll Value 2	The value for the database register field to signify that the recipient is enrolled.
Enroll If Password Exists	Whether or not to set the registration state to true if the password exists (override the check for the register column and value).

Parameter	Definition
Case Insensitive Lookup	Specifies whether case insensitive lookups are allowed.

ChainedUpdateRepository

Parameter	Definition
Name	Name of the chained repository.

<Name of Chained Lookup you added>

Parameter	Definition
Name	Name of the item in the chained lookup
Update Name	Name of the update module associated with this item in the chain.

<Name of Chained Lookup Item you added>

Parameter	Definition
Name	Name of the item in the chained lookup
Update Name	Name of the update module associated with this item in the chain.

PGPUpdateRepository

Parameter	Definition
Name	Name of the PGP update repository.

<Name of PGP Update Repository you added>

Parameter	Definition
Name	Name of the repository.
Class	Name of the class that implements the type of update.

Update Service Name	Name of the EJB service to bind the update to.
Application Name	Used to identify the Application Name, a method for grouping the update. Used to group identities in CertLookup.

JMS CONFIGURATIONS

JMS Persistence

Parameter	Definition
DataSource	Name of the datasource.
Database Type	Specify the type of the database. Valid values are Hypersonic, Oracle/DB2/MSSQL, and MYSQL.

JMS Queues

Parameter	Definition
Name	Name for this queue configuration.
Initial Context Factory	Factory class name to create the initial context.
Queue Connection Factory	JNDI name of the JMS queue connection factory.
Queue Name	JNDI name of the JMS queue.
Provider URL	Provider URL to locate the JMS Queue. For local queue, leave this blank.
User Name	User name for the JMS Queue. For local queue, leave this blank.
Password	Password for the JMS Queue. For local queue, leave this blank.
Delivery Mode	Specifies delivery mode. Values are Persistent and Non-Persistent.
Maximum Depth	Estimated maximum depth of queue.

JMS Topics

Parameter	Definition
Name	Name of the Topic List.

<Name of Added Topic>

Parameter	Definition
Name	Name of the JMS topic. This is the name that the encryption server looks for. A default is supplied. The only requirement is that it follow the format of topic/.
Topic Connection Factory	Connection factory used to connect to the topic.
Name	Name of the topic.
Provider URL	JNDI Provider URL to locate the JMS topic. For local topic, leave this blank.
File Catalog	Points to a file in the conf directory that contains all of the files requiring publishing/subscribing to by this topic. Default value = FileCatalog.txt
User Name	Optional. The username that the administrator provides for the JMS topic.
Password	Optional. The password that the administrator provides for the JMS topic.
Initial Context Factory	Initial context factory for the topic Lookup.
Type	Type of topic. Valid values are Publisher and Subscriber.

ENCRYPTION TOKENS

Parameter	Definition
Name	Name of the encryption token.

<Name of Added Token>

Parameter	Definition
Name	Name of the encryption token.
Description	Connection factory used to connect to the topic.

WEB SERVICES

Secure Response

WebSecurity

Parameter	Definition
Allow HTTP	Click to enable the use of HTTP.
Allow NonSecure Headers	Enables non-secure headers.
Allowed Domains	List of domains to allow sending reply. The from email address or at least one email address in the To list should have a domain that matches one from this list to apply this rule.
All Recipients Must Match Domain	Names of the domains that will receive the nonsecure reply email.

Response-Message

Parameter	Definition
Email Charset	Charset to be used for the body of the secure reply email.
Email MIME Type	MIME type to be used for the body of the secure reply email.
Email Content Encoding	The content-transfer-encoding to be used for the secure reply email body. The value has to be “8-bit” or “Base64” for supporting I18N data.
Attachment Content Encoding	The content-transfer-encoding to be used for the attachment file included in the secure reply email. The value has to be “8-bit” or “Base64” for supporting I18N data.
Convert SingleByte Kana to DoubleByte Kana	Applies only if the I18N data under consideration is Japanese data with the charset of “iso-2022-jp”. With this option selected, the secure-reply web service converts the reply email data entered from single byte kana to double byte kana before it is sent as an email.
Disallow Attachments with these Extensions	Do not allow attachments that have the extension specified here.

Form

Parameter	Definition
Offer CC	Turn carbon copy reply on and off.
Offer BCC	Turn blind carbon copy reply on and off.
Offer Attachment	Allow attachment with reply.
Freeze Subject	Make the Subject field non-editable.
Freeze CC	Make the CC field non-editable.
Freeze Bcc	Make the Bcc field non-editable.
Subject Reply Prefix	When the user clicks the "Reply" or "Reply All" button in an envelope to reply to the sender or all recipients of an email, a blank email compose page is displayed. Text in this "Subject Reply Prefix" field is added to the beginning of the reply's subject. For example, if the original email's subject is "Q4 results" and this field contains "RE:" then the subject of the reply will be "RE: Q4 results". A space is automatically added between the prefix text and the original subject.
Subject Forward Prefix	This is similar to the "Subject Reply Prefix" field. This text, though, is added to the beginning of the email's subject when the user clicks the "Forward" button in an envelope. This field is typically set to "FWD:".
Include Attachments when Forwarding	When checked, a secure forward will automatically include any attachments from the original message. Note that this option only has an effect when the envelope is opened by the online opener. If the envelope is opened using the applet then the forward will not contain any attachments.
Offer Secure Option	Offer secure option.
Max Upload Size	Max upload size.
Upload Directory	Upload directory.
EnvelopeOpener Storage Directory	The directory used by the online opener to store temporary files (e.g., attachments). This is the directory that will be searched when looking for attachments for secure forward. If blank, the java.io.tmpdir system property will be used. This configuration must match the temporary storage directory configured under Web Services > EnvelopeOpener > Base Directory.

Parameter	Definition
Maximum Session Timeout Interval	Maximum session timeout interval.

Mail Server

Parameter	Definition
Mail Service Name	Mail server name.

Key Server

KeyServerDB

Parameter	Definition
DataSource Prefix	JNDI namespace prefix used to look up the DataSource.
Datasource Name	Name of the DataSource used for the keystore database (This is a drop down combo box of all the DataSources that are configured under DSDataSources).
Database Username	Not currently used.
Database Password	Not currently used.
Database Table Name	Database tablename where the keystore is stored.
Factory	JNDI Factory Class. This Factory Class is used for JNDI lookup and should correspond to the Provider URL specified below.
Provider	The URL that points to the JNDI Provider to use for JNDI lookup.

Lookup

Parameter	Definition
Sender Lookup Provider	Sender lookup provider.
Recipient Lookup Provider	Recipient lookup provider.

Mail Server

Parameter	Definition
Mail Service Name	Mail server to connect to when sending return receipts. The mail server is configured on the Mail Services node of the Administration Console (on the Configuration tab, navigate to Configuration > Mail Services > Mail Service List).

ReturnReceipt

Parameter	Definition
Mail Body Charset	Charset to be used for the return receipt that is sent for registered envelopes. The default is “iso-8859-1” which indicates plain us-ascii format and should be changed to the desired character encoding.
Email Subject	Email subject to use for read receipts.
Template File	Template file for the text body used by read receipts.

Sender Authentication

Parameter	Definition
Session Timeout	Idle timeout value for the authentication session if used in context of the keysever. (Default = 1200)
Single Sign On Authentication Manager	Authentication provider to use for certificates, cookies and single sign-in.
Username and Password Authentication Manager	Authentication provider to use for password authentication.
Max Password Retries	Maximum number of times the sender is allowed to retry entering their password until they are locked out.
Denied Network Addresses	A comma separated list of network addresses that will be denied access to the application.
Allowed Network Addresses	A comma separated list of network addresses specified in the same format as any other 'Net' matcher. Messages coming from clients in this list will NOT have the IronPort Encryption appliance headers removed from the email message.

Recipient Authentication

Parameter	Definition
Username and Password Authentication Manager	Authentication provider to use for password authentication.

Envelope

Parameter	Definition
Check Access Rules	Check access rules using a key server token.
Access PostX Registration Data	Is user registration information stored in the IronPort Encryption appliance database.
Enable Traffic Encryption	Enable traffic encryption.
Validate Email Addresses	When checked, the key server validates all email addresses it receives before using them. When unchecked, it trusts the email addresses to be legitimate. The default is checked.
Maximum Open Attempts	Maximum attempts a user can make to open a registered envelope before it is locked.
Minimum Message Security	The lowest message security that will be allowed. Any message with a message security level lower than this value will be rejected and either spooled or bounced.
Envelope Poll Parameters:	
Keyserver Wait Interval	Number of milliseconds the server will wait before trying to results returns again.
Minimum Poll Interval	Minimum number of milliseconds the envelope will wait between poll requests.
Maximum Poll Interval	Maximum number of milliseconds the envelope will wait between poll requests.
Total Wait Time	Total Number of milliseconds the envelope will wait for a valid response from the key server.

Master Keys

Parameter	Definition
Enable Master Keys	Select to enable master keys.
Master Key	Master key.

Domain Master Key

Parameter	Definition
Domain Name	Domain name for the master key.
Master Key	Master key.

P3P Policy

Parameter	Definition
Organization Name	The name of the organization that will go into Privacy Policy.
URL Prefix	The URL prefix.

Envelope Opener

Parameter	Definition
Legacy Support:	
Open Pre-5.3 Envelopes	Check to allow envelopes generated with pre-5.3 systems to be opened.
Maximum Parts per Envelope	Maximum number of parts to allow in pre-5.3 envelopes. There are about 348 parts per megabyte of payload; use -1 for no limit.
Registered Envelope Support:	
Internal Key Server URL	URL used by the envelope to contact the key server.
Keyserver Host	Host on which the key server resides.
Key Server Proxy	Name of the key server proxy configuration.
Error Pages:	
Base Location	Base URL of envelope opener error pages.
Temporary Storage:	
Base Directory	The directory used by the online opener to store temporary files. If blank, the java.io.tmpdir system property will be used. UNC paths are supported (e.g., //server/path).
Mobile Device Support:	
Temp file expiry (hrs)	The maximum age of a temporary file before it is permanently deleted from the server. The default value is 8 hours.
Page title	The title and heading shown on the Mobile Device Support authentication page.

Admin

Parameter	Definition
Monitor Accounts Query Time Range	The Monitor Accounts subtab includes this many hours of data.

Console Security

Parameter	Definition
Single Sign On Authentication Manager	Authentication provider to use certificates, cookie and single sign-on.
Username and Password Authentication Manager	Authentication manager used for password authentication.
Maximum Failed Login Attempts	Maximum number of unsuccessful login attempts.
Denied Network Addresses	Comma separated list of network addresses that are denied access to the application.
Allowed Network Addresses	Comma separated list of network addresses that are permitted access to the application.

WebSafe

Parameter	Definition
Maximum Custom Folders	A WebSafe client user cannot create more customer folders than this specified value.
Send Return Receipt	If enabled this parameter applies to all emails composed from WebSafe email client and the outgoing emails contain standard SMTP header information requesting return receipt. A return receipt notification email is sent to the WebSafe sender mailbox for each new email opened by the recipient. The notification is in the form of a "Message Disposition Notification" as per RFC 2298. Please note that not all external email clients will respect this SMTP header for Return Receipt and hence RR is not guaranteed for emails sent out to the external world.
Add X-Header to WebSafe Emails	The SMTP X-header that gets added to all outgoing emails from WebSafe. Please see the section *WebSafe Headers* in this chapter for more information.
Messages Per Page	Specifies the number of emails to be listed on each page of the web mail user interface. If the number of emails exceeds this limit the remaining emails are listed on a new page and you can navigate between pages using the "Prev" and "Next" buttons.

Parameter	Definition
Compose Template Path	WebSafe supports templates to be used when composing a new email. These templates are designed by the enterprise and specifies each new composed email to have certain pre-filled values, restrict certain parameters like cc or attachments, specify custom parameters, list allowable or restricted attachments, max limit for attachment size, etc. These templates are defined in XML format and this parameter specifies the path where these templates are present.
Compress Messages	Compresses all messages stored in WebSafe mailboxes before storage.
JNDI Provider URL	The JNDI Provider location that needs to be specified especially if the WebSafe Client is running on a separate system other than the WebSafe Server component. This URL points to the JNDI Provider to use for JNDI lookup.
JNDI Factory Class	The JNDI Factory Class that needs to be specified especially if the WebSafe Client is running on a separate system other than the WebSafe Server component. This Factory Class is used for JNDI lookup and should correspond to the Provider URL specified above.
Default Mailbox Expiration Period (days)	WebSafe supports aging feature for all the messages it stores in its content database. This parameter specifies the default value of the expiry duration for each new mailbox that is created by the administrator. The value is used to form the expiry date for all emails composed from WebSafe. However this value will be useful to detect expiry only if the email is sent within the WebSafe domain to another WebSafe mailbox. This mailbox global value can be changed on a per email basis in future releases.
Default No Return Receipt Notification (days)	WebSafe supports requesting return receipts for emails sent out from its webmail client. In addition if the email is not read within a specified duration, especially for time-sensitive communications, the sender can be informed in order to take further action. If the email is not read within the specified days a notification email is send to the sender to that effect. The notification is in the form of a “Message Disposition Notification” as per RFC 2298. However this value will be useful for no RR notifications only if the email is sent within the WebSafe domain to another WebSafe mailbox. This mailbox global value can be changed on a per email basis in future releases.

Parameter	Definition
Content Encryption Algorithm	Specifies the encryption algorithm to be used for encrypting the email content when storing in the database for emails composed through WebSafe email client. The current version of the server does not support encryption of the content and hence this option will not have any significant effect. In the future, this parameter will allow the administrator to choose the encryption algorithm from values like RC4, 3DES etc.
Content Encryption Token	Specifies the encryption token.
Postmaster Email Address	The email address of the postmaster.
X-Header to Encrypt Clear Archived Messages on Resend	Header added to resent messages which were archived unencrypted and are resend in "As Is" mode. For example, X-PostX-Secure.
Custom Property File Name	The property file that contains configuration values that are customer specific. Use the **Select** button to navigate to the file.
Allow Secure Compose Without Token	Select to allow secure compose without token.
Attachment Template Type	Name of the attachment template.
Attachment Template File	File containing the attachment template. Use the **Select** button to navigate to the file.
Maximum Post Size (KBs)	This parameter limits the maximum size of data posted to WebSafe from the recipient's client machine. This parameter directly affects the maximum size of allowed attachments and should match the size accordingly.
Password Challenge Questions	Select the password challenge question you want to use from the drop-down.
Registration Cleanup Time	Number of days before unused registration messages expire.
Enable CAPTCHA	Display the CAPTCHA image that the user must type.

Parameter	Definition
Enable X509 certificate enrollment	Check to enable X509 certificate enrollment. When this parameter is checked, users will see an option to upload an X509 certificate on their enrollment page. Uploading of X509 certificates is optional; users can continue the registration process normally even if they don't have X509 certificates. The system will not accept expired X509 certificates. The email address in the X509 certificate should match the email address for which the certificate is being registered.
Enable PGP certificate enrollment	Check to enable PGP certificate enrollment. When this parameter is checked, users will see an option to upload a PGP certificate on their enrollment page. Uploading of PGP certificates is optional; users can continue the registration process normally even if they don't have PGP certificates. The system will not accept expired PGP certificates.

Mail Service

Parameter	Definition
Mail Service	Used to send return receipt notification emails and emails composed from within WebSafe. The default mail server is "localhost" which is usually the machine that runs the mail server for the IronPort Encryption appliance.

Session

Parameter	Definition
Session Timeout (secs)	The session logic of WebSafe will automatically logout any recipient when no action is detected for specific duration of time. This duration in seconds is specified here.
Maximum Failed Login Attempts	Specifies the maximum number of password attempts before the user is blocked from further access. A blocked user needs to be enabled by the administrator before he can successfully login to this account.
Maximum Password Recover Attempts	Specifies the number of failed attempts after which the user's status will change to SUSPENDED when the user goes through the Forgot Password link.

Notifications

Parameter	Definition
Register Notification:	
Send Register Notification	Send notification on registration.
Template File	Name of the template file.
Template File Encoding	Encoding that the file is given when it is stored.
Template File Charset	Charset used for the email that the file becomes.
Email Subject	Email subject for register notification mail.
Password Change Notification:	
Send Password Change Notification	Send notification on password change.
Template File	Name of the template file.
Template File Encoding	Encoding that the file is given when it is stored.
Template File Charset	Charset used for the email that the file becomes.
Email Subject	Email subject for password change notification file.
Temporary Password Notification:	
Email Subject	The subject of the temporary password notification message.
Message From Address	The temporary password email will be from this email address.
Text Message Template File	The name of the text template file that contains the temporary password message.
Text Message Encoding	Encoding that the file is given when it is stored.
Text Message Charset	Charset used for the email that the file becomes.
HTML Message Template File	The name of the HTML template file that contains the temporary password message.
HTML Message Encoding	Encoding that the file is given when it is stored.
HTML Message Charset	Charset used for the email that the file becomes.

Parameter	Definition
Change Password URL	The URL of the page for the notification message that is sent to users required to change their temporary password. By default this value is server URL/websafe.

Mail Quota

Parameter	Definition
Default Mail Box Quota (MBs)	The default disk quota or space allocated for each mailbox when created by the admin.
Mailbox Quota Limit Percentage	The % limit for the mailbox quota that when reached WebSafe will give an error on the Compose screen and not allow the user to send any email. (Default = 120%)
Maximum Mailbox Quota (MBs)	The % of the mailbox space that can be used before a warning message is sent. (Default = 100%)

Archives

Parameter	Definition
X-Header for Clear Archived Messages on Resend	Header added to resent messages which were archived unencrypted and are resend in “As Is” mode. For example, X-PostX-NoSecure.
Custom Search Fields	A list of custom property fields associated with archived messages which are allowed in the archival search. For example, CustomerID,PlanID,JobID.
Custom Display Fields	A list of names for the custom property fields associated with archived messages which are allowed in the archival search. These display names match 1:1 with the search fields used in Archival. For example, Customer ID,Plan ID,Job ID
Allow Resend As Is	Send messages as they currently are without a new password.
Allow Resend Using a New Password	Send messages with a new password.
Allow Resend Using Configured Lookup	Send Messages encrypted using a configured lookup.

Parameter	Definition
Allow Administrator To View User MailBox/Archived Messages	Determines whether the WebSafe or archive administrator will get the ability to view all messages. If this parameter is not checked, the administrator can still search and manage or resend all messages, but he cannot view them.
X-Header for Resent Emails	Header added to resent messages which were archived unencrypted and are resend in “As Is” mode. For example, X-PostX-NoSecure.
Names of Active Archive Applications	A comma-separated list of applications that are actively being used for archive purposes.

Activation

Parameter	Definition
Destination	Activation destination. Valid values are recipient, sender, and administrator.
Confirmation URL	URL used in the activation email to confirm the registration.
Cancellation URL	URL used in the activation email to cancel the registration.
Message From Address	The email address the activation is from.
Message Subject	The activation email subject.
Administrator Email	If administrator is selected above, then this is the message destination.
Text Message Template File	Text file containing the email body used for the activation email.
Text Message Encoding	Encoding used for the text message.
Text Message Charset	Charset used for the text message.
HTML Message Template File	HTML file containing the email body used for the activation email.
HTML Message Encoding	Encoding used for the HTML message.
HTML Message Charset	Charset used for the HTML message.
Success Notification:	
Send Email	Select to inform users when their accounts have been successfully activated.
Email Subject	The subject of the successful activation email.
Text Template File	The text template of the successful activation email.
Text Encoding	Encoding used for the text version of the successful activation email.
Text Charset	Charset used for the text version of the successful activation email.
HTML Template File	The HTML template of the successful activation email.
HTML Encoding	Encoding used for the successful activation email.
HTML Charset	Charset used for the successful activation email.

Parameter	Definition
Cancel Notification:	
Send Email	Select to inform users when their account activation has been canceled.
Email Subject	The subject of the canceled activation email.
HTML Template File	The HTML template of the canceled activation email.
HTML Encoding	Encoding used for the canceled activation email.
HTML Charset	Charset used for the canceled activation email.
Text Template File	The text template of the canceled activation email.
Text Encoding	Encoding used for the text version of the canceled activation email.
Text Charset	Charset used for the text version of the canceled activation email.
Expire Notification:	
Expiration Period	Number of days before activation requests expire. A zero value indicates they will never expire.
Activation Email Subject	The subject of the expired activation email.
HTML Template File	The HTML template of the expired activation email.
HTML Encoding	Encoding used for the expired activation email.
HTML Charset	Charset used for the expired activation email.
Text Template File	The text template of the expired activation email.
Text Encoding	Encoding used for the text version of the expired activation email.
Text Charset	Charset used for the text version of the expired activation email.
Activation Reminder:	
Email Subject	The subject of the activation reminder email.
HTML Template File	The HTML template of the expired activation email.
HTML Encoding	Encoding used for the expired activation email.

Parameter	Definition
HTML Charset	Charset used for the expired activation email.
Text Template File	The text template of the expired activation email.
Text Encoding	Encoding used for the text version of the expired activation email.
Text Charset	Charset used for the text version of the expired activation email.

Password

Parameter	Definition
Minimum Password Length	The password management system within WebSafe uses this value to enforce minimum password length.
Enforce Alphanumeric Passwords	If checked, the password management system within WebSafe will enforce all passwords to be alphanumeric.
Enforce Mixed-Case Passwords	If checked, the password management system within WebSafe will enforce all passwords to be mixed case.
Enforce Special Character in Passwords	If checked, the password management system within WebSafe will enforce all passwords to contain special characters.
Enforce Case-Sensitive Password	If this parameter is set checked, then passwords will be case sensitive. Since the database for pxenroll and WebSafe are the same, the sensitivity set in one affects the other. Therefore it is recommended that you set both to either sensitive or not.
Password Encryption Algorithm	The administrator can select the password-hashing algorithm used by WebSafe before storing the passwords to the IronPort Encryption appliance DataStore. The values available for selection are “SHA-1”, “MD5” and “Plain”.
Enforce Password History	Password History allows you to specify frequency with which a password can be reused. This configuration parameter determines how you are going to use this feature. Options are: Disable – Do not use the password history feature By Duration – Enforce the password history by duration By Count – Enforce the password history by count

Parameter	Definition
Password History Duration (days)	The number of days that must pass prior to a password being reused.
Password History Count	The number of times that a password can be changed prior to allowing its reuse.
Forgot Password:	
Forgot Password Type	Specifies the action to take when a forgotten password occurs. Value are Temporary Password and User-Reset.
Temporary Password Expiration (hrs)	Number of hours until temporary password expires.

Large File Support

Parameter	Definition
Attachment Upload Directory	Specifies the temporary directory to hold the attachment files during compose of new emails and display of old emails. The attachment files are stored in this temporary directory for a short time and within specific directories for each mailbox. Default is postxwebsafe.
MIME File Directory	Directory to save the MIME message in when file save is triggered.
Trigger File Size	File size that triggers files to be saved to disk.
Document Repository Name	Name of the document repository.
Download Action	Download location.

Security

Parameter	Definition
Single Sign On Authentication Manager	Used for authentication that is using providers that DO NOT require a username and password to be entered by the user. This includes X509 certificates, remember me cookie and single sign on.
Username and Password Authentication Manager	Used for authentication that is using providers that DO require a username and password to be entered by the user. This includes the default IronPort Encryption appliance database, Kerberos, Lookup and LDAP.

Parameter	Definition
Denied Network Address	List of network addresses that are denied access to the application. (Comma separated)
Allowed Network Address	List of network addresses that are allowed access to the application. (Comma separated)

SECURITY

Authentication

Parameter	Definition
Max Password Age (Internal PostX Users)	The number of days a password is allowed before forcing the user to change it. 0 means disabled.

Single Sign on Authentication

Parameter	Definition
URL	URL path for the servlet request filter.

defaultX509Provider

Parameter	Definition
Provider Type	Authentication provider type. Display-only field.
Authentication Provider Name	Authentication provider name. Display-only field.
Enabled	Select to enable the provider.
Trust Level	Sets the security trust level for authentications granted by this provider.
Load User from Database	Populate the user information from the database.
Proxy Support Enabled	Enabled if X509 Client Authentication is used behind a proxy.
Header Attribute Name	Name of the HTTP header where the X509 certificate is located.

defaultCookieProvider

Parameter	Definition
Provider Type	Authentication provider type. Display-only field.
Authentication Provider Name	Authentication provider name. Display-only field.
Enabled	Select to enable the provider.
Trust Level	Sets the security trust level for authentications granted by this provider.
Cookie Name	The name of the cookie used to remember the user authentication details.
Token Validity	The duration of how long the token is valid for in minutes.
Case Sensitive Username	Determines if the username is case sensitive.

Username and Password Authentication

PostXDatabase
Providers - PostX Authentication Provider

Parameter	Definition
Provider Type	Authentication provider type. Display-only field.
Authentication Provider Name	Authentication provider name. Display-only field.
Enabled	Select to enable the provider.
Trust Level	Sets the security trust level for authentications granted by this provider.

Providers - Lookup Authentication Provider

Parameter	Definition
Provider Type	Authentication provider type. Display-only field.
Authentication Provider Name	Authentication provider name. Display-only field.
Lookup Name	Lookup name.
Enabled	Select to enable the provider.

Parameter	Definition
Encryption Type	Encryption type for this specific authentication provider.
Trust Level	Sets the security trust level for authentications granted by this provider.

Providers - LDAP Authentication Provider

Parameter	Definition
Provider Type	Authentication provider type. Display-only field.
Authentication Provider Name	Authentication provider name. Display-only field.
Enabled	Select to enable the provider.
Trust Level	Sets the security trust level for authentications granted by this provider.
Connect Securely	Select to allow a secure (i.e., SSL) connection to the LDAP server.
Server Name	Host name of the LDAP server.
Port Number	Port number that the LDAP server is listening on.
Logon to Server	Logon to the LDAP server to perform searches.
User Name	User name used to logon the server.
User Password	Password used to logon the server.
RootDN	RootDN for the directory tree.
Subcontext	Subcontext that is appended to the RootDN for queries.
User Authentication Method	Method used for user authentication.
Query String	Query string that is used when searches are disabled.
Enable Subtree Search	Enables searches of the directory substring.
Login Attribute Name	Name of the attribute used to compare login names.
Time Out	The connection timeout in milliseconds.
Password Attribute	Schema name of the password attribute.
Authentication DAO	Authentication DAO.

Providers - Kerberos Authentication Provider

Parameter	Definition
Provider Type	Authentication provider type. Display-only field.
Authentication Provider Name	Authentication provider name. Display-only field.
Enabled	Select to enable the provider.
Kerberos Configuration File	Pathname of the Kerberos configuration file.
Add Kerberos Realm	Appends the Kerberos Realm to the User ID to create a fully qualified User ID.
Kerberos Realm	Name of the Kerberos Realm.
Authentication DAO	The name of the authentication DAO to retrieve the User Info. (Optional)
Lookup Name	If a lookup is required to map an email address to external user ID. (Optional)
Identity Attribute	Attribute that contains the ID of the Kerberos user.
Trust Level	Sets the security trust level for authentications granted by this provider.

Database Security

Security Realms

Parameter	Definition
Realm Name	Name of the security realm.
Realm Type	Specifies whether the realm is transaction datasource or non-transactional datasource.
Principal Name	Your username.
JDBC Username	JDBC username.
JDBC Password	JDBC password.

Trust Stores

Parameter	Definition
Trust store file path	Trust store file path.
Trust store password	Trust store password.

Certificate Verification

Parameter	Definition
Verify certificate chain	If selected, it will verify the certificate chain. This is a global configuration for certificate verification. The settings will be used in the SMIMEHandler and Registered Envelope applications when verify certificate option is selected in the applications.
Verify revocation status	If selected, it will verify the revocation status.This is a global configuration for certificate verification. The settings will be used in the SMIMEHandler and Registered Envelope applications when verify certificate option is checked in the applications.
Proxy for CRL download	Proxy for CRL download

SCHEDULING

Scheduler

Parameter	Definition
Threads	Threadpool threads.
Member of Cluster	Select to enable clustering.

Scheduled Task List

The following configuration parameters are universal to all scheduled tasks. For parameters associated with specific tasks, please refer to *Chapter 12: Scheduling Tasks* in the *IronPort Encryption Appliance Operations manual*.

Parameter	Definition
Task Name	Name of task. (Display only)
Task Type	Type of task. (Display only)
Mail Service	Mail service for sending the email.
Repeat Interval (mins)	Run the task at the specified minute. Maximum value is 59 minutes. Minimum value is 0.
Use Repeat Interval Instead of Cron Expression	If true, use the "Minute Repeat Interval" parameter. If false, use the cron values below.
Minute	Cron expression string for minutes.
Hour	Cron expression string for hours.
Day of Month	Cron expression string for day of month.
Month	Cron expression string for month.
Day of Week	Cron expression string for day of week.
Year	Cron expression string for year.

TASKS

File Monitor/Scheduler Tasks

Parameter	Definition
Name	Name of the task.
Task Type	Task type. Display-only field.
Description	Description for this particular task.
Command	Enter the command.
Arguments	Command line arguments.
Append Stdout	Do you want to save the STDOUT text.
Append Stderr	Do you want to save the STDERR text.
Stdout File	Where to save STDOUT text.
Stderr File	Where to save STDERR text.
Working Dir	Working directory for the command line.

MONITOR SERVICES

Database Monitor

Parameter	Definition
Database Monitoring Interval	Specifies time interval in seconds between runs of the database monitor
DataSource Used	Datasource used for the SQL query.
SQL Query Run	SQL query used for monitoring database.
Enable Database Monitoring	A flag that turns on/off the database monitor
Enable Actions to Resolve Database Problems	A flag that enables Actions to fix PostXDatabase Connectivity when it is broken.

MAIL SERVICES

Mail Service LIst

Parameter	Definition
Name	Name of the mail7 service.
Mail Server Host	Mail server host.
Mail Server Port	Port number the mail server is using.
Postmaster Email Address	From address. (Default=postmaster@<appliance_hostname>)
SMTP Server Hello Name	SMTP Server Hello Name. Display-only field.
Mail Debug Flag	If checked, enables debugging output from the javamail classes.

DATABASE

PostXJNDILookup

Parameter	Definition
JNDI URL Provider	Provider of the JNDI Name Space Service.
Initial Context Factory	Factory to be used to do initial context lookup.
JNDIPrincipal	Value of the User ID from the active user registry in a Global Security enabled WebSphere Application Server.
JNDICredentials	Value of the user's password.

Index

X