APPLICATION ACCESS MANAGER

(Agentless Central Credential Provider CCP)

AAM INTEGRATION - TECHNICAL DOCUMENTATION TEMPLATE

Name of Company: Palo Alto Networks

Website: https://www.paloaltonetworks.com/

Name of Product: Cortex XDR

Version: 2.6

Date: October 14, 2020

PARTNER SOLUTION OVERVIEW

Cortex XDR™ is a detection and response platform that integrates endpoint, network, and cloud data to stop sophisticated attacks. It unifies prevention, detection, investigation, and response in one platform for security and operational efficiency. Combined with Managed Threat Hunting service, Cortex XDR provides round-the-clock protection and industry-leading coverage of MITRE ATT&CK® techniques.

The Palo Alto Networks Broker is a secured virtual machine (VM), integrated with Cortex XDR, that bridges the local network and Cortex XDR. By setting up the broker, a secure connection is established in which endpoints routing, log and file collection and forwarding for analysis and network and endpoint scans are made available.

Version: 2.6

Platform components:

- Cortex XDR Server
- Cortex XDR Endpoint
- Cortex Broker VM

KEY BENEFITS

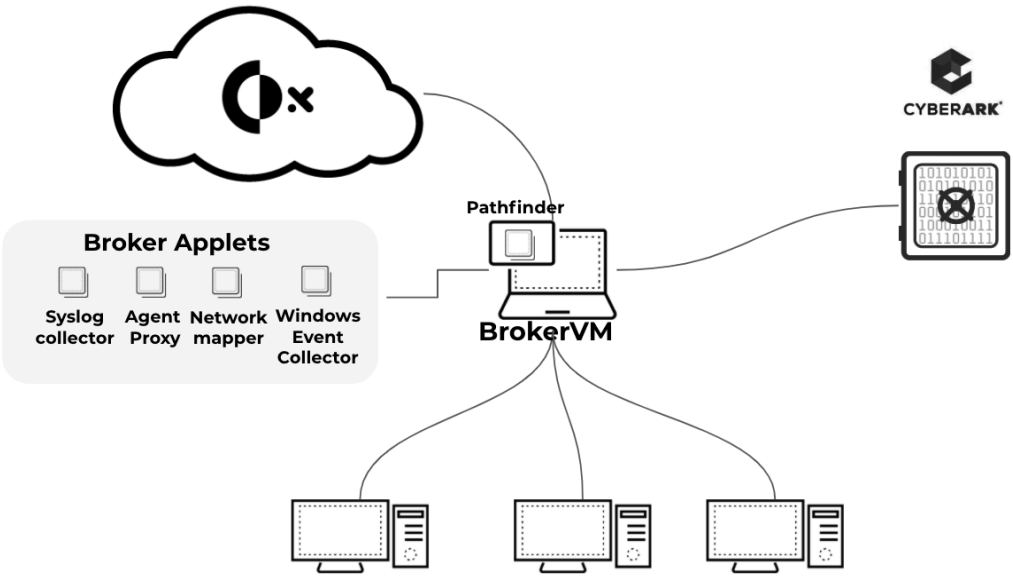
Benefits of Cortex XDR:

- Detect advanced attacks with analytics: Uncover threats with AI, behavioral analytics, and custom detection rules.
- Drastically reduce alerts: Avoid alert fatigue with a unified incident engine that intelligently groups related alerts.
- Investigate faster: Verify threats quickly by getting a complete picture of attacks with root cause analysis.
- Stop attacks without degrading performance: Obtain the most effective endpoint protection available with a lightweight agent.
- Maximize ROI: Use existing infrastructure for data collection and control to lower costs.

Benefits of integrating Cortex XDR with CyberArk AAM:

- Reducing exposure of sensitive organizational information to multiple interfaces

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION



The Pathfinder applet on the Broker VM integrates with CyberArk AAM to acquire credentials when it needs to interact with endpoints.

AAM INTEGRATION

- The AAM integration is part of the Pathfinder applet, running on the Broker VM.
- The broker VM is a secured virtual machine (VM), integrated with Cortex XDR, that bridges the local customer network and Cortex XDR.
- Pathfinder is an applet running on the broker VM, that deploys a non-persistent data collector on network hosts, servers, and workstations that are not managed by a Cortex XDR agent. The collector deployment is triggered when an unmanaged host was part of a security event seen on XDR. This method provides additional visibility into unmanaged endpoints and enhances investigation tools.

CREDENTIAL RETRIEVAL

- When Cortex XDR decides that a data collector should be deployed on a host, it triggers a request for the Pathfinder applet that is running on the Broker VM. The Broker VM is deployed within the customer's network and has access to the hosts.
- When Pathfinder is configured to use CyberArk AAM as the credentials provider, it queries the AAM API for the credentials to use to access a host.
- When the credentials are no longer in use, they are discarded. Pathfinder keeps the credentials only in memory for the time it needs to access a host.
- The certificate that is used for CyberArk AAM authentication is stored encrypted in Broker VM's database.

- Pathfinder supports only Windows hosts.

REQUIREMENTS

- Cortex XDR Pro per EP or XDR Pro per TB license
- Activated XDR tenant
- Activated Broker VM
- Activated Pathfinder applet on the VM

AAM INSTALLATION

Refer to the “Credential Provider Implementation Guide” for CyberArk Agentless installation and configuration.

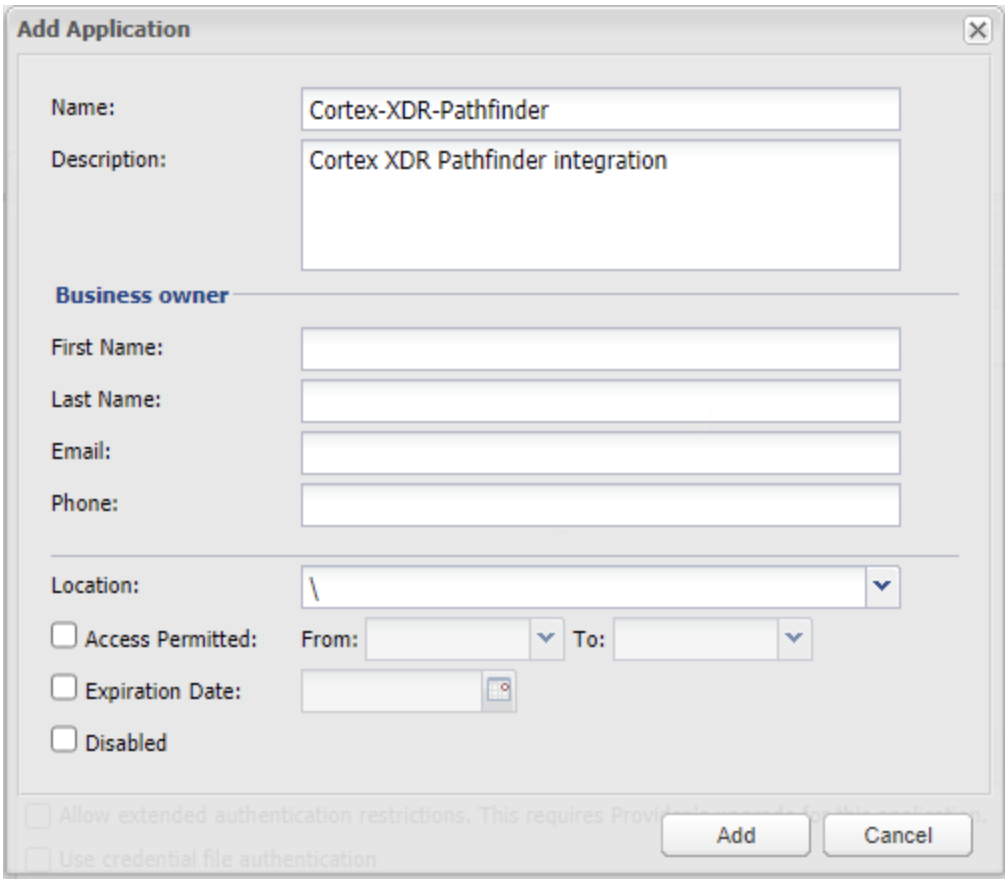
AAM CONFIGURATION

The following sections provide details on Cortex XDR Pathfinder configuration with CyberArk AAM.

DEFINING THE APPLICATION ID (APPID) AND AUTHENTICATION DETAILS

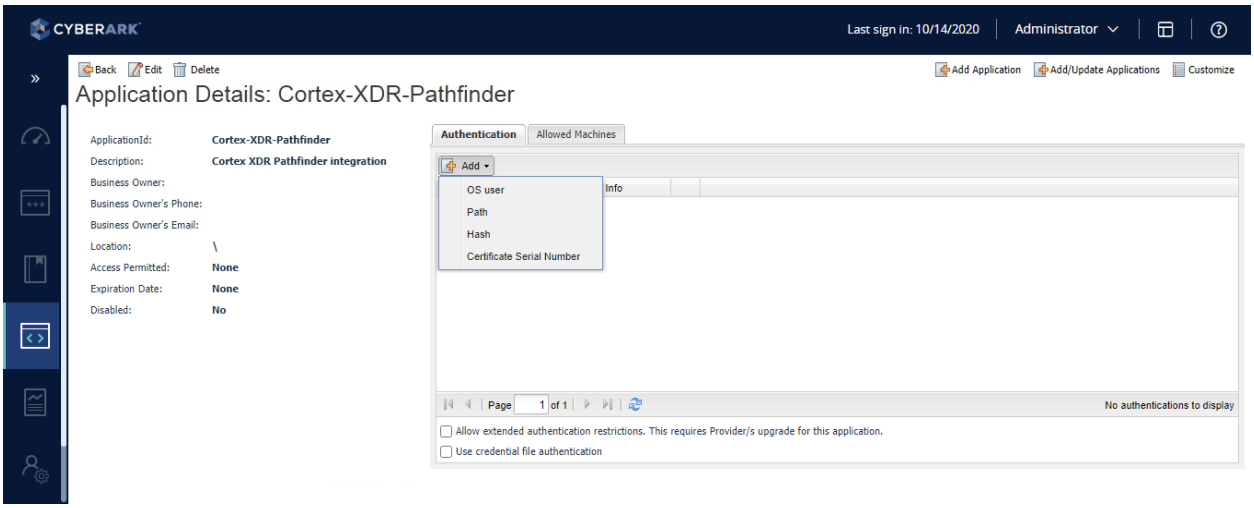
To define the application, define it manually through the CyberArk Password Vault Web Access (PVWA) interface:

- Log in as user allowed to manage applications (it requires Manage Users authorization)
- In the Applications tab, click **Add Application**. The Add Application page appears.

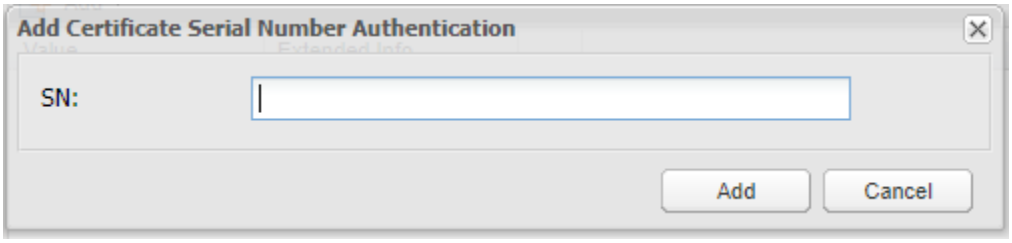


- Specify the following information:
  - In the **Name** box, specify the unique name (ID) of the application. The recommended Application ID for this integration is: Cortex-XDR-Pathfinder
  - In the **Description** box, specify a short description of the application that will help you identify it.
  - In the **Business owner** section, specify contact information about the application's business owner.
  - In the **Location** box, specify the location of the application in the Vault hierarchy. If a location is not selected, the application will be added in the same location as the user who is creating this application.

- Click **Add**. The application is added and is displayed in the Application Details page.



- Check the **Allowing extended authentication restrictions** box. This enables you to specify an unlimited number of machines and Windows domain OS users for a single application.
- Specify the application's **Authentication** details. This information enables the Credential Provider to check certain application characteristics before retrieving the application password.
- In the Authentication tab, click **Add**. A drop-down list of authentication characteristics is displayed.
- Select the authentication characteristic to specify.
- Specify the Certificate Serial Number.



PROVISIONING ACCOUNTS AND SETTING PERMISSIONS FOR APPLICATION ACCESS

For the application to perform its functionality or tasks, the application must have access to particular existing accounts, or new accounts to be provisioned in CyberArk Vault.

In the Password Safe, provision the privileged accounts that will be required by the application. You can do this in either of the following ways:

- **Manually** – Add accounts manually one at a time, and specify all the account details.
- **Automatically** – Add multiple accounts automatically using the Password Upload feature.

  For this step, you require the **Add accounts** authorization in the Password Safe.

For more information about adding and managing privileged accounts, refer to **the Privileged Access Security Implementation Guide.**

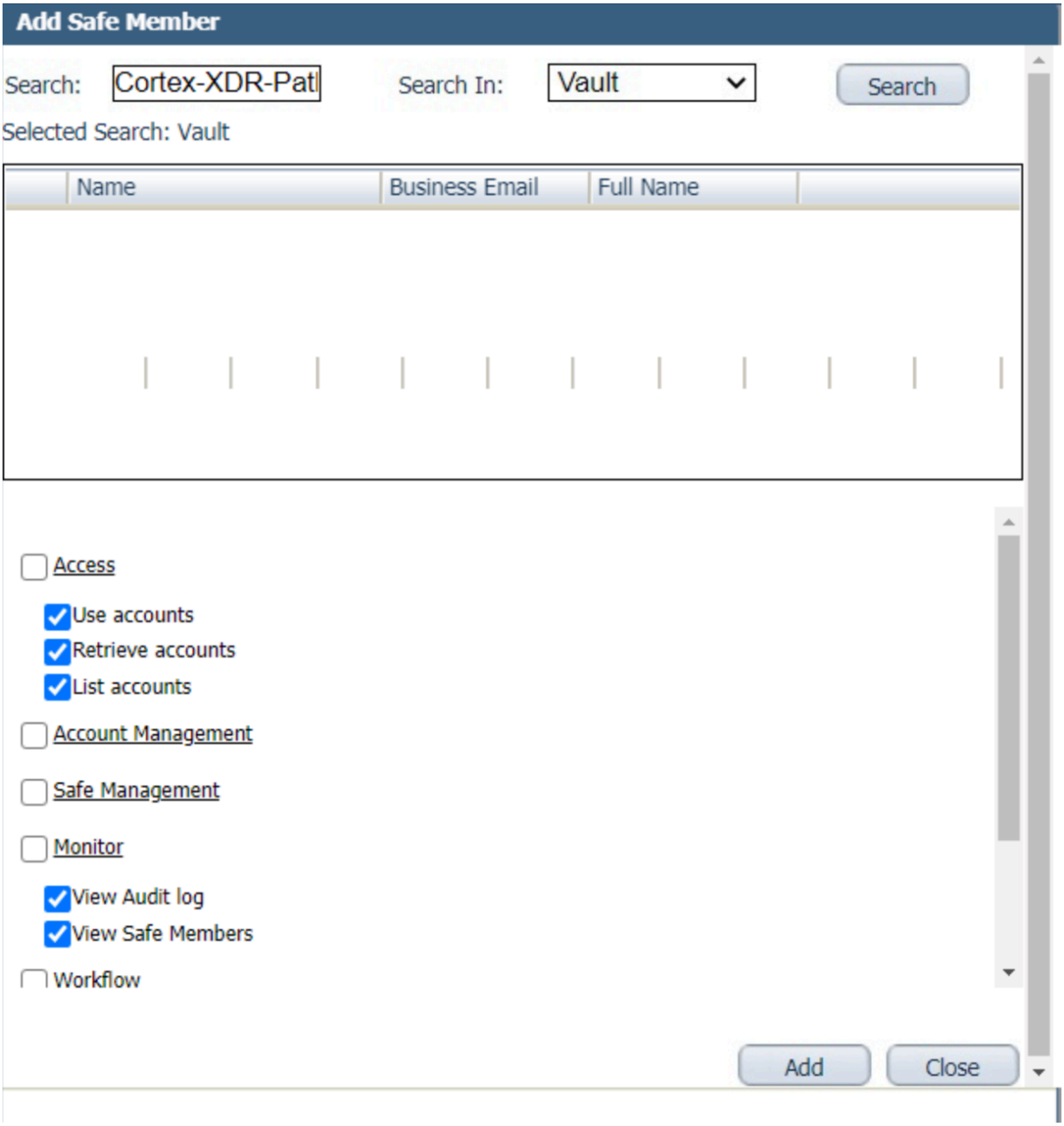
Once the accounts are managed by CyberArk, make sure to setup the access to both the application and CyberArk Application Password Providers serving the Application.

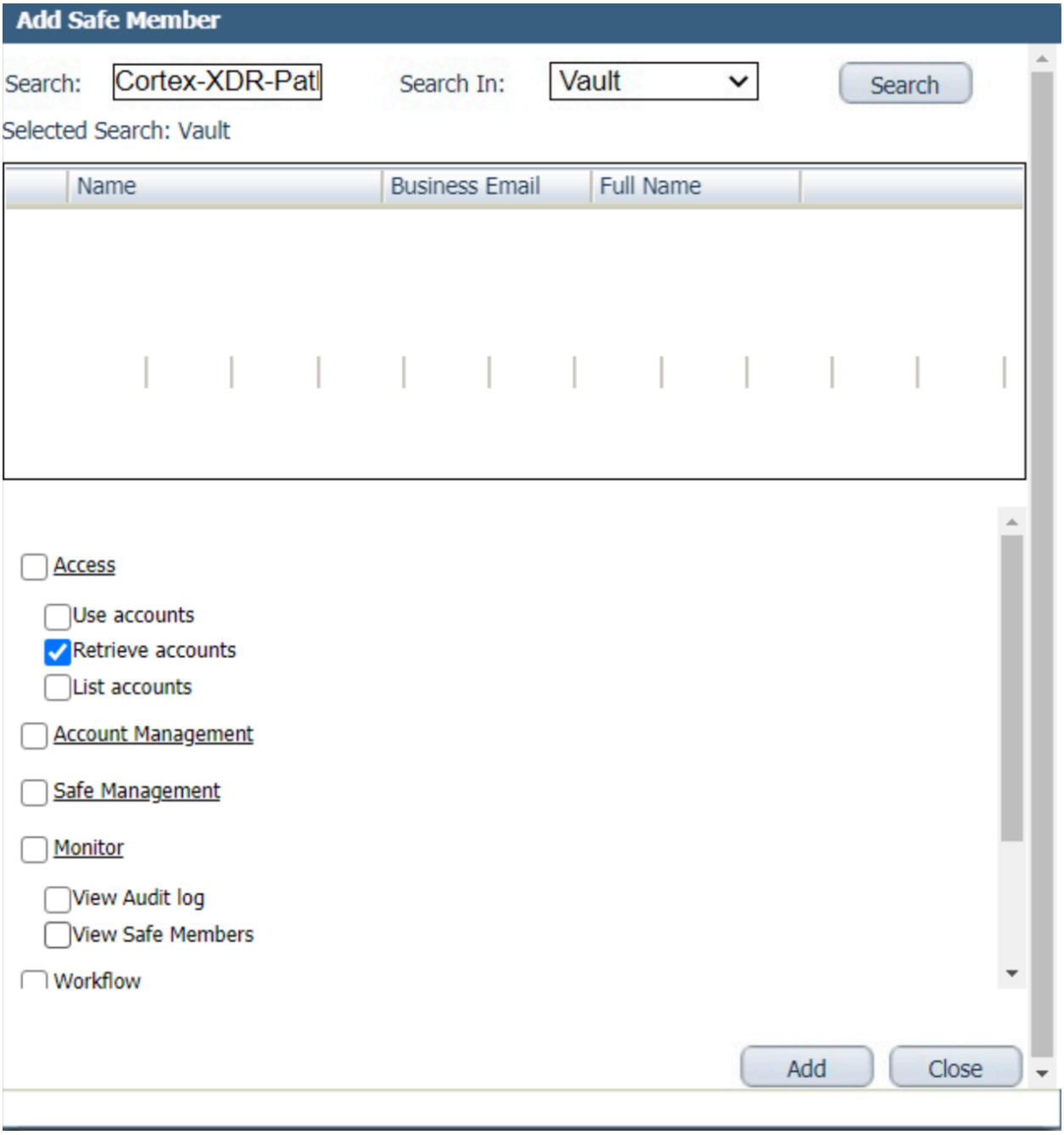
Add the provider user (where the Central Credential Provider is installed) and application users as members of the Password Safes where the application passwords are stored. This can either be done manually in the Safes tab, or by specifying the Safe names in the CSV file for adding multiple applications.

- Add the Provider user as a Safe Member with the following authorizations:
  - List accounts
  - Retrieve accounts
  - View Safe Members

  Note: When installing multiple Providers for this integration, it is recommended to create a group for them, and add the group to the Safe once with the above authorization.

- Add the application (the APPID) as a Safe Member with the following authorizations:
  - Retrieve accounts


Add Safe Member
Search: Cortex-XDR-Patl
Search In: Vault
Search
Selected Search: Vault
Name
Business Email
Full Name
Access
Use accounts
Retrieve accounts
List accounts
Account Management
Safe Management
Monitor
View Audit log
View Safe Members
Workflow
Add
Close



- If the Safe is configured for object level access, make sure that both the provider user and the application have access to the password(s) to retrieve.

For more information about configuring Safe Members, refer to the **Privileged Access Security Implementation Guide.**

CORTEX XDR PATHFINDER INSTALLATION & INTEGRATION CONFIGURATION

Refer to Activate Pathfinder for setup instructions for Pathfinder.

PARTNER CONTACT INFO

Business Contact	Name	Monique Kerstens
	Email	mkerstens@paloaltonetworks.com
	Tel	(408) 706-4733
Technical Contact	Name	Daphna Shemesh
	Email	dshemesh@paloaltonetworks.com
	Tel	+972 (50) 252-0481
Support Contact	Name	Support
	Email	support@paloaltonetworks.com
	Tel	866 898 9087