



CA-PAM Testing and Configuration Guide

5/8/2017

Rev 1.2

Table of Contents

Introduction.....	3
Assumptions	3
Avaya Products Tested for Login Capability	4
CA-PAM Solution Description.....	6
PIV/CAC authenticated MFA access	6
CA-PAM Password Management and Synchronization.....	7
Installing the CA-PAM client.....	8
Root Accounts	8
The “Config” Account	8
The “Super” Account	8
Accessing CA-PAM.....	11
Configuring CA-PAM.....	13
Adding a CA-PAM Administrators group	13
Adding a CA-PAM Administrative user	15
Adding an HTTP(S) Service for Management of the Target System	18
Adding a Service for Putty SSH	20
Adding a Device	22
Adding a Targeted Application	26
Adding a Targeted Account	28
Adding a Policy	30
Testing the Connections.....	34
Configuring PIV User Login access to CA-PAM	40
Configuring PIV User Access to Target Systems	43
Configuring the Group.....	43
Configuring the Group Policy	45
Appendix A	48
Best Practices for Securing the Target Systems	48
Configuring CA-PAM for ACCCM	49

Introduction

Computer Associates' Privileged Access Manager (CA-PAM) is a product that facilitates secure access control to customer target systems using Multi-Factor Authentication (MFA) by PIV or CAC smart card. CA-PAM is a fully featured and robust secure access control product that can perform many complex functions to enhance an organization's credential security.

This paper is not intended to provide a comprehensive overview of CA-PAM, its architecture or its features and functionality. Instead, this paper is focused solely on one feature that CA-PAM provides, secure credential management of end systems through the enablement of Multi-Factor Authentication (MFA) using customer PIV or CAC smart cards.

Assumptions

This paper is not intended to replace the CA-PAM product documentation that can be found at <https://docops.ca.com/ca-privileged-access-manager/2-8-1/EN>. Please reference the CA-PAM product documentation in order to prepare the items below that are assumed to be in place prior to using this document.

- Assumptions
 - The CA-PAM server (OVA or bare-metal) has already been installed and configured with at least one administrative super user that can configure the CA-PAM system, is on the network and is verified to be communicating on the network
 - The required x.509 certificates reflecting the customer's PKI infrastructure have been installed to the CA-PAM server and are functional. This includes any and all root and intermediate certificate authority certificates and CRL's, if in use. OCSP is supported by CA-PAM if CRL's are not being used by the customer
 - The privileged end user(s) have a valid PIV or CAC card issued by the customer's PKI with certificate chaining up to the customer's root CA
 - The privileged end user(s) have a USB smartcard reader and the appropriate supplicant middleware installed, the testing achieved in this document used ActiveClient 6.2.0.50 supplicant on a Windows 10 workstation
 - The CA-PAM client has been installed to the CA-PAM Administrator's workstation and access by the administrator has been verified to the CA-PAM and the user has the appropriate rights assigned to manage the CA-PAM server (if using an account other than the "super" user.)

Avaya Products Tested for Login Capability

Testing of CA-PAM took place in February, 2017 at Avaya's Highlands Ranch facility. This testing was focused solely on the ability of CA-PAM to properly login to each of the components below by Web GUI, SSH and/or Thick Client where applicable. Not all products in the list use all of the access methods and these are noted in the table as N/A. There were some systems that were not available or were determined to be a sub-component of another interface that was being tested; those occurrences are noted in the table below.

The version of CA-PAM that was tested at Highlands Ranch was 2.8.1. More recently, the system was upgraded to 2.8.2 to correct a problem with installation of a new perpetual license. Limited spot testing has been performed on 2.8.2 and no issues have been noted.

Once CA-PAM was proven to have successfully logged in to each system via each supported method, no further testing was attempted. ***The testing did not attempt to determine if any configuration problems might be presented by the use of the Chromium browser versus IE, Chrome or Firefox.*** Most systems had no issues; however the following anomalies were noted:

- AES initially had problems with “learning” of the username/password credential fields on the AES Web interface login screen. The AES team has corrected the sign-on web page problem in a patch due for release in AES 6.3.3, SP 8, June 2017. The patch was tested with CA-PAM and the issue has been resolved. This fix will also be applied to future 7.x releases of AES when they become Generally Available.
- ACCCM initially prevented right-clicking on the sign-on web page. This prevented CA-PAM from learning the username/password credential fields. The ACCCM R&D team corrected this by providing a secondary URL to be used. This was tested and validated to work correctly.
 - However, per the ACCCM development team, the only browser that can be used to manage ACCCM is Internet Explorer, for a variety of reasons. This means that the built-in Chromium browser to CA-PAM cannot be used and that a local browser installation on the privileged users' pc must be called by CA-PAM. This calls for different configuration steps than are normally executed in the section “Adding an HTTPS Service” below. The workaround configuration for ACCCM is covered in Appendix A
 - Issues with this approach are:
 - When CA-PAM calls the “default” browser as set on the users' machine, this **may or may not** be IE, it could be Firefox or Chrome
 - When configured to use the browser on the users' pc, CA-PAM cannot pass the credentials to the system transparently and they must be known to the end user and entered manually. This is CA recommendation and there are no known secure workarounds

Table of Tested Systems/Results

Login Capability/Method			
CA-PAM version tested = 2.8.1			
Product/Version	WEB Access	SSH Access	Thick Client Access (requires RDP Jump Box)
AES 6.3.3	PASS – login issue to be corrected in SP8 in June, 2017	PASS	N/A
CM/CMM 6.3.111	PASS	PASS	ASA thick client not available to test, thick clients must use RDP jump box
CM/CMM 7.0.1	PASS	PASS	ASA thick client not available to test, thick clients must use RDP jump box
SMGR 7.0.1	PASS	PASS	N/A
SM 7.0.1	N/A	PASS	N/A
G450	N/A	PASS	N/A
CMS 17.0	N/A	PASS	CMS Supervisor thick client not available to test, thick clients must use RDP jump box
WFO 15.1 QM	PASS	N/A	Thick client not available to test, thick clients must use RDP jump box
WFO 15.1 ACR	PASS	PASS	N/A
WFO 15.1 KMS encryption	unable to test, no system available	unable to test, no system available	unable to test, no system available
WFO 15.1 WFM 12.1	PASS -managed thru QM	PASS -managed thru QM	N/A
WFO 15.1 Speech Analytics Mutare	unable to test, no system available	no system available to test	unable to test, no system available
WFO 15.1 DPA - Desktop Process Analytics	unable to test, no system available	unable to test, no system available	unable to test, no system available
AEP 7.1 EPM	PASS	PASS	N/A
AEP 7.1 TTS Text to Speech	PASS - managed thru EPM browser	N/A	N/A
AEP 7.1 Speech Recognition Mutare	PASS - managed thru EPM browser	N/A	N/A
AEP 7.1 POM - Proactive Outreach Manager	PASS - managed thru EPM browser	N/A	N/A
Meeting Exchange 6.2	no system available to test; VA using different solution for MX	no system available to test; VA using different solution for MX	no system available to test; VA using different solution for MX
AAC8	N/A	PASS	Unable to test; should use RDP jump box w/o issue as CA-PAM cannot interop with the Java browser used by AAC8
ACCCM 7.1.2.2	FAIL – ACCCM requires IE as the browser, this eliminates using the built-in Chromium browser with CA-PAM. Workaround is documented in Appendix A, but it does require that the end user	N/A	N/A

	know the UN/PW credentials to ACCCM in order to input them manually; secondary method is to use an RDP jump box, this also requires the user to know the credentials to the system		
CPOD COM 3.1.2/VPS 1.1.2	PASS	PASS	N/A
CPOD Unisphere EMC 5.3.2	PASS	N/A	N/A
CPOD IPFM 2.1.2	PASS - managed via SMGR	PASS	N/A
CPOD VPFM 2.1.1	PASS - managed via SMGR	PASS	N/A
CPOD PVM 2.1.1	PASS - managed via SMGR	PASS	N/A
CPOD ADS (SAL) 2.1	unable to test, no system available	unable to test, no system available	unable to test, no system available
CPOD Riverbed NLB-RIV	unknown system	unknown system	unknown system
CPOD VmWare vCenter	VmWare is believed to have its own MFA capabilities. Although CA-PAM supports integration with VmWare, configuration is extremely complex and CA recommended either use VmWare native MFA or use a CA-PAM RDP jump box to manage VmWare based systems	N/A	PASS, using Jump Box
CPOD Management Server Console (MSC)	N/A	N/A	PASS

Other Platforms not listed for VA but tested since we had access			
AES 7.0.1	PASS – login issue fixed in SP 4 due April 3, 2017	PASS	N/A
AES 7.1.1	PASS – login issue will be fixed in GA load when released	PASS	N/A
VSP 4K	N/A	PASS	N/A
VSP 7K	N/A	PASS	N/A

CA-PAM Solution Description

PIV/CAC authenticated MFA access

This document describes configuration of CA-PAM to provide Multi-Factor Authentication credential security to Avaya target systems. To provide this functionality, CA-PAM acts as a credential “gateway” between the privileged user’s workstation and the target system that is being managed. CA-PAM is configured with the usernames and passwords for the target system’s management interfaces, these are stored in CA-PAM’s secure vault. The privileged user

authenticates to the CA-PAM server by 2-Factor authentication using their CAC or PIV card. CA-PAM then presents the privileged user with the list of systems that they are authorized to manage as well as the interfaces they are allowed to manage through, such as SSH or Web GUI.

In most cases the username/password credentials are never exposed to the privileged user and CA-PAM handles the authentication to the target system transparently. This greatly enhances the target system's credential security because it limits knowledge of username/password credentials for a given system to a limited subset of individuals. However, for instances in which an RDP jump box must be used for management via a thick client, the credentials for that system must to be known to the user as CA-PAM cannot transparently pass the credentials via RDP. Additionally, testing showed that for ACCCM, the credentials would also have to be known to the user whether it is managed by jump box or via the called local web browser, see Appendix A for more information on ACCCM.

CA-PAM Password Management and Synchronization

If the organization chooses to make use of CA-PAM's password management/synchronization functionalities, then the passwords on the target system can be managed by CA-PAM, effectively ensuring that no individual knows the username/password credentials to the target system. An administrator can then "check out" the password from CA-PAM for a defined period of time if they need to access the target system out of band. The password is automatically expired and replaced with a new password unknown to all. The "check-out" method of providing a password when needed leaves an audit trail behind for non-repudiation that identifies the PIV authenticated user that checked out the password as well as the IP address, timestamp and other information.

Another benefit of this method of credential management is that a system need only be configured with limited accounts for access. For example, 5 privileged system administrators could all use the same "admin" named account via CA-PAM with CA-PAM providing the audit trail for which PIV authenticated user accessed the system and at what time. This reduction in available accounts on a system such as a RedHat Linux system serves to decrease the attack surface of the system and minimize the number of potential entry points that could be exploited by a malicious actor.

NOTE: The password management and synchronization functionalities of CA-PAM described above are an advanced topic and are beyond the scope of MFA and not the subject of this paper. However, it is anticipated that customers may elect to take advantage of this feature of CA-PAM. Please consult with your Avaya or CA representative if you wish to enable this feature.

Installing the CA-PAM client

Root Accounts

CA Privileged Access Manager provides a default 'config' account to access the Configuration settings of the server during initial server installation, and a 'super' account to access the full menu.

NOTE: Server installation and configuration of the network interfaces and other settings for initial CA-PAM provisioning is beyond the scope of this document and product documentation for CA-PAM should be consulted for these procedures. Please consult CA product documentation if further information is needed by referencing *CA Privileged Access Manager -2.8_ENU – Implementing – 20170217.pdf*.

The “Config” Account

The “config” account is used for initial setup of the server.

The “Super” Account

CA-PAM has a preconfigured administrative user account: *super*. The *super* (or root) account has global access to all accessible settings. The *super* account cannot be deleted.

NOTE: While the *super* account appears in the administration user list (Administration Menu: **Users, Manage Users**), the *config* account does not.

The following instructions assume that the CA-PAM server has been successfully installed and network connectivity to it has been established.

1. To install the CA-PAM client, begin by initiating an https session to the IP Address of the installed CA-PAM server using a web browser on the PC that is to have the client installed.

2. The following screen will be presented:

ca technologies CA Privileged Access Manager

Username:

Password:

Authentication Type: Local ▼

Login

This is a test of the warning banner

Download CA PAM Client ▼

- Windows
- Mac OS X
- Linux x86
- Linux x64

Figure 1

3. Select the drop down arrow next to **Download CA PAM Client** and select the OS for the workstation, in this case Windows.
4. After the client downloads, execute it to begin the installation
5. Select the default setting at each prompt during installation
6. Start the client
 - a. The client will automatically check for updates each time it is launched and will download them automatically
7. Restart the client when the update is completed

8. When the client restarts you will be presented with the following screen:

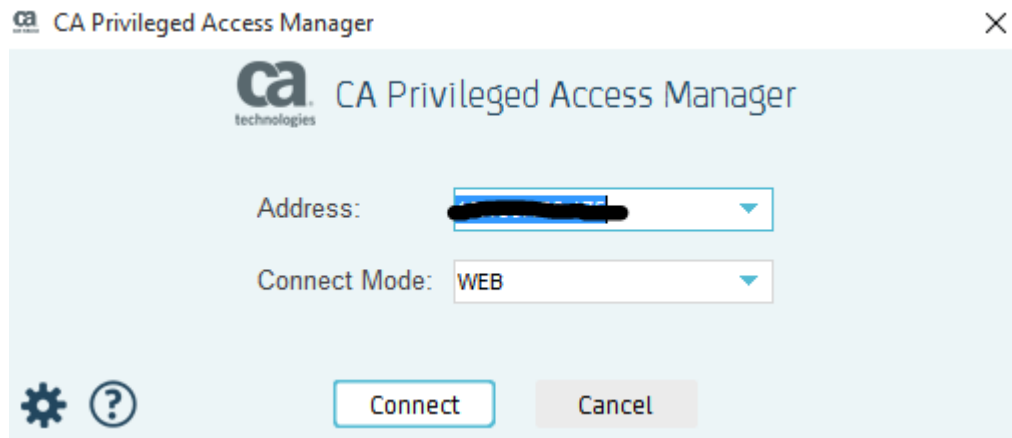


Figure 2

9. Leave the connect mode as **WEB** and press **Connect**
10. If you receive a certificate error that the CA-PAM server certificate cannot be verified, click **View Certificate** and then **Import** the certificate to the workstation's local certificate store
11. Press **Connect**
12. The following screen will be presented:

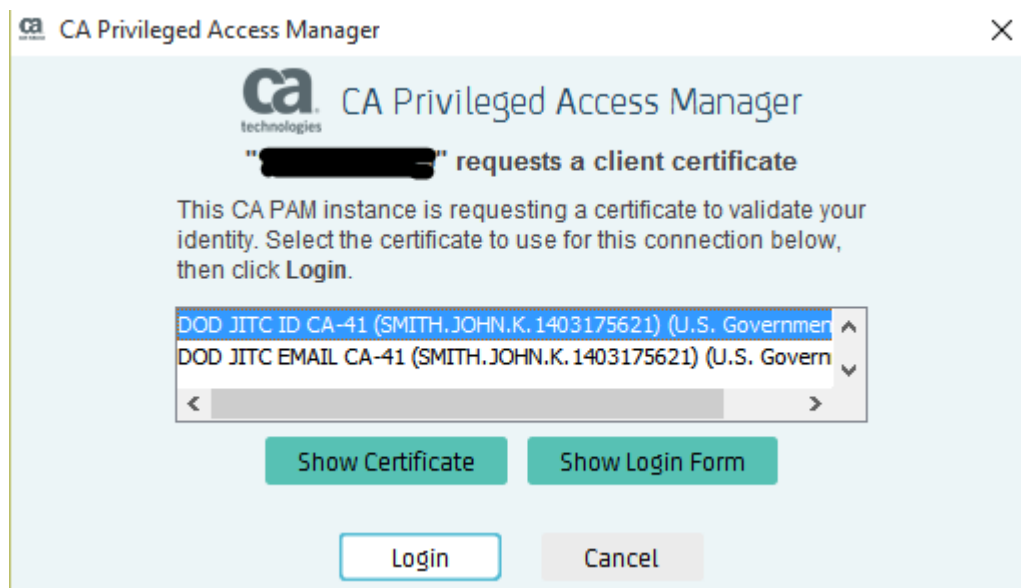


Figure 3

NOTE: The example above shows PIV users that are available on the local workstation to make a connection to CA-PAM with, ignore any PIV users that may appear in the box above at this time

13. Press **Show Login Form** to move to a username/password login page for CA-PAM management, the following screen will be presented:

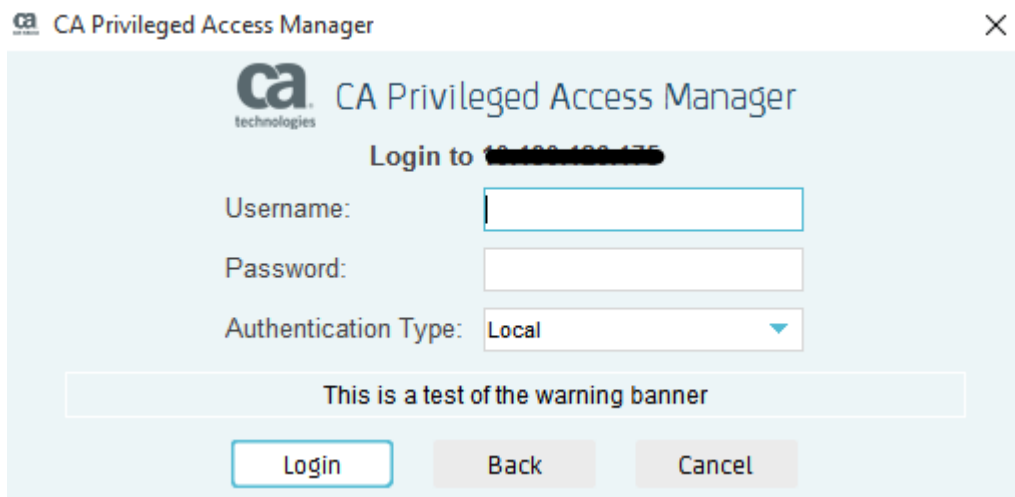
The image shows a screenshot of the CA Privileged Access Manager login window. The window has a title bar with the CA logo and the text "CA Privileged Access Manager" and a close button (X). Inside the window, the CA logo and "CA Privileged Access Manager" are displayed at the top. Below this, it says "Login to 10.100.100.175". There are three input fields: "Username:" with a text box, "Password:" with a text box, and "Authentication Type:" with a dropdown menu showing "Local". Below these fields is a warning banner that says "This is a test of the warning banner". At the bottom are three buttons: "Login", "Back", and "Cancel".

Figure 4

14. During the initial installation of the CA-PAM server the default administrative user “super” was created. Login in as the user “super” with the password of “super.” If you are prompted to change the password, do so now.

Accessing CA-PAM

1. After logging in as the user “super,” you will be presented with the following screen, this screen gives an overall view of system activity and health.

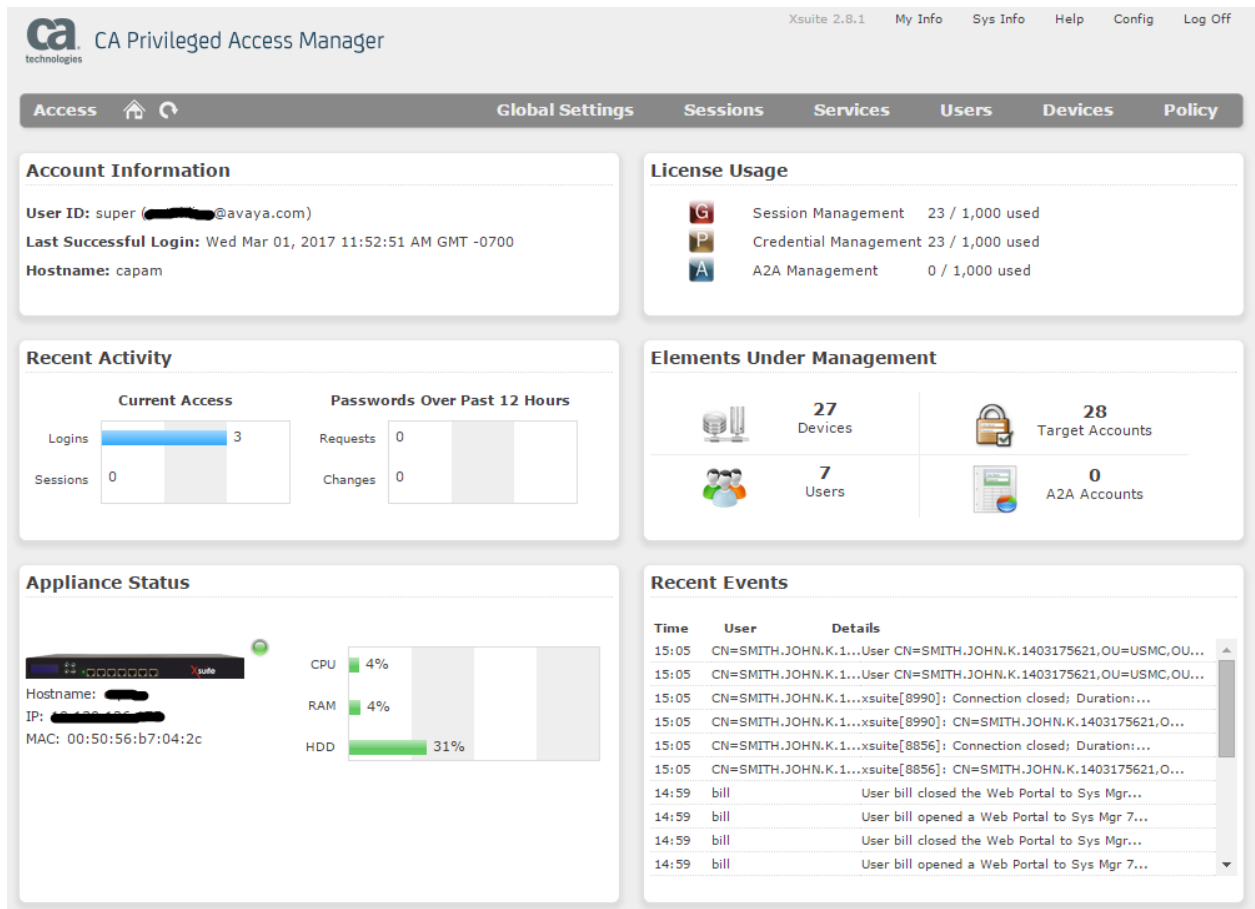


Figure 5

Configuring CA-PAM

Adding a CA-PAM Administrators group

Adding a CA-PAM administrators' group may not always be necessary, but is included here for completeness in the event a customer would like to use it. Please note, group names can be imported from the customers' LDAP, please consult the CA-PAM product documentation as this is beyond the scope of this document.

1. In this step you will create a CA-PAM Administrator's group for easy grouping of all individuals that should have access to CA-PAM configuration settings.

Select **Users** in the grey menu bar at the top and then select **Manage Groups**:

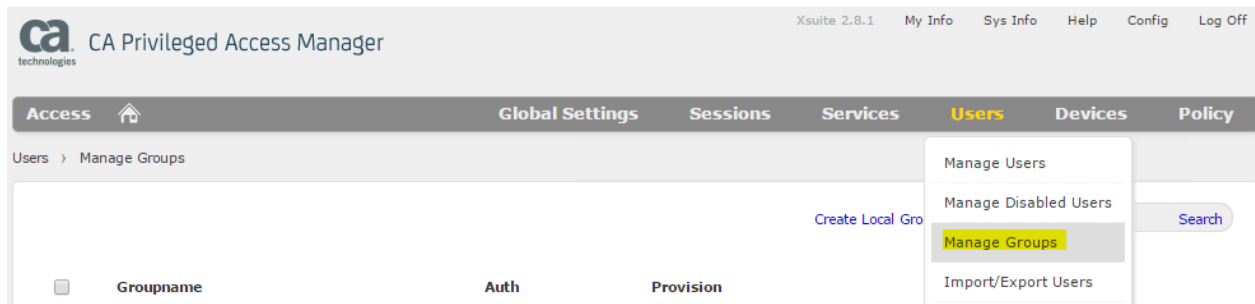


Figure 6

2. This screen will show you the list of configured groups, select **Create Local Group**:

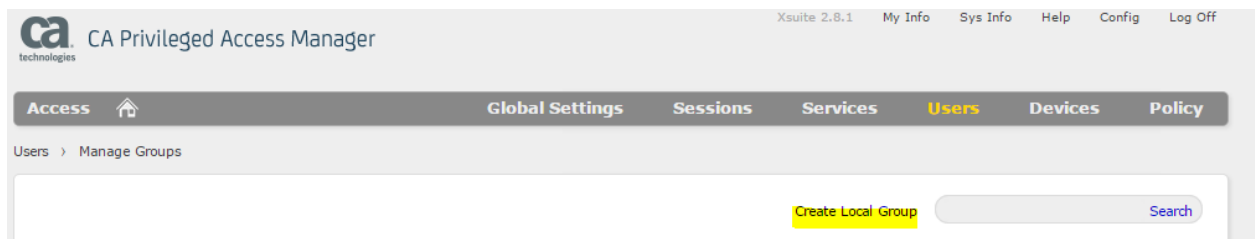


Figure 7

3. You will now be presented the following screen:

The screenshot shows the 'Create Local Group' interface. At the top right, there are links for 'Create Local Group' and 'Search'. Below these are tabs for 'Groupname', 'Auth', 'Provision', and 'Description'. The 'Groupname' tab is active. The form is divided into several sections: 'Basic Info' with fields for 'Groupname', 'Applet Recording Warning' (set to 'No'), and 'Description'; 'Authentication' with a dropdown for 'Authentication' (set to 'Local') and a field for 'Login IP Ranges'; 'Roles' with a dropdown for 'Available Roles' (set to 'Select a Role') and a list of roles including 'Standard User' with a 'Remove' link; 'Access Time' with an 'Add Rules' link; and 'Users' with a large text area. 'Save' and 'Cancel' buttons are located at the top and bottom of the form.

Figure 8

4. In the **Groupname** box, enter a name for the group.
5. Enter a **Description** if desired
6. Set Authentication to **Local**
NOTE: CA-PAM supports SAML as an authentication option. However SAML based authentication is beyond the scope of this document. CA-PAM product documentation should be consulted if required.
7. You may choose to restrict the IP address that a member of the group is allowed to connect to CA-PAM on by adding an IP address or range to the **Login IP Ranges**
 - a. Single IP addresses, CIDR format ranges, host IP ranges and delimiters are allowed, please refer to CA PAM product document *CA Privileged Access Manager -2.8_ENU – Implementing – 20170217.pdf*, page 225 for detailed information.
8. Select a **Role** for this group. In this case we are creating a group for named CA-PAM administrators therefore you should assign the **Global Administrator** role from the drop-down box:

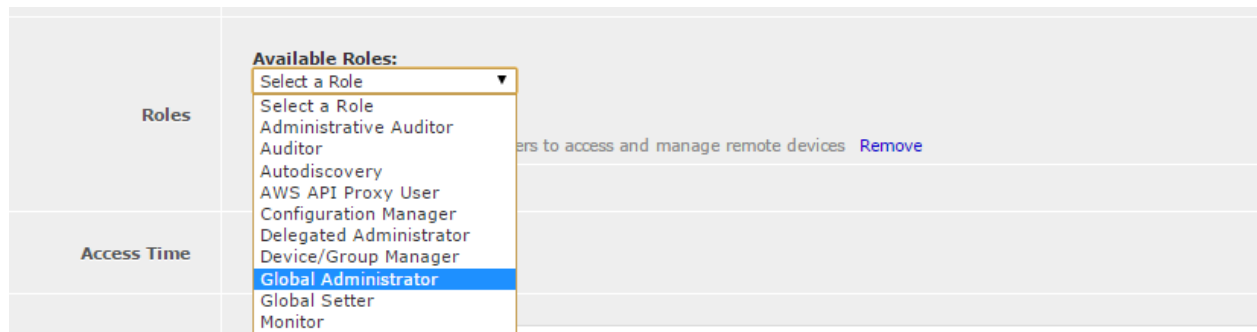


Figure 9

9. If the customer chooses, under **Access Time**, times can be assigned in which the members of the group are allowed to access CA-PAM.
10. Lastly, **Users** can be assigned to this group. At this time, we have not yet made a named user account so this will be blank
11. Click **Save** at the bottom of the screen
12. The group should now appear in the list of groups available

Adding a CA-PAM Administrative user

1. In this step a new user will be added with rights to fully manage and configure the CA-PAM system.
NOTE: This user is not the user that an administrator of an Avaya product will use to manage the Avaya end system.

Select **Users** in the grey menu bar at the top and then select **Manage Users**:

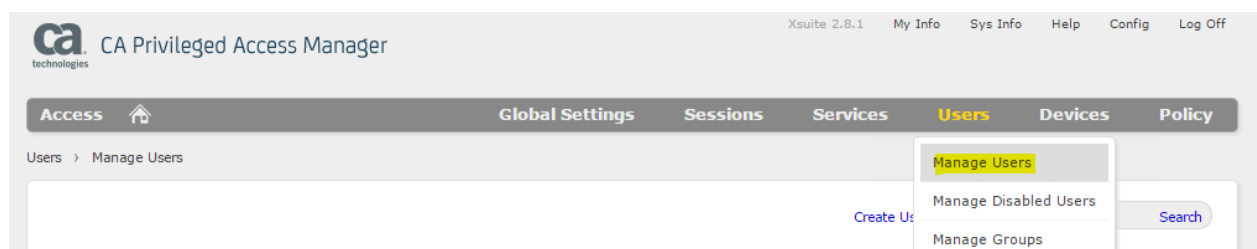


Figure 10

2. This screen will show you the list of configured users, select **Create User**:

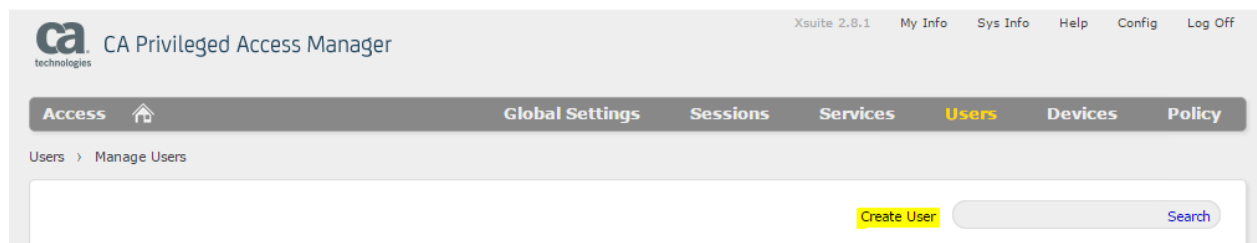


Figure 11

3. The following screen will be displayed:

Basic Info	Username: <input type="text"/> Keyboard Layout: <input type="text" value="AUTO"/> Firstname: <input type="text"/> Lastname: <input type="text"/> Password: <input type="password"/> Re-Password: <input type="password"/> RDP Username: <input type="text"/> Mainframe Display Name: <input type="text"/> Description: <input type="text"/>
Contact Info	Phone: <input type="text"/> Cell phone: <input type="text"/> e-mail: <input type="text" value="ttester@testy.com"/>
Administration	Authentication: <input type="text" value="Local"/> Account Status: <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled Activate Account: <input checked="" type="radio"/> Now <input type="radio"/> Later Terminate Session Upon Account Expiration: <input type="radio"/> Yes <input checked="" type="radio"/> No Account Expiration: Year <input type="text"/> Month <input type="text"/> Day <input type="text"/> Hour <input type="text"/> : Min <input type="text"/> Email on Login: <input type="text"/> Email Self on Login: <input type="checkbox"/> Login IP Ranges: <input type="text"/>
Roles	Available Roles: <input type="text" value="Select a Role"/> Standard User — Allows users to access and manage remote devices Remove View Inherited Roles
Access Time	Add Rules
Groups	Available Groups: <input type="text" value="Select a User-Group"/> <input type="button" value="Add"/> None Selected
API Keys	Create New API Key
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

Figure 12

NOTE: Fields in **RED** are required

4. Enter the **Username**
5. Enter the user's **Firstname**
6. Enter the user's **Lastname**
7. Enter the user's **Password**
8. Re-Enter the user's **Re-Password**
9. If desired, enter a **Phone** and **Cell Phone** number for the user
10. Enter the user's **e-mail** address
11. Select **Local** in the **Authentication** drop-box
 - a. Other methods of Authentication are beyond the scope of this document. Consult CA PAM product documentation for further information

12. Ensure the **Account Status** is **Enabled**
13. Choose to activate the account **Now** or **Later**
14. Enter an **Account Expiration** date and time if desired
15. Enter an email address that will be notified each time this user logs in in the **Email on Login** box
16. If the user should be emailed himself when his account is used to login, check the **Email Self on Login** box
17. You may choose to restrict the IP address that the user is allowed to connect to CA-PAM on by adding an IP address or range to the **Login IP Ranges**
 - a. Single IP addresses, CIDR format ranges, host IP ranges and delimiters are allowed, please refer to CA PAM product document *CA Privileged Access Manager -2.8_ENU – Implementing – 20170217.pdf*, page 225 for detailed information.
18. If the user is to be added as a member of a group, it is not necessary to assign a **Role** to the user. If groups are not being used, then assign a role to the individual user, in this case assign the **Global Administrator** role since we are creating a secondary CA-PAM administrator account.
19. Under **Groups** in the drop-box select the group created in the previous step
20. To verify that the user has in fact inherited the rights from the group, click **Save** then click on the just created user to re-open its configuration
21. Under **Roles** click **View Inherited Roles**

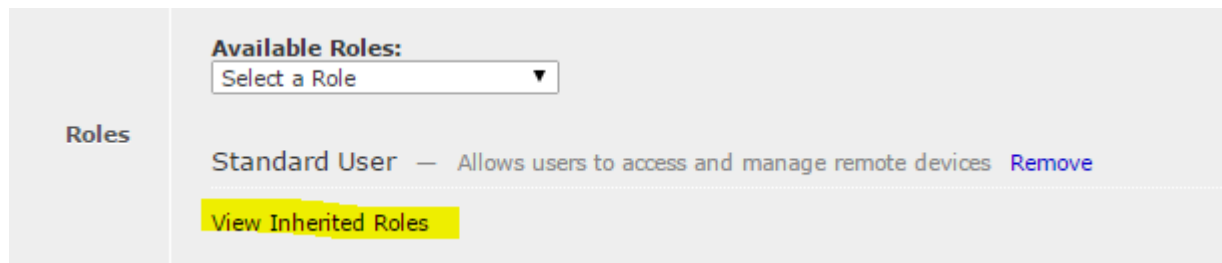


Figure 13

22. The inherited role from the group created previously is now displayed:

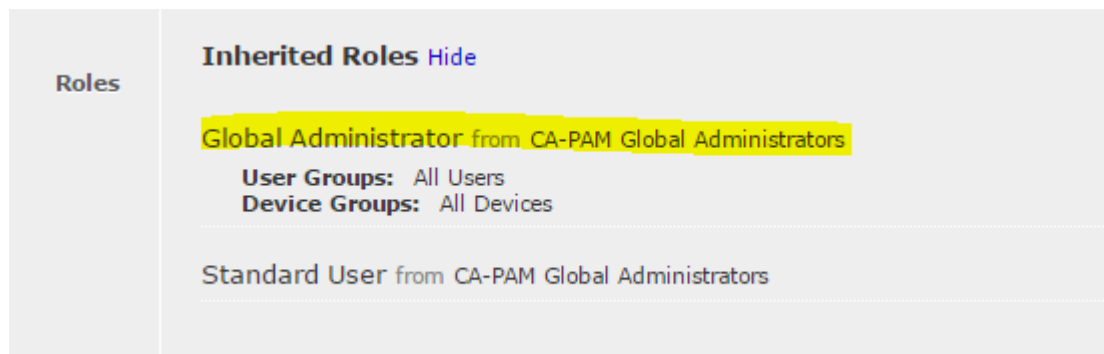


Figure 14

23. Login as the new user and verify that you can view the configuration setting menu items in the grey menu bar:



Figure 15

Adding an HTTP(S) Service for Management of the Target System

If management to the target Avaya system is via a Web GUI, then it is necessary to add an http(s) **Service** by following the instructions in this section. *If http(s) is not going to be used to manage the device, you may skip this section and move ahead to **Adding a Service for Putty SSH**.*

1. Sign in to CA-PAM either as the user *super* or the Global Administrator user that you created in the steps previously. Navigate to the **Services** configuration area of CA-PAM by clicking **Services** on the grey menu bar in Figure 16 and then selecting **TCP/UDP Services**.

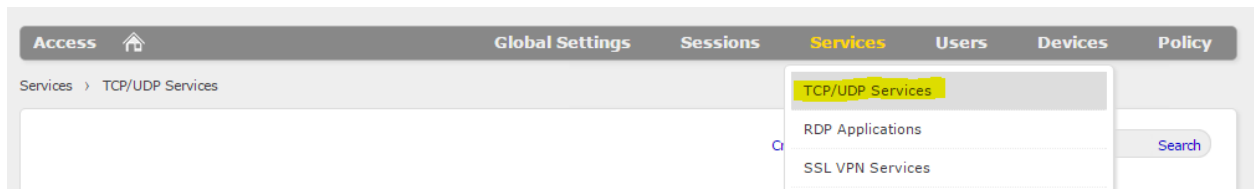


Figure 16

2. Then select **Create TCP/UDP Service**

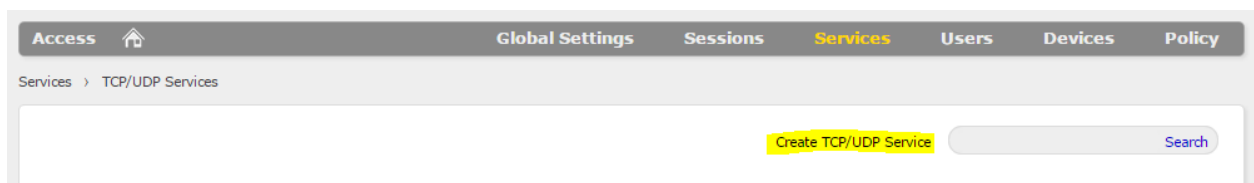


Figure 17

3. The following screen will be displayed:

Save Cancel					
Basic Info	Service Name: <input type="text"/>	Local IP: 127.0.0.1	Port(s): <input type="text"/>	Protocol: TCP ▼	Comments: <input type="text"/>
Administration	Enable: <input checked="" type="checkbox"/>	Show in Column: <input type="checkbox"/>	Application Protocol: Disabled ▼	Client Application: <input type="text"/> Ex. C:\Program\PUTTY.exe -ssh <Local IP> <First Port>	
Web Portal	Launch URL: <input type="text"/> Ex. https://<Local IP>:<First Port>/page.html		Host Header: <input type="text"/>		Hide From User: <input type="checkbox"/>
	Browser Type: Native Browser ▼		Aliases: <input type="text"/> Ex. host1, host2		
Save Cancel					

Figure 18

4. On the screen that is displayed above:
 - a. Enter the **Service Name**, this should be descriptive and include the protocol in the name for easy identification (ie., "SysMgr 7.0.1 https")
 - b. Do not change the local IP from the loopback address that is shown (127.0.0.1)
 - c. Enter the **Port** used to communicate via http(s), using the format Port:Port, you must include the ":"
 - i. The first port listed is the port that CA-PAM will communicate on directly to the end device, for http this is generally port 80, for https this is generally port 443
 - ii. The second port listed can be any random number that is a legal port address, this is used for the internal CA-PAM proxy on the user's pc, **do not leave the second port blank, you MUST enter one; ensure that the port is not already in use by CA-PAM for another service**
 - d. Select the correct **Protocol**
 - e. In the **Application Protocol** pulldown select **Web Portal**

NOTE: At this point a number of boxes may appear/disappear
 - f. In the **Web Portal** section change the **Browser Type** via the pulldown **Xceedium Browser**

NOTE: At this point a number of boxes may appear/disappear
 - g. Ensure that the **Enable** box is checked in the **Administration** section
 - h. In the **Auto-Login Method** pulldown select **Xsuite HTML WebSSO (be careful not to select the "HTTP" option which looks very similar)**

NOTE: At this point a number of boxes may appear/disappear
 - i. In the **Launch URL** box, copy and paste the example just below it, excluding the "page.html" portion

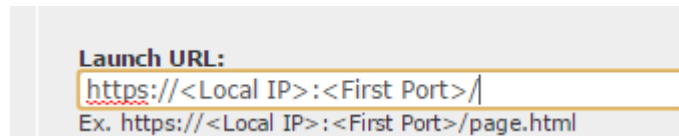


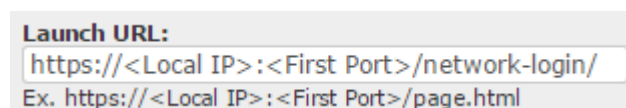
Figure 19

- j. In a separate browser window navigate to the URL of the Web GUI interface of the device that you intend to manage:



Figure 20

- k. Copy the end of the full URL (highlighted above) and paste it onto the end of the **Launch URL** box
 - i. Do NOT insert the actual IP address or the port on this line, they will be auto-inserted by configuration from other screens, leave the <Local IP> and <First Port> tags as they are
- l. When complete the box should look like this:



- m. Un-check the **Route Through Xsuite** box
- n. When finished the screen should appear as below:

The screenshot shows a configuration window for 'SysMgr 7.x https'. At the top, there is a header bar with the service name, port (443:222), status (Yes), protocol (TCP), and local IP (127.0.0.1). Below this are 'Save', 'Cancel', 'Copy', and 'Delete' buttons. The main area is divided into three tabs: 'Basic Info', 'Administration', and 'Web Portal'.

- Basic Info:** Contains fields for 'Service Name' (SysMgr 7.x https), 'Port(s)' (443:222), 'Protocol' (TCP), and 'Comments' (empty text area).
- Administration:** Contains checkboxes for 'Enable' (checked) and 'Show in Column' (unchecked), a dropdown for 'Application Protocol' (Web Portal), and a dropdown for 'Auto-Login Method' (Xsuite HTML WebSSO).
- Web Portal:** Contains a 'Launch URL' field with a template and example, a 'Browser Type' dropdown (Xceedium Browser), checkboxes for 'Hide From User' and 'Route Through Xsuite' (both unchecked), and an 'Access List' text area.

At the bottom of the window are 'Save', 'Cancel', 'Copy', and 'Delete' buttons.

Figure 21

- o. Click **Save**

Adding a Service for Putty SSH

There may be situations in which a privileged user would rather use an SSH client that they are comfortable with using rather than the built-in SSH client inherent to CA-PAM. Many administrators prefer to use Putty for SSH communications and have customized fonts, screen colors and other settings within Putty that they are accustomed to. For these situations, CA-PAM can execute the Putty executable on the user's PC and then act as a proxy between the local Putty and the managed end device in order to keep the secure credential relationship intact.

NOTE: *It is not necessary to create a service for SSH sessions that will use the built-in CA-PAM SSH client. If the customer has no need to use Putty for SSH management, you may skip forward to the section **Adding a Device**.*

1. Repeat steps 1 and 2 from the "Configuring and HTTP/HTTPS Service" section above
2. In the screen that appears, configure per these instructions:
 - a. When entering the **Service Name**, this should be descriptive and include the protocol in the name for easy identification (ie., "SSH via Putty")
 - b. Do not change the local IP from the loopback address that is shown (127.0.0.1)
 - c. Enter the **Port** for SSH communications using the format Port:Port, you must include the ":" (22:4321)
 - a. The first port listed is the port that CA-PAM will communicate on via SSH to the end device, in this case port 22 for SSH

- b. The second port listed can be any random number that is a legal port address, this is used for the CA-PAM internal proxy on the user's pc, **do not leave the second port blank, you MUST enter one**
3. Select the correct **Protocol** if not already selected
4. Ensure that the **Enable** box is checked
5. In the **Application Protocol** pulldown select **SSH**

NOTE: At this point a number of boxes may appear or disappear
6. In the **Client Application** box enter the path to the Putty executable on the end users' PC's

NOTE: All privileged users that use the Putty method of SSH management via CA-PAM will need to have Putty installed in the same path, unless they all have the PATH to the Putty executable set in each pc's environment variables. If environment paths are set, then CA-PAM can then call "putty.exe" and the entire path as shown below does not need to be configured. Otherwise, a service will have to be built for each user that is using a different Putty installation path, this is not recommended as it will lead to unwieldy administration within CA-PAM

 - c. The entire string in the **Client Application** box should be:
 - i. "C:\{path to Putty executable}" -ssh <Local IP> <First Port> -l <username>

NOTE: Include the quotes in the string above to eliminate any problems with whitespace in the path

NOTE: Do NOT insert the actual IP address or the username on this line, they will be auto-inserted by configuration from other screens, leave the <Local IP> <First Port> and <username> tags as they are
7. When finished the screen should appear as below:

AES 7.0.1 SSH		22	Yes	TCP	127.0.0.1
<div>Save Cancel Copy Delete</div>					
Basic Info	Service Name: <input type="text" value="AES 7.0.1 SSH"/>	Local IP: <input type="text" value="127.0.0.1"/>	Port(s): <input type="text" value="22:4321"/>	Protocol: <input type="text" value="TCP"/>	Comments: <input type="text"/>
Administration	Enable: <input checked="" type="checkbox"/>	Show in Column: <input type="checkbox"/>	Application Protocol: <input type="text" value="SSH"/>	X11: <input type="checkbox"/>	Client Application: <input <first="" <local="" (x86)\putty\putty.exe\"="" -ssh="" c:\program="" files="" ip>="" port>"="" type="text" value="\"/> <p>Ex. C:\Program\PuTTY.exe -ssh <Local IP> <First Port></p>
Web Portal	Launch URL: <input type="text"/> <p>Ex. https://<Local IP>:<First Port>/page.html</p>	Host Header: <input type="text"/>	Aliases: <input type="text"/> <p>Ex. host1, host2</p>	Hide From User: <input type="checkbox"/>	Browser Type: <input type="text" value="Native Browser"/>
<div>Save Cancel Copy Delete</div>					

Figure 22

8. Click **Save**

Adding a Device

The next step in CA-PAM configuration is to add the device that is intended to be managed by CA-PAM.

1. On the top grey menu bar, select **Devices** and then select **Manage Devices**

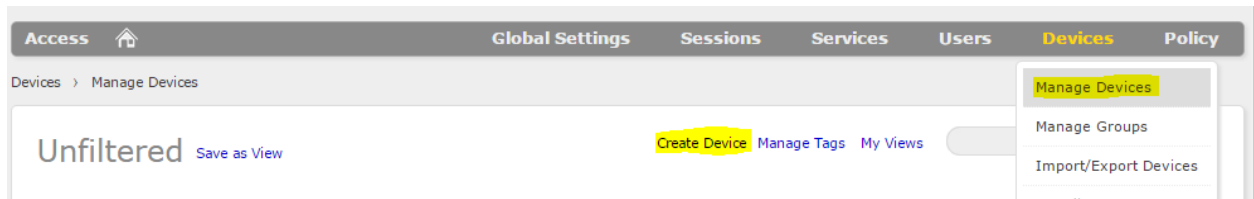


Figure 23

2. Select **Create Device** as highlighted above in Figure 23

3. The following screen will open:

Access [Home](#) Global Settings Sessions Services Users **Devices** Policies

Devices > Manage Devices

Unfiltered [Save as View](#) [Create Device](#) [Manage Tags](#) [My Views](#) [Search](#)

	Name	Address	Location	Description	OS
<div>Save Cancel</div>					
Basic Info	<div>Device Name: <input type="text"/></div> <div>Address: <input type="text" value="Scan"/></div> <div>Operating System: <input type="text" value="Linux"/></div> <div>Location: <input type="text"/></div> <div>Device Type: <input checked="" type="checkbox"/> Access <input type="checkbox"/> Password Management <input type="checkbox"/> A2A</div> <div>Description: <input type="text"/></div> <div>Special Type: <input type="radio"/> Yes <input checked="" type="radio"/> No</div>				
Tags	<input type="text"/> To add a new tag, type it and press Enter				
Access Methods	Add: VNC Telnet SSH Serial Power RDP KVM				
Services	None Selected Add				
Monitoring	Configure Device Monitoring				
Terminal	<div>Term Type: <input type="text" value="vt100"/> Key Mapping: <input type="text" value="xterm-vt220"/></div> <div><input type="checkbox"/> "End" to Select <input type="checkbox"/> Terminal Customization</div>				
Transparent Login	<input checked="" type="radio"/> None <input type="radio"/> sudo/pbrun				
Groups	<input type="text"/>				
<div>Save Cancel</div>					

Figure 24

- Enter the **Device Name**, this should be descriptive and should **not** include any protocols in the name (ie., SysMgr 7.0.1)
- Select the appropriate **Operating System** in the pulldown
- For **Device Type** leave **Access** checked and check **Password Management**
NOTE: Clicking on **Password Management** may cause some boxes to appear or disappear
- Enter the **IP address** of the device to be managed in the **Address** box

Basic Info

Device Name:

Address:

Operating System:

Location:

Save Cancel

Figure 25

- The **Description** and **Location** boxes can be filled in if desired

9. If the device is to be managed by https, then move down to the **Services** section and select **Add**. Then select the https service for the system that was created earlier
10. Move up to the **Access Methods** section
 - a. If the privileged users will use the CA-PAM built-in SSH client, then select **SSH** in this section



Figure 26

- b. The **Access Methods** section should now look like this:

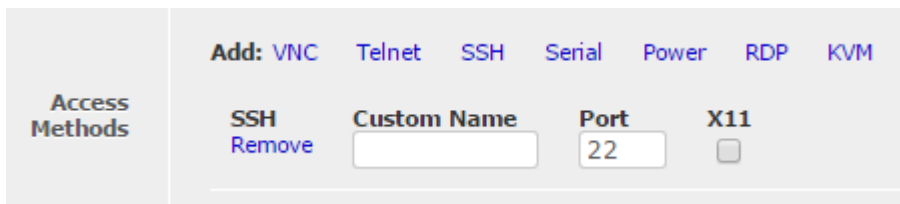


Figure 27

You do not need to fill in the **Custom Name**, only check the **X11** box if X11 forwarding is needed. Configuration of X11 forwarding is beyond the scope of this document.

11. If the privileged users will use their local installation of Putty or other client that was previously configured as a Service, then move to the **Services** section and select **Edit**
- NOTE:** If a previous service has not already been added, then the **Services** section will show **Add** rather than **Edit**. The example in Figure 28 below shows that the https Service for Sys Mgr 7.0.1 has already been added.

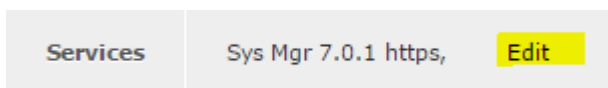


Figure 28

In the dropdown that appears, select the “SSH via Putty” service that was created in the first section above.

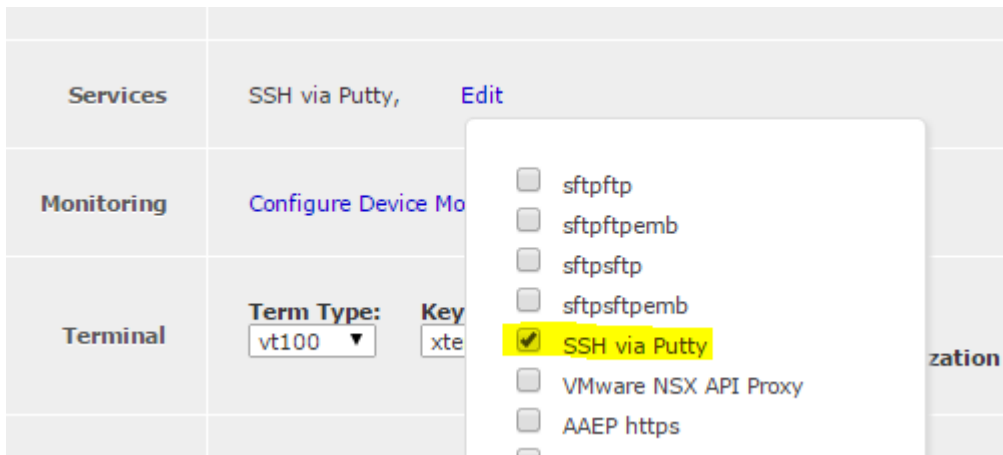


Figure 29

- a. The **Services** section should now look like this:

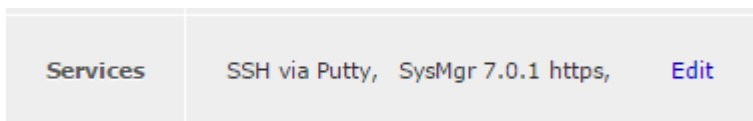


Figure 30

- b. At this point, there is nothing further to configure for **Devices**. Please refer to the CA-PAM official product documentation for information on the **Monitoring, Groups, Terminal** settings and **Transparent Login** options that are available on this screen. Configuration of these items is beyond the scope of this document.
- c. At the bottom of the screen select **Save and Add Target Applications**

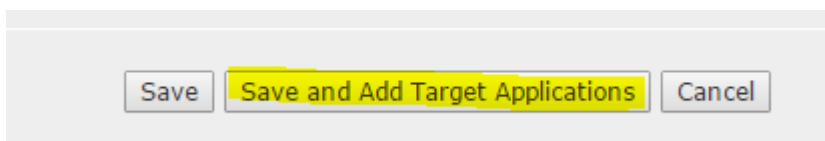


Figure 31

Adding a Targeted Application

Follow the instructions below to add a **Targeted Application**

1. After Step 11c in Figure 31 above you should now be viewing a screen similar to this:

Go to Accounts List

Application List

Show: ☐ All ☐ Filter By: Application Name Search

Displaying 1-15 of 30

Application Name	Application Type	Host Name	Device Name
<input type="checkbox"/> AES 6.3	Generic	[Redacted]	AES 6.3
<input type="checkbox"/> AES 7.0.1 WEB/SSH	Generic	[Redacted]	AES 7.0.1
<input type="checkbox"/> WFO QUALITY	Generic	[Redacted]	WFO QUALITY
<input type="checkbox"/> WFO ACR 15.1	Generic	[Redacted]	WFO ACR 15.1
<input type="checkbox"/> Session Manager 7.x SSH	Generic	[Redacted]	SessMgr7.x
<input type="checkbox"/> Avaya CM 7	Generic	[Redacted]	CM 7
<input type="checkbox"/> Aura Conferencing	Generic	[Redacted]	Aura Conferencing
<input type="checkbox"/> Test RH6.5 SSH	UNIX	[Redacted]	Test RH6.5
<input type="checkbox"/> ACCCM Web	Generic	[Redacted]	ACCCM
<input type="checkbox"/> VSP4K SSH	Generic	[Redacted]	VSP4K
<input type="checkbox"/> VSP7K SSH	Generic	[Redacted]	VSP7K
<input type="checkbox"/> CPOD MSC RDP	Generic	[Redacted]	CPOD MSC RDP
<input type="checkbox"/> CPOD Unishpere Remote EMC Web	Generic	[Redacted]	CPOD Unishpere Remote EMC
<input type="checkbox"/> CPOD COM/VPS SSH	Generic	[Redacted]	CPOD COM/VPS
<input type="checkbox"/> CPOD VPFM	Generic	[Redacted]	CPOD VPFM

Add Delete

Figure 32

2. Select the **Add** button at the bottom right of the screen to add a **Targeted Application**, the following screen is presented:

Go to Accounts List

Application Details

Host Name

Device Name

Application Name

Application Type

Password Composition Policy

Descriptor 1

Descriptor 2

Save Cancel

Figure 33

3. Select the magnifying glass at the end of the **Host Name** box as shown in Figure 33 above. A list of the **Devices** that have been previously configured within CA-PAM are presented. Select the **Device** that was configured in the steps above.

4. The IP address of the device will be populated in the **Host Name** field as well as the **Device Name** that was previously configured.
5. Enter an application name in the **Application Name** box, this should be descriptive such as “Sys Mgr 7.0.1 Web” or “Sys Mgr 7.0.1 SSH”

Application Details

Host Name	<input type="text" value="10.10.10.10"/>	?
Device Name	<input type="text" value="Sys Mgr 7.0"/>	
Application Name	<input type="text" value="Sys Mgr 7.0.1 Web"/>	
Application Type	<input type="text" value="Generic"/>	▼
Password Composition Policy	<input type="text" value="-- None --"/>	▼
Descriptor 1	<input type="text"/>	/
Descriptor 2	<input type="text"/>	/

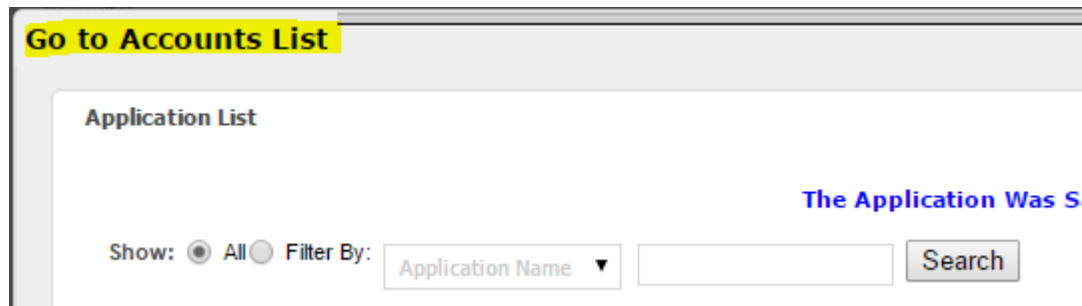
Figure 34

6. Leave the **Application Type** as **Generic**. Setting the application type to a setting such as **Unix** for a Linux based system will enable numerous more options that are beyond the scope of this document. If the customer elects to use the **Password Synchronization** capabilities of CA-PAM, then this setting cannot be **Generic** and a selection must be made. Again, **Password Synchronization** is beyond the scope of this document.
7. If a **Password Composition Policy** (password complexity policy) has been previously created, then you can select it here. Configuration of the **Password Composition Policy** is beyond the scope of this document.
NOTE: If the password complexity policy that is chosen differs from the password complexity policy that is currently configured on the target device, then there will be errors. We suggest that you select **None** here during deployment and initial staging.
NOTE: After deployment, Avaya services may return and setup password complexity policies that mirror that of the target system or may enable and configure **Password Synchronization** if the customer desires.
8. Select **Save**
9. If the system is to be managed by both Web GUI and by SSH **AND** each management method has different login credentials, then you must create a separate **Targeted Application** for each method by repeating the steps above for the 2nd management method. For example, a **Targeted Application** of “Sys Mgr 7.0.1 Web” and “Sys Mgr 7.0.1 SSH.” If the two management methods use the same username and password for access, then you need only create one **Targeted Application** and it could be named “Sys Mgr 7.0.1 Web/SSH” for example.

Adding a Targeted Account

Follow the instructions below to add a **Targeted Account**

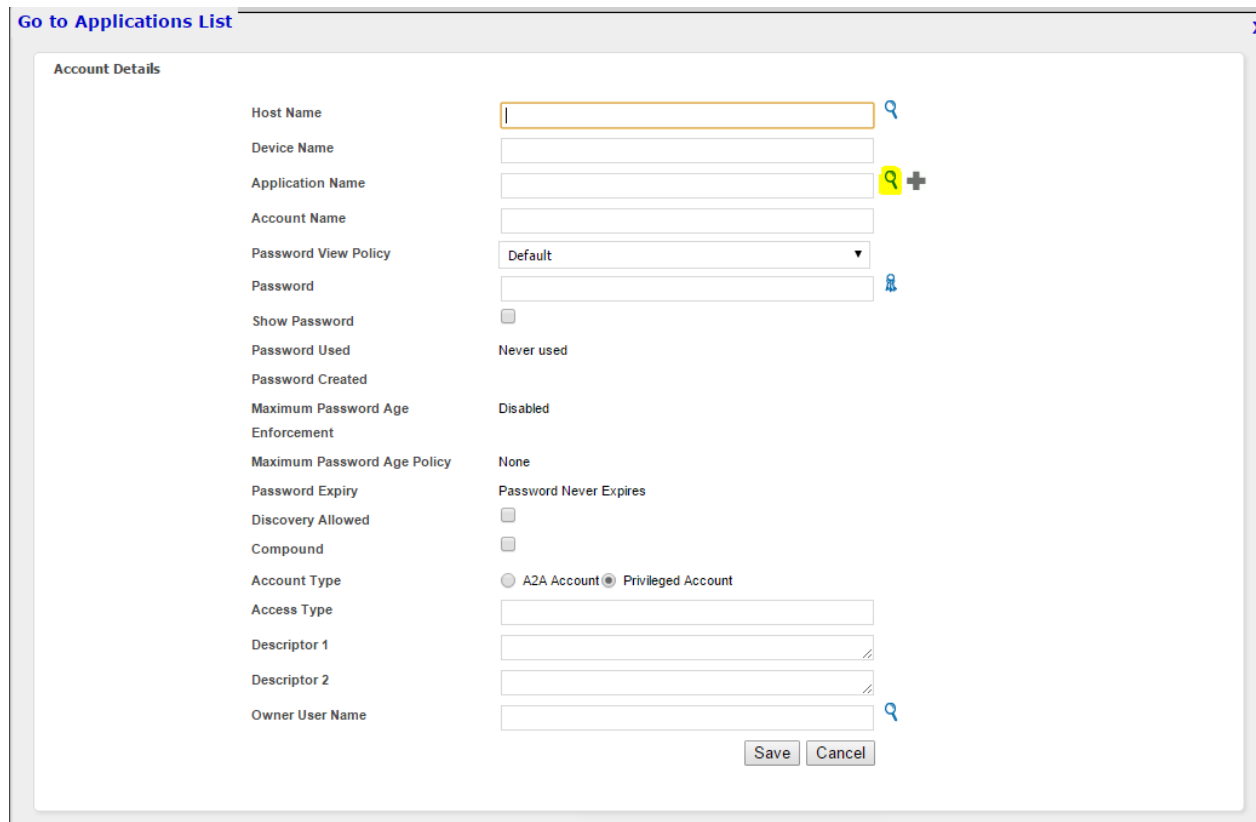
1. From the **Targeted Application** list, at the top left of the screen click **Go to Accounts List**



The screenshot shows a web interface. At the top, there is a button labeled "Go to Accounts List" which is highlighted with a yellow background. Below this, the "Application List" section is visible. It includes a "Show:" section with radio buttons for "All" (selected) and "Filter By:". To the right of "Filter By:" is a dropdown menu labeled "Application Name" and a search box. A "Search" button is located to the right of the search box. Above the search box, the text "The Application Was S" is partially visible in blue.

Figure 35

2. At the bottom right of the screen that is presented, click **Add**
3. The following screen should be displayed:



The screenshot shows a web interface titled "Go to Applications List". Below the title is the "Account Details" form. The form contains the following fields and controls:

- Host Name: Text input field with a magnifying glass icon.
- Device Name: Text input field.
- Application Name: Text input field with a magnifying glass icon and a plus sign.
- Account Name: Text input field.
- Password View Policy: Dropdown menu with "Default" selected.
- Password: Text input field with a magnifying glass icon.
- Show Password: Checkbox.
- Password Used: Text input field with "Never used" as the value.
- Password Created: Text input field.
- Maximum Password Age: Text input field with "Disabled" as the value.
- Enforcement: Text input field.
- Maximum Password Age Policy: Text input field with "None" as the value.
- Password Expiry: Text input field with "Password Never Expires" as the value.
- Discovery Allowed: Checkbox.
- Compound: Checkbox.
- Account Type: Radio buttons for "A2A Account" and "Privileged Account" (selected).
- Access Type: Text input field.
- Descriptor 1: Text input field.
- Descriptor 2: Text input field.
- Owner User Name: Text input field with a magnifying glass icon.

At the bottom right of the form are "Save" and "Cancel" buttons.

Figure 36

4. To the right of the **Application Name** field, select the magnifying glass as shown above in Figure 36
5. This will present a list of configured **Targeted Applications**. Select the **Targeted Application** that was created in the previous step

6. The **Host Name**, **Device Name** and **Application Name** fields will be automatically populated
7. In the **Account Name** field enter the username for the account. If the Targeted Application is the Web GUI interface, then enter the username for the Web GUI, and likewise if the Targeted Application is for SSH.
8. In the **Password** field enter the password for the management interface you are configuring, click **Show Password** to verify it was entered correctly
9. **Password View Policy** is beyond the scope of this document and works in conjunction with **Password Synchronization** if the customer should choose to use it
10. The screen should now look like this:

Figure 37

11. Click **Save**
12. Verify that the **Targeted Account** that you just created is listed in the **Account List** screen
13. Repeat for any additional **Targeted Accounts** that are required, in general there will be one for Web based management and another for SSH based management
14. At the top right of the **Account List** screen, click the blue **X** to exit the screen

Figure 38

15. You will now be returned to the main Devices screen

Adding a Policy

The Policy is what ties together the Service, Device, Targeted Application and Targeted Account. Execute the following steps to create a Policy.

1. In the grey menu bar select **Policy** and then **Manage Policies**

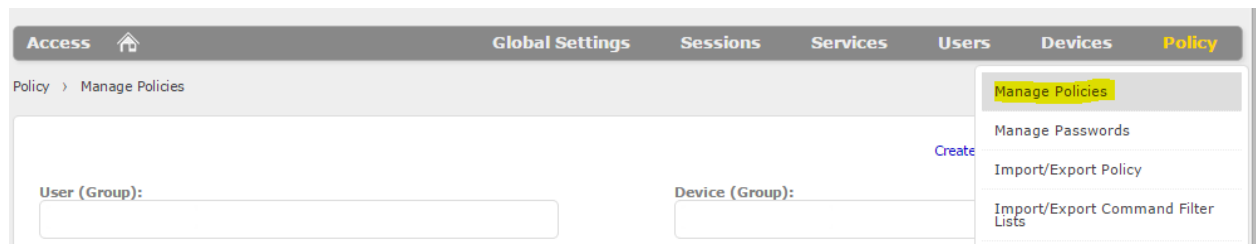


Figure 39

2. Place your cursor in the **User (Group)** field and from the pop-up select the Privileged User or group (if groups are configured) that should have access to the device for management purposes
NOTE: Note it is assumed that users and/or groups have already been created in the CA-PAM system and that PIV enabled users have already been approved for access to CA-PAM. See CA-PAM documentation for further information
3. Place your cursor in the **Device (Group)** field and from the pop-up select the Device that is to be managed via this policy
4. The screen should now look like this:

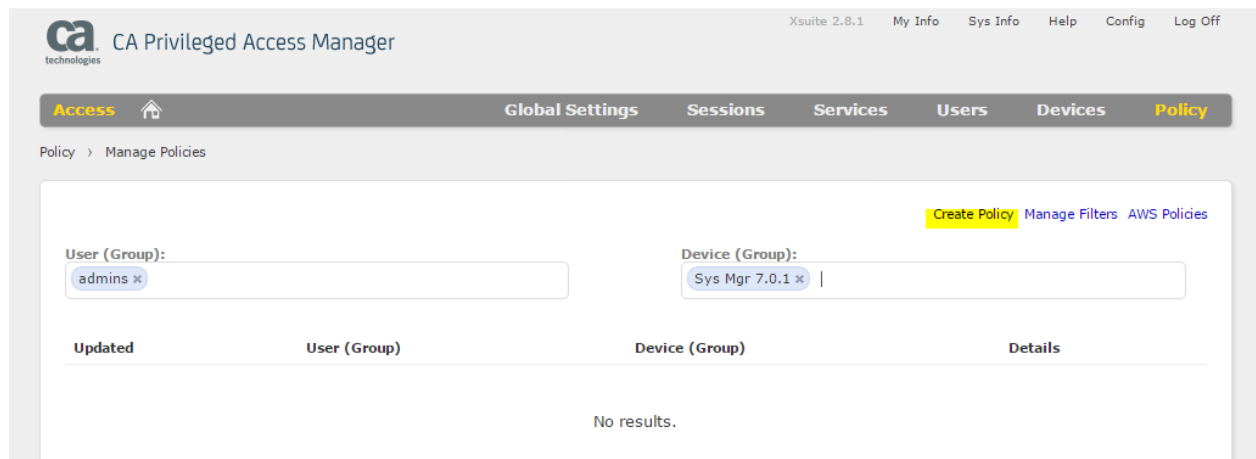


Figure 40

5. Select **Create Policy** as shown in Figure 40 above

6. The screen should now look like this:

The screenshot shows the 'Updated' tab of a policy configuration interface. At the top, there are two dropdown menus: 'User (Group):' with 'admins' selected and 'Device (Group):' with 'Sys Mgr 7.0.1' selected. Below these are 'Save' and 'Cancel' buttons. The main content area is a table with columns: 'Access', 'Services', 'Passwords', 'OOB & Power', 'Filters', 'Recording', and 'CA PAM Server Control'. Each row has a 'None Selected' status and an 'Add' link. The 'OOB & Power' row has checkboxes for 'KVM:', 'Power:', and 'Serial:'. The 'Filters' row has dropdowns for 'Command Filters:' and 'Socket Filters:', and a checkbox for 'Restrict login if agent is not running:'. The 'Recording' row has checkboxes for 'Graphical:', 'Command Line:', 'Bidirectional:', 'Web Portal:', and 'On Violation:'. The 'CA PAM Server Control' row has a checkbox for 'Login Integration:'. At the bottom are 'Save' and 'Cancel' buttons.

Updated	User (Group)	Device (Group)	Details
	admins	Sys Mgr 7.0.1	
Access	None Selected		Add
Services	None Selected		Add
Passwords	None Selected		Add
OOB & Power	KVM: <input type="checkbox"/> Power: <input type="checkbox"/> Serial: <input type="checkbox"/>		
Filters	Command Filters: None Selected <input type="button" value="Add"/> Socket Filters: None Selected <input type="button" value="Add"/> Restrict login if agent is not running: <input type="checkbox"/>		
Recording	Graphical: <input type="checkbox"/> Command Line: <input type="checkbox"/> Bidirectional: <input type="checkbox"/> Web Portal: <input type="checkbox"/> On Violation: <input type="checkbox"/>		
CA PAM Server Control	Login Integration: <input type="checkbox"/>		

Figure 41

7. In the **Access** section, select **Add** and then place a check in the **SSH:22** box if the user is to manage the device using CA-PAM's built-in SSH client
 - a. Click **Edit** and place your cursor in the empty box to the right and select the Application and user/group that appears that matches the SSH login for the system
8. In the **Services** section, select **Add** and then place a check in the box for each service that you wish to enable for users. In this example it could be **SSH via Putty** if the user is to manage the device using their locally installed Putty SSH client using CA-PAM as a proxy or it could be **Sys Mgr 7.0.1 https** if the system is to be managed by the Web GUI, or it could be that the user needs both options
 - a. For each service, place your cursor in the empty box to the right and select the appropriate **Targeted Account** for that **Service**

<div>Save Cancel</div>	
Access	SSH:22 [Sys Mgr 7.0.1 SSH — admin], Edit
Services	SysMgr 7.0.1 https [Sys Mgr 7.0.1 https — admin] SSH via Putty [Sys Mgr 7.0.1 SSH — admin] Edit
Passwords	<div>None Selected Add</div> <div> <input checked="" type="checkbox"/> SysMgr 7.0.1 https Sys Mgr 7.0.1 https — admin ✕ <input checked="" type="checkbox"/> SSH via Putty Sys Mgr 7.0.1 SSH — admin ✕ </div>
OOB & Power	<div> <div>KVM: <input type="checkbox"/></div> <div>Power: <input type="checkbox"/></div> <div>Serial: <input type="checkbox"/></div> </div>

Figure 42

9. **NOTE: IT IS NOT REQUIRED TO ENABLE THE PASSWORDS SECTION UNLESS PASSWORDS ON THE TARGET SYSTEMS ARE INTENDED TO BE MANAGED BY CA-PAM VIA ITS “PASSWORD MANAGEMENT” FEATURE-SET. CONFIGURATION OF THIS PARAMETER PERMITS THE END USER TO VIEW THE USERNAME/PASSWORD CREDENTIALS ON THE HOME ACCESS SCREEN IN THE TARGET APPLICATIONS COLUMN. FOR THIS REASON, IT IS NOT RECOMMENDED TO CONFIGURE THE PASSWORDS SECTION IN BASIC DEPLOYMENTS.**

If you choose to proceed despite the above warning, In the **Passwords** section, select **Add** and then place a check in the box next to each Application

- a. Place your cursor in the empty box to the right and select the appropriate **Targeted Account** for each Application

Services	SysMgr 7.0.1 https [Sys Mgr 7.0.1 https — admin] SSH via Putty [Sys Mgr 7.0.1 SSH — admin] Edit
Passwords	Sys Mgr 7.0.1 SSH [admin], Sys Mgr 7.0.1 https [admin], Edit
OOB & Power	<div> <div>KVM: <input type="checkbox"/></div> <div>Power: <input type="checkbox"/></div> <div>Serial: <input type="checkbox"/></div> </div> <div> <input checked="" type="checkbox"/> Sys Mgr 7.0.1 SSH admin ✕ <input checked="" type="checkbox"/> Sys Mgr 7.0.1 https admin ✕ </div>

Figure 43

10. The screen should now look like this:

Create Policy Manage Filters AWS Policies

User (Group): Device (Group):

Updated	User (Group)	Device (Group)	Details
	admins	Sys Mgr 7.0.1	<div>Save Cancel</div>
Access	SSH:22 [Sys Mgr 7.0.1 SSH — admin], Edit		
Services	SysMgr 7.0.1 https [Sys Mgr 7.0.1 https — admin] SSH via Putty [Sys Mgr 7.0.1 SSH — admin] Edit		
Passwords	Sys Mgr 7.0.1 SSH [admin], Sys Mgr 7.0.1 https [admin], Edit		
OOB & Power	KVM: <input type="checkbox"/> Power: <input type="checkbox"/> Serial: <input type="checkbox"/>		
Filters	Command Filters: <input type="text" value="None Selected"/> Socket Filters: <input type="text" value="None Selected"/> Restrict login if agent is not running: <input type="checkbox"/>		
Recording	Graphical: <input type="checkbox"/> Command Line: <input type="checkbox"/> Bidirectional: <input type="checkbox"/> Web Portal: <input type="checkbox"/> On Violation: <input type="checkbox"/>		
CA PAM Server Control	Login Integration: <input type="checkbox"/>		
<div>Save Cancel</div>			

Figure 44

11. Click **Save**

12. At this point, if you have configured an SSH Service for Putty usage, you must restart the CA-PAM session in order for the CA-PAM SSH proxy to begin listening on the port that you configured as the second port for SSH when you set up the SSH Service.

a. To do this, navigate to the **Access** page on the far left of the grey menu bar by clicking on **Access**

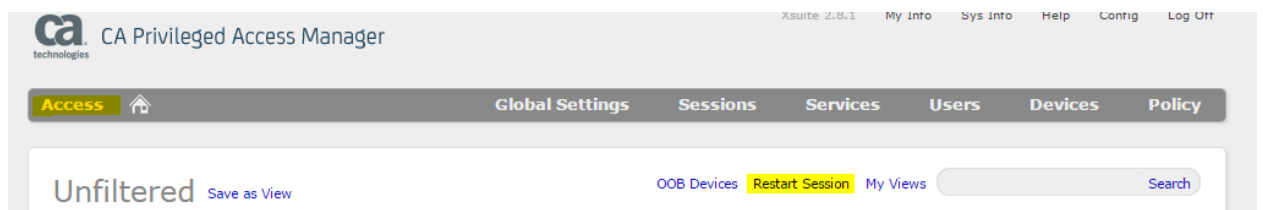


Figure 45

b. Click **Restart Session** just under the grey bar as highlighted in Figure 45 above.

Testing the Connections

1. Now it's time to test the management connections that have been created
 - a. On the **Access** page is a list of all of the systems and access methods for each system that has been configured, the page should look something like this:

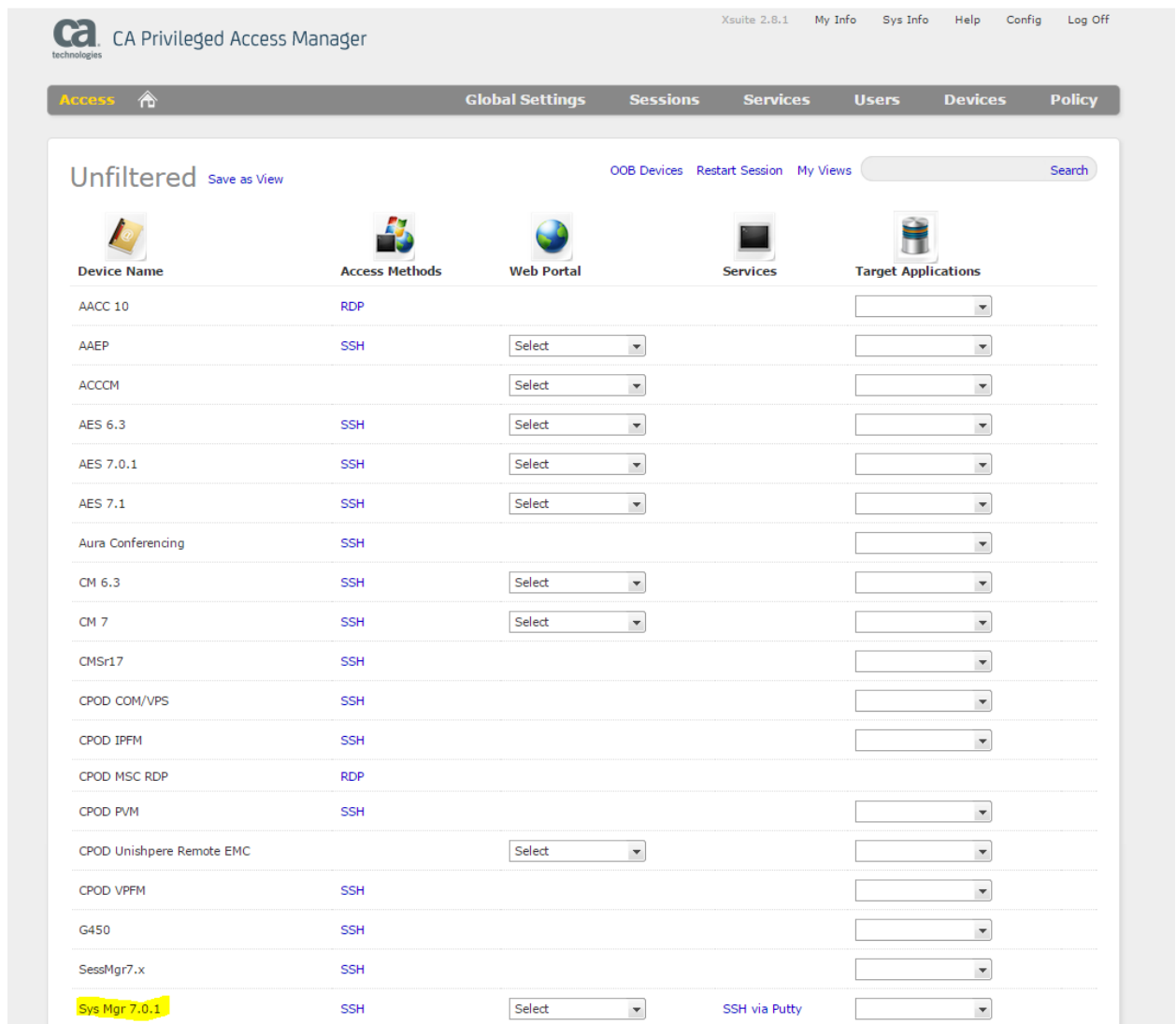


Figure 46

In this example, the Sys Mgr 7.0.1 Device we have setup and the methods of access we have created for it are at the bottom of the screenshot in Figure 46.

- b. Begin by clicking the blue “SSH” link for the Device to make an SSH connection using CA-PAM’s built in SSH client
 - i. The built-in SSH client will start and CA-PAM will pass the credentials assigned to this user to the Avaya server device
 - ii. If the connection fails, double-check that the username/password were entered correctly

1. Navigate to the **Policy → Manage Passwords** screen
2. In the top grey menu bar select **Targets → Accounts**
3. Click the **Account Name** for the account you want to check
4. Click the eyeball to the right of the **Password** field to view the configured password

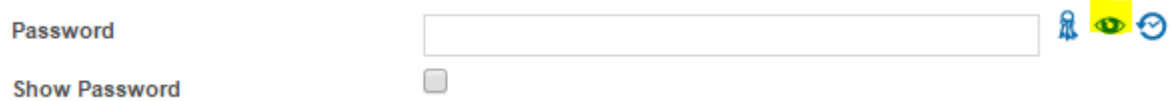


Figure 47

5. You can also use a Putty client to SSH directly to the Avaya device to ensure that the username/password combination are correct
- iii. If the connection is successful an SSH window such as this with a command prompt will open. Please note that the credentials passed to the SSH server are not known to the end user:

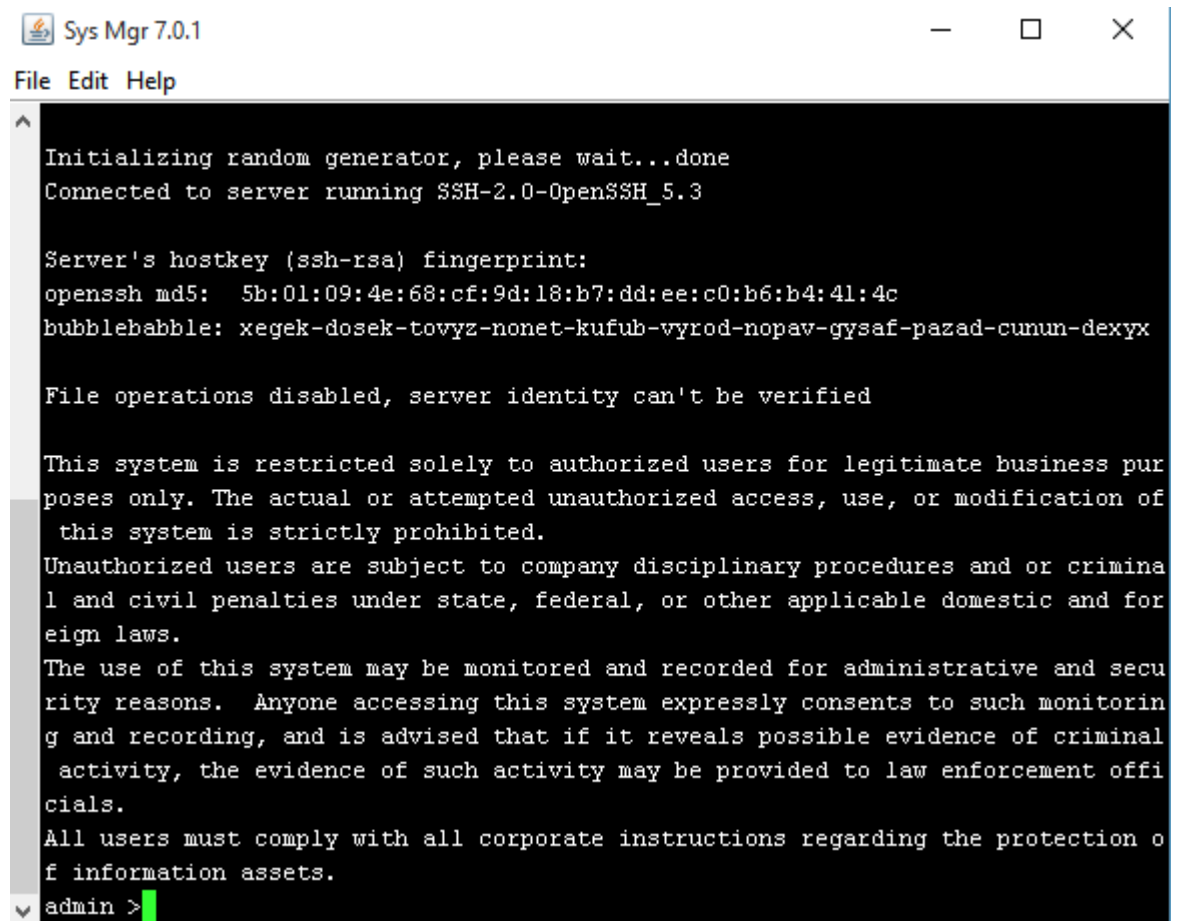


Figure 48

- c. Test the link for **SSH via Putty**
 - i. On the **Access** page, select “SSH via Putty.” Putty will immediately launch with the top bar showing that it is connecting to the CA-PAM proxy that is listening on 127.0.0.1. In the background CA-PAM is passing the credentials to the Avaya end device.

- ii. A successful connection will show a command prompt and the <username>@<system name> at the top left of the Putty window as shown in Figure 49 below:

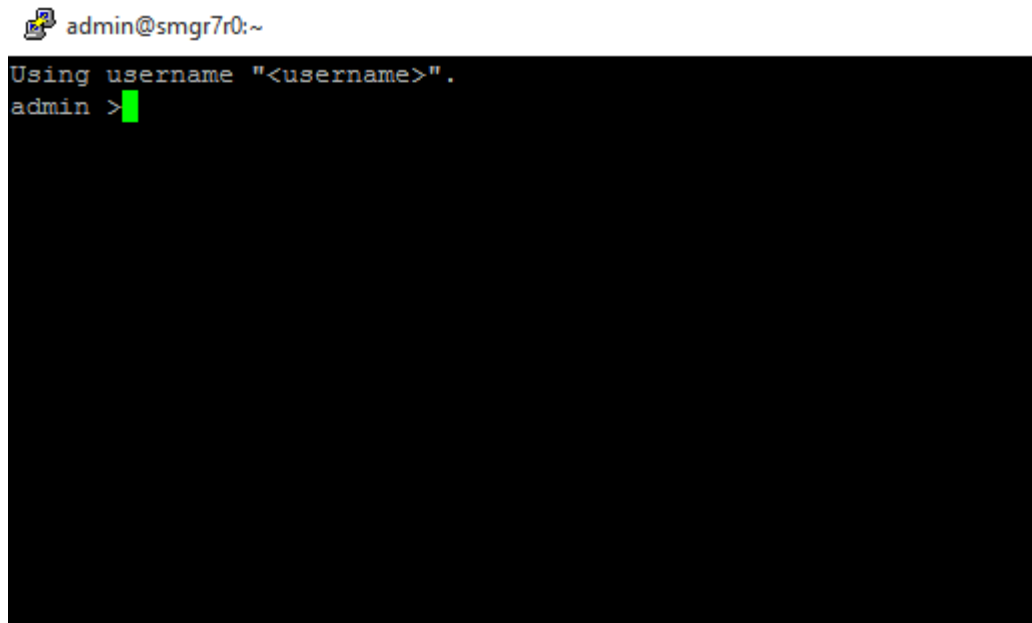


Figure 49

d. Testing the Web GUI interface

In order for CA-PAM to pass the credentials to a web-based login page, it necessary to “teach” CA-PAM which field is to receive the username, password and the submit button.

- i. From the **Access** screen, in the **Web Portal** column open the pulldown and select the **Learn** option:

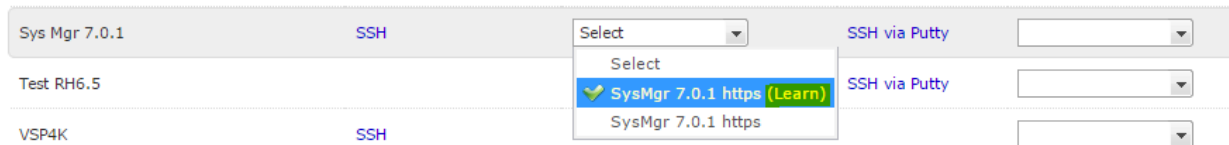


Figure 50

- ii. This will open CA-PAM’s built in browser (Chromium) with the login page of the target system displayed:

System Manager

AVAYA

Aura® System Manager 7.0

Recommended access to System Manager is via FQDN.

[Go to central login for Single Sign-On](#)

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.

This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited.

Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

All users must comply with all corporate instructions regarding the protection of information assets.

User ID:

Password:

Log On

Cancel

[Change Password](#)

Supported Browsers: Internet Explorer 9.x, 10.x or 11.x or Firefox 36.0, 37.0 and 38.0.

Figure 51

- iii. To “teach” CA-PAM the username field, you must right-click in the User ID field and select **Mark Accountname Field**:

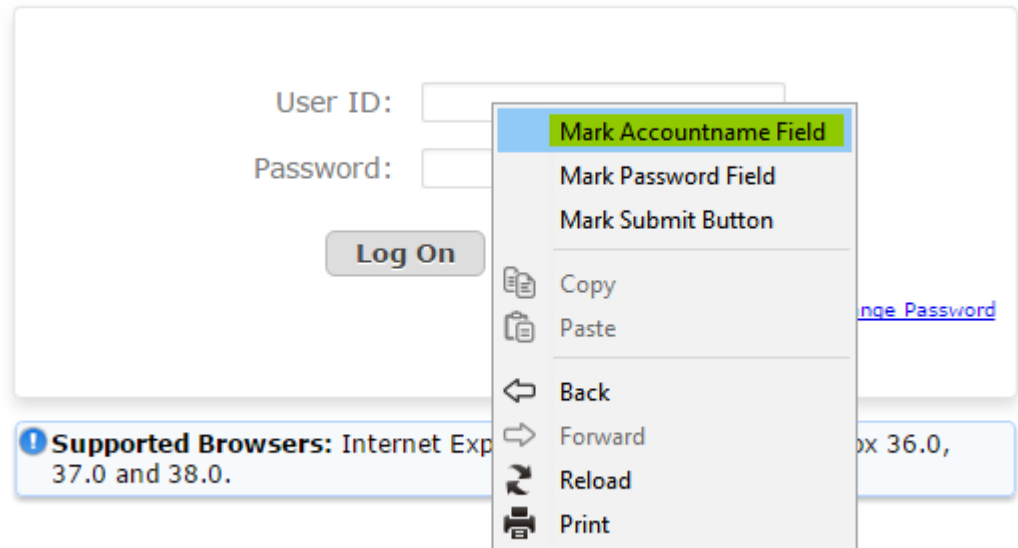


Figure 52

- iv. Repeat by right-clicking in the password field and selecting **Mark Password Field**:

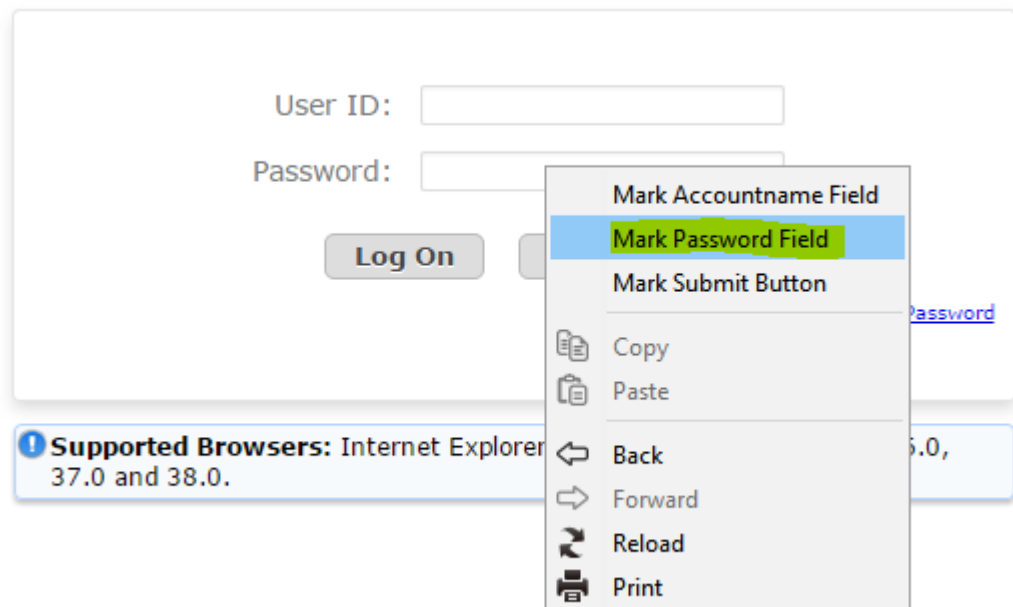


Figure 53

- v. Repeat again by right-clicking on the Log On button and selecting **Mark Submit Button**:

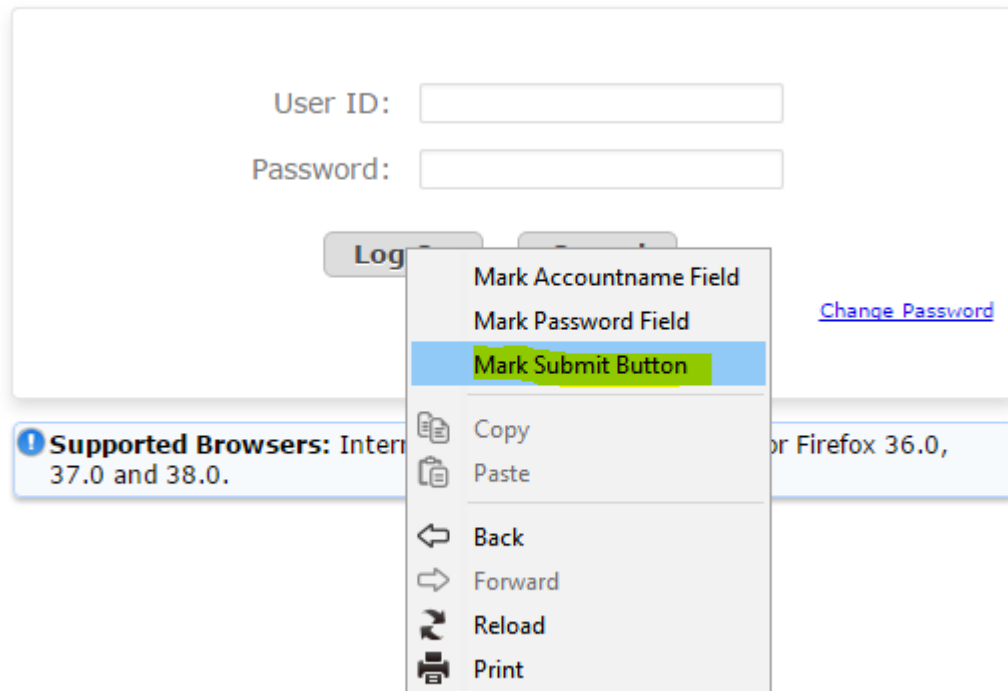


Figure 54

- vi. Click on the save button which is the disk icon in the top right of the screen

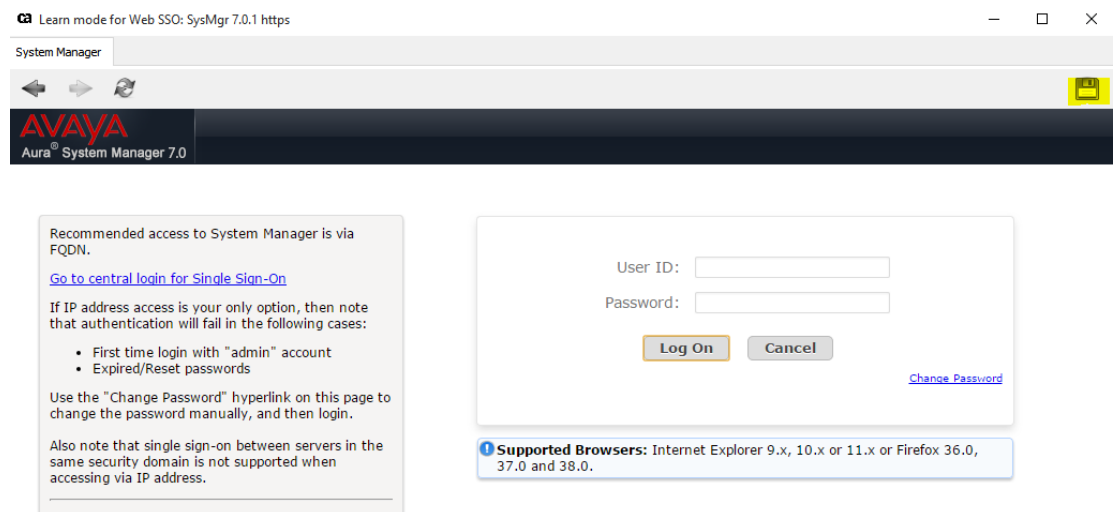


Figure 55

A message stating that the configuration is saved and the browser will close is displayed.

- vii. On the **Access** screen in the Web Portal column for the system, use the pulldown and select the system to open an https session to. Do not select the **Learn** option again.

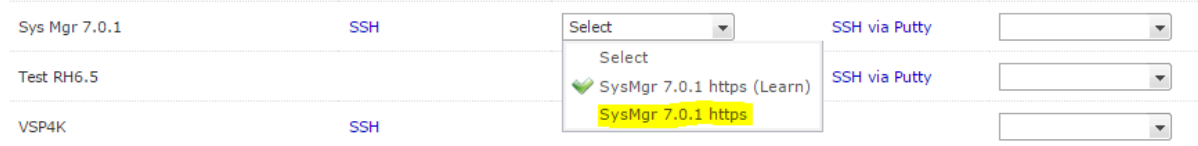


Figure 56

- viii. The CA-PAM browser will now open and a screen advising you to wait while CA-PAM passes the credentials to the target system and logins in is displayed. Upon successful connection, the System Management interface for the system should open as in in Figure 57 below:

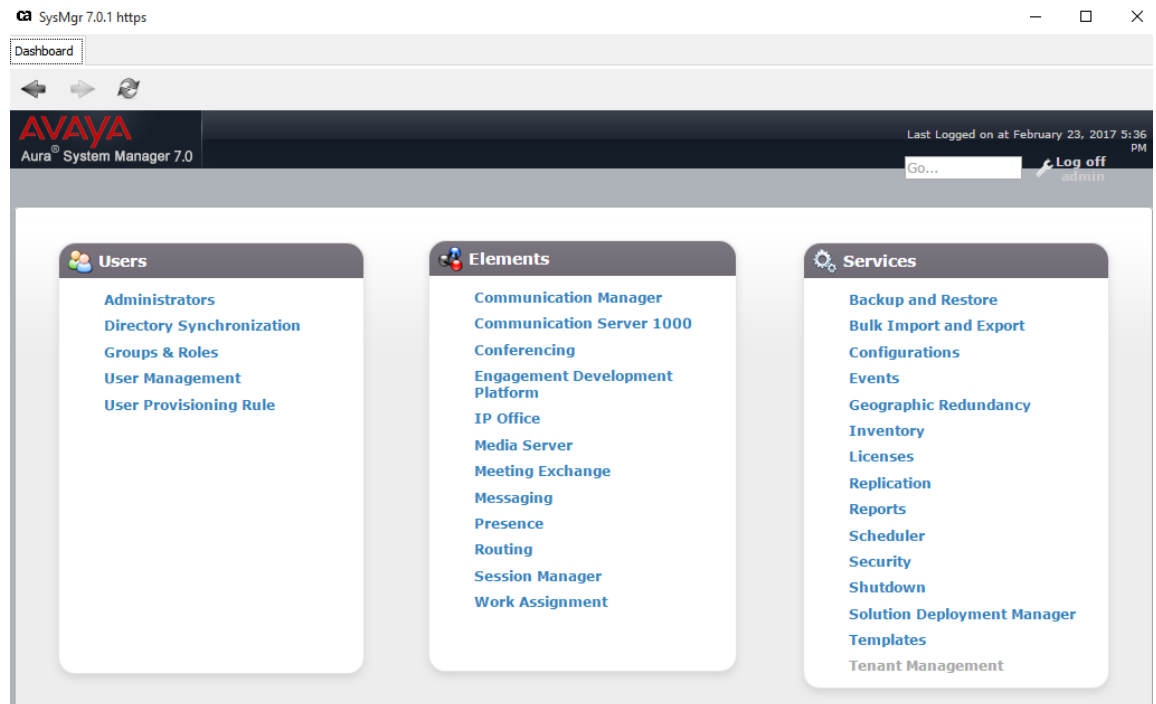


Figure 57

Configuring PIV User Login access to CA-PAM

The primary reason for the implementation of CA-PAM is to provide access to the target devices using Multi-Factor Authentication. Thus far, everything previously has been configured via a 'Super User' non-MFA account. The following steps will describe configuring a PIV-enabled user to access target systems and how to limit the systems and methods that user has access to via group membership and policy.

NOTE: This section assumes that the user has installed the ActiveClient smart card supplicant (or other supplicant) to their pc and has verified that their PIV/CAC card is viewable and the information stored on it can be viewed after entering the card's PIN. In addition the Root CA certificate and any intermediate CA certificates in the chain must be installed to the user's pc certificate store.

1. Launch the CA PAM client per normal with the PIV enabled user's PIV card inserted into the card reader
2. The client will open and display the certificates on the PIV card

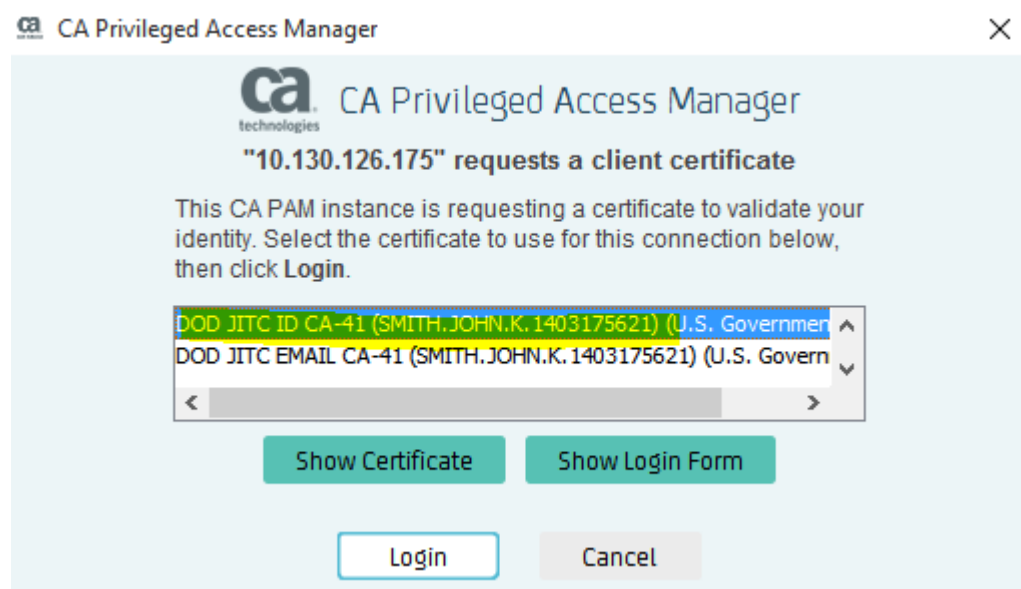


Figure 58

3. Select the proper certificate.
NOTE: Most PIV cards include multiple certificates for multiple usage scenarios. In the example above there is an identity cert and a certificate to be used for email encryption. Please ensure that you select the identity certificate.
4. Select the **Login** button, you will be presented a small window to enter the PIN for the PIV card, enter the PIN and press **OK**

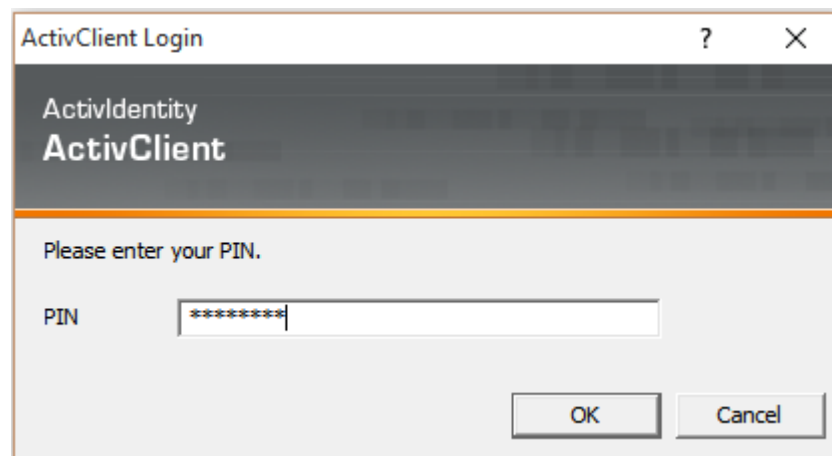


Figure 59

5. The authentication should fail and you will be presented with the following error message.

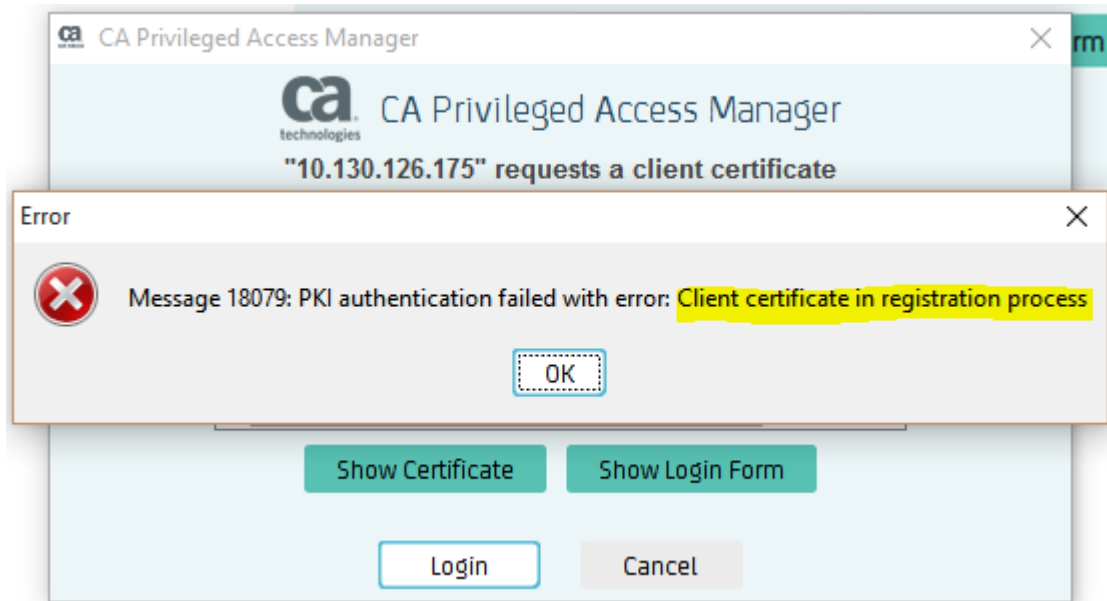


Figure 60

6. The error above is received because the PIV user is unknown to CA-PAM at this point. By attempting to connect this PIV user to CA-PAM, CA-PAM has added this PIV user to a list of users that must be approved for access by a CA-PAM administrator before they are allowed to connect.
 - a. Log in to CA-PAM as the Super User and proceed to **Users** and **Approve CAC User**:

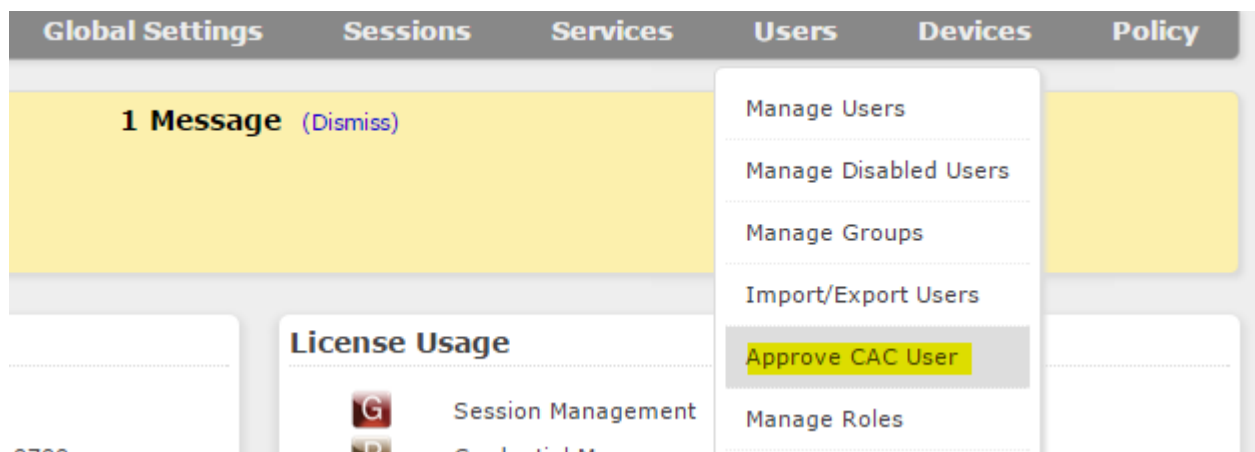


Figure 61

7. In the screen displayed, the PIV user should now be visible in the approval list, select **Approve** and **Update** to approve the PIV user's access to the CA-PAM system.

Delete	Approve	Subject	Subject Alternative Name
<input type="radio"/>	<input checked="" type="radio"/>	CN=SMITH.JOHN.K.1403175621,OU=USMC,OU=PKI,OU=DoD,O=U.S. Government,C=US1403175621117274@mil	

Update Reset

Figure 62

8. Log off of CA-PAM
9. In the CA-PAM client, again select the identity certificate from the PIV card and select **Login** as in step 2 above.
10. Verify that successful login is achieved. **NOTE:** Unless the PIV card has been removed and re-inserted into the card reader, you may not be prompted for the PIN again since the first attempt likely cached it.
11. Because this PIV user is a new user they currently do not have access to manage any target devices via CA-PAM.

Configuring PIV User Access to Target Systems

PIV users are no different than non-PIV users in CA-PAM. Both can be assigned to groups and roles that define their access to the CA-PAM system as well as to the target system and the methods allowed to access them.

Using the PIV user that was approved for access in the preceding section, we will now grant this user rights to manage one of the target systems. This can be done on an individual user basis or can be done via membership in a group. In this example, we will configure a group with permissions to manage a target system and make the PIV user a member of the group.

Configuring the Group

1. Login as the Super User
2. In the grey menu bar navigate to **Users** and **Manage Groups**
3. This presents the list of configured groups, at the top right select **Create Local Group**

Global Settings Sessions Services **Users** Devices Policy

Create Local Group Search

Auth	Provision	Description
------	-----------	-------------

Figure 63

4. Enter a name for the group, in this example **"Sys Mgr 7.0.1"** to identify the group
5. Select a role for members of this group from the dropdown list
 - a. By default the **Standard User** role is applied to this group, it can be removed if desired

- b. For this example we will leave **Standard User** as the role for this group as we do not want members of this group to have access to configuration of CA-PAM itself

Create Local Group Search

Groupname Auth Provision Description

Save Cancel

Basic Info

Groupname: Sys Mgr 7.0.1 Applet Recording Warning: No Description:

Authentication

Authentication: Local Login IP Ranges:

Roles

Available Roles: Select a Role

Standard User — Allows users to access and manage remote devices Remove

Access Time

Add Rules

Users

Save Cancel

Figure 64

- c. Place the cursor in the **Users** box in order to select the PIV user to add as a member of the group, select the PIV user from the choices that appear.

Access Time Add Rules

Users

bill — brenda — crystall — mark — mel — SMITH.JOHN.K.1403175621 — super — First name Last Name

Copy Delete Manage Policy View Policy

Displaying 1 - 3

Figure 65

- d. Select **Save**, the newly created group should now appear in the list of groups

Configuring the Group Policy

A policy must now be created that defines which group is permitted to access which target system and by what methods.

- 1. In the grey menu bar select **Policy** and then **Manage Policies**

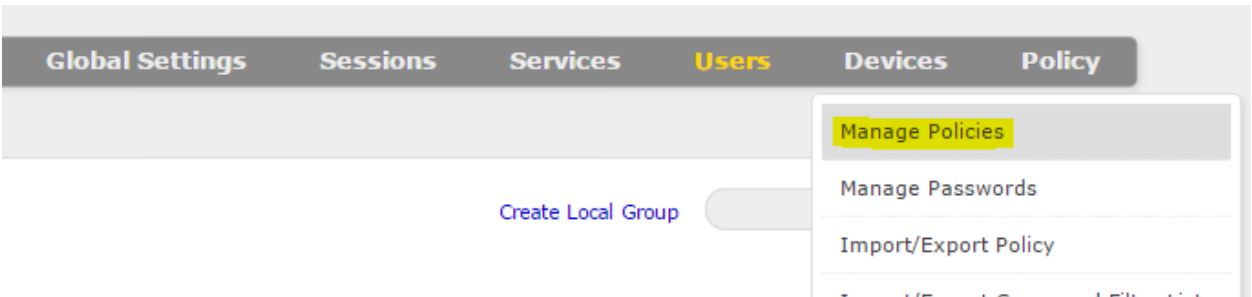


Figure 66

- 2. Place the cursor in the **User (Group)** box and in the window that appears; select the Sys Mgr 7.0.1 Group that was created previously

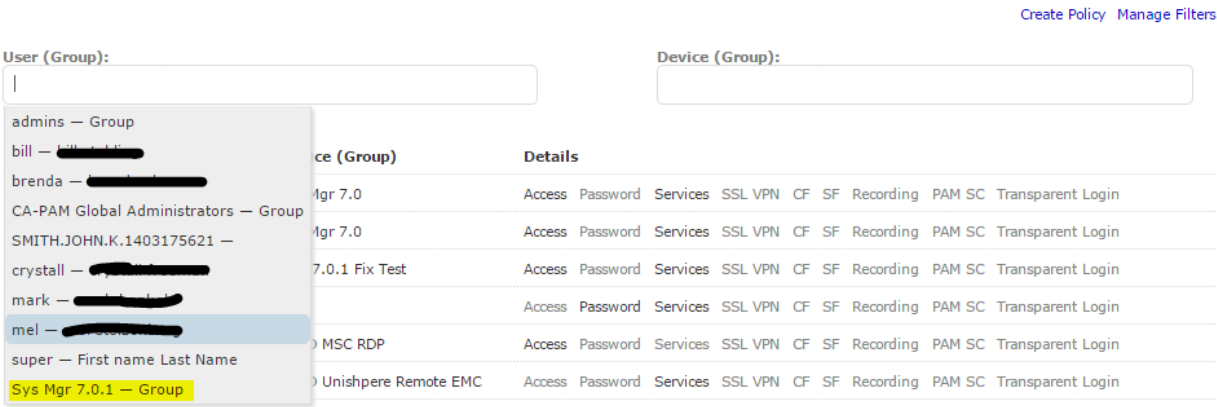


Figure 67

- 3. Place the cursor in the **Device (Group)** box and in the window that appears, select the **Sys Mgr 7.0** Device and then select **Create Policy**

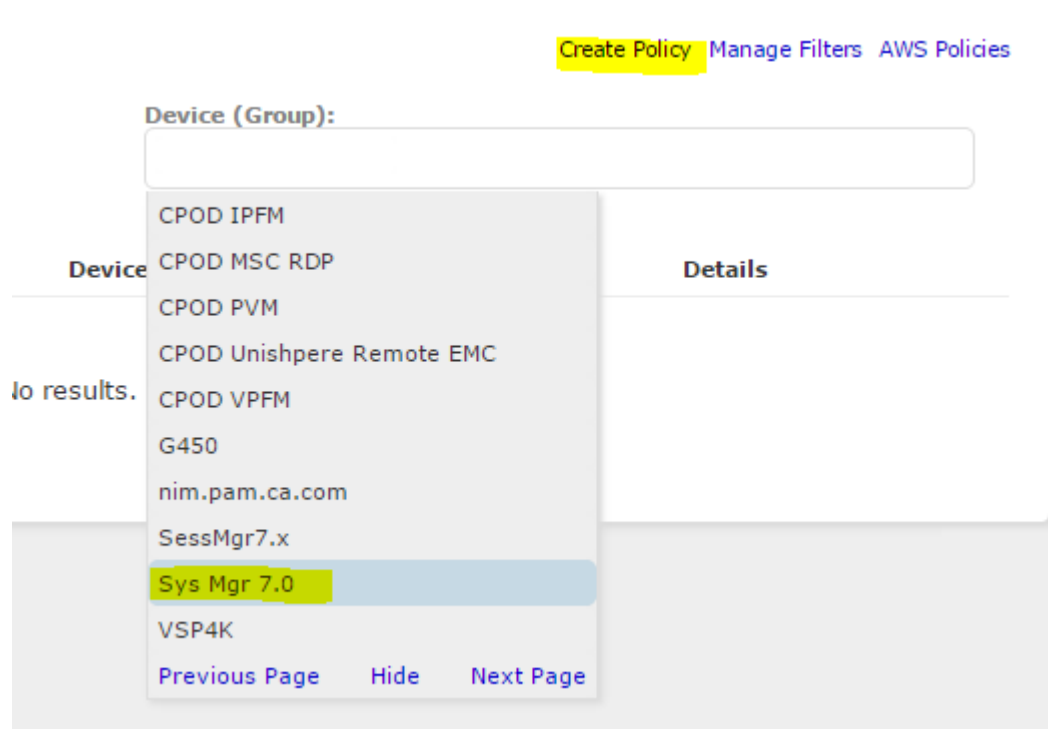


Figure 68

4. Now add the appropriate **Access** and **Services** in the same manner in which the previous policy was created earlier in this document. **NOTE: IT IS NOT RECOMMENDED TO SET THE PASSWORDS FIELD UNLESS CA-PAM'S "PASSWORD MANAGEMENT" FEATURE IS BEING USED TO MANAGE CREDENTIALS ON THE TARGET SYSTEMS. CONFIGURING THE "PASSWORDS" SECTION MAKES THE USERNAME/PASSWORD CREDENTIALS VISIBLE TO THE END-USER ON THE MAIN ACCESS SCREEN IN THE TARGETED APPLICATIONS COLUMN.**

User (Group):

Sys Mgr 7.0.1 x

Device (Group):

Sys Mgr 7.0 x

Updated	User (Group)	Device (Group)	Details
	Sys Mgr 7.0.1	Sys Mgr 7.0	
	<div>Save</div> <div>Cancel</div>		
Access	SSH:22 [Sys Mgr 7.0. ssh — admin], Edit		
Services	Sys Mgr 7.0 https [Sys Mgr 7.0 https — admin] Sys Mgr ssh [Sys Mgr 7.0. ssh — admin] Edit		
Passwords	None Selected Add		
OOB & Power	<div>KVM:</div> <div>Power:</div> <div>Serial:</div> <div><input type="checkbox"/></div> <div><input type="checkbox"/></div> <div><input type="checkbox"/></div>		
Filters	<div>Command Filters:</div> <div>Socket Filters:</div> <div>Restrict login if agent is not running:</div> <div>None Selected ▼</div> <div>None Selected ▼</div> <div><input type="checkbox"/></div>		
Recording	<div>Graphical:</div> <div>Command Line:</div> <div>Bidirectional:</div> <div>Web Portal:</div> <div>On Violation:</div> <div><input type="checkbox"/></div> <div><input type="checkbox"/></div> <div><input type="checkbox"/></div> <div><input type="checkbox"/></div> <div><input type="checkbox"/></div>		
CA PAM Server Control	<div>Login Integration:</div> <div><input type="checkbox"/></div>		
	<div>Save</div> <div>Cancel</div>		

Figure 69

5. Select **Save**.
6. Logout of CA-PAM.
7. Log back in to CA-PAM as the PIV user and verify that this user now has visibility to the Systems and management methods that he was granted access to via the group membership and that he does not have visibility to any other systems.





Unfiltered Save as View		OOB Devices Restart Session My Views <div>Search</div>	
			
Device Name	Access Methods	Web Portal	Services
Sys Mgr 7.0	SSH	Sys Mgr 7.0 https	Sys Mgr ssh
Displaying 1 - 1			

Figure 70

NOTE: Because the group that this user belongs to was only granted rights as **Standard User**, the grey menu bar and other options related to configuration of CA-PAM are not available.

Appendix A

Best Practices for Securing the Target Systems

One concern with implementation of a product such as CA-PAM is the possibility that an end user or attacker armed with the IP address of the target system could potentially bypass CA-PAM and CA-PAM authentication methods by using SSH or a Web Browser to connect directly to the target system, thereby defeating the use of CA-PAM for MFA.

Avaya recommends the following actions be implemented in order to mitigate the risk of such access, consult specific product documentation for instructions to implement the proper ACL's on each Avaya target system.

- Implement “deny-by-default” ACL's on all target systems that deny all traffic to the management interface and only permit SSH (TCP 22), Web traffic (TCP 80,443) or traffic that originates from the specific IP address of the CA-PAM server and/or the thick client jump box.
 - If a thick client on an RDP Jump Box is used, then the Port/Protocols of the thick client as well as the IP address of the Jump Box will need to be excepted from the deny-by-default ACL.
 - For Linux-based systems this is accomplished in IPtables for RedHat 6 and firewalld for RedHat 7.
 - Windows systems also fully support deny-by-default firewall rules with exceptions for permitted traffic types.
- Management interfaces for the target systems and the CA-PAM server should reside in the same isolated management VLAN.
 - The CA-PAM server and any workstations used to connect to it in order to manage target systems should have IP interfaces in the management VLAN only
 - Use VLAN separation with 802.1q VLAN tags to keep management traffic separate from production traffic on the target Avaya system. Preferably, use different Ethernet interfaces on the target system to physically separate the management and production traffic onto different hardware NICs
 - Configure local firewall rules, routers and switches to prevent leaking of the management VLAN into the production network
- Limit the number of privileged user accounts that exist on the target system.
 - CA-PAM passes credentials to the target system transparently to the user. This allows multiple users to login to a target system on a single account in order to manage it. CA-PAM then logs all of the necessary information for non-repudiation for that connection, including the PIV-enabled username, timestamps, IP address, etc, etc.
 - Reducing the number of human interactive accounts on the target system significantly reduces the attack surface of the system as errors are often made with manual administration of target system accounts, such as idle accounts with no expiration, non-removal of accounts used by departed personnel, etc., each of which present an attack vector waiting to be exploited
 - Furthermore, if configured with off-box storage, CA-PAM has the capability to record each user's full session and every action the user has executed in that session
- Physical security of all systems is paramount, including any dedicated Windows based RDP Jump Boxes. Avaya target systems, RDP jump boxes and the CA-PAM server should be housed not only in secure rooms with controlled ingress/egress systems in place, but should also be deployed in cabinets with locking doors with proper door key management controls in place

Configuring CA-PAM for ACCCM

Because ACCM only supports the Internet Explorer browser for configuration, the built-in Chromium CA-PAM browser cannot be used. Although a credentialed connection to ACCCM can be made with the Chromium browser, certain functionalities needed to configure the ACCCM system will not be available using it.

1. Begin by creating the https service for ACCCM. In the grey menu bar navigate to **Services** and in the drop down to **TCP/UDP Services**.

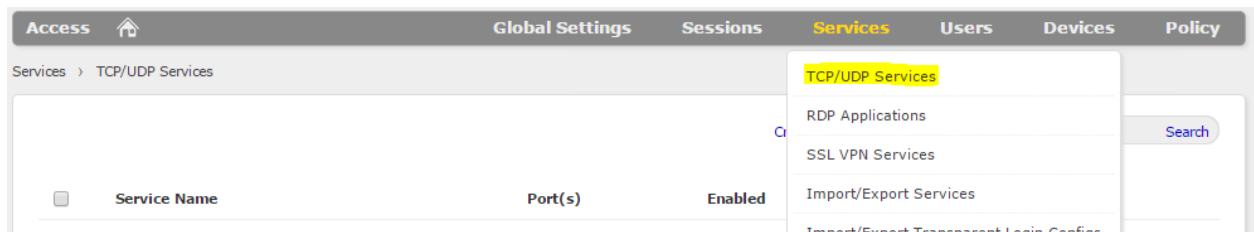


Figure 71

2. In the next screen enter the **Service Name** and the **Port:Port**
3. In the **Application Protocol** select **Web Portal**
4. For **Browser Type** select **Native Browser**
5. For **Auto-login Method** select **Disabled**
6. In the **Launch URL** field copy the string below the box up to the last “/”, then enter ACCCMPortal at the end of the URL. The full string should read: **http://<Local IP>:<First Port>/ACCCMPortal**
7. Uncheck the box **Route through Xsuite**

8. The screen should now look like this:

The screenshot displays the ACCEM configuration interface. At the top, a header bar shows the service name 'ACM http', the port '80:989', the status 'Yes', the protocol 'TCP', and the IP address '127.0.0.1'. Below this header are buttons for 'Save', 'Cancel', 'Copy', and 'Delete'. The main configuration area is divided into three tabs: 'Basic Info', 'Administration', and 'Web Portal'. The 'Basic Info' tab is active, showing fields for 'Service Name' (ACM http), 'Local IP' (127.0.0.1), 'Port(s)' (80:989), 'Protocol' (TCP), and 'Comments'. The 'Administration' tab shows 'Enable' (checked), 'Show in Column' (unchecked), 'Application Protocol' (Web Portal), and 'Auto-Login Method' (Disabled). The 'Web Portal' tab shows 'Launch URL' (http://<Local IP>:<First Port>/ACCEMPortal), 'Host Header', 'Aliases', 'Browser Type' (Native Browser), 'Hide From User' (unchecked), and 'Route Through Xsuite' (unchecked). At the bottom of the configuration area are buttons for 'Save', 'Cancel', 'Copy', and 'Delete'.

Figure 72

9. Select **Save**
10. Proceed to configure the ACCEM **Device, Targeted Application, Targeted Account and Policy** as described earlier in this document
11. When finished, proceed to the **Access** screen and select the ACCEM http service and verify that the connection succeeds. The default browser on the user's machine should be called by CA-PAM. *If any other browser other than IE opens with the connection, then you must stop and set IE as the default browser on the pc. **NOTE: At this time there is no way to call a specific browser similar to how the Putty executable was called previously in this document***
12. Using this method the privileged end-user must know the UN/PW credentials to log in to ACCEM since CA-PAM is unable to transparently pass them. When the link to the ACCEM http is clicked to start the session, a small grey box is displayed with a link for **View Credentials**. Click this link to view the credentials to be used to log in manually to ACCEM.

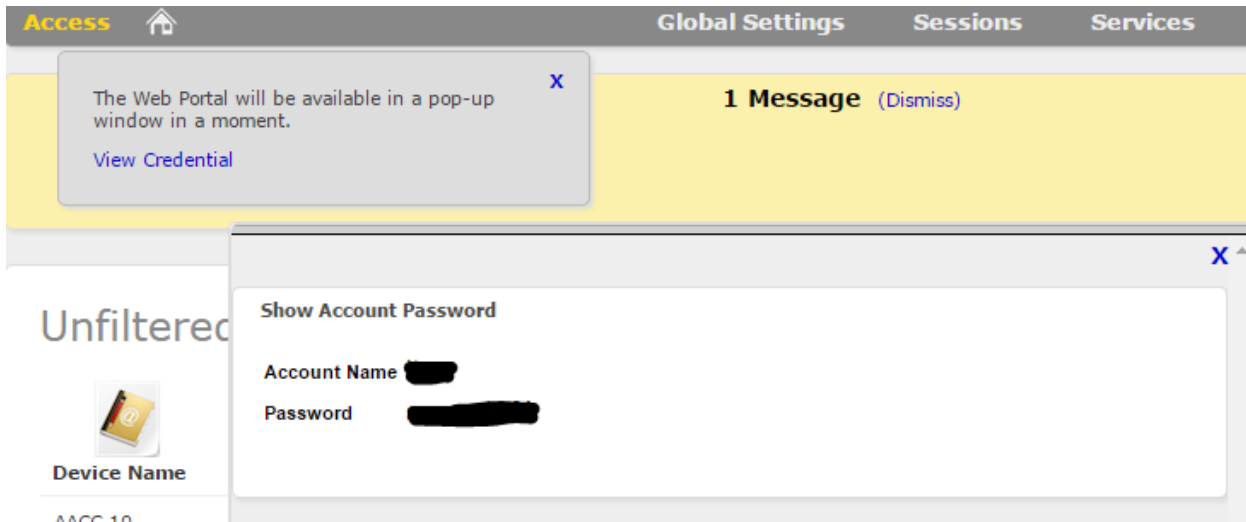


Figure 73

13. Log in to ACCCM and verify that the connection is made