Proofpoint Threat Response

Threat Response Auto Pull (TRAP) - Installation Guide
Copyright Notice

Copyright 2018, Proofpoint, Inc. All Rights Reserved. No part of this document may be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form without prior written consent from Proofpoint, Inc.

Warranties and Disclaimers

Proofpoint, Inc. assumes no responsibility for errors or omissions in this publication or other documents which are referenced in or linked to this publication. This publication is provided “as is” without warranty of any kind and is subject to change without notice. Screen shot and illustrations may not represent the latest version of the software but are appropriate to explain the related text.

If you have any questions for our technical support staff, please contact us at either 877-64-POINT or at https://proofpointcommunities.force.com/.
## Table of Contents

**Threat Response Auto Pull (TRAP) - Installation Guide** ............................................. 4

**TRAP installation requirements** ......................................................................................... 4
  - Virtual machine requirements ............................................................................................. 4
  - Active Directory Requirements ......................................................................................... 5
  - Exchange Web Services Requirements ............................................................................. 5
  - Supported Exchange Versions ............................................................................................ 5
  - Required ports for network communication ...................................................................... 6
  - Supported browsers ........................................................................................................... 6
  - Supported hypervisors ....................................................................................................... 6

**Initial TRAP configuration** .................................................................................................... 6
  - Building TRAP VM ............................................................................................................. 6
  - Initial configuration wizard ............................................................................................... 7
  - License installation ............................................................................................................ 9
  - Logging into TRAP ............................................................................................................ 10

**Active Directory and LDAP** ................................................................................................. 10
  - Server Configuration ......................................................................................................... 10
  - LDAP attribute selection ................................................................................................. 11
Threat Response Auto Pull (TRAP) - Installation Guide

Installation guide provides information on how to get Threat Response Auto Pull (TRAP) up and running in your environment. The Installation guide includes the list of hardware requirements, all the major steps to install Threat Response Auto Pull image in VMware environment, configure required bootstrap services, and perform initial configuration.

TRAP installation requirements

Virtual machine requirements

TRAP Auto Pull (TRAP) is a stand-alone virtual appliance. It is distributed as an OVA file, and can be downloaded from the Proofpoint Customer Portal.

The virtual machine requires the following, minimum hardware configuration for production deployments:

- 4x vCPU Cores (8x vCPU cores recommended)
- 8 GB RAM (16 GB RAM recommended)
- 20 GB HDD (base system)
- 500 GB HDD (local databases and backups)
- 1 network adaptor (default E1000)

For administration and general usage, TRAP will need one IP address allocated to it for network access. If you plan to build a cluster for high-availability, you will need one local IP per-system, plus a single management IP to be shared between the systems.
Active Directory Requirements

Active Directory enables Threat Response Auto-Pull to gather details about users in alerts including information such as group membership, department, location, and more. Threat Response Auto-Pull requires read-only permissions in Active Directory.

Exchange Web Services Requirements

Threat Response Auto-Pull requires the connection with Exchange Web Services to perform email quarantine action. To configure Exchange EWS, you will need the following information:

- **Exchange Web Services:**
  - **EWS URL:** Based on your Exchange deployment you will need the Exchange Web Services URL. If you have a hybrid Exchange setup, you can configure both Exchange on-premise and Office 365 EWS URLs.
    - **On-premise Exchange:**
      - https://yourexchangehost.yourdomain.com/ews/exchange.asmx
      - In most cases, this host is same as the one that is hosting the Exchange OWA service.
    - **Office 365:**
      - https://outlook.office365.com/ews/exchange.asmx
  - (Optional) **EWS Certificate:** If you are using a self-signed certificate on Exchange CAS server for EWS service, you will need to import the cert to TRAP certificate store.
  - **Exchange Service Account:** TRAP requires a service account with the privilege to quarantine messages in targeted mailboxes. This service account must meet the following requirements:
    - The service account must have an associated mailbox
    - The service account must have permission to scan targeted mailboxes.
      - Choose one of the two supported exchange permission models:
        - **Application Impersonation role** (recommended): Grant explicit application impersonation role to the Exchange service account used for TRAP. Please ensure that this account has no other Exchange permissions or roles assigned.
        - **Full Access permission:** The Exchange service account used for quarantining has “Full Access” permission to all mailboxes.
    - **Exchange Throttle Setting:** To enable faster email quarantine rates, we recommend exempting this service/user account from any EWS Throttling limitations you may have configured on Exchange CAS server.

Supported Exchange Versions
TRAP supports the following:

- Office 365

Required ports for network communication

TRAP requires the following ports to be opened for management purposes, and to allow it to communicate with your devices. Refer to the table below for a list of ports that should be allowed between TRAP and other systems.

<table>
<thead>
<tr>
<th>Port</th>
<th>Direction</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP/443</td>
<td>&quot;Any&quot; to TRAP</td>
<td>TRAP GUI &amp; HTTPS alert listeners</td>
</tr>
<tr>
<td>TCP/8080</td>
<td>Admin Network to TRAP</td>
<td>Appliance Management Console</td>
</tr>
<tr>
<td>TCP/22</td>
<td>Admin Network to TRAP</td>
<td>SSH access to CLI</td>
</tr>
<tr>
<td>TCP/443</td>
<td>TRAP to &quot;overcast.proofpoint.com&quot;</td>
<td>Communication with Overcast (alert enrichment)</td>
</tr>
<tr>
<td>TCP/443</td>
<td>TRAP to “tap-api-v2.proofpoint.com”</td>
<td>Pulling alerts from TAP</td>
</tr>
<tr>
<td>TCP/443</td>
<td>TRAP to Exchange/O365/Gmail</td>
<td>Used to quarantine messages</td>
</tr>
<tr>
<td>TCP/389</td>
<td>TRAP to LDAP Server</td>
<td>Query LDAP for user details</td>
</tr>
<tr>
<td>TCP/25</td>
<td>TRAP to Mail Server</td>
<td>Notifications &amp; alerts via email</td>
</tr>
<tr>
<td>UDP/53</td>
<td>TRAP to DNS Server</td>
<td>DNS services</td>
</tr>
<tr>
<td>UDP/123</td>
<td>TRAP to NTP Server</td>
<td>NTP services</td>
</tr>
</tbody>
</table>

Supported browsers

TRAP supports the following browsers:

<table>
<thead>
<tr>
<th>Browser</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google Chrome</td>
<td>51.0 +</td>
</tr>
<tr>
<td>Mozilla Firefox</td>
<td>47.0 +</td>
</tr>
</tbody>
</table>

Supported hypervisors

Today TRAP supports the following virtualization environments:

- VMware ESX/ESXi

Initial TRAP configuration

Building TRAP VM
Importing TRAP to VMware

This example shows how to configure the Proofpoint TRAP on VMware ESX 5.5.

Note
This example assumes you have downloaded the OVA file from the Proofpoint Customer Portal as described in your Proofpoint Welcome letter.

To install TRAP in a VMware environment:

1. Start the VMware vSphere Client on your workstation.
2. Log in to the VMware ESXi server that will host the VM.
3. Select File > Deploy OVF Template to open the Deploy OVF Template dialog box.
   
   **Note:** the installation steps are listed in the panel on the left. You can use this list to follow your progress.
4. Go to the Deploy from file field and browse to the TRAP OVA file.
5. Click Open, then click Next.
6. Verify the OVF Template details then click Next.
7. Review the TRAP End User License Agreement.
8. Click Accept, then click Next.
9. Accept or change the default name in the Name and Location field, then click Next.
10. Select the resource pool for this VM, then click Next.
11. Select the data store to use for the TRAP files, then click Next.
12. Map the networks in the OVF template to your networks, then click Next.
   
   **Note:** The managed devices must be reachable from the TRAP virtual appliance.
13. Review the settings and click Finish to begin installing TRAP.
   
   **Note:** The system takes a few minutes to import the virtual appliance. Do not shut down the application during this process.

Initial configuration wizard

Once you deployed the TRAP VM, you can proceed with the initial configuration. First of all, you need to start TRAP.

1. In the vSphere Client, select the TRAP appliance that was just installed, right-click the name, then click Power > Power On.
2. Click the Console tab to emulate a console port.
3. Go to the next section to begin configuring the TRAP appliance.
Once TRAP is started, you can proceed with the initial configuration wizard. This will take up to 5 minutes.

1. Open a console window to start the initial configuration wizard.
2. Enter `admin` at the login prompt and press `Enter`.

   **Note:** If the system prompts you for a password, enter: proofpoint

3. Enter `yes` at the Do you want to use the wizard...? prompt and press `Enter`.
4. Enter a name you want to assign to this virtual machine at the **Hostname** prompt and press `Enter`.

   **Note:** Record it in the following Gather TRAP Configuration Information section.

5. (Optional) Select `yes` for DHCP and press `Enter`, if you want to use DHCP to get the IP address for TRAP.
6. Enter a password of your choice at the **password** prompt then press `Enter`. Record it in the following Gather TRAP Configuration Information section.
7. Re-enter your password when prompted and press `Enter` to save your changes and exit the program.

   **Note:** When you enter and re-enter your password, no keystrokes are displayed on the console; however, the password is being entered.

8. Enter your admin email address and press `Enter`.
9. Scroll through the list of available time zones to find the code for your time zone. Enter `n` (for next) and press `Enter` to scroll to the next batch or `p` (for previous) and press `Enter` to scroll to the previous batch. Codes for the US mainland time zones are:
   - US/Eastern: 509
   - US/Central: 507
   - US/Mountain: 513
   - US/Pacific: 514
10. Enter either the text string or the numeric value for the time zone then press `Enter`.
11. At the NTP Server prompt, enter your **NTP server name** if you want to use an NTP server or enter `No` if you do not then press `Enter`.
12. Review the information that you entered. To change an answer, enter the step number then press `Enter`. To proceed, press `Enter` to save changes and exit the wizard.

### Determining DHCP address

If DHCP was selected during the setup wizard, use the steps below to display the system’s IP address.

1. Log in to the TRAP console.
2. Enter `enable` at the hostname prompt and press `Enter`.
3. Enter `show interfaces eth0` at the hostname# prompt and press `Enter`.
4. Note and record the IP address in the Gather TRAP Configuration Information section below since you will not be able to copy and paste it from the console script window.
5. Type `exit` to log out of the console.

Gather TRAP configuration

This section provides you with an easy way to record important TRAP configuration information:

<table>
<thead>
<tr>
<th>Gather the following information</th>
<th>Record information here</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td></td>
</tr>
<tr>
<td>VM username</td>
<td></td>
</tr>
<tr>
<td>VM password</td>
<td></td>
</tr>
<tr>
<td>TRAP IP address</td>
<td></td>
</tr>
<tr>
<td>Hostname of virtual machine</td>
<td></td>
</tr>
</tbody>
</table>

Use this information to open and get started using TRAP, as described in the next chapter.

License installation

Use the steps in this section to install the TRAP License.

1. Open the Proofpoint Welcome email containing your license.
2. Locate and copy the license key to use in step 7 below.
3. In the browser window, enter `https://ptr_ip_address:8080`.
4. Provide the Proofpoint **username** and **password** then press Enter to open the **Proofpoint Appliance Management Console window.**
   Use the IP address assigned to the TRAP virtual machine in the Deploying the Virtual Machine section earlier in this chapter or go to the Gather TRAP Configuration Information if you recorded the IP address there.
5. Click the **Setup tab** then click **Licensing** in the left menu.
6. Paste the **Proofpoint license key** you copied from the Proofpoint Welcome email (in step 2 above) into the text field below Add New License.
7. Click Add Licenses then click Save in the top right corner of the window to validate and save the license.
TRAP licenses have expiration dates. Twenty-eight days before your license expires, TR opens a pop-up message each time you log in reminding that your license will expire soon. Once it expires, you will not be able to log in until you enter a new license in the Proofpoint Appliance Management console window. To renew your license, contact Sales at 1-877-634-7660.

Logging into TRAP

Use the steps in this section to run TRAP in a browser window.

1. Open a supported browser.
2. Navigate to https://ptr_ip_address to open the Proofpoint TRAP login window.
   This is the IP address assigned to the TRAP virtual machine when you set up your virtual environment in the Deploying the Virtual Machine section of the previous chapter.
3. Enter your username and password into TRAP login window.
   This is the admin password you created for yourself when you set up the virtual machine in the Deploying the Virtual Machine section and recorded in the section, Gather TRAP Configuration Information.
4. Click Login to open the TRAP Dashboard window. Initially, this window will be empty of data.

Active Directory and LDAP

LDAP / Active Directory support enables TRAP to map users to alerts that it receives, and to retrieve details about user accounts, such as location and group membership. The configuration is broken up into the two sections below.

Server Configuration

Create a server listing in TRAP to tell the systems which LDAP server to query for user information. Multiple servers can be created.

1. Log in to TRAP.
2. Navigate to System Settings > Contextual Data Sources > LDAP Servers.
3. Click the blue Add (+) button next to LDAP Servers to bring up the New LDAP Server panel.
4. Set the following fields:
   - IP/Hostname: `<ldap_hostname_or_ip>`
   - Port: `<ldap_port>`
   - SSL: Check to enable SSL encryption
   - Search Base: `<directory_path>` (e.g., DC=domain,DC=com)
   - Requires Authentication (Optional)
5. Save changes.

The authentication username may vary in syntax depending on your directory server’s authentication requirements. In most cases, the full, distinguished name (DN) for the user should be used as the username.

LDAP attribute selection

TRAP allows you to configure the user attributes that will be pulled from your LDAP / Active Directory server. By default, the system is configured to collect and display the following common user attributes:

- Display Name
- Telephone Number
- Mobile Number
- Email Address
- Company
- Department
- Street Address
- City
- State
- Country
- Group Memberships
To add, or remove items from this list, use the steps below.

1. Log in to TRAP.
2. Navigate to Settings > Contextual Data Sources > Displayed User Attributes.
3. Select attribute that you would like to be displayed for users.
   - Place a checkmark next to items in Available Attributes to select them
   - Uncheck items in Selected Attributes to remove them
4. Re-order the Selected Attributes by dragging-and-dropping items into your preferred order. This is how they will be displayed in the UI.
5. Click Save.