proofpoint essentials

Getting Started Guide

Proofpoint Essentials

Hi and welcome to Proofpoint Essentials! If this is your first time using Proofpoint Essentials, here's a great way to start. We'll walk you through the essential first steps so your team can work efficiently and productively in the system.

April 2015

Important Information

The following information applies to Proofpoint Essentials US1 data center only.

User Interface Access	• https://us1.proofpointessentials.com
MX Records	• mx1-us1.ppe-hosted.com • mx2-us1.ppe-hosted.com
Proofpoint Essentials IP Addresses *Proofpoint Essentials must be able to deliver email to the organization mail environment. It will be necessary for exceptions to be added to the firewall for these IP addresses.* *Port 25 for SMTP Traffic* *Port 389 for LDAP (If using Active Directory to load users)*	• 67.231.152.0/24 • 67.231.153.0/24 • 67.231.154.0/24 • 67.231.155.0/24 • 67.231.156.0/24 67.231.144.0/24 67.231.145.0/24 67.231.146.0/24 67.231.147.0/24 • 67.231.148.0/24 • 148.163.128.0/19
Additional IPs Addresses (For Customers using Archiving) *Ports 143 & 993 for IMAP*	50.19.242.23 • 46.51.173.223 •
Smart Host	• outbound-us1.ppe-hosted.com
SPF	• "v=spf1 a:dispatch-us.ppe-hosted.com ~all"

About

This document contains specific information related to accessing and configuring Proofpoint Essentials. For additional information please refer to the Proofpoint Essentials Administrator Guide.

Getting Access

You should already have received Proofpoint Essentials login information. If you do not have this information, please contact your partner.

Sign in to the Proofpoint Essentials Interface as an Admin

1. Open an Internet browser on your computer and enter the interface URL.
2. Login using your supplied credentials.
    - Enter your username (This will be your email address).
    - Enter your password (Use the password supplied in the welcome email).

Update Your Password

1. While logged into the user interface, navigate to Users & Groups > Users tab.
2. Locate your account by name in the list.
3. Click on your Name.
4. Enter a new password in the Password and Retype Password fields.
5. Click Save.

Your password is set. You must use this password the next time you log in to the user interface.

Review Company Setup

1. While logged into the user interface, navigate to Company Settings > Profile tab.
2. Click on Change Profile Information.
3. Ensure that all fields are populated with accurate information (e.g. Country, Time zone, etc.).
4. Click Save.

Configure / Add Domain

Update Domain

1. While logged into the user interface, navigate to Company Settings > Domains tab.
2. Select the domain you wish to update and click Edit.
3. Enter the messaging server information (IP Address or Fully---Qualified Domain Name).
4. Enter an SMTP failover location (Optional).
5. Set Enable email relay? to Yes.
6. Click Save.

Once you save the changes, Proofpoint Essentials will attempt to validate the information you have added including MX Records and access to the specified messaging server.

New domains as well as changes to existing domains are applied every half-hour.

Add New Domain

1. Click Add New Domain.
2. Enter the domain name.
3. Enter the messaging server information (IP Address or Fully-Qualified Domain Name).
4. Enter an SMTP Failover location (Optional).
5. Click Save.

New domains as well as changes to existing domains are applied every half-hour.

Loading Users

Once your subscribed domains are accurate you should now import your users. Proofpoint Essentials allows organizations to load users in several ways:

1. Active Directory Sync ○ Active Directory sync can be used to load mail-enabled objects (e.g. users, distribution groups, mail enabled public folders, etc.) from an organization's Active Directory directly to Proofpoint Essentials.
    - This can be done on a one-time or ad-hoc basis.
        - This method can also be used to perform ongoing (daily) updates.
2. CSV
    - Support for two formats: Standard, Postini
        - Standard CSV file can contain user information such as SMTP Address, first and last name as well as user aliases.
        - Postini CSV file supports the Google Postini user export file format.
            - The import process will automatically create allow and block lists for each user imported.
    - There is also support for an additional Postini format referred to as the Postini Alias CSV. This file format can be used to load Postini alias addresses after the Postini Users CSV has been used to import users.
3. SMTP Discovery ○ When enabled, SMTP discovery will accept email traffic for non-registered users based on predefined settings (e.g. number of times where the SMTP address has been identified). It will also send out a weekly report to the organization administrator so that they can set the address as either invalid or active.
    - SMTP Discovery is disabled when Active Directory is selected for loading users and is optional when CSV upload is selected.
4. Manual ○ Users can be added manually through the user interface.

Adding Users by Active Directory

1. While logged into the user interface, navigate to Company Settings > Import Users tab.
2. Select the Active Directory tab.
3. Select the initial profile of the users you are loading.

End Users receive a welcome letter once added to the system. The welcome letter will include details about the quarantine email as well as login information to access the user interface.

Silent Users do not receive a welcome letter when loaded into the system. Their profile can be changed (i.e. to an end user)

at a later stage.

4. Specify the URL or IP Address to access the organization's Active Directory.

Port 389 (LDAP) will need to be accessible to Proofpoint Essentials IPs in order for this method to be used.

5. Enter an Active Directory username and password that can be used to import email-enabled objects such as users, Security Groups and Distribution Lists.
6. Enter the Base DN

This is the LDAP query that Proofpoint Essentials will execute to capture all mail-enabled object information. If you do not know what your base DN is please consult your network administrator.

7. Choose what items you would like to sync.
8. Choose additional sync options (e.g. updated synchronized accounts, etc.).
9. Choose if you would like to enable a daily sync between Proofpoint Essentials and the organization's Active Directory.
10. Click Save.

Once the settings are saved you will need to execute the import. To do this:

1. Click on the Users & Groups tab.
2. Click on the Active Directory tab.
3. Click Search.
4. Click Execute.

The Active Directory sync will overwrite previously created accounts along with their permissions. Therefore, you will need to update the organization admin account. Refer to the Manually Adding Users section in order to update user settings.

Adding Users by CSV

1. While logged into the user interface, navigate to Company Settings > Loading Users tab.
2. Select the CSV tab.
3. Select the CSV file format.

To view a sample format of the file you have selected click CSV file format instructions.

4. Select the initial profile of the users you are loading.

End Users receive a welcome letter once loaded into the system. The welcome letter will include details about the quarantine email as well as login information to access the user interface.

Silent Users do not receive a welcome letter when loaded into the system. Their profile can be changed (i.e. to an end user) at a later stage.

5. Click Choose File
6. Locate the file you wish to import.
7. Click Upload.

A validation page will appear displaying the results (success, failures) from the CSV import. Users that have already been created will not be overwritten but will be indicated as an error (duplicate).

Note: To use the Postini Alias CSV file format you must have already loaded users.

Adding Users by SMTP Discovery

1. While logged into the user interface, navigate to the Company Settings > Features tab.
2. Ensure SMTP Discovery is checked.
3. If it is not checked, check and Click Save.
4. Click the SMTP Discovery tab.
5. Select the initial profile of the users that are created.

End Users receive a welcome letter once loaded into the system. The welcome letter will include details about the quarantine email as well as login information to access the user interface.

Silent Users do not receive a welcome letter when loaded into the system. Their profiled can be changed (i.e. to an end user) at a later stage.

6. Update SMTP Discovery settings based on preferences.

Inbound Detection Threshold: The number of times Proofpoint Essentials should see this email address before including it in the SMTP Discovery weekly digest.

Expiration: The number of times the address should appear in the SMTP Discovery weekly digest before expiring.
Expired Addresses Default to New User: When enabled will automatically make an address a licensed user once inbound detection and expiration settings have been met.

Auto-add Detected Alias Addresses: Will automatically add an address as an alias when identified.

Auto-add New Users Detected via Outbound: If the organization is filtering outbound email through Proofpoint Essentials, than this setting will automatically create licensed users for non-registered accounts.

Report on New Users: Will deliver a report to the organization administrator identifying new users that have been automatically created.

Report on New Aliases: Will deliver a report to the organization administrator identifying new aliases that have been automatically added.

Include Admin Contact: Will include the admin contact in the report.

7. Click Save.

Manually Add Users

1. While logged into the user interface, navigate to the Users & Groups > Users tab.
2. Click on Add a User.
3. Enter the user's first name.
4. Enter the user's last name.
5. Enter the user's primary email address.
6. Select the user's privileges.

End Users receive a welcome letter once loaded into the system. The welcome letter will include details about the quarantine email as well as login information to access the user interface.

Silent Users do not receive a welcome letter when loaded into the system. Their profile can be changed (i.e. to an end user) at a later stage.

7. Enter a password for the user (Optional).
8. Click Save.

New users are registered every half-hour. Therefore mail will not flow to the new user until the change is made. If SMTP Discovery is enabled, users will be able to receive email immediately.

Manage Users

Once users have been loaded initially, you can use the user interface to:

- Add new users.
- Update an existing user.
- Delete a user.

Add New User

1. While logged into the user interface, navigate to the Users & Groups > Users tab.
2. Click on Add a User.
3. Enter the user's first name.
4. Enter the user's last name.
5. Enter the user's primary email address.
6. Select the user's privileges.

End Users receive a welcome letter once loaded into the system. The welcome letter will include details about the quarantine email as well as login information to access the user interface.

Silent Users do not receive a welcome letter when loaded into the system. Their profile can be changed (i.e. to an end user) at a later stage.

7. Enter a password for the user (Optional).
8. Click Save.

New users are registered every half-hour. Therefore mail will not flow to the new user until the change is made. If SMTP Discovery is enabled, users will be able to receive email immediately.

Update Existing User

1. While logged into the user interface, navigate to the Users and Groups tab.
2. Select the user you wish to update.

If necessary you can use the search field to locate the user by name.

3. Update the user's information as needed.
4. Click Save.

Delete User

1. While logged into the user interface, navigate to the Users & Groups > Users tab.
2. Check the checkbox next to the user you wish to delete.
3. Select Delete from the Action drop down list.
4. Click Apply.
5. Click OK on the confirmation window that appears.

Mass Update

The mass update feature allows you to apply a change across all or a large set of users. For example, if you have loaded users as silent users you may want to change them to an end user to ensure they receive the quarantine digest and can login into the system.

1. While logged into the user interface, navigate to the Users & Groups > Users tab.
2. Select Mass Update from the Action drop down list.
3. Select the appropriate option from the list displayed (e.g. user privileges).

If you are changing silent users to end users you will want to send users a welcome email. Make sure the "send welcome email" checkbox is checked.

4. Click Update Users.

Additional Configuration

Update Spam Configuration

The spam configuration has been set to meet the needs of most organizations. You can adjust the Spam Sensitivity for an organization if desired.

1. While logged into the user interface, navigate to the Company Settings > Spam tab.
2. Click and drag the slider left (more aggressive) or right (less aggressive).

The default value is 7.

3. Choose additional options as needed.
4. Click Save.

Update Digest Configuration

The quarantine digest is enabled by default. It is configured to send a daily digest to all end users. You can adjust the digest configuration if desired.

1. While logged into the user interface, navigate to the Company Settings > Digests tab.
2. Adjust configuration as needed.
3. Click Save.

Cutover

Once configuration and validation has completed, the companies MX records can be updated to direct to the Proofpoint Essentials service. Please note that updates to MX records may take a few minutes to apply. MX records for this environment are listed in the Important Information section.

Validation

Message logs can be used to validate mail flow once a customer has updated their MX records to flow email through Proofpoint Essentials.

View Logs

1. While logged into the user interface, navigate to the Logs tab.
2. Click on the Licensed tab.
3. Select Any from the Status drop-down menu.
4. Click Search.

The search results will show you all recent email traffic that Proofpoint Essentials has filtered.