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
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
**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.

**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.
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.

![Image of the Personal Email Manager interface]
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 SENSITIVE
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.

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

<table>
<thead>
<tr>
<th>Action</th>
<th>From</th>
<th>Subject</th>
<th>Date</th>
<th>Classified As</th>
</tr>
</thead>
<tbody>
<tr>
<td>Receive</td>
<td><a href="mailto:spammer1@pemtest.com">spammer1@pemtest.com</a></td>
<td>As fast as 30 minutes.</td>
<td>Apr 1, 2009 09:14 PDT</td>
<td>Spam</td>
</tr>
</tbody>
</table>

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.

For further enquiries please contact the helpdesk.
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.

---

### Personal Email Manager

**My Junk Email**

These email messages have been blocked.

They are automatically deleted, gradually over time.

<table>
<thead>
<tr>
<th>Action</th>
<th>From</th>
<th>Subject</th>
<th>Date (PST)</th>
<th>Classified As</th>
</tr>
</thead>
<tbody>
<tr>
<td>Receive</td>
<td><a href="mailto:spammer4@spamdomain.com">spammer4@spamdomain.com</a></td>
<td>festive less part</td>
<td>Wednesday, April 1, 2009 2:07 PM</td>
<td>Spam</td>
</tr>
<tr>
<td>Receive</td>
<td><a href="mailto:spammer4@spamdomain.com">spammer4@spamdomain.com</a></td>
<td>Sex can</td>
<td>Wednesday, April 1, 2009 2:07 PM</td>
<td>Spam</td>
</tr>
<tr>
<td>Receive</td>
<td><a href="mailto:spammer4@spamdomain.com">spammer4@spamdomain.com</a></td>
<td>his archibald to melstone</td>
<td>Wednesday, April 1, 2009 2:07 PM</td>
<td>Spam</td>
</tr>
<tr>
<td>Receive</td>
<td><a href="mailto:spammer3@spamdomain.com">spammer3@spamdomain.com</a></td>
<td></td>
<td>Wednesday, April 1, 2009 12:46 PM</td>
<td>Spam</td>
</tr>
<tr>
<td>Receive</td>
<td><a href="mailto:spammer3@spamdomain.com">spammer3@spamdomain.com</a></td>
<td></td>
<td>Wednesday, April 1, 2009 12:46 PM</td>
<td>Spam</td>
</tr>
<tr>
<td>Receive</td>
<td><a href="mailto:spammer2@spamdomain.com">spammer2@spamdomain.com</a></td>
<td></td>
<td>Wednesday, April 1, 2009 9:16 AM</td>
<td>Spam</td>
</tr>
<tr>
<td>Receive</td>
<td><a href="mailto:spammer2@spamdomain.com">spammer2@spamdomain.com</a></td>
<td></td>
<td>Wednesday, April 1, 2009 9:16 AM</td>
<td>Spam</td>
</tr>
<tr>
<td>Receive</td>
<td><a href="mailto:spammer2@spamdomain.com">spammer2@spamdomain.com</a></td>
<td></td>
<td>Wednesday, April 1, 2009 9:16 AM</td>
<td>Spam</td>
</tr>
<tr>
<td>Receive</td>
<td><a href="mailto:spammer2@spamdomain.com">spammer2@spamdomain.com</a></td>
<td></td>
<td>Wednesday, April 1, 2009 9:14 AM</td>
<td>Spam</td>
</tr>
<tr>
<td>Receive</td>
<td><a href="mailto:spammer1@pomtest.com">spammer1@pomtest.com</a></td>
<td>Relax and take the time</td>
<td>Wednesday, April 1, 2009 9:14 AM</td>
<td>Spam</td>
</tr>
<tr>
<td>Receive</td>
<td><a href="mailto:spammer1@pomtest.com">spammer1@pomtest.com</a></td>
<td>As fast as 30 minutes.</td>
<td>Wednesday, April 1, 2009 9:14 AM</td>
<td>Spam</td>
</tr>
</tbody>
</table>
Inbound Notification Messages

- Inbound Notifications provide the facility to:
  - Request to receive a blocked email and, optionally, add the sender to the Always Allowed list.
  - Click the Personal Email Manager link to log into the interactive facility.

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.

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

<table>
<thead>
<tr>
<th>Action</th>
<th>From</th>
<th>Subject</th>
<th>Date</th>
<th>Classified As</th>
</tr>
</thead>
<tbody>
<tr>
<td>Receive</td>
<td><a href="mailto:spammer1@pemtest.com">spammer1@pemtest.com</a></td>
<td>As fast as 30 minutes.</td>
<td>Apr 1, 2009 09:14 PDT</td>
<td>Spam</td>
</tr>
</tbody>
</table>

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.

For further enquiries please contact the helpdesk.
Outbound Notification Messages

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

From: Email_Admin@LPDEMO.com [Email_Admin@LPDEMO.com]
To: Sean A. Haight
Cc: 
Subject: Action required for your blocked email: his archbold to melstone
Attachments: 

Sent: Mon 4/6/2009 7:26 AM

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: 

☐ Deliver ☐ Do not Deliver

Otherwise it will be deleted in approximately 14 days.

For further enquiries please contact the helpdesk.
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.
Requirements
### Requirements

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

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirement</th>
</tr>
</thead>
</table>
| 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 |
**Minimum System Requirements**

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

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

- 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 3 GHz or higher
- 2 GB RAM minimum, 4 GB recommended
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
Post-Installation

Configuration
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.
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.
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.

[Image of the Personal Email Manager Database configuration window]

Database server: [WS-SHAIGHT-DEMO]
Port: 1433

- Use Windows authentication
- Use SQL Server authentication

User name: [Field for user name]
Password: [Field for password]
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/
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
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:

<table>
<thead>
<tr>
<th>Domain Admin Account:</th>
<th>PEMDemo1</th>
</tr>
</thead>
<tbody>
<tr>
<td>DC DNS Name or IP Address:</td>
<td>DEMO-DC.ILPDEMO.COM</td>
</tr>
<tr>
<td>Base DN:</td>
<td>DC=ILPDEMO, DC=COM</td>
</tr>
</tbody>
</table>

(Optionalally) 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](http://go.microsoft.com/fwlink/?LinkId=100114)
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.
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.
Configuring Web Server Ports

- Click **PEM Web Server** on the main screen to set port numbers for the Personal Email Manager Web server.

  ![PEM Web Server Settings](image)

  **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 PEMAadmin 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 PEMAadmin password, click **PEMAadmin Password** on the main screen to display the PEMAadmin Password dialog box.

![PEMAadmin Password dialog box]

- Enter your password and confirm.
- Click save to commit the changes.
- No restart of the service is required.
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
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.
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 GoDaddy root and intermediate certificates:**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>a) Install root certificate</td>
<td>keytool -import -alias root -keystore pemserver.keystore -trustcacerts -file &quot;valicert_class2_root.crt&quot;</td>
</tr>
<tr>
<td>b) Install first intermediate certificate</td>
<td>keytool -import -alias cross -keystore pemserver.keystore -trustcacerts -file &quot;gd_cross_intermediate.crt&quot;</td>
</tr>
<tr>
<td>c) Install second intermediate certificate</td>
<td>keytool -import -alias intermed -keystore pemserver.keystore -trustcacerts -file &quot;gd_intermediate.crt&quot;</td>
</tr>
</tbody>
</table>

**Example installation of Verisign root and intermediate certificates:**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>a) Install root certificate</td>
<td>keytool -import -alias root -keystore pemserver.keystore -trustcacerts -file &quot;AddTrustExternalCARoot.crt&quot;</td>
</tr>
<tr>
<td>b) Install first intermediate certificate</td>
<td>keytool -import -alias intermediate1 -keystore pemserver.keystore -trustcacerts -file &quot;NetworkSolutions_CA.crt&quot;</td>
</tr>
<tr>
<td>c) Install second intermediate certificate</td>
<td>keytool -import -alias intermediate2 -keystore pemserver.keystore -trustcacerts -file &quot;UTNAddTrustServer_CA.crt&quot;</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Email queue</th>
<th>Inbound/Outbound</th>
<th>Users</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anti-Spam Agent</td>
<td>Inbound</td>
<td>All users</td>
</tr>
</tbody>
</table>

- 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.

Inbound Notification Email Timing

Set when you want users to be notified about blocked inbound email.

- **On these days and at these times**
  - Check the days you want to receive notifications:
    - Mon, Tue, Wed, Thu, Fri
  - Set time:
    - 06:00
    - 14:00
    - 17:30

- **At these intervals**
  - Every 4 hours from midnight.
  - Notifications will be sent at: 00:00, 04:00, 08:00, 12:00, 16:00, 20:00

- **Immediately**

Click **OK** or **Cancel**.
- 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**

- 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: [ ] 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
Upcoming 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