Introduction to Personal Email Manager for Websense Email Security

Goals and Objectives

- **Introduction to Personal Email Manager**

- **Pre-Installation**
    - ✓ Supported platforms
    - ✓ Minimum system requirements
    - ✓ SQL deployment scenarios

- **Post-Installation**
    - ✓ **Configuration**
    - ✓ **SSL certificate management**
        - • Installing a self-signed certificate
        - • Installing a certificate from a Certificate Authority (CA)
        - • Installing an intermediate certificate from a Certificate Authority (CA)

- **Administration**
    - ✓ Configure Personal Email Manager enabled queues
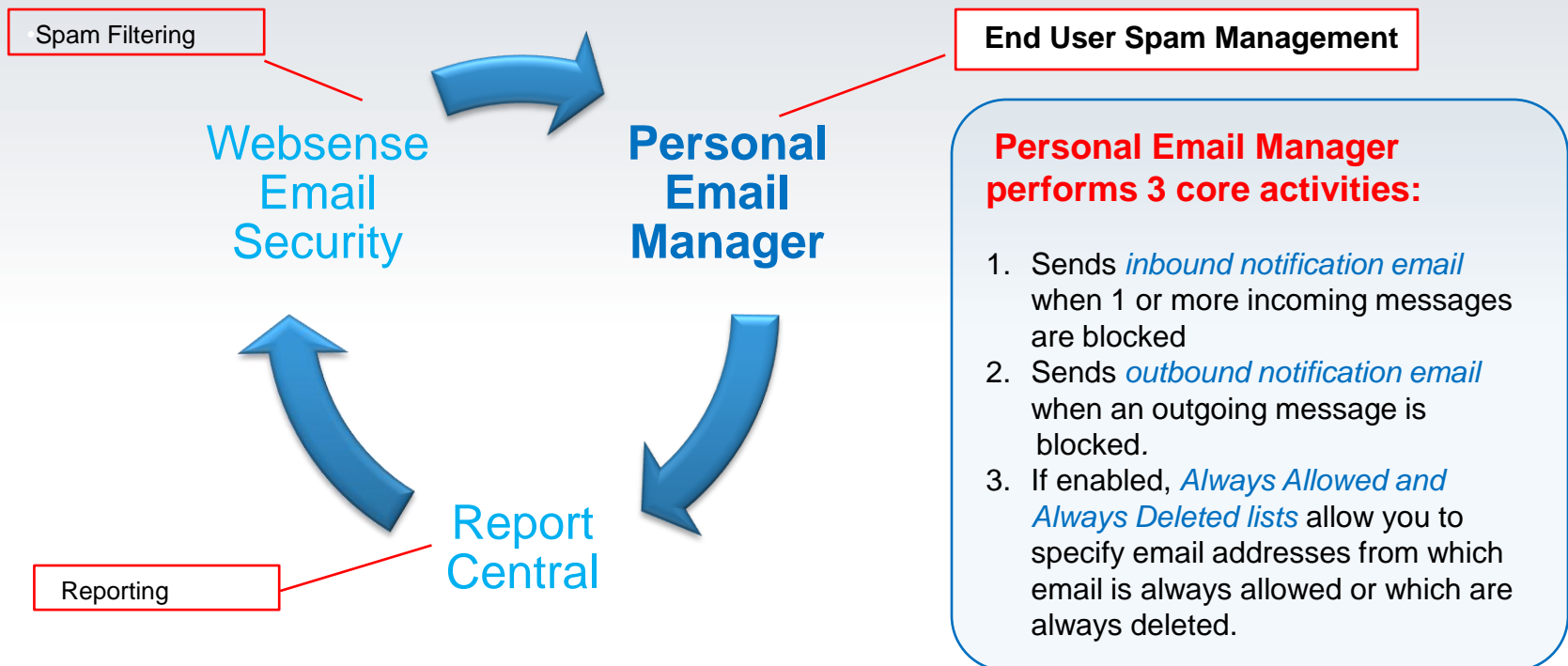   - ✓ Configure inbound notifications

websense
ESSENTIAL INFORMATION PROTECTION™

Presenter

Sean Haight

- **Title: Technical Support Analyst**
- **Accomplishments:**

  Actively supporting:
  - Websense Email Security
  - Websense Web Filter
  - Websense Data Security Suite
- **Education / Certifications:**
  - UCSD Certified UNIX Administrator
- **Qualifications:**
  - Web Filtering Expert
  - Trainer

websense
ESSENTIAL INFORMATION PROTECTION™

Introduction to Personal Email Manager

Websense® Email Security provides a comprehensive layer of protection against threats such as viruses, spam, and other undesirable malware.

Occasionally, Websense® Email Security may block email that is safe and wanted. **Personal Email Manager** is an optional facility that notifies you about blocked email and provides the means to manage it. Personal Email Manager includes a Web-based user interface and scheduled notifications to manage isolated emails.

Spam Filtering

End User Spam Management

Websense Email Security

Personal Email Manager

Report Central

Reporting

Personal Email Manager performs 3 core activities:

1. Sends *inbound notification email* when 1 or more incoming messages are blocked
2. Sends *outbound notification email* when an outgoing message is blocked.
3. If enabled, *Always Allowed and Always Deleted lists* allow you to specify email addresses from which email is always allowed or which are always deleted.

websense®
ESSENTIAL INFORMATION PROTECTION™

The Personal Email Manager Web User Interface

- **Personal Email Manager** includes an interactive facility for managing blocked inbound email and maintaining the Always Allowed and Always Deleted lists (i.e., personal whitelist and blacklist).

- **In the Personal Email Manager My Junk Email interface, you can:**
  - View a list of all blocked inbound email.
  - Preview blocked email.
  - Request to receive blocked email.
  - Elect to delete all blocked email.
  - Add or remove addresses in the Always Allowed or Always Deleted lists.

WEBSENSE® **Email Security**   **Personal Email Manager**

My Junk Email
These email messages have been blocked.

My Junk Email
Click Receive to release an email to your inbox   7 Messages

Action	From	Subject	Date (PST)	Classified As
Receive | Preview	bmb3tlhcs@vispa.com	Remember your first kiss?	Today 11:58 AM	Spam
Receive | Preview	ouellette@columbia.com	drugstore coupon	Today 11:58 AM	Spam
Receive | Preview	alenafranches8987@vispa.com	options contracts	Today 11:58 AM	Spam
Receive | Preview	hhb22ihmo@eslistas.net	Surprise your wife/gf	Today 11:58 AM	Spam
Receive | Preview	swilson@shemail.com	Fw: Shasha Rides	Today 11:55 AM	Inappropriate Material
Receive | Preview	jarkonsson@skandy.se	FW: Hot Pictures	Today 11:55 AM	Inappropriate Material
Receive | Preview	postmaster@cby-bank.de	Hey Sweetie	Today 11:55 AM	Inappropriate Material

7 Messages

Tasks
- ⭐ Add to Favorites
- 🗑 Delete all Junk Email
- ✅ Edit Always Allowed list
- ❌ Edit Always Deleted list

websense®
ESSENTIAL INFORMATION PROTECTION™

Launching Personal Email Manager

- **Launch Personal Email Manager in one of two ways:**
  - Select **Start > Programs > Personal Email Manager > Administrator**, or
  - Click the link to Personal Email Manager in an inbound notification email.
- **PEMAdmin is the default administrator account.**
  - Cannot be deleted
  - Must be used when logging into Personal Email Manager for the first time
  - Can be the sole administration account
- **To perform administration tasks, you must log in as PEMAdmin or have administrator privileges.**

> **Note:** PEMAdmin account is CASE SENSATIVE

websense
ESSENTIAL INFORMATION PROTECTION™

Logging into Personal Email Manager

- Click the Personal Email Manager link in your notification email.
- If you have bookmarked the page, open your browser and select the link from your list of favorites.

From:	Email_Admin@ILPDEMO.com [Email_Admin@ILPDEMO.com]	Sent: Wed 4/1/2009 9:16 AM
To:	Sean A. Haight	
Cc:		
Subject:	You have 1 blocked email	
Attachments:		

The following emails addressed to you have been blocked since Apr 1, 2009 09:16 PDT:

Action	From	Subject	Date	Classified As
Receive	spammer1@pemtest.com	As fast as 30 minutes.	Apr 1, 2009 09:14 PDT	Spam

Go to Personal Email Manager to see all of your blocked email and to set options.
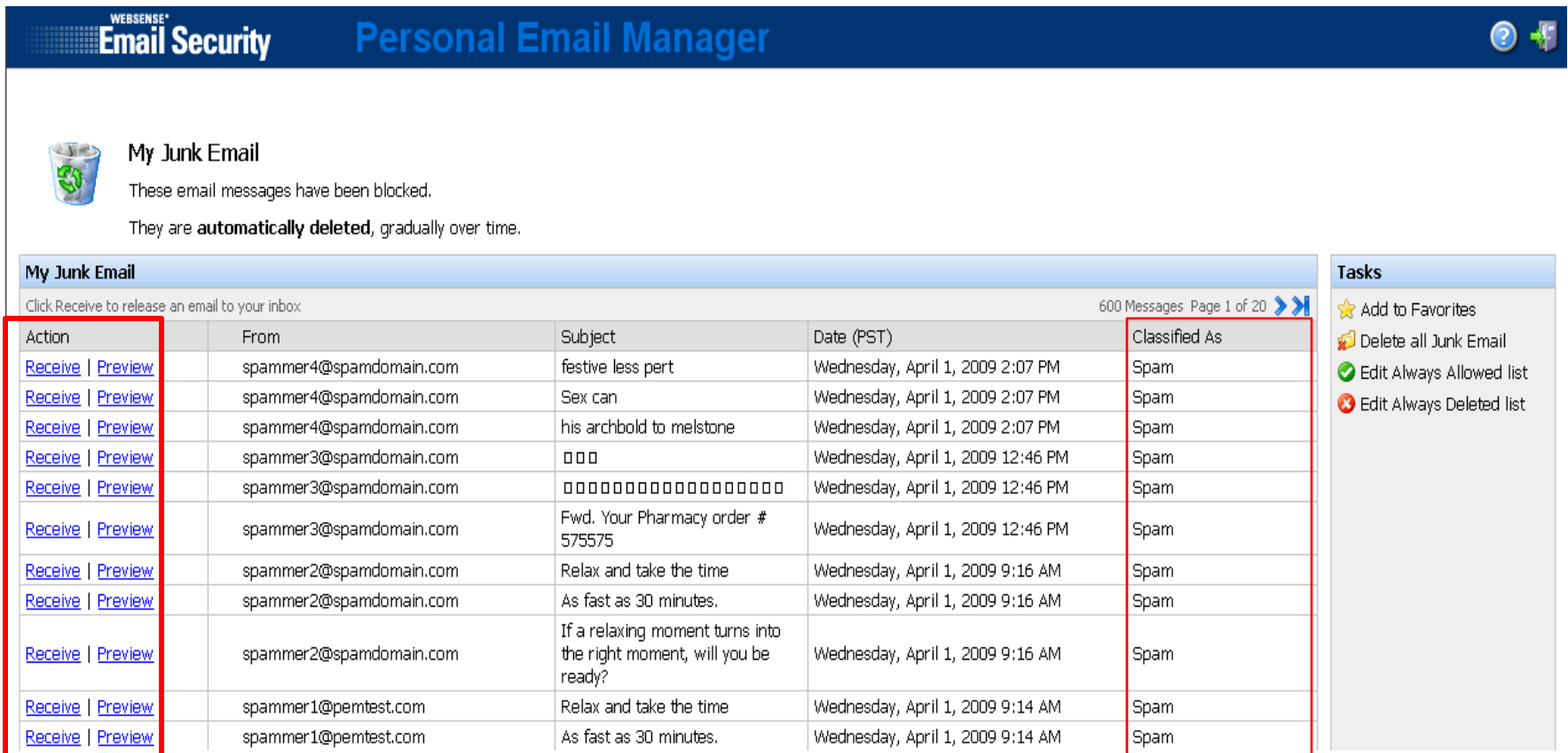
These emails will be **deleted** in approximately 14 days.

WEBSENSE®
Email Security

For further enquiries please contact the helpdesk

Done   Local intranet   100%

websense®
ESSENTIAL INFORMATION PROTECTION™

My Junk Email Page

- **The My Junk Email page provides a list of all blocked inbound email.**
- The **Action column** includes **Receive** and **Preview** links.
  - ➢ Click a link to initiate that action.
  - ➢ Clicking Receive delivers the original email to the recipient

Inbound Notification Messages

- Inbound Notifications are generated when an email is isolated to a PEM enabled queue.
- Inbound Notifications can be sent immediately or scheduled delivery times can be configured for up to 3 times per day
- Click the Personal Email Manager link to log into the interactive facility.

From:	Email_Admin@ILPDEMO.com [Email_Admin@ILPDEMO.com]	Sent: Wed 4/1/2009 9:16 AM
To:	Sean A. Haight	
Cc:		
Subject:	You have 1 blocked email	
Attachments:		

The following emails addressed to you have been blocked since Apr 1, 2009 09:16 PDT:

Action	From	Subject	Date	Classified As
Receive	spammer1@pemtest.com	As fast as 30 minutes.	Apr 1, 2009 09:14 PDT	Spam

Go to Personal Email Manager to see all of your blocked email and to set options.

These emails will be **deleted** in approximately 14 days.

WEBSENSE®
Email Security

For further enquiries please contact the helpdesk

websense®
ESSENTIAL INFORMATION PROTECTION™

Outbound Notification Messages

- Provides a facility to release the email as you deem appropriate.

From:	Email_Admin@ILPDEMO.com [Email_Admin@ILPDEMO.com]	Sent: Mon 4/6/2009 7:28 AM
To:	Sean A. Haight	
Cc:		
Subject:	Action required for your blocked email: his archbold to melstone	
Attachments:		

Please decide what to do with your blocked email.

Reason:	Classified as **Spam**
To/Cc/Bcc:	haight@websense.com
Subject:	his archbold to melstone
Date:	Apr 6, 2009 07:26 PDT
Attachments:	0

✔ Deliver   ✖ Do not Deliver

Otherwise it will be deleted in approximately 14 days.

WEBSENSE®
Email Security

For further enquiries please contact the helpdesk

websense
ESSENTIAL INFORMATION PROTECTION™

User Demo: Releasing Isolated Email

Demonstrate the ability to release of emails that have been isolated by Websense Email Security to PEM enabled queues

- **Learn how to:**
  - Launch Personal Email Manager.
  - Log in using Active Directory credentials

- **Use My Junk Email page to:**
  - Preview isolated messages.
  - Release and receive isolated messages.
  - Edit Always Allowed and Always Deleted lists.

- **Use Notification Emails to:**
  - Release and receive isolated messages.

websense
ESSENTIAL INFORMATION PROTECTION™

Requirements

Requirements

Personal Email Manager is compatible with the following operating systems and applications.

Component	Requirement
Operating systems	Windows 2000 Server SP4 Windows 2000 Advanced Server SP4 Windows Server 2003 Standard Edition SP2 Windows Server 2003 Enterprise Edition SP2
Applications	Internet Explorer 6.0 and 7.0 Firefox 1.5 and later
Database	MSDE 2000 SP4 SQL Server Express 2005 SP2 SQL Server 2005 SP2
LDAP	Active Directory for Windows Server 2000 and 2003 Lotus Domino 6.5

websense
ESSENTIAL INFORMATION PROTECTION™

Minimum System Requirements

Personal Email Manager has notably higher minimum system requirements when installed on the same server as **Websense Email Security.**

Component	Requirement
Processor: PEM alone PEM with Websense Email Security	Intel Pentium IV processor, 2 GHz or higher Intel Pentium IV processor, 3 GHz or higher
Memory: PEM alone PEM with Websense Email Security	1 GB RAM minimum, 2 GB recommended 2 GB RAM minimum, 4 GB recommended
Disk Space: PEM alone PEM with Websense Email Security	500 MB Minimum Disk Space, 1 GB recommended 2.2 GB Minimum Disk Space, 3.2 GB recommended
Display	Super VGA (800 x 600) or higher resolution video adaptor and monitor
Networking	TCP/IP installed and configured

SQL Server Deployment Considerations

Dedicated versus centralized database server

- **Centralized SQL server**
  - Logging data for multiple Websense Email Security servers is collected in a single, centralized database.
  - This configuration is preferred for Websense Email Security logging when used with Personal Email Manager.

- **Dedicated SQL server**
  - Logging data is collected in separate databases for each Websense Email Security server.
  - This SQL configuration does NOT allow for centralized management when Personal Email Manager is deployed with multiple Websense Email Security servers and is not recommended.

websense
ESSENTIAL INFORMATION PROTECTION™

SQL Deployment Scenarios

- Single Websense Email Security Server with a dedicated SQL server

- Multiple Websense Email Security Servers, each with a dedicated SQL server

- Multiple Websense Email Security Servers with one centralized SQL server

SQL Deployment Scenarios

Single Websense Email Security server with a dedicated SQL server

SQL Engine

STEMConfig

STEMFriendlyName

STEMLog

PEMLog

PEMConfig
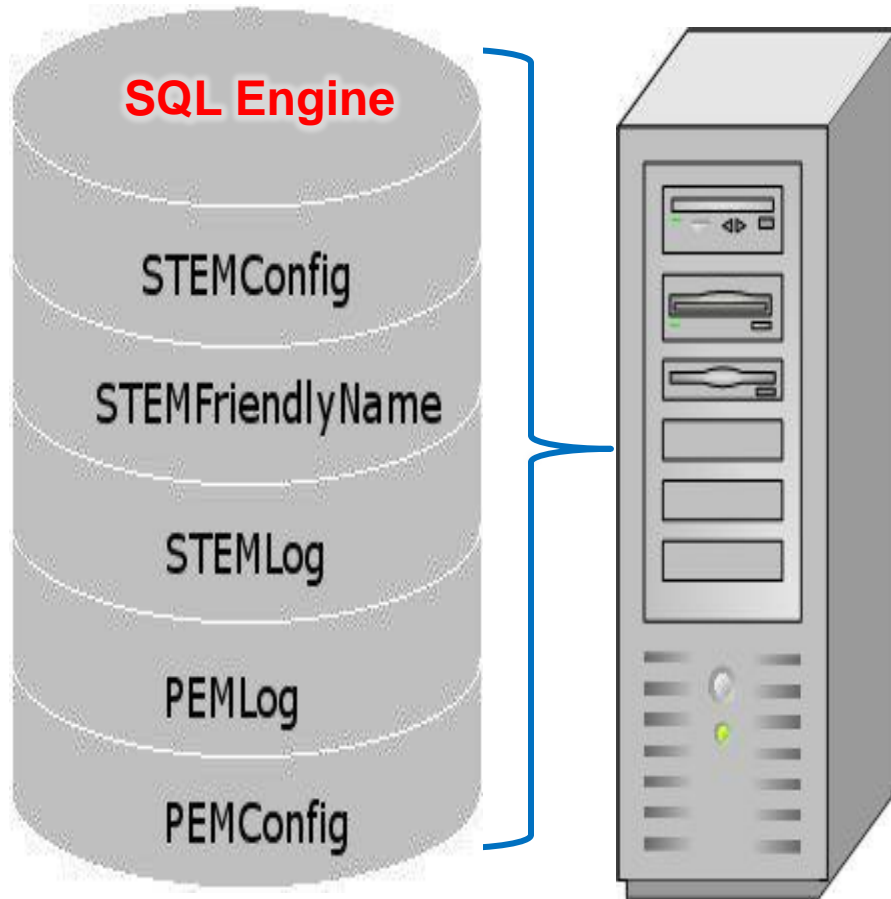
- Personal Email Manager is installed on a Websense Email Security server running a dedicated SQL server.
- All Websense Email Security and Personal Email Manager databases share the same SQL instance.
- System requirements are notably higher:

Minimum system requirements:
• Intel Pentium IV processor <u>3 GHz or higher</u>
• <u>2 GB RAM minimum</u>, 4 GB recommended

websense
ESSENTIAL INFORMATION PROTECTION™

SQL Deployment Scenarios

Multiple Websense Email Security servers, each with a dedicated SQL server

Personal Email Manager must be deployed and configured for each Websense Email Security server.

Email isolated by Websense Email Security in segment A must be released via the Web UI from a Personal Email Manager server located in segment A.

Email isolated by Websense Email Security in segment B must be released via the Web UI from a Personal Email Manager server in segment B.
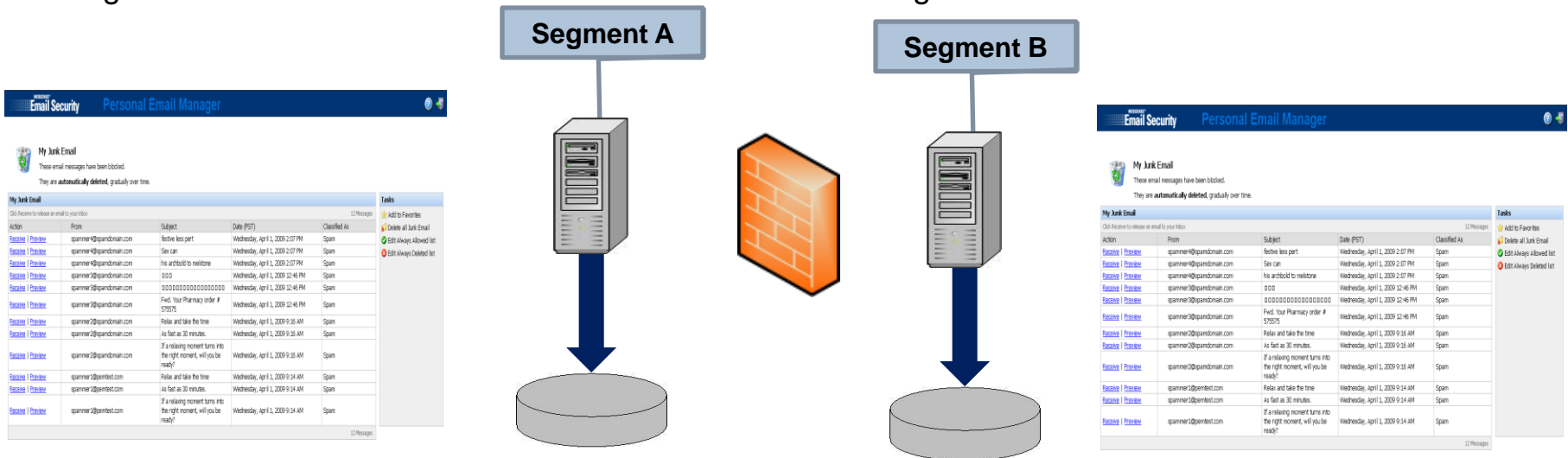
SQL Deployment Scenarios

Multiple Websense Email Security servers with one centralized SQL server

- Allows Personal Email Manager to receive regular updates from all Websense Email Security servers without deployment of additional Personal Email Manager servers
- Lets you release messages from all Websense Email Security servers via the Personal Email Manager Web user interface or scheduled inbound notification reports

Centralized SQL Configuration

Centralized STEMLog
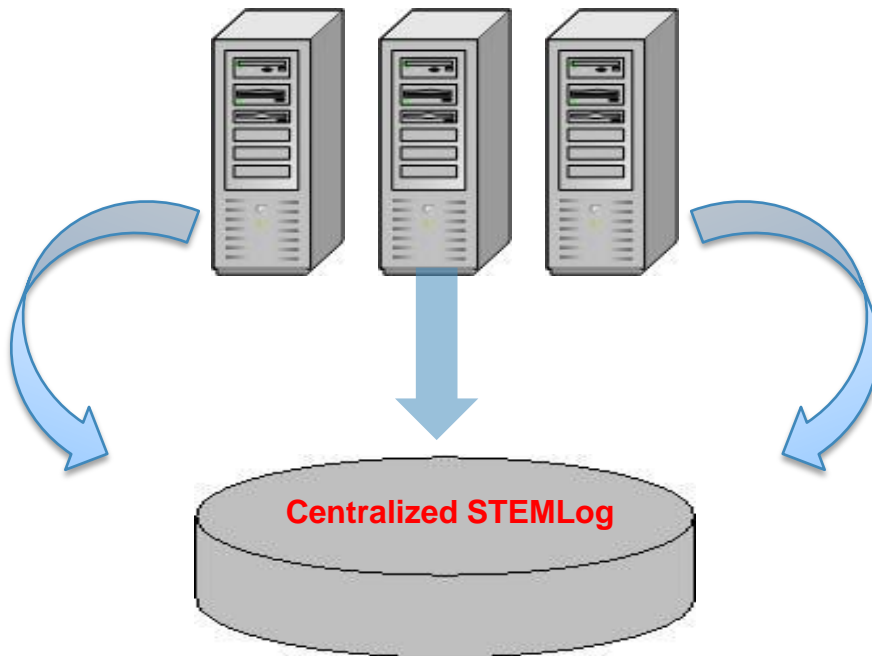
Configuration

Personal Email Manager Configuration Tool

Configure Personal Email Manager initially during installation.

The Personal Email Manager Configuration Tool allows you to change configuration settings, test connectivity, and control the Personal Email Manager service after installation.
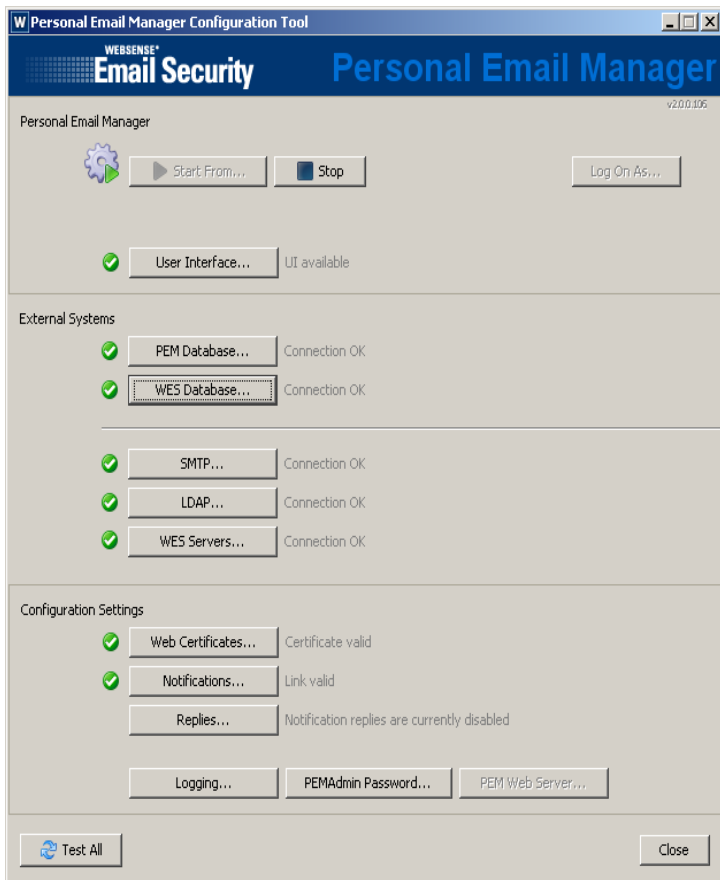
Use the Personal Email Manager Configuration Tool to:

- Specify the Windows user account under which the Personal Email Manager service runs.
- Test the Personal Email Manager Web user interface.
- Manage connections to the external systems.
- Configure the Personal Email Manager database.
- Configure Websense Email Security database.
- Configure SMTP servers.
- Configure LDAP servers.
- Configure Websense Email Security servers.

websense
ESSENTIAL INFORMATION PROTECTION™

Stopping and Restarting the Service

- If a restart is required, the following message appears next to the Stop button:
  "Restart to apply changes."
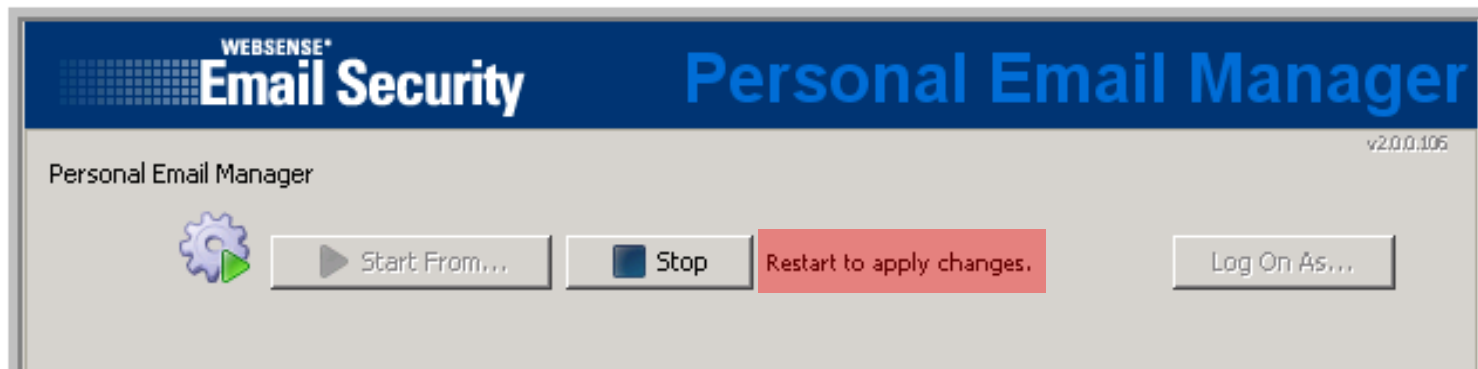
- A restart is required if you:
  - Change the connection definitions of any external service.
  - Change the settings for certificates, notifications, or replies.
  - Change the port settings for the Personal Email Manager Web server.
  - Apply a hotfix.

- You do *not* need to stop and restart Personal Email Manager if you change only the logging level or the PEMAdmin password.

websense
ESSENTIAL INFORMATION PROTECTION™

Starting the Service

If only the configuration has changed, or the unprocessed message backlog is not large:

- Click **Start From**, then click **Start** in the dialog box that appears. The service is started and blocked email is processed.
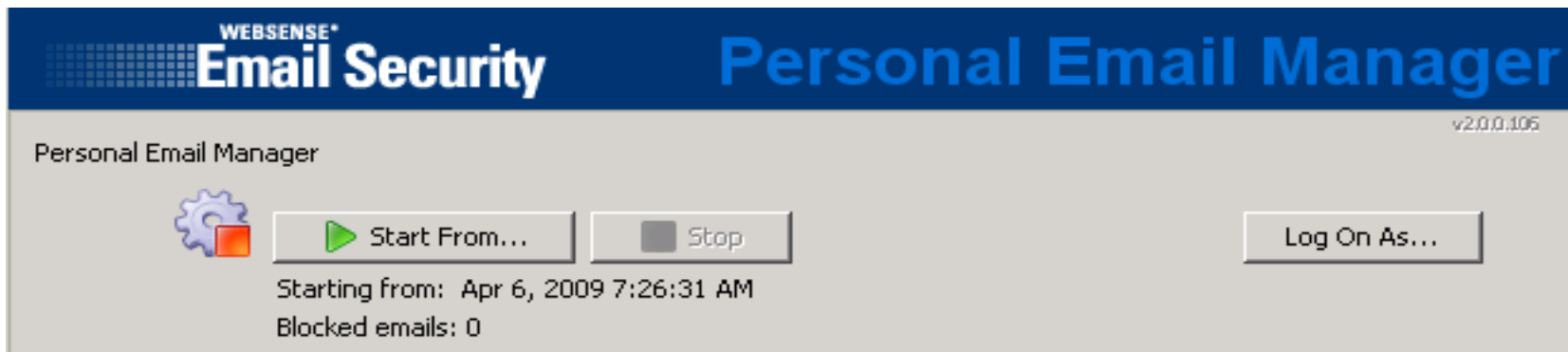
If the service has been stopped for a while, or a large backlog of unprocessed blocked messages exists:

- Adjust the date and time to limit blocked email processing to a recent period. Unprocessed email that is older than the Start From date is not processed.

External Systems: Database Servers

To change the connection specifications for the Personal Email Manager or Websense Email Security database servers, click the appropriate External Systems button:

1. Enter the name or IP address of the database server.

2. Enter the server's TCP port number. Default = 1433

3. Select the method of authentication.

4. With SQL authentication, enter the server login details.

External Systems

✅	PEM Database...	Connection OK
✅	WES Database...	Connection OK
✅	SMTP...	Connection OK
✅	LDAP...	Connection OK
✅	WES Servers...	Connection OK

Personal Email Manager Database ✕

Database server: WS-SHAIGHT-DEMO

Port: 1433

⦿ Use Windows authentication
○ Use SQL Server authentication

User name:

Password:

Refresh DB Lists

Config DB: PEMConfig ▾

Log DB: PEMLog ▾

🔄 Test   ✅ Connection OK

Save   Cancel
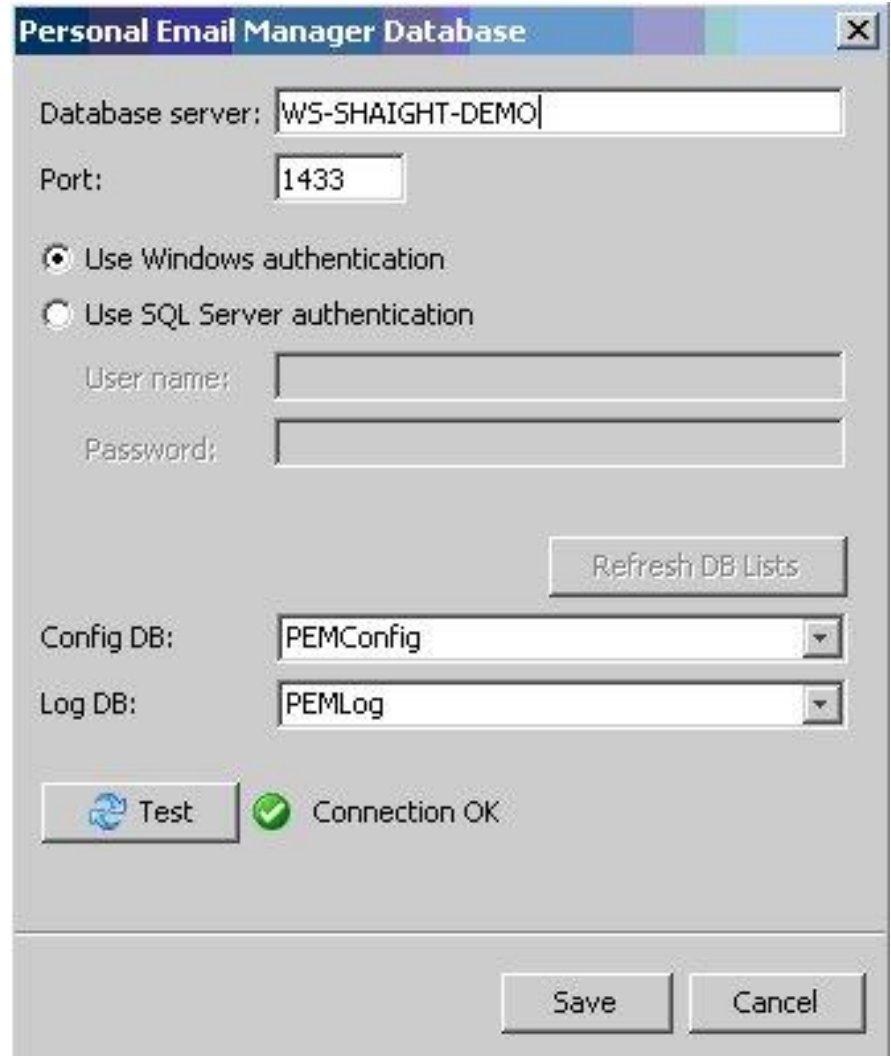
External Systems: Database Servers

- Click **Refresh DB Lists** to refresh the lists for the selected server and to inspect the names of the selected and available databases.

- Click an entry to select it.

- Click **Test** to validate the settings and test the connection.

NOTE:
Should the test fail, an error description is displayed next to **Test**. For more information about the error, examine the configuration log file.

Default Location of PEMConfigurator.log:
/Program Files/Personal Email Manager/Configuration Tools/Logs/

Personal Email Manager Database

Database server: WS-SHAIGHT-DEMO

Port: 1433

◉ Use Windows authentication
○ Use SQL Server authentication

User name:
Password:

Refresh DB Lists

Config DB: PEMConfig
Log DB: PEMLog

Test ✓ Connection OK

Save   Cancel

websense
ESSENTIAL INFORMATION PROTECTION™

External Systems: SMTP Server

The SMTP server acts as a mail relay for Personal Email Manager to send blocked notification email to the end users. (The SMTP server is not typically the Websense Email Security server.)

To change the connection, click SMTP:

1. Enter the name or IP address of the SMTP server. This is typically the name of your organization's email server.

2. Enter the TCP port number. Default = 25

External Systems

✅	PEM Database...	Connection OK
✅	WES Database...	Connection OK
✅	SMTP...	Connection OK
✅	LDAP...	Connection OK
✅	WES Servers...	Connection OK

SMTP Settings

The SMTP server sends the PEM notifications.

SMTP server: 127.0.0.1

Hint: This should be your organization's mail server, not your Websense Email Security server.

Port: 25

Test ✅ Connection OK

Save   Cancel

websense
ESSENTIAL INFORMATION PROTECTION™

LDAP Integration Demo for Active Directory

■ **Learn how to:**

– Create LDAP connection to Active Directory

– Verify LDAP connectivity using built-in search filters used to query for:

- *User Logins*
- *Email Address associated with LDAP user accounts*
- *Partial User, Group, and OU Names*
- *Distinguished Names*

LDAP Demonstration requires a valid:	
Domain Admin Account:	PEMDemo1
DC DNS Name or IP Address:	DEMO-DC.ILPDEMO.COM
Base DN:	DC=ILPDEMO, DC=COM

■ **(Optionally) Windows Server 2003 Support Tools for LDP:**

– Use to browse the LDAP directory tree, verify a successful bind and obtain the Base DN for the configuration tool.

– **Download Link:** http://go.microsoft.com/fwlink/?LinkId=100114

websense
ESSENTIAL INFORMATION PROTECTION™

Configuration Settings

In the Configuration Settings section of the Personal Email Manager Configuration Tool, you can:

- Control the event logging level.
- Change the password for the PEMAdmin account.
- Configure the ports used by the Personal Email Manager Web server.
- Manage Secure Sockets Layer (SSL) certificates.
- Configure and test the URL link to Personal Email Manager block notification emails.
- Configure and test the Personal Email Manager notification reply settings.

websense
ESSENTIAL INFORMATION PROTECTION™

Changing the Event Logging Level

- Click **Logging** on the main screen to change the logging level and other settings related to the Personal Email Manager log file.

- Personal Email Manager sends log entries to an XML file named "server.log." The log file can help diagnose Personal Email Manager problems.
- In the **PEM Logging** dialog box, specify the amount of detail recorded in the log file from the following options:
    - Error – Only serious errors are logged.
    - Warning – (default) Serious errors and minor problems are logged.
    - Information – All Personal Email Manager operations are logged.
    - Debug – Extensive information on Personal Email Manager and underlying framework is logged.

websense
ESSENTIAL INFORMATION PROTECTION™

Configuring Web Server Ports

- Click **PEM Web Server** on the main screen to set port numbers for the Personal Email Manager Web server.
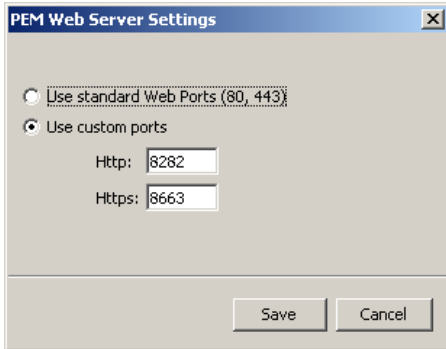
Note:
This dialog is available only when the Personal Email Manager service is stopped.

- Personal Email Manager uses ports for secured (HTTPS) and unsecured (HTTP) connections to the Personal Email Manager Web interface:

HTTP ports (default = 8282) – Used for unauthenticated requests from notification email
http://<servername or ip>:8282/PEM

HTTPS ports (default = 8663) – Used with SSL encryption for authenticated Personal Email Manager Web interface sessions to prevent compromise of end-user passwords.
https://<servername or ip>:8663/PEM

Changing the PEMAdmin password

- Because this account may be the only Personal Email Manager administrator account, and the password could be lost, you can reset this password.
- To change the PEMAdmin password, click **PEMAdmin Password** on the main screen to display the PEMAdmin Password dialog box

- Enter your password and confirm

- Click save to commit the changes

- No restart of the service is required

SSL Certificate Management

SSL Certificate Demo:
Creating and Installing a Self-signed SSL Certificate

- Created during initial installation for use by the Personal Email Manager
- Valid for 90 days
- Ensures that user names and passwords, in particular LDAP domain passwords, are sent encrypted during login

SSL Certificate Management   ✕

Current SSL certificate:

Alias name: pem-ssl
Creation date: Mar 5, 2009
Entry type: PrivateKeyEntry
Certificate chain length: 1
Certificate[1]:
Owner: CN=WS-SHAIGHT-DEMO, OU=Personal Email Manager, O=Websense, L=San Diego, ST=California, C=US
Issuer: CN=WS-SHAIGHT-DEMO, OU=Personal Email Manager, O=Websense, L=San Diego, ST=California, C=US
Serial number: 49b0034c
Valid from: Thu Mar 05 08:52:28 PST 2009 until: Wed Jun 03 09:52:28 PDT 2009
Certificate fingerprints:
         MD5: B4:50:19:4D:55:6C:B7:4E:83:3C:54:5A:66:9C:78:B0
         SHA1: 87:DB:4E:4E:4E:88:F8:0D:B3:87:0B:BC:1B:72:A9:29:22:2E:DD:42
         Signature algorithm name: SHA1withRSA
         Version: 3

✔ Certificate valid

Installing a Certificate from a Certificate Authority (CA)

- **To begin the installation process:**
  - Click, **Generate CSR** to generate a certificate signing request (CSR)**.**

- **The Certificate Signing Request screen:**
  - Displays the contents of the request and additional steps to be taken.

- **The CA will return the signed certificate:**
  - Read the CA's installation instructions to determine if additional root or intermediate certificates are required.

- **After any intermediate certificates are installed, click Import Certificate.**
  - In the "File – Open" dialog box, navigate to the location of the certificate and select it.

- The **Import Trusted Certificate** screen displays the details of the certificate.

- Click **Import** to complete the installation.

SSL Certificate Management

Certificate Signing Request

Steps:

1. Submit this Certificate Signing Request (CSR) to your Certificate Authority.
2. They will return the signed certificate.
3. Use the Import Certificate function to install it.

Certificate Signing Request:

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBxTCCAS4CAQAwgYQxCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpDYWxpZm9ybmlhMRIwEAYDVQQH
EwlTYW4gRGllZ28xETAPBgNVBAoTCFdlYnNlbnNlMR8wHQYDVQQLExZQZXJzb25hbCBFbWFpbCBN
YW5hZ2VyMRgwFgYDVQQDEw9TWURRQURFTExXT1JLMDIwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
AoGBANML2FhgOwh2jsDxMLvuKVGRyOwSr+eSb+4bUbAS+ZPWrdbpYzxjXytDZQtgYcSLluhlouc4
DQQyJIsQHzS6sUG6+uEwc5bo+N3l2BVihLslGFIGHcwLDiQfdBOYJkyjEAm8AzeeneknIWeIVUHc
JclLkdD26UmgUIzjfkUOSWYtAgMBAAGgADANBgkqhkiG9w0BAQUFAAOBgQCphJffbOCW3KSOO2bY
hRn6dJ2bKC4TleMaGJxv/He8SogkpHwOWl5OtCIjTV+jLuefksPkD3NpCU4i/dvsfNuqt29Y+aQv
/O9XaxLgto4EajfG+W4IBmXuM4HHTex6/DIJmluET9ttUnkkD5Icwmlv4RWiQ6Bk4kzSyd9nz59y
BA==
-----END NEW CERTIFICATE REQUEST-----
```

Copy   Close

Import Trusted Certificate

Certificate details:

Eigner: CN=SYDQADELLWORK02, OU=Personal Email Manager, O=Websense, L=San Diego, ST=California, C=US
Aussteller: CN=SYDQADELLWORK02, OU=Personal Email Manager, O=Websense, L=San Diego, ST=California, C=US
Seriennummer: 47c5f98c
Gültig von: Wed Feb 27 16:00:12 PST 2008 bis: Tue May 27 17:00:12 PDT 2008
Digitaler Fingerabdruck des Zertifikats:
        MD5: 52:C1:99:07:B4:50:53:B1:B5:02:E4:4B:8F:94:D3:9D
        SHA1: 55:5F:1A:D7:76:15:4A:9A:35:D3:E7:3F:92:A1:86:67:5F:0B:74:60
        Unterschrift-Algorithmusname: SHA1withRSA
        Version: 3

Import   Cancel

Installing an Intermediate Certificate from a Certificate Authority

- Additional certificate requirements should be stated in the CA's certificate installation instructions.
- Follow the instructions for Tomcat 5.x to obtain the necessary additional certificates directly from the CA.

1. Obtain the root and intermediate certificates from the CA.
2. Import the root and intermediate certificates using the java keytool
3. Import the SSL certificate issued by the CA using the java keytool.

Example installation of Verisign root and intermediate certificates:

a) Install root certificate :
keytool -import -alias root -keystore pemserver.keystore -trustcacerts -file "AddTrustExternalCARoot.crt"

b) Install first intermediate certificate :
keytool -import -alias intermediate1 -keystore pemserver.keystore -trustcacerts -file "NetworkSolutions_CA.crt"

c) Install second intermediate certificate:
keytool -import -alias intermediate2 -keystore pemserver.keystore -trustcacerts -file "UTNAddTrustServer_CA.crt"

Example installation of GoDaddy root and intermediate certificates:

a) Install root certificate :
keytool -import -alias root -keystore pemserver.keystore -trustcacerts -file "valicert_class2_root.crt"

b) Install first intermediate certificate :
keytool -import -alias cross -keystore pemserver.keystore -trustcacerts -file "gd_cross_intermediate.crt"

c) Install second intermediate certificate:
keytool -import -alias intermed -keystore pemserver.keystore -trustcacerts -file "gd_intermediate.crt"

Personal Email Manager
Web-based UI

Best Practices for Queue Configuration

- It's common practice to initially set up only the Anti-Spam Agent queue.
    - This queue is the most likely to have incorrectly identified spam (false positive)

- Recommended settings for Anti-Spam Agent queue:

Email queue	Inbound/Outbound	Users
Anti-Spam Agent	Inbound	All users

- You may also choose to PEM enable queues used to isolate message from custom dictionary rules which are more likely to catch false positives.

NOTE:

- Do *not* enable queue management for **Anti-Spam Agent - DFP.** The DFP queue contains 100% spam email, which does not need user management.

Configuring Inbound Notification Timing

- Set the time interval in which Personal Email Manager sends blocked inbound notification email.
- Settings do not apply to queues individually configured to send notifications.

User Demo: Personal Email Manager Administration

- Configure Personal Email Manager enabled queues.
- Grant administrator access to LDAP user and log in as administrator.
- Modify user settings.

Personal Email Manager - General Options
Set up general options.

☑ Allow users to manage their own Always Allowed lists
Ensure that Always Allowed processing is activated on suitable queues.

    ☑ When releasing blocked inbound email, offer user option to add sender to Always Allowed list.

        ☐ Select the user option by default.
        Not recommended. Users tend to add one-off addresses, impacting system performance.

☑ Allow users to manage their own Always Deleted lists
☑ Keep copies of Always Deleted email
    Audit Queue: [PEM Audit ▾]

Display previews of blocked inbound email as
◉ HTML
◯ Plain text

☑ Show list of reviewers in confirmation email for Request Review actions
Recommended: Enables users to quickly track down progress of urgent requests

☐ Include friendly names with addresses when processing blocked email
Not Recommended: Inbound spam email generates many random friendly names
    Maximum names: [3]   per email address

[OK] [Cancel]

Questions?

- As many questions as possible will be answered in the allotted time.
- Responses to all questions submitted will be posted online on the Support Webinar home page approximately one week from today.
- To review answers to your questions, go to:
  - http://www.websense.com/content/SupportWebinars.aspx

websense
ESSENTIAL INFORMATION PROTECTION™

May 2009 Webinar

Filtering Remote Users with Websense Web Filter version 7

Date: May 20, 2009, 8:30 A.M. (GMT -8:00)

How to register:

http://www.websense.com/F97762289