Proofpoint Essentials

Best Practice Guide for New Partners

The following guidelines aim to provide new indirect partners with best practices for managing their Proofpoint Essentials customer base.

Contents:

©2016 Proofpoint, Inc. Proofpoint Essentials is a trademark of Proofpoint, Inc.

1. Prior to logging in to the Interface

Account Creation:

Proofpoint will set you up with an account on Proofpoint Essentials. This will allow you to manage your own organization as a Partner but more importantly it enables you to manage all of your Customers using Proofpoint Essentials. The Proofpoint Essentials console can be accessed here: https://us1.proofpointessentials.com.

Documentation:

We recommend that you familiarize yourself with the material listed below. These materials can be found under the Documentation Section of our Getting Started Page here: https://www.proofpoint.com/us/proofpoint-essentials-getting-started.

1. Admin guide
2. Getting Started Guide
3. End User Guide

Knowledge Base:

The Proofpoint technical team also keeps an updated Knowledge Base (KB) for FAQs and common provisioning best practices. The KB can be found here: http://support.proofpointessentials.com/index.php/Knowledgebase/List

2. Exploring the Interface:

Partner NFR: As a Partner we give you 50 licenses of the Professional Package free of charge for your internal use only. Upon initial login, your settings for your internal service are visible. Accessing the Customer Tab is where you create and manage Customers.

Branding Tab: Upload your Partner logo here and by default it will appear in your end Customer's console and notifications.

Customers Tab:

- **Add a Customer:** Use the provisioning wizard to create Customer accounts.
- **Show/Hide:** The Customers Tab is designed to provide as much information as possible – use the 'Show/Hide' option to choose the Customer statistics you would like to see.
- **Templates (Admin Guide under the Manage Customers Tab>Using Templates):** Templates allow you to create a pre-determined set up for Customers you decide to apply that template to. Templates can be found under the Customers Tab and attributed to a new Customer during the provisioning process. Please note templates can only be leveraged when provisioning new Customers. See Section 6 below for our recommended template settings.
- **Automation Settings:** Another best practice is to use Automation Settings found under the Customers Tab. Automation Settings allow you to create catch all policies for your Customer base. For example, you are able to enforce User Capping, disable the SMTP Discovery tool and set Customers to auto-renewal.

3. New Customer Set Up

Partners will have their own processes for adding Customers, however please note the best practice recommendations below in order:
**You can find configuration details in the Getting Started Guide on our Getting Started Page linked above.*

- Partner Admin provisions Customer Account using the provisioning wizard under Customers Tab.
- Partner clicks on newly created Customer Account.
- Provision the remaining domains, primary SMTP delivery points, sending servers, filters and users.
- Partner/Customer adds Proofpoint DC IP ranges into Customer's firewall alongside existing solution IPs.

©2016 Proofpoint, Inc. Proofpoint Essentials is a trademark of Proofpoint, Inc.

- Partner/Customer reduces Customer domains' TTL so Proofpoint MX records propagate quicker.
- Partner/Customer configures send connector on Customer's mail server to push SMTP to the Proofpoint Essentials smart host.
- Configure SPF records so that your domain(s) are associated with the Proofpoint IP's when sending outbound – SPF information is provided in the Getting Started Guide linked above.
- After ensuring SMTP Discovery is enabled or users are added explicitly, MX records can be changed.
- After 24 hours, remove previous solution's IP range (if applicable) from firewall SMTP rules.

4. Managing your Customers:

- **Licensed Logs:** It is important to note that in order to search Logs for an entire organization, selecting 'Licensed' is required within the Logs Section. 'Unlicensed' Logs will search mail for users not yet registered; for example, those discovered (but not added) using SMTP Discovery. Filters created by administrator will not run for unlicensed users.
- **Permalinks:** When interacting with support, best practice is to provide them with the message Permalink. The Permalink allows support to view the email detail without having to find it in the Logs. Permalinks are located under the Details Tab of the Logs.
- **Reports:** Reports are a great way for end Customers and Admins to understand the amount of clean mail, spam, viruses and advanced attacks that Proofpoint is processing. Reports are displayed in 60 minute segments and by default a report will show the last 24 hours – it is advisable to expand the report timeframe to 30 days using the drop down menu.

5. User Creation Management

There are 4 ways to create users, user aliases and functional accounts (e.g. distribution lists). You should determine which method you are going to use before changing MX records to Proofpoint.

Explicit User Creation: Proofpoint only accepts mail traffic when users are created in the console.

- **Active Directory Sync:** Best practice is to use AD sync as this will provide the most accurate representation of your local user config including the ability to automatically pull in Functional Accounts. MS Active Directory is the only LDAP supported system today, increased functionality and our ability to integrate with alternative systems is coming soon.

  Before you begin, you will need the following:

  a. An inbound connection that allows Proofpoint Essentials IP range to connect to your domain controller

  b. A user account with read permissions to Active Directory

  c. A user account with administrator privileges to Proofpoint Essentials

  d. The Base DN (Distinguished Name)

  - The Base DN is the starting point for directory server searches
  - For example: DC=mycompany,DC=com, the Connector starts from this DN to create the list of users and groups to sync.

Support for LDAP and LDAP over SSL:

The standard protocol for reading data to Active Directory is LDAP. LDAP traffic is unsecured by default. To make LDAP traffic secure, you can use the Secure Sockets Layer/Transport Layer Security (SSL/TLS) protocols. This combination is referred to as LDAP over SSL –- or LDAPS.

To setup your domain controller to accept LDAP over SSL, please refer to the following Microsoft article: How to enable LDAP over SSL (https://support.microsoft.com/en-ca/kb/321051).

©2016 Proofpoint, Inc. Proofpoint Essentials is a trademark of Proofpoint, Inc.

Manually Perform Active Directory Sync:

If you checked Sync Every 24 Hrs in the Active Directory settings, a sync is automatically performed. Otherwise, you need to force a sync.

1. On the Users & Groups tab, click Active Directory
2. Click Search
3. Review the search results
4. Click Execute

Useful Tools:

Additional Configuration details can be found in our KB article here: http://support.proofpointessentials.com/index.php?/Knowledgebase/Article/View/183/0/setting-up-of-active-directory-ldap-discovery

Troubleshooting LDAP connections and configuration: http://jxplorer.org/

Query strings Essentials uses to retrieve users/groups can be found below:

- Enabled Users, Groups, Functional Accounts: "(&(|(objectCategory=Group)(objectCategory=publicFolder)(&(objectCategory=Person)(userAccountControl:1.2.840.113556.1.4.803:=512)(!(userAccountControl:1.2.840.113556.1.4.803:=2)))))"
- Distribution Group: "['samaccounttype'][0] == 268435457"
- Public Folder: "['objectclass']['publicFolder'] && ['proxyaddresses']"
- Security Group: "['objectclass']['group'] && ['proxyaddresses']"
- Shared Mailbox: "['msexchrecipienttypedetails'][0] == 4"
- Inactive Users: "(&(objectCategory=Person)(userAccountControl:1.2.840.113556.1.4.803:=512(userAccountControl:1.2.840.113556.1.4.803:=2))"

- **CSV upload:** The CSV upload option will allow you to complete a one-time import of your primary and alias user addresses. With this upload option, Functional Accounts will have to be added manually under your 'Users & Groups' Tab under the 'Functional Accounts' Tab.
- **Manual User Creation:** You can manually create a user and/or alias under the Users & Groups Tab by clicking 'Add a User', or by clicking on an existing user, clicking on the 'Aliases' Tab and clicking 'Add Alias'.

Automatic User Creation:

SMTP Discovery: This user creation model automatically creates new users based on inbound and outbound email traffic. We recommend SMTP Discovery in the event that you cannot sync with Active Directory or upload users via CSV file. The inherent problem with SMTP Discovery is that it will not recognize alias email addresses or distribution lists correctly, and they will appear as billed users unless they are manually modified.

To use SMTP Discovery:

1. Enable SMTP Discovery under the Features tab.
2. Under the SMTP Discovery tab:
   - Set your Inbound Detection Threshold to 6 or more
   - Set the number of times you would like to be notified about an address before it expires to 3

©2016 Proofpoint, Inc. Proofpoint Essentials is a trademark of Proofpoint, Inc.

- Enable all of the following: Auto-add Detected Alias Addresses, Auto-add New Users Detected via Outbound, Report On New Users, Report On New Aliases, Include Admin Contact in the Report.

3. After SMTP Discovery is enabled and email traffic is flowing through Proofpoint's filters, we will begin creating new user accounts. The weekly emailed report will provide a list of users that have been discovered and you need to confirm to have them added to your account. We suggest reviewing that list in the console on a regular basis (at least weekly). To review in the console, you must go to the SMTP Discovery tab under the Users & Groups section.

In this list, you can do the following:

- Add as Account (billed end user)
- Add as Alias (to its primary billed end user account)
- Mark as Invalid (we will not accept traffic for invalid accounts)

FUNCTIONAL ACCOUNTS – Please note that if you notice that a Functional Account has appeared on your SMTP Discovery list, you will want to navigate to your Functional Accounts tab under 'Users & Groups' and add the discovered address as a Functional Account. In doing so, it will ensure you aren't billed for the account, and the account will be automatically removed from your SMTP Discovery list.

User Creation and Licensing:

- **Billing:** Billing is based on active users in the system. The following roles are considered active/billable users:
  - Channel Admin User
  - Organization Admin User
  - End-user
  - Silent User
- **Aliases and Functional Accounts:** Aliases and Functional Accounts are not considered billable users but are still protected. Aliases and Functional Accounts, which are correctly configured, shall not be counted as billable accounts provided each person who has access to such Aliases and Functional Accounts has a separate account on the Customer's mail server for the receipt of messages or data within such Customer's e-mail system or network.
- **End- User Capping:** Partners do have the ability to establish User Capping for their Customer Accounts. To enable a User Cap, you will want to navigate to the Customer, click on their 'Licensing' Tab. By enabling User Capping, please be aware that should your Customer try to add more than the 'Licensed for User' total, they will receive an alert letting them know they have reached their Cap and to contact their Partner Administrator to add additional licenses. A less aggressive approach, should you wish for them to be able to add users when necessary, would be to 'Enable Email Notifications' so that you can receive an alert should they go over the 'Licensed for Users' total.
- **Licensed for User vs Active Users:** The purpose of the 'Licensed for Users' total is to give Partners the opportunity to enable capping or a notification around user quantity, but it is not considered to be the billable total. Billing will consider the 'Active Users' total. Please see the 'Billing' Section above for more information.

©2016 Proofpoint, Inc. Proofpoint Essentials is a trademark of Proofpoint, Inc.

6. Recommended Setting for Templates

These are recommendations of settings to enable beyond Proofpoint's default settings. Partners are encouraged to test the service to find what works for them, and then create a template so that activating new Customer accounts on Proofpoint Essentials is as easy as possible.

Profile

- Set Time Zone,
- Add Admin Contact (Org Administrator at the Customer site if applicable, this user has the option to receive some reports, such as the SMTP Discovery report if enabled)
- Billing Contact
- Tech Contact (by default this will be the Technical Contact at the Partner site, we don't recommend altering this field)

Features

- Enable necessary check boxes and set Instant Reply to desired durations (up to 30 days).
- Uncheck SMTP Discovery if using AD Sync, CSV, or manual user creation.

SMTP Discovery

- Include Admin Contact in the Report

Filters

- Create New Inbound by Attachment Type for all Windows executable components, installers and other vulnerabilities and Other executable components and installers (12 total file types).

  *Please note that Proofpoint will block .js, .exe, .dll and .bat file types by default at part of our zero-day filter.

- Action should be Quarantine and Hide Log From Non-Admin Users. (McAfee SaaS Email Protection & Continuity blocked all executables and scripts by default).

Sender Lists

- Add your Partner domain to the Safe Sender List (for templates only)

URL Defense

- Add your Partner domains to the Exclude URLs that contain specified domains/IP addresses field (for templates only)
- Exclude active domains associated with this organization

Spam

- Current Trigger Level = 7
- Quarantine email suspected of being phish
- Require administrator privileges to release suspected phishing email
- Include an easy-spam-reporting disclaimer in passed email
- Quarantine inbound email sent by active domains associated with this organization
- Please note that if you change settings in Spam Tab under a live Customer account, you must check Update spam detection settings above for all existing user accounts before saving changes or changes will only apply to new users and not to existing users.

©2016 Proofpoint, Inc. Proofpoint Essentials is a trademark of Proofpoint, Inc.

Digests

- Only include messages quarantined since the last Quarantine Digest was sent: Yes
- Interval between Quarantine Digest checks: 12
- Exclude messages from the Quarantine Digest that are most likely to be spam
- Please note that if you change settings in Digest Tab under a live Customer account, you must check Update Quarantine Digest settings for all existing user accounts before saving changes or changes will only apply to new users and not to existing users.

Notifications

- Add your helpdesk ticketing information to the Welcome Email and Password Reset email templates
- In the Welcome Email, encourage your end-users to add a mobile number to their profile when creating a password

Access Control

- Add New Access Control for End User Role. Hide everything except Settings and Sender Lists (Proofpoint allows end-users more control over their email than some services. We recommend reviewing those controls to ensure they are right for your customer.
- Add New Access Control for Organization Admin Role. Upon provisioning of a new account, the system requires creation of a Customer Organization Admin. Best practices to determine which access control settings are right for your Organization Admins at each customer site.

About Proofpoint
Proofpoint Inc. (NASDAQ:PFPT) is a leading security-as-a-service provider that focuses on cloud-based solutions for threat protection, compliance, archiving & governance, and secure communications. Organizations around the world depend on Proofpoint's expertise, patented technologies and on-demand delivery system to protect against phishing, malware and spam, safeguard privacy, encrypt sensitive information, and archive and govern messages and critical enterprise information.

©Proofpoint, Inc. Proofpoint is a trademark of Proofpoint, Inc. in the United States and other countries. All other trademarks contained herein are property of their respective owners.

892 Ross Drive
Sunnyvale, CA 94089
1.408.517.4710
www.proofpoint.com