**Overview**

With the release of CA Privileged Access Manager 2.7, CA PAM now provides more streamlined and enhanced Device and Account discovery within a revamped user interface. This document describes how both features work with detailed steps so that the CA PAM users can quickly learn how they work and use them effectively.

**Device Discovery**

Device Auto-discovery is an alternative to manually adding or importing target devices to the product register on your available network.

1. **Defining and Scheduling a Device Scan**
	* + This new capability will allow you to pre-define the criteria for scanning new devices within your enterprise and bring under the management of CA PAM
	* Specify IP addresses or ranges to include or exclude
	* Specify access methods, services and target applications
	* Create multiple profiles for different sub-nets or areas within your network
		+ Option to automatically bring newly found devices under the management of CA PAM.
		+ Scans can be either *scheduled* or run *“on-the-fly”.*

**Steps to Define a Device Scan**:

* 1. From the homepage, go to ***Devices-> Auto-discovery***
	2. Click on the ***Device Scan Profiles*** tab and Click Add
	3. Enter Profile information
	4. Enter any IP address/ranges or device name inclusions and exclusions
	5. Select/Specify your Access Methods, Services, Device Groups, Tags, Target Applications.
	6. Click on the ***Schedule*** tab and define the frequency of the scheduled scan.
	7. Click Ok



**Steps to Schedule a Scan**:

1. From the homepage, go to Devices-> Auto-discovery
2. Click on the ***Device Scan Profiles*** tab
3. Enter Profile information
4. Enter any IP address/ranges or device name inclusions and exclusions
5. Select/Specify your Access Methods, Services, Device Groups, Tags, Target Applications
6. Click on the ***Schedule*** tab and define the frequency of the scheduled scan.
7. Click **OK**



1. **Running a Device Scan**
	* + We can run a device scan ‘on-the-fly’.

**Steps to Run a Device Scan:**

* 1. Click on the Device Scan Profile tab
	2. Select a Device Scan Profile
	3. Click Run

While running, the scan will show up in the Discovery Jobs tab. When it’s complete you can view the results in the Device Scan History tab.



1. **Bringing Devices Under Management**

The Discovered Devices tab on the Auto-discovery panel displays a list of all devices that it has ever discovered, their Operating Systems, their scan status, and Latest Discovery Time. A checkbox indicates whether CA Privileged Access Manager manages the device.

* + To manage a device, select it by clicking its row or checking the box to the left of its device name. The Manage button above the Is Managed column activates. Click Manage, and answer the dialog box. You can also click the Manage All button to manage all listed devices.
	+ The Export button sends detailed information on each discovered device to a CSV file.
	+ The Update button is active for one device at a time. Click Update to display the Update Discovered Device window.

**Steps:**

1. Click on the ***Discovered Devices*** tab
2. Select which devices you would like to bring under management
3. Click ***Manage***



1. **Viewing and Exporting Device Scan History**

You can view all summary results and scan details from within the Device Scan History tab. From here you can select devices to bring under management, export scan history to CSV files, and view error log messages.

**Steps:**

1. Click on the ***Device Scan History*** tab
2. Double-click on a scan profile and individual scan
3. Select which devices to bring under management, export scan info to CSV or view log messages.

 ****

**Account Discovery**

CA Privileged Access Manager now provides Credential Management Account discovery and registration. Account discovery is an alternative to manually adding or importing target accounts with their associated passwords. In addition, key discovery is also provided, but is limited to reporting discovered keys rather than creation of managed key records. The product supports discovery of Linux, UNIX, Windows Domain Service, and LDAP accounts.

## Account Discovery Prerequisites

Before you perform Discovery, the product needs to know where to look, so target servers need to exist. Applications and administrative accounts need to be provisioned in Credential Manager as target accounts. This administrative account needs to be verified in Credential Manager.

1. Register target servers
2. Register applications

**Application LINUX/UNIX**



**Application Windows**



**Application LDAP**

****

1. Allow Discovery in Accounts

Account properties include a checkbox to indicate that the account is available as a credential for the discovery process. Any accounts that do not have this box checked are not used as credentials for a discovery scan.



**Steps to Create an Account Scan:**

* 1. From the homepage, go to ***Policy->Manage Passwords***
	2. Go to ***Targets->Discovery***
	3. Click on the ***Scan Profiles*** tab
	4. Click ***Add***
		1. Enter Profile Information
		2. Select Servers to include in the scan
		3. Select frequency of the scan
	5. Click ***Ok***

 **Steps to Bring Accounts Under Credential Management:**

1. Go to Targets->Discovery
2. Click on the Discovered Accounts Tab
3. Select the accounts you wish to manage
4. Click Manage



Refer [Account Discovery](https://docops.ca.com/display/CAPAM/Account%2BDiscovery) and [Device Discovery](https://docops.ca.com/display/CAPAM/Device%2BDiscovery) documentation for more information.