



# EMG Admin Guide

Credential Manager

12.1.0

Copyright ©2021 Echoworx Corporation

Proprietary and confidential - For use by the intended recipient only

Product Release: 12.1.0

Publication Date: Wednesday, July 21, 2021

Copyright © 2003-2021, Echoworx Corporation

4101 Yonge St, Suite 708, Toronto, ON, M2P 1N6, Canada

All rights reserved.

This product or document is distributed under licenses restricting its use, copying, distribution, and decompilation. This document is provided for informational purposes only and Echoworx makes no warranties, either express or implied, in this document. Information in this document, including URL and other internet website references, is subject to change without notice. The entire risk of the use or the results of the use of this document remains with the user.

Unless otherwise noted, the example companies, organizations, products, domain names, email addresses, logos, people, places and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, email address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Echoworx Corporation.

Echoworx may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Echoworx, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

# Contents

---

<b>About the EMG Console</b>	<b>5</b>
First-Time Log In	5
Access the EMG Console	7
<b>Profile Management</b>	<b>9</b>
Credentials Management	10
Manage Keys and Certificates	11
Search a PDF User	19
Set a Recipient Preference	20
Expire a PDF Password	21
Reset a PDF User	21
Delete a PDF User	22
Migrate PDF Password Histories	22
Unlock a PDF User	22
Disable a PDF User's Time-Based One-Time Password (TOTP)	23
Search a Web Portal User	23
Reset a Web Portal User	24
Delete a Web Portal User	24
Unlock a Web Portal User	25
Disable a Web Portal User's Time-Based One-Time Password (TOTP)	25
Migrate off PGP Email Encryption to Echoworx Email Encryption	26
Frequently Asked Questions (FAQs)	27
<b>Reports</b>	<b>29</b>
Message Report	29
Message Status Reference	31
Audit Trail Report	36
Policy Report	37
Message Status Reference	39

---

Summary Reports ..... 39

# About the EMG Console

The EMG Console provides an interface for Echoworx Email Encryption customers to manage the credentials of users who send and receive encrypted email. Optional credentials for employees who send secure email include S/MIME private keys or PGP private keys. Different credentials for external recipients include x509 certificates, PGP public keys, Secure PDF passwords, and Web Portal accounts.

The Administrator will use this console to perform credential management such as importing keys, or resetting a PDF or web portal account when the user has forgotten their password. In addition to credential management, reports are available for troubleshooting purposes such as finding a particular secure email and confirming the type of encryption used.

Your logo and other Echoworx Email Encryption settings are not edited through this console. Changes to your Echoworx Email Encryption service can be arranged by contacting Support.

To continue with Credential Management, you must log in to the EMG Console.

## First-Time Log In

When a new user with any Admin or Reseller role is setup in the EMG Console, an automated email is sent to the user's mailbox. This email contains the username, temporary password and login page link to access the Admin Console.

## Encrypted Mail Gateway Console - Getting Started Information

This email contains the information you will need to log in to the Encrypted Message Gateway Console. The temporary password will expire after 1 days.

### Login Information

You have been assigned the following role: ADMIN

User Name:	<a href="#">bob.smith@demo.com</a>
Password:	G5Xv3R2X
Click the link below to go to the login page:	
<a href="#">https://demo.com/login.htm</a>	

**Note:** The first-time login credentials are valid for a limited period of time as set by the system administrator. In the above example, the credentials are valid for a day. The value can be changed on the System Settings page.

Click the link at the end of the email to open the EMG Console login screen. Enter the username and temporary password provided in the email and click **Login** to log in for the first time.

On the **Change Password** screen, set a new permanent password to replace the temporary one provided in the email. Click **Change** to save the new password.

## Change Password

Old Password:

\*\*\*\*\*

New Password:

\*\*\*\*\*

Confirm New Password:

\*\*\*\*\*

Change

Cancel

**Note:** The password must contain a minimum of 8 and a maximum of 64 characters, including at least one upper case, one lower case, one numerical and one special character.

You can now use the username and new password to access the Admin Console.

## Access the EMG Console

To access the EMG Console:

1. Navigate to the admin console URL.
2. Enter your username and password.
3. Click **Login**. The **My Profiles** page appears. If you are a Reseller Administrator, the **My Profiles** page appears.

PROFILE : [username] | [Change Profile](#)

### My Profiles

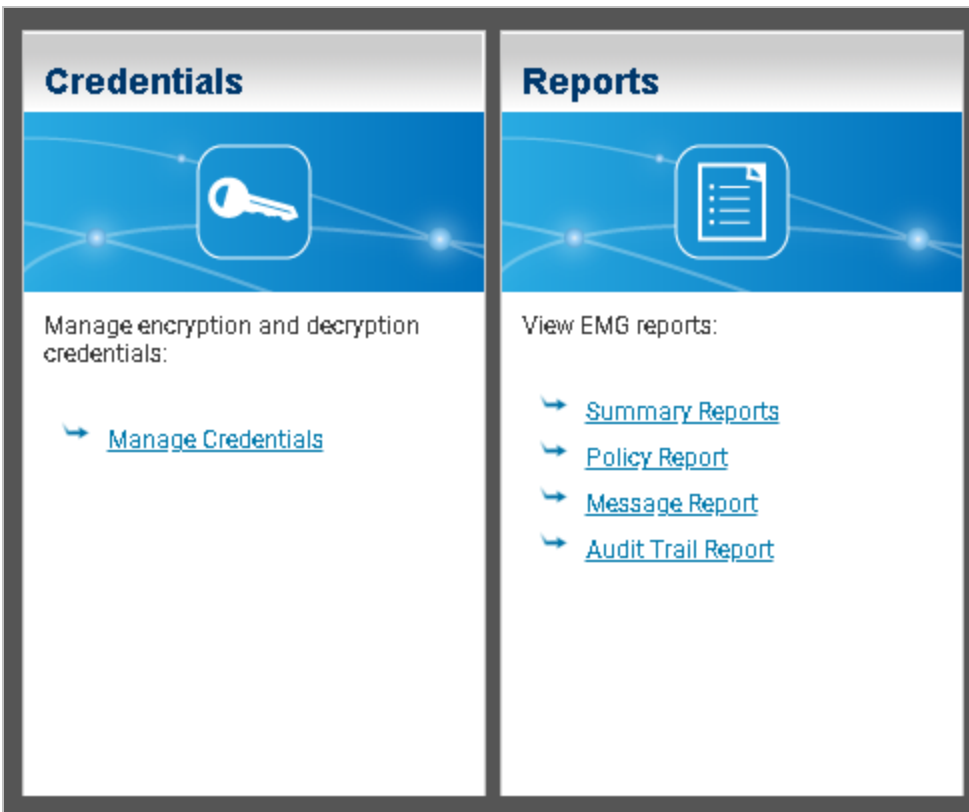
[Default Profile Management](#)  
The Default Profile Management allows you to add/update/delete default policies and view reports for all profiles.

**Custom Profile Management**  
The Custom Profile Management allows you to add/update/delete policies and view reports for all profiles.

Select a profile:

Or, specify a domain:

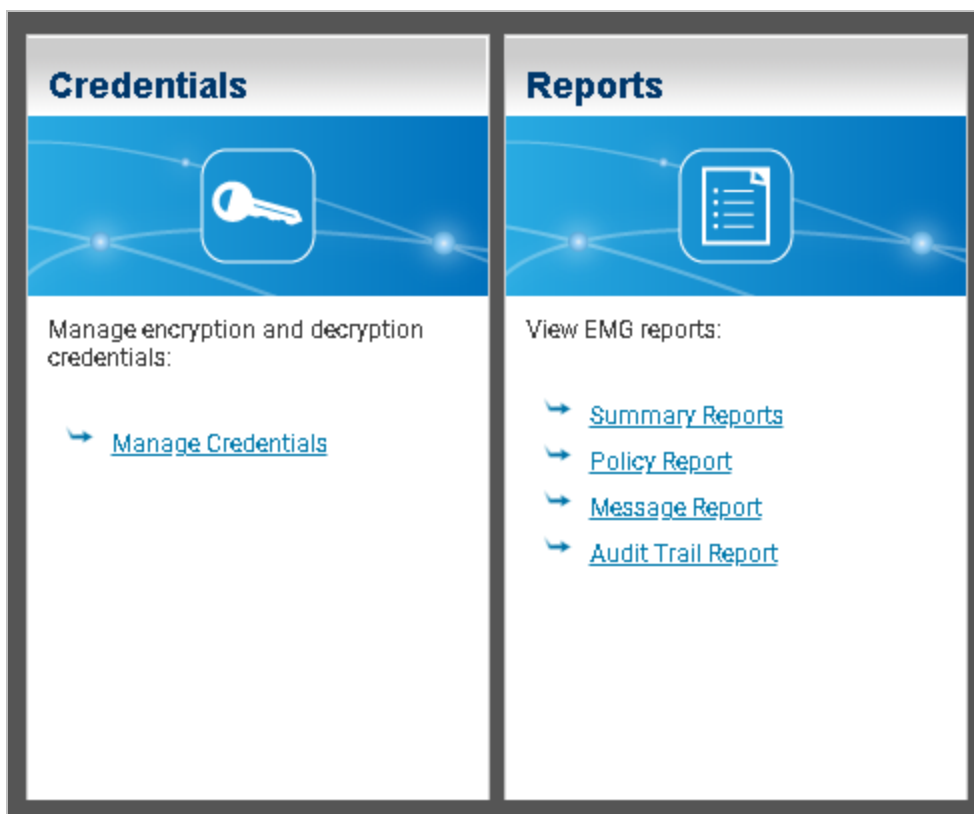
Or, if you are an Enterprise Administrator, the profile settings page appears.





# Profile Management

Each EMG Enterprise profile (usually referred to as simply "profile") comprises a set of domains, and a set of policies, credentials, and miscellaneous options that are applied to messages from those domains. The profile management screen links to all of these settings, and a set of [reports](#).



# Credentials Management

The **Credentials Management** page is used to add third-party credentials for decryption and certificates for encryption. When messages are being sent through the Encrypted Mail Gateway for encryption/decryption, it will first check for credentials that have been uploaded to the **Credentials Management** page.

The **Credentials Management** page is divided into tabs by standard: PGP, S/MIME, PDF Passwords, and Web Portal. The PGP tab, for example, contains tools for finding and managing PGP keys in the EMG database.

**Note:** The action of performing credential searches for PGP, S/MIME, PDF Passwords, and Web Portal is audited in Audit Trail Report.

To access the **Credentials Management** page:

1. Log in to the EMG Console.
2. To access the **Credentials Management** page, perform either of the following steps:
  - a. Click **Home** from the menu.
  - b. Under the **Credentials** tile, click **Manage Credentials**. The **Credentials Management** page appears.

OR

- a. Click **Credentials** from the menu. The **Credentials Management** page appears.

PROFILE : [username] | [Change Profile](#)

## Credentials Management

PGP	S/MIME	PDF Passwords	Web Portal
<b>Import &amp; Generate PGP Keys</b>			
Key Pairs ⓘ <input type="button" value="Import"/> <input type="button" value="Invite"/> <input type="button" value="Bulk Invite"/> <input type="button" value="Generate"/> <input type="button" value="Bulk Generate"/>			
Public Keys ⓘ <input type="button" value="Import"/> <input type="button" value="Invite"/> <input type="button" value="Bulk Invite"/>			
<b>Global PGP Directory</b>			
Profile LDAP Entries <input type="button" value="Sync"/> <input type="button" value="Remove All"/>			
<b>Search PGP Keys</b>			
Email: <input type="text"/> ⓘ <input type="checkbox"/> Deactivated <input type="checkbox"/> Expired <input type="checkbox"/> Domain Keys <input type="button" value="Search"/> ⓘ <input type="button" value="Deactivate All"/>			
Type	Email / Domain	ID	Expiry Date
Generation Type		Actions	

## Manage Keys and Certificates

The **Credential Management** page allows users to perform the following operations:

- [Import a Private Key](#)
- [Import a Public Key or Certificate](#)
- [Bulk-Import PGP Private Keys](#)
- [Generate a Private PGP Key](#)
- [Generate Bulk Private PGP Keys](#)
- [Send Bulk Invites for Uploading Private PGP Keys](#)
- [Send Bulk Invites for Uploading Public Keys](#)
- [Deactivate a Private PGP or S/MIME Key](#)
- [Download a Key](#)
- [Delete a Key](#)
- [Working with PDF Passwords](#)
- [Working with Web Portal Accounts](#)

### Import a Private Key

Private keys can be uploaded and used to automatically decrypt incoming email messages, and to sign outgoing messages based on your enterprise signing policy. This is useful for enterprises with existing PGP or S/MIME infrastructure that wish to transit seamlessly to the Echoworx Email Encryption Portal.

**Note:** An expired key may be used for decryption, but not for signing.

To add a private key:

1. On the **Credentials Management** page, select **PGP** or **S/MIME** tab.
2. Under **PGP** tab, click **Import** besides **Key Pairs**. The **Import** dialog opens.
  - a. **Credential File** - Click **Choose File** to browse and select the appropriate private key (\*.P12, \*.PFX or \*.ASC) file.
  - b. **Email** - Enter the email address associated with the private key. Alternatively, you can choose to import the email address from the private key directly by selecting the **Import email addresses from key** checkbox.
  - c. **Password** - Enter the password for the private key.
  - d. Click **Ok**. The private key appears in the search results list.

3. Under the **S/MIME** tab, click **Import** besides **Private Keys**. The **Import** dialog opens.
  - a. **Credential File** - Click **Choose File** to browse and select the appropriate private key (\*.P12, \*.PFX or \*.ASC) file.
  - b. **Email** - Enter the email address associated with the private key.
  - c. **Password** - Enter the password for the private key.
  - d. Click **Okay**. The private key appears in the search results list.

## Import a Public Key or Certificate

Certificates can be uploaded and mapped to a specific domain or email address:

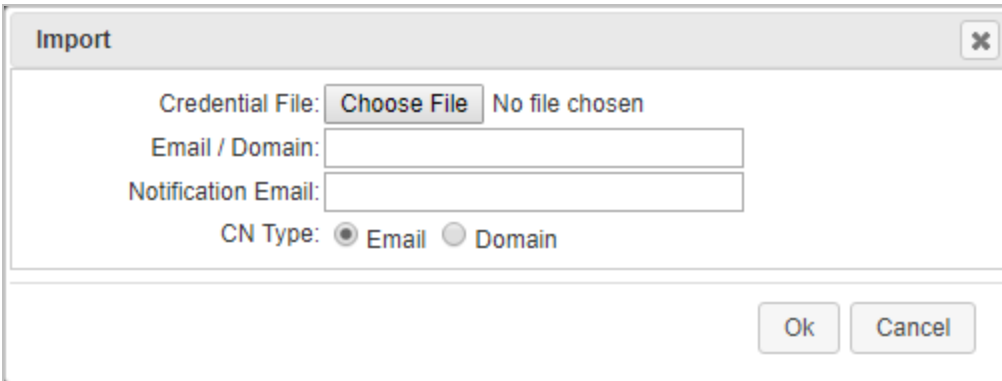
- **By Domain:** If you upload a certificate and then map it to a domain (for example, bankabc.com), all email messages that match that domain (that is, bankabc.com) are encrypted using the uploaded certificate.
- **By Email Address:** If you upload a certificate and then map it to an email address (for example, jim@bankabc.com), all email messages that match that email address (that is, jim@bankabc.com) are encrypted using the uploaded certificate.

**Note:** When both a domain and an individual user certificate are available for encryption, the user certificate takes precedence.

When a public key is about to expire, EMG sends a notification to the specified notification email address to request a new/updated key. EMG will not use an expired public key to encrypt a message.

To add a certificate:

1. On the **Credentials Management** page, select **PGP** or **S/MIME** tab.
2. Under **PGP** tab, click **Import** besides **Public Keys**; or under **S/MIME** tab, click **Import** besides **Certificates**. The **Import** dialog opens.



- a. **Credential File** - Click **Choose File** to browse and select the appropriate certificate (a PEM-formatted certificate; for example, \*.CER, \*.PEM or \*.ASC) file.
- b. **Email / Domain** - Enter the appropriate email address or domain.
- c. **Notification Email** - Enter the appropriate notification email address.
- d. **CN Type** - If you entered an email address in step 2 (b), select **Email**, else select **Domain** if you entered a domain.
- e. Click **Ok**. The public key or certificate appears in the search results list.

**Note:** When adding a PGP public key, only the first public key block in the PGP (.asc) file is uploaded and stored.

## Bulk-Import PGP Private Keys

PGP Universal Server can export multiple PGP keys as a single .asc file. It is recommended that you import no more than 500 keys at once. To bulk import these keys:

1. On the **Credentials Management** page, select **PGP** tab.
2. Click **Import** besides **Key Pairs**. The **Import** dialog opens.

- a. **Credential File** - Click **Choose File** to browse and upload your .asc file.
- b. Check the **Import email addresses from key** box.
- c. **Password** - Enter the .asc file password.
- d. Click **Ok**. Each public/private key stored in the .asc file appears in search results list.

**Note:** The notification email address for bulk-imported PGP keys will be reused from.

## Generate a Private PGP Key

Private PGP keys can be created by the user through a simple web interface. If you do not need to export the private key for use outside of EMG, it is recommended that you use the Auto PGP Key Generation feature instead.

**Note:** Auto-generated keys cannot be exported.

To generate a private key:

1. On the **Credentials Management** page, click **PGP** tab.
2. Click **Generate** besides **Key Pairs**. The **Generate** dialog opens.

- a. **Personal Name** - Enter the user's personal name (real name).
- b. **Email** - Enter the user's email address.

- c. **Password** - Enter a password.
- d. Click **Ok**. The key is generated and appears on the search results list.

## Generate Bulk Private PGP Keys

An EMG administrator can send bulk private key notification messages to end users by creating and uploading a CSV file with the necessary information.

**Note:** Bulk generation is not available for S/MIME keys.

To create the required CSV file:

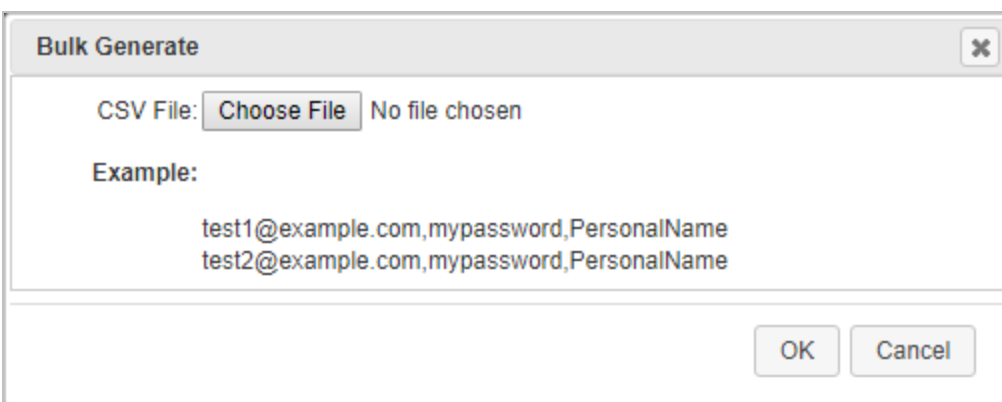
1. Open a spreadsheet editor.
2. Create a file using the following format (one entry per line):

```
[user's email address],[user's password],[private key type; PGP],[Personal  
name - PGP keys only]  
For example:  
test1@abc.com,123456,PGP,PersonalName  
test2@abc.com,678910,PGP,Eugene Belford
```

3. Save the document as a CSV file.

To generate bulk private keys:

1. On the **Credentials Management** page, select **PGP** tab.
2. Click **Bulk Generate**. The **Bulk Generate** dialog opens.



- a. **CSV File** - Click **Choose File** to browse and select the **.CSV** file you created above.
- b. Click **OK**. The PGP keys are generated and appear on the search results list.

## Send Bulk Invites for Uploading Private Keys

EMG administrators can send bulk notifications to end users wanting to use their private keys by creating and uploading a plain-text file containing a list of email addresses. This option should be used for internal users only; external users should not be asked to upload their private key.

To create a plain-text file for bulk notifications:

1. Open a document editing application.
2. Create a file using the following format:

```
[user's email address]
```

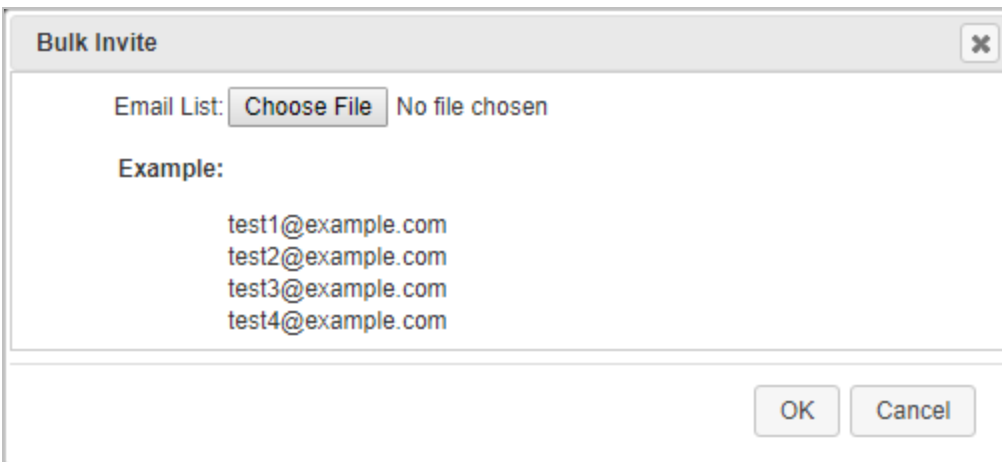
For example:

```
test1@abc.com  
test2@abc.com
```

3. Save the document as a plain text file.

To send bulk notifications:

1. On the **Credentials Management** page, select **PGP** or **S/MIME** tab.
2. Under **PGP** tab, click **Bulk Invite** besides **Key Pairs**; or under **S/MIME** tab, click **Bulk Invite** besides **Private Keys**. The **Bulk Invite** dialog opens.



- a. **Email List** - Click **Choose File** to browse and select the plain text file you created above.



- b. Click **OK**. A notification message is sent to each end-user with a link to the EMG web page where they can upload their private keys. After each user uploads their private key, it will appear in the Private Keys search results.

## Send Bulk Invites for Uploading Public Keys

EMG administrators can send bulk notifications to end users wanting to use their public keys by creating and uploading a plain-text file of the users' email addresses. This option should be used for external users (recipients) only.

To create a plain-text file for bulk notifications:

1. Open a document editing application.
2. Create a file using the following format:

```
[user's email address]
```

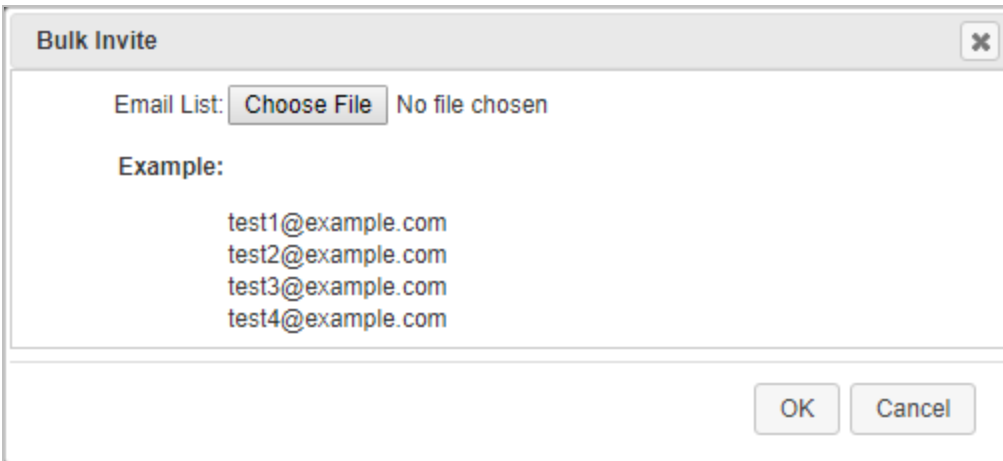
For example:

```
test1@abc.com  
test2@abc.com
```

3. Save the document as a plain text file.

To send bulk notifications:

1. On the **Credentials Management** page, select **PGP** or **S/MIME** tab.
2. Under **PGP** tab, click **Bulk Invite** besides **Public Keys**; or under **S/MIME** tab, click **Bulk Invite** besides **Certificate**. The **Bulk Invite** dialog opens.




- a. **Email List** - Click **Choose File** to browse and select the plain text file you created above.
- b. Click **OK**. A notification message will be sent to each end user with a link to an EMG web page where they can upload their public keys. After each user uploads their public key, it will appear in the **Public Certificates** search results.

## Deactivate a Private PGP or S/MIME Key

To stop using a private key for signing, but keep the private key in the system for decryption, you can deactivate the private key.

If the key type is PGP and auto PGP key generation is enabled, a new key pair is created. If auto generation is off, the public key is retained, but is not attached to outgoing messages.

1. On the **Credentials Management** page, click **PGP** or **S/MIME** tab.
2. Click **Search**. A list of keys appears.
3. Click  icon next to the private key or key pair that you want to deactivate. A confirmation prompt appears.
4. Click **Yes** to permanently deactivate the private key.



**Warning:** Deactivated keys cannot be re-activated.

## Download a Key

You can download any imported manually generated key. You cannot download auto-generated private keys.


To download an existing public or private key:

1. On the **Credentials Management** page, click **PGP** or **S/MIME** tab.
2. Click **Search**. A list of private keys appears.

3. To download a public key, click  icon next to the key you want to download.
4. To download a private key, click  icon next to the key you want to download. A warning prompt appears.
  - a. To download the private key, click **Ok**.

## Delete a Key

To remove a private key:

1. On the **Credentials Management** page, click **PGP** or **S/MIME** tab.
2. Click **Search**. A list of private keys appears.
3. Click  icon next to the key you want to remove. A confirmation prompt appears.
4. Click **Yes** to permanently delete the private key.

**Note:** Auto-generated private keys cannot be removed; they must instead be deactivated. This ensures that the private key remains in the database for decryption.

## Manage PDF Passwords

Search a PDF User

To view a list of PDF users:

1. On the **Credentials Management** page, click **PDF Passwords** tab.
2. Enter a string in the **Email** field.
3. Click **Search**. A list of users for the specified search string is displayed.

### Credentials Management

PGP
S/MIME
PDF Passwords
Web Portal

Search PDF Passwords

Email:  ☐ Search All Profiles ⓘ

Search

†This report will display a maximum of 50 users.

PDF/Zip Users

Email	Enterprise	Locale	Last Used	Password Status ⓘ	Preference	Actions
sasqa5@demobank.com	demonstrationbank	<a href="#">en_US</a>		<a href="#">Expired</a>	<a href="#">WEB</a>	Migrate Keys Delete Reset
sasqa6@demobank.com	demonstrationbank	<a href="#">unspecified</a>		No History	<a href="#">PDF</a>	Delete
sasqa7@demobank.com	demonstrationbank	<a href="#">en_US</a>	6/26/19 3:52 PM	<a href="#">Expired</a>	<a href="#">WEB</a>	Migrate Keys Delete Reset
sasqa8@demobank.com	demonstrationbank	<a href="#">en_US</a>	3/15/19 10:17 AM	<a href="#">Active</a>	<a href="#">PDF</a>	Migrate Keys Delete Reset Expire Key

#### Set a Recipient Preference

You can view each user's preferred delivery method (WEB or PDF) in the user details. You can manually update the user preference, as well, if required.

To update the user preference,

1. On the **Credentials Management** page, click **PDF Passwords** tab.
2. Enter a string in the **Email** field.
3. Click **Search**. A list of users for the specified search string is displayed.
4. Under the **Preference** column, click the preference to change it for a particular user. A dialog appears.
  - a. Select the required preference from the drop-down list.
  - b. Click **Ok**.

**Credentials Management**

PGP | S/MIME | **PDF Passwords** | Web Portal

Search PDF Passwords

Email:  ☒ Search All Profiles ⓘ

†This report will display a maximum of 100 results.

Email	Enterprise	Preference	Actions
sasqa5@demobank.com	demonstrationbank	<b>PDF</b>	<input type="button" value="Migrate Keys"/> <input type="button" value="Delete"/> <input type="button" value="Reset"/>
sasqa6@demobank.com	demonstrationbank	<a href="#">WEB</a>	<input type="button" value="Delete"/>
sasqa7@demobank.com	demonstrationbank	<a href="#">WEB</a>	<input type="button" value="Migrate Keys"/> <input type="button" value="Delete"/> <input type="button" value="Reset"/>
sasqa8@demobank.com	demonstrationbank	<a href="#">PDF</a>	<input type="button" value="Migrate Keys"/> <input type="button" value="Delete"/> <input type="button" value="Reset"/> <input type="button" value="Expire Key"/>

#### Expire a PDF Password

You can manually expire a PDF user's current PDF password. You may choose to do this to force the user to choose a new PDF password for the their next PDF message.

To expire a user's PDF password:

1. On the **Credentials Management** page, click **PDF Passwords** tab.
2. Enter a string in the **Email** field.
3. Click **Search**. A list of users for the specified search string is displayed.
4. To expire a PDF password for a specific PDF user, click **Expire Key**. A confirmation prompt appears.
5. Click **Yes**. The PDF password, for the specified user, expires.

#### Reset a PDF User

Resetting a user might be necessary if that user has forgotten their recovery information. Resetting a PDF user will delete their account recovery information so that they can re-enter that information. The deleted recovery information can include challenge questions and alternate email addresses, if they exist for the environment that the user is in. Administrators should take care to verify the authenticity of any recovery information reset request.

To reset a PDF user:

1. On the **Credentials Management** page, click **PDF Passwords** tab.
2. Enter a string in the **Email** field.
3. Click **Search**. A list of users for the specified search string is displayed.
4. To reset a PDF user's recovery information, click **Reset**. A confirmation prompt appears.
5. Click **Ok**. The user will receive a recovery notification from Echoworx Email Encryption Portal.

### Delete a PDF User

You can delete a PDF user's password history from the EMG database. This will permanently remove the email address and all associated PDF Passwords.

**Warning:** If a user requests to be deleted, they should be advised to save a copy of their PDF Password history beforehand. When you delete a PDF user, that user's password history is gone forever; it cannot be recovered.

To delete a PDF user:

1. On the **Credentials Management** page, click **PDF Passwords** tab.
2. Enter a string in the **Email** field.
3. Click **Search**. A list of users for the specified search string is displayed.
4. To delete a PDF user, click **Delete**. A confirmation prompt appears.
5. Optionally, enter a reason of deleting a user.
6. Click **Ok**. All the PDF passwords of the specified user are deleted.

### Migrate PDF Password Histories

To move a specific user's PDF Password history to a new email address:

1. On the **Credentials Management** page, click **PDF Passwords** tab.
2. Enter a string in the **Email** field.
3. Click **Search**. A list of users for the specified search string is displayed.
4. To migrate the keys, **Migrate Keys**. The **Migrate Keys** dialog appears.
  - a. **New Email** - Enter the user's new email address to which the PDF password history is to be moved.
  - b. Select the enterprise from the drop-down list.
  - c. Click **Ok**. The password history of the specified user is assigned to the new email address.

### Unlock a PDF User

You can unlock a PDF user account after a user locks their account. A user may have their account locked after failing to log in because they entered an incorrect password more times than they are permitted to. Their account will be unlocked automatically after the lock time expires. The values of maximum failed attempts allowed and lock time are configurable through EMX policies. The administrator can unlock the user account when the user is looking for immediate assistance.

To unlock a user:

1. On the **Credentials Management** page, click **Web Portal** tab.
2. Enter a string in the **Email** field.
3. Select the **User Type** as either **User Accounts** or **Question/Answer Messages** from the drop-down list.
4. Click **Search**. A list of users for the specified search string is displayed.

5. To unlock a user, click **Unlock**. A confirmation prompt appears.
6. Click **Yes**. The user is unlocked.

#### Disable a PDF User's Time-Based One-Time Password (TOTP)

If necessary, you can disable a PDF user account's 2-step verification upon their request. If you disable a user's 2-step verification, the verification information stored with that account will be deleted. 2-step verification will not be required when the user logs in and, if the 2-step verification is set as mandatory for the environment, the user will be required to set it up again when they login next.

To disable TOTP:

1. On the **Credentials Management** page, click **Web Portal** tab.
2. Enter a string in the **Email** field.
3. Select the **User Type** as either **User Accounts** or **Question/Answer Messages** from the drop-down list.
4. Click **Search**. A list of users for the specified search string is displayed.
5. To disable TOTP, click **Disable TOTP**. A confirmation prompt appears.
6. In the confirmation message, enter a reason why TOTP is being disabled for this user.
7. Click **OK**. TOTP is disabled for the user.

## Manage Web Portal Accounts

#### Search a Web Portal User

To view a list of web portal users:

1. On the **Credentials Management** page, click the **Web Portal** tab.
2. Enter a string in the **Email** field.
3. Select the **User Type** as either **User Accounts** or **Question/Answer Messages** from the drop-down list.
4. Click **Search**. A list of users for the specified search string is displayed.

### Credentials Management

PGP

S/MIME

PDF Passwords

Web Portal

Search Web Portal Users

Email:

User Type: User Accounts

Search

†This report will display a maximum of 50 web portal users.

Web Portal Users

Email	Enterprise	Name	Last Login	Create Date	Status	Recovery Options	TOTP	Actions
juser1@demobank.com	demonstrationbank	J User	1/30/20 6:53 PM	9/3/19 5:59 PM	Registered User	Challenge Questions	ON	Delete Reset Disable TOTP
jlive3@demobank.com	demonstrationbank			10/3/19 6:47 PM	Pending User		OFF	Delete Reset
juser3@demobank.com	demonstrationbank			7/9/19 7:13 PM	Pending Internal User		OFF	Delete Reset
juser4@demobank.com	demonstrationbank	Julie User	1/30/20 8:50 PM	7/11/19 8:32 PM	Registered User	Challenge Questions	ON	Delete Reset Disable TOTP
jmluser1@demobank.com	demonstrationbank	Jon M	2/3/20 9:38 PM	9/3/19 2:57 PM	Registered User	Challenge Questions	ON	Delete Reset Unlock

#### Reset a Web Portal User

Resetting a user might be necessary if that user has lost their recovery information. Resetting a Web Portal user will delete their account recovery information so that they can reenter that information. The deleted recovery information can include challenge questions and alternate email addresses, if they exist for the environment that the user is in. Administrators should take care to verify the authenticity of any recovery information reset request.

To reset a web portal user:

1. On the **Credentials Management** page, click **Web Portal** tab.
2. Enter a string in the **Email** field.
3. Select the **User Type** as **User Accounts** from the drop-down list.
4. Click **Search**. A list of users for the specified search string is displayed.
5. To reset a web portal user's recovery information, click **Reset**. A confirmation prompt appears.
6. Click **Yes**. The user will receive a recovery notification from Echoworx Email Encryption Portal.

#### Delete a Web Portal User

You can delete a web portal user's account including all the messages from the EMG database.

To delete a web portal user:



1. On the **Credentials Management** page, click **Web Portal** tab.
2. Enter a string in the **Email** field.
3. Select the **User Type** as either **User Accounts** or **Question/Answer Messages** from the drop-down list.
4. Click **Search**. A list of users for the specified search string is displayed.
5. To delete a web portal user, click **Delete**. A confirmation prompt appears.
6. Optionally, enter a reason of deleting a user.
7. Click **Ok**. The web portal user is deleted.

#### Unlock a Web Portal User

You can unlock a web portal user account after a user locks their account. A user may have their account locked after failing to log in because they entered an incorrect password more times than they are permitted to. Their account will be unlocked automatically after the lock time expires. The values of maximum failed attempts allowed and lock time are configurable through EMX policies. The administrator can unlock the user account when the user is looking for immediate assistance.

To unlock a user:

1. On the **Credentials Management** page, click **Web Portal** tab.
2. Enter a string in the **Email** field.
3. Select the **User Type** as either **User Accounts** or **Question/Answer Messages** from the drop-down list.
4. Click **Search**. A list of users for the specified search string is displayed.
5. To unlock a user, click **Unlock**. A confirmation prompt appears.
6. Click **Yes**. The user is unlocked.

#### Disable a Web Portal User's Time-Based One-Time Password (TOTP)

If necessary, you can disable a web portal user account's 2-step verification upon their request. If you disable a user's 2-step verification, the verification information stored with that account will be deleted. 2-step verification will not be required when the user logs in and, if the 2-step verification is set as mandatory for the environment, the user will be required to set it up again when they login next.

To disable TOTP:

1. On the **Credentials Management** page, click **Web Portal** tab.
2. Enter a string in the **Email** field.
3. Select the **User Type** as either **User Accounts** or **Question/Answer Messages** from the drop-down list.
4. Click **Search**. A list of users for the specified search string is displayed.
5. To disable TOTP, click **Disable TOTP**. A confirmation prompt appears.
6. In the confirmation message, enter a reason why TOTP is being disabled for this user.
7. Click **OK**. TOTP is disabled for the user.

## Migrate off PGP Email Encryption to Echoworx Email Encryption

Echoworx Email Encryption allows a customer with a PGP Universal Server (for the purposes of email encryption) to migrate away from this infrastructure and replace it entirely with Echoworx Email Encryption functionality.

The existing PGP public/private keys for all enterprise employees can be imported into Echoworx Email Encryption for a smooth transition that will not impact external partners and recipients. For email encryption to recipients that do not have PGP keys, the Echoworx Email Encryption secure web portal replaces the PGP Universal secure portal.

The steps to migrate are as follows:

1. Update email routing to route emails to Echoworx Email Encryption. Depending on your deployment, this may involve an Echoworx Partners' Mail Filtering services, or a DLP appliance, or the Microsoft Exchange Server. The configuration details involved for this step are out of scope of this document. All Echoworx Email Encryption deployment models are supported.
2. Define Encryption Policies (i.e. rules to encrypt) in the appropriate policy engine. These encryption policies should replicate any encryption rules that exist in the PGP Universal Server.
3. Export the Enterprise Signing private key out of the PGP Universal Server.
4. Import the Enterprise Signing private key (from step 3) into the EMGAdmin Console. Please refer to "Credentials Management" on page 10 for instructions.
5. Export all user keys from the PGP Universal Server. This can be achieved with a bulk export operation that places multiple user keys into a single file. It is recommended to restrict a single file to 500 users or less (to keep these key files at a reasonable size).
6. Import all user keys from step 5 into EMG. Please refer to "Manage Keys and Certificates" on page 11 for instructions.
7. In EMG, turn on automatic PGP private-key generation. Please refer to "Manage Keys and Certificates" on page 11 of this document for instructions. In addition, enable signing of these keys with the Enterprise key.

**Note:** The original keys from the PGP Universal server (imported during step 6) are used until they reach their natural expiry as defined in the certificate. At that point new keys are created automatically by EMG.

8. Add any public Third Party PGP directories to EMG.
9. (Optional) Deploy the Echoworx Email Encryption Outlook Add-In to all users in the enterprise, giving them a simple Encrypt button to initiate encryption.

## Frequently Asked Questions (FAQs)

### Can an end user have multiple keys in the system?

There can only be one public certificate in the system for a particular email address. Uploading a new certificate will delete any previous certificate.

There can be several private keys in the system for a particular email address. Only one private key is active at a given time. The last private key to be uploaded (or generated) is the active private key. The active private key is used to digitally sign outbound messages, and decrypt inbound messages. The other archived private keys are used to decrypt inbound messages.

### Are PGP or S/MIME private keys ever deleted?

Private keys are never deleted, unless this action is initiated (using the Admin Console) by an authorized Administrator. It is best-practise to keep expired private keys archived in the system in the event a message arrives that has been encrypted with that corresponding public key.

### What key size and algorithm is used to generate PGP keys?

PGP private keys generated by Echoworx Email Encryption are 2048 bit RSA key pairs.

### What algorithm is used to encrypt PGP messages?

PGP messages are encrypted with a 3DES symmetric key (168 bits). Then this symmetric key is encrypted using the PGP public key pair (see Q3).

### What happens when a certificate is approaching expiry?

Seven days before a certificate expires, Echoworx Email Encryption will check if there is a corresponding private key, and if automatic key generation (PGP only) is enabled. In this case, a new private key and certificate are created automatically.

Five days before a certificate expires, Echoworx Email Encryption will notify the owner of the certificate by email that they should upload a new certificate (and private key if relevant).

## **What happens when a public certificate is expired?**

Echoworx Email Encryption will not use expired public certificates to encrypt messages. Expired certificates are ignored by Echoworx Email Encryption. Future messages sent to this recipient are sent to the secure web portal rather than encrypted using the end-user's certificate.

## **What happens if an inbound encrypted message cannot be decrypted?**

If Echoworx Email Encryption does not have a private key necessary to decrypt a particular email, it will still be delivered to the Enterprise end-user. If the end-user cannot decrypt the message themselves, they will need to contact the sender of the message, exchange updated certificates, and ask that the message be resent.

# Reports

EMG can generate four different reports to provide you with relevant statistics, troubleshooting, and auditing information.

## Message Report

Displays delivery-related information about each message, such as the mail action, delivery status, or any related errors or exceptions.

## Policy Report

Displays policy-related information about each message, such as which policies were triggered, and which content triggered those policies.

## Summary Reports

A collection of statistical reports.

## Audit Trail Report

This report tracks all admin actions.

## Message Report

A common issue with message delivery systems is that errors and exceptions may occur while messages are being processed. In order to manage these issues, the EMG Message Report displays information about each message, such as whether it has been successfully delivered or if there are any related errors/exceptions.

**Note:** The action of fetching a message report is audited in EMG.

## View the Message Report

To view the Message Report page:

1. Log in to the EMG Console.
2. To access **Message Report** page perform either of the following steps:
  - a. Click **Home** from the menu.
  - b. Under the **Reports** tile, click **Message Report**. The **Message Report** page appears.

OR

- Click **Reports > Message Report**. Hover mouse over **Reports** menu. A menu opens.
- Click **Message Report** from the menu. The **Message Report** page appears.

## Search for Messages

The Message Report allows you to locate specific messages by filling out any of the following criteria on the search page.

To locate a message, enter the desired search criteria, and click **Search**.

### Criteria (search by Message Info):

<b>Profile</b>	The profile that the sender's domain is mapped to.
<b>From / To</b>	The message report returns messages newer than the date specified in the <b>From</b> field, and older than the date specified in the <b>To</b> field.
<b>Status</b>	Status of the message (see <a href="#">Message Status Reference</a> below)
<b>Action</b>	Message status details. For example, which delivery channel was used to deliver the message.
<b>Sender</b>	The sender's email address
<b>Recipient</b>	The recipient's email address
<b>Recipient Domain</b>	The recipient's email domain

### Criteria (Search by Message ID)

<b>Echoworx Msg ID</b>	<p>The unique identifier assigned to the message by EMG. Use this value to locate a single message. The EMG assigned message ID can be found in the <b>x-echoworx-msg-id</b> header of the message.</p> <p>For example, <b>x-echoworx-msg-id: 28a50bf1-f92a-46bf-b702-ca84d9e50ca6</b></p>
------------------------	--

## Criteria (Search by Original Message ID)

<b>Original Message ID</b>	<p>The unique MIME header that is assigned to the message. Use this value to locate a single message. The MIME header can be found in the <b>Message-ID</b> header of the message.</p> <p>For example, <b>Message-ID</b>: &lt;CAFFgv31JJ1Eqg79wY6PDpTvPgG1nkoT0X+c-QBT6oxKD1hFi4g@mail.echoworx.com&gt;</p>
----------------------------	---

## Message Status Reference

The Message Report screen displays the following statuses for each message:

Status	Description
<b>UNPROCESSED</b>	This is the default status of a message (i.e., no policies/actions have been applied to it). All messages have an 'Unprocessed' status when they first arrive in EMG.
<b>FAILED</b>	The message cannot be sent. For this status, a <b>Send</b> button appears next to the message, by which you can re-send the message.
<b>ERROR</b>	The message has caused an unexpected system-level error. For this status, a <b>Send</b> button appears next to the message, by which you can re-send the message.
<b>MALFORMED_ERROR</b>	The headers of the message that do not conform to RFC standards are considered to be malformed. The message is neither processed, nor sent.
<b>TLS_FAILURE</b>	EMG attempts to connect to the recipient's mail server to verify if TLS is a suitable delivery method for that recipient. At least one additional attempt is scheduled to occur for this message before TLS is no longer considered as a delivery method.
<b>LOGGED</b>	The message has triggered the 'Log and Continue' action.
<b>PROFILE_REDIRECTED</b>	The message has been redirected to another profile on EMG for processing.
<b>SENT</b>	The message was sent successfully.
<b>DISCARDED</b>	A policy triggered a 'discard' action on the message, or if an incoming encrypted message cannot be decrypted by EMG.
<b>HPS_ERROR</b>	HPS is offline or has returned an error. EMG will try to resend the message indefinitely until it sends successfully.
<b>IGNORED</b>	The message cannot be processed by EMG and is not sent.
<b>RST</b>	The message with ERROR status is sent back to EMG for reprocessing. When this message does not make it back to EMG because of some failure, the message is marked with the <b>RST</b> status.
<b>READY_NOTIFY</b>	The status of a new message before it gets processed.

## Action

The **Action** drop-down list displays a list of email actions against which the search results can be filtered. The following table lists all available actions and their description:

Action	Description
<b>BOUNCE</b>	Non-Delivery Receipt (NDR) sent
<b>BOUNCE_BACK_ERROR</b>	NDR sent – message rejected due to an error during processing
<b>BOUNCE_BACK_INVALID_RECIPIENTS</b>	NDR sent – message rejected due to incorrect or non-existent recipient email address
<b>BOUNCE_BACK_NONSUBSCRIBER</b>	NDR sent – message rejected as no delivery method is found
<b>BOUNCE_BACK_OVERSIZE</b>	NDR sent – message rejected due to mail message exceeding the size limit specified in the System Settings - <b>Pre-encryption Message Size Limit</b>
<b>BOUNCE_BACK_TLS_FAILURE</b>	NDR sent – message undelivered due to TLS failure. This occurs if TLS is the only delivery method that is enabled or if a decrypted message could not be relayed via TLS.
<b>DECRYPTED_PGP_DELIVER_TRUSTED_TLS</b>	Inbound PGP message decrypted. Message delivered over a secure TLS channel.  <b>Note:</b> This action is listed when Decryption SMTP server is not used; i.e., <b>MX Lookup</b> checkbox is checked under <b>Decryption Mail Server Settings</b> section on <b>System Settings</b> page.
<b>DECRYPTED_SM_DELIVER_TRUSTED_TLS</b>	Inbound Echoworx Email Encryption Encrypted mail message decrypted. Message delivered over a secure TLS channel.  <b>Note:</b> This action is listed when Decryption SMTP server is not used; i.e., <b>MX Lookup</b> checkbox is checked under <b>Decryption Mail Server Settings</b> section on <b>System Settings</b> page.
<b>DECRYPT_BOUNCE_BACK_NO_SIGNATURE</b>	Message decrypted but bounced back due to missing signature (key)
<b>DECRYPT_BOUNCE_BACK_SIGNATURE_FAILURE</b>	Message decrypted but bounced back due to mismatch in the signature (key)
<b>DECRYPT_PGP</b>	Inbound PGP message decrypted. Message delivered over Decryption SMTP server.  <b>Note:</b> This action is listed when Decryption SMTP server is used.
<b>DECRYPT_PGP_ATTACHMENT</b>	Only the .pgp attachment is decrypted and not the entire message
<b>DECRYPT_RELAYED</b>	EMG is unable to decrypt inbound PGP or S/MIME message. Encrypted message relayed to recipient.
<b>DECRYPT_SM</b>	Inbound Echoworx Email Encryption Encrypted mail message decrypted. Message delivered over Decryption SMTP server.



Action	Description
	<b>Note:</b> This action is listed when Decryption SMTP server is used.
DELIVER	Message sent as a plain text message. No encryption policy triggered.
DELIVER_TRUSTED_TLS_DIRECT_DOMAIN	Message sent via a secure TLS channel
DELIVER_TRUSTED_TLS_PROXY_DOMAIN	Message sent
DISCARD	Message deleted. This occurs when the <b>Discard</b> mail action is triggered by the policy.
ENCRYPT_ATTACHMENT_ONLY	Only the attachment is encrypted, triggered by the <b>Attachment Encryption</b> setting.
ENCRYPT_ATTACHMENT_ONLY_PENDING_PSK	Attachment only encryption. Message delivered to the web portal for the recipient to select a password.
ENCRYPT_DC	Web Portal encrypted message
ENCRYPT_DC_PSK	Web Portal encrypted message with Question-Answer hint
ENCRYPT_DC_UNAUTHENTICATED	Web Portal message that does not require a password for authentication
ENCRYPT_DC_VERIFICATION_CODE	Web Portal message that requires a verification code for authentication
ENCRYPT_DELIVER_OWNDOMAIN	Message delivered within the sender's domain
ENCRYPT_DELIVER_TRUSTEDDOMAINDOMAIN	Message delivered via Domain-to-Domain delivery method
ENCRYPT_EXTERNAL_PGP	Message encrypted with PGP certificate from external LDAP and delivered. External PGP certificate servers are configured on the <b>LDAP Key Server Settings</b> screen.
ENCRYPT_EXTERNAL_SMIME	Message encrypted with x.509 certificate from external LDAP and delivered. External X.509 certificate servers are configured on the <b>LDAP Key Server Settings</b> screen.
ENCRYPT_LOCAL_PGP	Message encrypted with PGP certificate from EMG database and delivered
ENCRYPT_LOCAL_SMIME	Message encrypted with x.509 certificate from EMG database and delivered
ENCRYPT_REGULAR_EMX	Message encrypted with Echoworx Global Directory EMX (Web Portal) credentials
ENCRYPT_SECUREMAIL	Message encrypted with Echoworx Global Directory Encrypted Mail credentials
ENCRYPT_SECUREREADER	Message encrypted with Echoworx Global Directory Encrypted Mail Reader credentials
ENCRYPT_SECURE_PDF	Message encrypted as a secure PDF
ENCRYPT_SECURE_PDF_PENDING_PSK	Message encrypted as a secure PDF and delivered to the Web Portal for the recipient to select a password

Action	Description
ENCRYPT_SECURE_PDF_PSK	Message encrypted as a secure PDF and delivered to the Web Portal with a sender-set password
LOG_AND_CONTINUE	Message triggered policy with <b>Log and Continue</b> action
LOG_AND_SEND	Message triggered policy with <b>Log and Send</b> action Message sent in plain text
REDIRECT_PROFILE	Message triggered policy with <b>Redirect Profile</b> mail action. The message is redirected to the profile selected in the 'Redirect Profile' action for further processing.

## Notify Status List

The **Notify Status** column contains status codes. The meaning of each status code is specified in the table below:

Notify Status Code	Description
YES	Notification sent
NO	Notification not yet sent
NDR	Non-delivery Receipt sent
ERR	Returned when 'Notify on Error' is turned on
NONDR	Returned if there is an invalid <b>From</b> address  Returned when you stop the NDRs being sent for the messages in the following statuses: ERROR, FAILED, IGNORED, and TLS_FAILURE.
EO	<b>Enable Override</b> - Notification sent per header ( <b>notified per x-echoworx-send-encryptnotification header</b> )
DO	<b>Disable Override</b> - Notification not sent per header ( <b>notified per x-echoworx-send-encryptnotification header</b> )
RNE	Message encrypted but notification not sent
DNN	No notification (notifications disabled)
NIO	Status for TLS messages when the <b>Disable encrypt notifications for TLS messages</b> setting is enabled

## Resend Failed Messages

You can use the Message Report to resend any message that appears in the search results. You can only resend messages that are included in your search results.

To resend all messages included in your search, perform a search and then click the **Resend All** button at the bottom of the list. This will resend all messages in the search result, not just those displayed on the current page.

To resend FAILED or ERROR messages only, perform a search and click the **Resend FAILED/ERROR for Search** button. This will send all FAILED or ERROR messages in the search result.

## Error Message Details

The **Error Message** column is populated by a **Details** link if a particular message encountered an error or failure during its life cycle. This also applies for messages that are in SENT status. Clicking the **Details** link opens a pop-up window which lists the reason(s) why the message previously failed or returned an error.

## Stop Non-Delivery Receipt (NDR)

When an email message delivery fails due to an invalid recipient email address, SMTP server failure, mailbox over quota, or any other issue, an NDR is sent to the sender of the email message to inform them about the failure.

Whenever the message fails to be delivered, an NDR is sent. Attempts to send the NDR for a failed message will be made until a defined resend notification cutoff threshold is reached. This threshold is configured in the **failed.message.resend.notification.cutoff.period** property on the **Advanced System Settings** page. The **Stop NDR** button appears in the report results against the failed message. It appears for the messages in the following statuses:

- ERROR
- FAILED
- IGNORED
- TLS\_FAILURE

To stop the NDR being sent for a failed message, click **Stop NDR**. The value of **Notify Status** for the failed message changes to **NONDR**. Once you click **Stop NDR**, the button disappears from the report results against the failed message.

To stop a message from being processed by EMG, click **Ignore**. An NDR will be sent once after the message is ignored unless the **Stop NDR** button is clicked.

The actions related to the **Ignore** and **Stop NDR** buttons will be audited.

## Message Report

Search By Message Info

Profile:	Status:	Sender:
<span></span>	<span>ERROR</span>	<input type="text"/>
*From:	Action:	Recipient:
<input type="text"/> 07-01-2020 <input type="text"/> 00 <input type="text"/> 00	<span></span>	<input type="text"/>
*To:		Recipient Domain: (Exact Match Only)
<input type="text"/> 07-30-2020 <input type="text"/> 23 <input type="text"/> 59		<input type="text"/>

At least one of Status, Sender, Recipient, or Recipient Domain is required.

## Report Results

Sender	Sent Date	Profile	Status	Action	Recipients	NotifyStatus	Error Message	
bob@demostrationbank.com	<a href="#">2020-07-28 23:54:32</a>	demostrationbank	ERROR		alissa@demostrationbank.com	NO	<a href="#">Details</a>	<input type="button" value="Send"/> <input type="button" value="Ignore"/> <input type="button" value="Stop NDR"/>
bob@demostrationbank.com	<a href="#">2020-07-28 23:53:29</a>	demostrationbank	ERROR		jamie@demostrationbank.com	NO	<a href="#">Details</a>	<input type="button" value="Send"/> <input type="button" value="Ignore"/> <input type="button" value="Stop NDR"/>
alice@demostrationbank.com	<a href="#">2020-07-28 23:50:43</a>	demostrationbank	ERROR		sandy@demostrationbank.com	NO	<a href="#">Details</a>	<input type="button" value="Send"/> <input type="button" value="Ignore"/> <input type="button" value="Stop NDR"/>
bob@demostrationbank.com	<a href="#">2020-07-28 23:25:54</a>	demostrationbank	ERROR		sophie@demostrationbank.com	NO	<a href="#">Details</a>	<input type="button" value="Send"/> <input type="button" value="Ignore"/> <input type="button" value="Stop NDR"/>

1 - 4 (4)  
First | Previous | Next | Last

## Audit Trail Report

The Audit-trail report tracks all admin actions performed through the EMG admin console. The following actions are included in the Audit Trail report:

- Create ADMIN user
- Delete ADMIN user
- Password reset of ADMIN user
- Login of ADMIN
- System setting page updates
- Server management
- Edit scheduler
- Add or remove profile
- Add or remove users
- Audit credentials
- Audit policy changes/update

**Note:** The action of fetching an audit trail report is audited in EMG.

To use the Audit Trail Report:

1. Log in to the EMG Console.
2. To access **Audit Trail Report** page perform either of the following steps:
  - a. Click **Home** from the menu.
  - b. Under **Reports** tile, click **Audit Trail Report**. The **Audit Trail Report** page appears.

OR

- a. Hover mouse over **Reports** menu. A menu opens.
  - b. Click **Audit Trail Report** from the menu. The **Audit Trail Report** page appears.
3. Enter the search criteria.
4. Click **Search**. The audit report matching your search criteria appears.

PROFILE : echoworx\_tech\_writers | [Change Profile](#)

### Audit Trail Report

**Search**

<b>Profile:</b> <input type="text" value="echoworx_tech_writers"/>	<b>Category:</b> <input type="text" value="CREDENTIALS"/>	<b>Email: (Exact Match Only)</b> <input type="text"/>
<b>*From:</b> <input type="text" value="04-22-2019"/> <input type="text" value="00"/> <input type="text" value="00"/>	<b>Action:</b> <input type="text" value="DELETE"/>	<b>User Role:</b> <input type="text"/>
<b>*To:</b> <input type="text" value="04-22-2019"/> <input type="text" value="23"/> <input type="text" value="59"/>		

**Report Results**

Date	Profile	Email	User Role	Action	Category	Description
2019-04-22 09:37:01.0	echoworx_tech_writers	bob.smith@...	ADMIN	DELETE	CREDENTIALS	PDF passwords for: [ewtestwriter@outlook.com] in enterprise: [demonstrationbank] have been deleted. Reason: [test].
2019-04-22 09:37:01.0	echoworx_tech_writers	bob.smith@...	ADMIN	DELETE	CREDENTIALS	User account in EMX for: [ewtestwriter@outlook.com] in enterprise(s): [demonstrationbank] has been deleted. Reason: [test].
2019-04-22 09:29:46.0	echoworx_tech_writers	bob.smith@...	ADMIN	DELETE	CREDENTIALS	PDF passwords for [ewtestwriter@outlook.com] in enterprise [demonstrationbank] have been manually expired.

1 - 3 (3)  
[First](#) | [Previous](#) | [Next](#) | [Last](#)

## Policy Report

Occasionally a message behaves unexpectedly because of an overaggressive or misconfigured email policy. The EMG Policy Report can help diagnose these problems by showing.

**Note:** The action of fetching a policy report is audited in EMG.

Enterprise Administrator access to Policy Report may be restricted/disabled by the system administrator.

## View the Policy Report

To use the Policy Report:

- 1. Log in to the EMG Console.
- 2. To access **Policy Report** page perform either of the following steps:
  - a. Click **Home** from the menu.
  - b. Under **Reports** tile, click **Policy Report**. The **Policy Report** page appears.

OR

- a. Hover mouse over **Reports** menu. A menu opens.
- b. Click **Policy Report** from the menu. The **Policy Report** page appears.

Policy Report

Search

Profile:  
\_\_default\_\_

From:  
05-02-2019 00:00

To:  
05-02-2019 23:59

Policy Details

Risk:

Policy Name:

Word List Name:

Matched Item:

Mail Action:

Message Details

Message ID: *(Exact Match Only)*

Sender:

Recipient:

Message Header:

Search

## Select Search Criteria

The Policy report allows you to locate messages that triggered a certain policy, or policies that were triggered by a certain message. Each row in the report results represents a single match.

To locate a message, enter the desired search criteria, and click **Search** to display the results on screen.

Profile	The profile that the sender's domain is mapped to.
From/To	The message report returns messages newer than the date specified in the From field, and older than the date specified in the To

EMG Admin Guide  
- 38 -

field.

### Policy Details (properties of the policy that was triggered by the message)

Risk	Status of the message (see <b>Message Status Reference</b> below)
Policy Name	The name of the policy that matched the message. Note that a single message may match multiple policies.
Word List Name	The name of the word list that matched
Matched Item	Name of the word that matched
Mail Action	The action associated with the triggered policy. For a description of each mail action, see

### Message Details (details of the message that triggered the policy)

Message ID	Echoworx Message ID
Sender	The sender's email address
Recipient	The recipient's email address
Message Header	Search the message header text

### Message Status Reference

The Message Manager page displays the following statuses for each message:

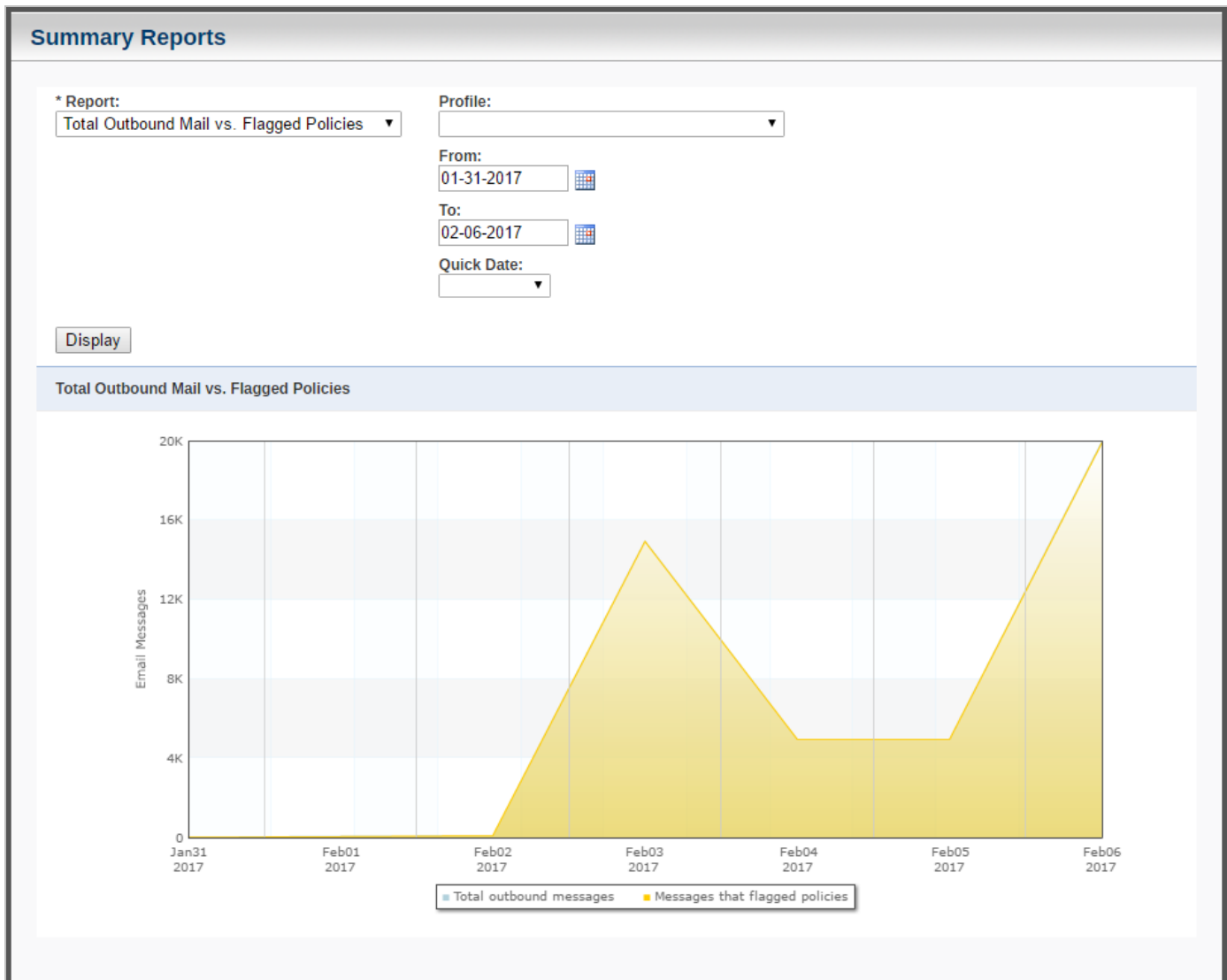
UNPROCESSED	This is the default status of a message (i.e., no policies/actions have been applied to it). All messages have an 'Unprocessed' status when they first arrive in EMG.
DISCARDED	A policy triggered a 'discard' action on the message, or if an incoming encrypted message cannot be decrypted by EMG.
FAILED	The message cannot be sent. For this status, a Send button appears next to the message, which will re-send the message when pressed.
ERROR	The message has caused an unexpected system level error. For this status, a Send button appears next to the message, which will re-send the message when pressed.
SENT	The message was sent successfully.
LOGGED	The message has triggered the "Log and continue" action.

## Summary Reports

The **Summary Reports** page is a collection of reports that provide statistical information for the current profile. Certain summary reports require a date range, others provide information about the current state of the system or profile. Read on for a brief description of each Summary Report.

**Note:** The action of fetching any of the summary reports is audited in EMG.

Enterprise Administrator access to the **Summary Reports** page may be restricted/disabled by the system administrator.



## User Credentials

The User Credentials Summary Report lists the total number of credentials of each type stored in the EMG database. This report is only available to system administrators.



## Key Metrics

The Key Metrics Summary Report provides a snapshot of the messaging activity under the selected profile for the specified period. The following table describes the

Total inbound messages	Number of messages received by EMG from domains that are mapped.
Total outbound messages	Number of messages sent to domains.
Messages that flagged policies	Number of messages that triggered one or more policies.
Total failed messages	Number of messages that could not be delivered after the maximum number of retries.
Total ignored messages	Number of messages that were rejected by EMG before processing.
Messages encrypted	Number of messages that were encrypted under the current profile.
Sender(s) who flagged policies	Number of unique users (i.e. email addresses) that sent one or more messages that into EMG and
Unique senders	Number of unique users (i.e. email addresses) that sent one or more messages into EMG
Total error messages	Number of messages that caused an error during processing by EMG.

## Total Outbound Mail vs. Flagged Policies

The **Total Outbound Mail vs. Flagged Policies** Summary Report displays a line graph with the number of outbound messages and the total number of messages that triggered one or more EMG policies, over the specified period.

## Risk Level of Flagged Policies

The **Risk Level of Flagged Policies** Summary Report displays a pie chart with the risk level of all flagged policies over the specified period.

## Top Flagged Policies

The **Top Flagged Policies Summary** Report displays a bar chart with the top five most commonly flagged policies over the specified period.

## Top Expressions that Flagged Policies

The **Top Expressions that Flagged Policies** Summary Report displays a bar chart with the top five most commonly matched list items over the specified period.

## Top Senders Who Flagged Policies

The **Top Senders who Flagged Policies** Summary Report displays a bar chart with the top five users (i.e. email addresses) in policy-flagging message volume over the specified period.

## Top Mail Actions

The **Top Mail Actions** Summary Report displays a bar chart with the top five most common mail action (such as Encrypt, or Log and Send) over the specified period.

## Top Delivery Channels

The **Top Expressions that Flagged Policies** Summary Report displays a bar chart with the top five most commonly used Delivery Methods over the specified period.