# Setting Up and Initial Configuration of Device

## Setting “super”

| **STEP** | **PICTURE/ILLUSTRATION** | **RATIONALE/**  **COMMENTS** |
| --- | --- | --- |
| Connect to IP Address of Device | https://pam-prod.pmusa.net |  |
| Just click OK to bypass the warning message about the license.  Enter User>**super** and password>**super**  and click “LOGIN” button |  | The “super” account is a local account defined within the internal (a.k.a. “Local”) |
| Change the super password and confirm (setting the password to “super” will not work).  Also set the email address.  And click the “OK” button to continue |  |  |
|  |  |  |

## Set “config” Login ID/Password or Change “super” Login ID

| **STEP** | **PICTURE/ILLUSTRATION** | **RATIONALE/**  **COMMENTS** |
| --- | --- | --- |
| Connect to the following URL | https://<IP of Device>/config |  |
| When prompted, use the User Name and password “config”  NOTE: Make sure to use “https” when attempting to connect. Otherwise, the appropriate login page will not appear |  |  |
| Click on the “Change Password” link to change the password for the “config” account or change the “super” username. |  |  |
| To change Config name or Password:  Set the Config User ID and/or matching Password & Confirm values. Click on the “Update” button to continue. |  |  |
| To change Super name:  Set the Login ID to new value. Enter the super current <password> value in the “Current Login Password” field. Click on the “Update” button to continue. |  |  |

## Obtain License Key for PAM

| **STEP** | **PICTURE/ILLUSTRATION** | **RATIONALE/**  **COMMENTS** |
| --- | --- | --- |
| Connect to IP Address of Device | https://<IP of Device> |  |
| Click on the “System Info” tab. |  |  |
| Sys Info Window should appear. Click on the “Download” icon to obtain the CA PAM Appliance Information to your desktop. |  | This file will be used to generate the license key that you will upload into the solution. |
| Open a Support ticket with “Broadcom Technical Support” <https://ca-broadcom.wolkenservicedesk.com/esd/allcases>  Provide you Site ID.  Also provide the following inform   1. Total number of users accessing the PAM Device 2. Total number of passwords being managed 3. Total number of A2A (application to application) will be managed. |  |  |
| Response from Technical Support (should be within an hour), will return the number of license keys equivalent to the number of system info files that you submitted. |  |  |
| Verify the Hardware ID matches the information in the downloaded license file name.  If so, “Upload License File” |  |  |
| Click on “Save New License” |  |  |
| Verify New License was applied and End Date is <blank> and Type is Perpetual |  |  |

# Configuring Backup – Windows Share (DB and Config file)

This process is broken down into two steps. The first step is to produce the network file share first. The second step is to configure the CA PAM appliance to utilize the share.

## Defining Windows File Share – Used by Appliance to Store Backups

| **STEP** | **PICTURE/ILLUSTRATION** | **RATIONALE/**  **COMMENTS** |
| --- | --- | --- |
| Log on to the target Windows Server with user. |  |  |
| Create User with appropriate access.  NOTE: In this example, a local account was created on the Windows Server. |  |  |
| Create Directory Location.  Go to the main directory where the folder(s) will exist. Right-click, and select New -> Folder |  |  |
| Change the folder name to the appropriate name.  For this, we created the “pam-rtp-dmz” directory. |  |  |
| Create sub-folders for separating Configuration/DB backups and SessionRecordings.  For this, we created the “dbcfg” and “sessrecs” folders. |  |  |
|  |  |  |
| Once the directory is created, right click on the newly created directory, and go to properties. |  |  |
| Click on the “Share” button. |  |  |
| In the next window, select the appropriate user.  Click on the Add button.  Change the permissions for this account to be both “Read/Write”.  Click on the “Share” button when ready.  In the next status, click on the “Done” button. |  |  |
| Goto Folder and click “Properties”  Goto “Sharing” tab  Verify the Shared “Network Path” |  |  |

## Configuring PAM Appliance to Utilize CIFS Storage Mount (Database and Config Backup)

| **STEP** | **PICTURE/ILLUSTRATION** | **RATIONALE/**  **COMMENTS** |
| --- | --- | --- |
| Connect to IP Address of CA PAM Device.  Use an account with the proper access to perform this function (e.g. “super”) | https://<IP of Device>  or use the PAM Client pointed to CA PAM Device |  |
| Click on the “Configuration” Menu Item.  Click on the “Database” link.  Click on the “Backup Scheduler” tab |  |  |

# Configure Routing to Syslog Server

This is to forward logs to syslog

|  | **STEP** | **PICTURE/ILLUSTRATION** | **RATIONALE/**  **COMMENTS** |
| --- | --- | --- | --- |
| 1 | Connect to IP Address of CA PAM Device.  Use an account with the proper access to perform this function (e.g. “super”) | https://<IP of Device>  or use the PAM Client pointed to CA PAM Device |  |
|  | Click on “Configuration”  Then on the left side click on the “Logs” then “Syslog” links |  |  |
| 2 | Enable the feature  Define IP Address  And press button “Update” to save |  |  |

# Session Recordings

## Enabling Session Recording - CIFS

Send all Appliance recording to an external shared location

|  | **STEP** | **PICTURE/ILLUSTRATION** | **RATIONALE/**  **COMMENTS** |
| --- | --- | --- | --- |
| 1 | Connect to IP Address of CA PAM Device.  Use an account with the proper access to perform this function (e.g. “super”) | https://<IP of Device>  or use the PAM Client pointed to CA PAM Device |  |
| 2 | Click on “Configuration”  Then on the left side click on the “Logs” then “Session Recordings” link, then select tab “External Storage” to enter details |  |  |
| 3 | Select the Protocol drop-down option for CIFS  Enter details for Share Path, Username (s-pam-cifs), Password, and Domain  Then on the bottom press “SAVE SETTINGS” and then “MOUNT” buttons |  | Mount Status will change to “Mounted” and Mount Availability will change to “Available” (this will sometimes take a few refreshes) |
| 4 | Select tab “Session Recording” to enter details  Check off both items for “Text based recordings” and “Graphical Session recordings”  Press “UPDATE” |  |  |
| 5 | Select tab “Access Policy” to enter details  Check off “Security Safe” or “Operational Safe”  Press “UPDATE” |  |  |

# Network setup

## RTS & RDE Sites for PROD/UTS – 2 Bonds

#### Network Setup

|  | **STEP** | **PICTURE/ILLUSTRATION** | **RATIONALE/**  **COMMENTS** |
| --- | --- | --- | --- |
| 1 | Connect to IP Address of CA PAM Device.  Use an account with the proper access to perform this function (e.g. “super”) | https://<IP of Device>  or use the PAM Client pointed to CA PAM Device |  |
|  | Click on “Configuration”  Then on the left side click on the **Network** “+” sign to expand, then click on the “Network Settings” links |  |  |
| 2 | At the top of the Network Settings window  Enter:  Hostname  Domain Name  Default Gateway  DNS Servers  Not using IPV6, so leave unchecked |  |  |
| 3 | Move to the middle of Network Settings  For GB1 and GB2  select BOND1  For GB3 and GB4  Select BOND2  Do not fill in any other field |  |  |
|  | Move to the bottom of Network Settings  Enter:  IPV4  Netmask  Speed  Duplex |  |  |
|  | After everything is entered, press “UPDATE” |  |  |

#### Add’l Routes Setup

|  | **STEP** | **PICTURE/ILLUSTRATION** | **RATIONALE/**  **COMMENTS** |
| --- | --- | --- | --- |
| 1 | Connect to IP Address of CA PAM Device.  Use an account with the proper access to perform this function (e.g. “super”) | https://<IP of Device>  or use the PAM Client pointed to CA PAM Device |  |
|  | Click on “Configuration”  Then on the left side click on the **Network** “+” sign to expand, then click on the “Additional Routes” links |  |  |
| 2 | Press button “Add” to enter Routes that BOND2 will use to make connections to other Appliances or Subnets |  |  |
| 3 | Enter:  Destination - <Appliance>  Netmask – 255.255.255.255  Gateway - <Gateway IP>  Metric – 1  Device – BOND2  Click “OK” |  |  |
| 4 | Finish loading all the Routes for all the Cluster Appliances |  |  |

## PROD Factories, UTS NSH, DMZ Site – 1 Bond

#### Network Setup

|  | **STEP** | **PICTURE/ILLUSTRATION** | **RATIONALE/**  **COMMENTS** |
| --- | --- | --- | --- |
| 1 | Connect to IP Address of CA PAM Device.  Use an account with the proper access to perform this function (e.g. “super”) | https://<IP of Device>  or use the PAM Client pointed to CA PAM Device |  |
|  | Click on “Configuration”  Then on the left side click on the **Network** “+” sign to expand, then click on the “Network Settings” links |  |  |
| 2 | At the top of the Network Settings window  Enter:  Hostname  Domain Name  Default Gateway  DNS Servers  Not using IPV6, so leave unchecked |  |  |
| 3 | Move to the middle of Network Settings  For GB1 and GB2  select BOND2  Do not fill in any other field |  |  |
|  | Move to the bottom of Network Settings  Enter:  IPV4  Netmask  Speed  Duplex |  |  |
|  | After everything is entered, press “UPDATE” |  |  |

# Cluster Setup – Starting/Re-Starting the Cluster

## Configure Clustering – Prod Site

There are a number of steps that are required prior to making sure the cluster is configured.

1. NTP is configured for all members of the cluster with same NTP servers
2. The Shared Key is defined on all members of the cluster.
3. Master will push Interface, so ALL appliances MUST HAVE the corresponding “Interface” setup (Bond2 for all Cluster communication traffic)
4. Members of the cluster are identified in each cluster site config (The Master Node needs to be on top of the site member list – so order is important)

|  | **STEP** | **PICTURE/ILLUSTRATION** | **RATIONALE/**  **COMMENTS** |
| --- | --- | --- | --- |
| 1 | Connect to IP Address of CA PAM Device.  Use an account with the proper access to perform this function (e.g. “super”) | https://<IP of Device>  or use the PAM Client pointed to CA PAM Device |  |
| 2 | Make sure that the NTP is configured and operational.  Click on “Configuration”  Then on the left side click on the “Date/Time”, then select tab “Time Servers” to view details.  Add server addresses that have the NTP service running  **And all cluster members in a site should work off the same NTP service.** |  |  |
| 3 | Select tab “NTP Status” to view details.  You must see “**sys.peer”** as a condition to show it is working properly  And all cluster members in a site should work off the same NTP service. |  |  |

|  | **STEP** | **PICTURE/ILLUSTRATION** | **RATIONALE/**  **COMMENTS** |
| --- | --- | --- | --- |
| 5 | Click on “Configuration”  Then on the left side click on the “Clustering”, then select tab “Local Settings” to view details.  Add a passphrase and generate a “Key”. That “Key” will be used for all cluster appliances  Select which Interface will be used for Cluster traffic > Bond2 |  |  |
| 6 | Select tab “Global Settings” to create a cluster.  Click button to “ADD” a new cluster.  Enter in the VIP address and host name for the cluster  Then add the cluster members and click “OK” |  |  |
| 7 | Now you can “SAVE CONFIG LOCALLY”  Then “SAVE TO CLUSTER”  And finally, “TURN CLUSTER ON” |  |  |
| 8 | Once it finishes, go to “Status” tab and see results |  |  |

# Setting up Connection to AD (LDAP)

This step is used to define a user store that will be used to authenticate to the device.

NOTE: Ability to login to the device can only be done by GROUPS. It cannot be done via a specific individual USER

NOTE: For AD authentication, a bind user (with read only) access is required.

| **STEP** | **PICTURE/ILLUSTRATION** | **RATIONALE/**  **COMMENTS** |
| --- | --- | --- |
| Connect to IP Address of CA PAM Device.  Use an account with the proper access to perform this function (e.g. “super”) | https://<IP of Device>  or use the PAM Client pointed to CA PAM Device |  |
| On Network Tools page, check “Domain” to resolve a list of Domain Controllers |  |  |
| On Device\Manage Device page, setup a “Domain” device  \*\* Only need Password Management |  |  |
| On Credential\Target Application page, setup application  LDAPS will use 636 (LDAP could use 389 if configured that way) |  |  |
| On Credential\Target Account page, setup account |  |  |
| Save then go back and change to Update both… |  |  |
| Click on the “Configuration” Menu Item.  Click on the “3rd Party” link.  Click on LDAP  Click on “Add” button to continue. |  |  |
| Enter the server name, the bind credentials, and the password for the bind account.  If you choose the Account first, previous fields will be auto-filled |  |  |
| Goto Attribute Tab  Enter the Unique Attribute for AD when PAM needs to pass on value to SAML |  |  |
| Click on the “OK” button to continue. |  |  |
| The success message after LDAP added. |  |  |

## Authorizing Access to PAM Device via Previously Defined LDAP

This step is used to define an AD Group that will be allowed access to login to the device.

**NOTE**: Ability to login to the device can only be done by GROUPS. It cannot be done via a specific individual USER

**NOTE**: If doing this as an initial test, you may need to assign the test group (or test user) with the role “Global Administrator” to test the login.

| **STEP** | **PICTURE/ILLUSTRATION** | **RATIONALE/**  **COMMENTS** |
| --- | --- | --- |
| Connect to IP Address of CA PAM Device.  Use an account with the proper access to perform this function (e.g. “super”) | https://<IP of Device>  or use the PAM Client pointed to CA PAM Device |  |
| Click in the “Users” Menu.  Click in the “Manage Groups” menu. |  |  |
| Click on the “Import LDAP Group” link.  An “CA PAM LDAP Browser” should appear. |  |  |
| Drop down to the appropriate LDAP Domain that will be used to locate the appropriate LDAP Group. |  |  |
| Locate the LDAP Groups to be imported.  Click on the check box to select the LDAP Groups.  When ready, click on the “Register selected groups with the PAM appliance” icon. |  |  |
| The Register LDAP Groups with the PAM Appliance windows select the Authentication Type “LDAP” in the drop-down.  Click on the “Register Groups” button to continue. |  |  |
| The LDAP Groups will be migrated in. The status should show registered.  Click on the “Close” button to continue. |  |  |
| Notice the LDAP Groups imported now have check marks next them in the LDAP Browser.  Continue the above steps to add additional LDAP Groups.  Close the PAM LDAP Browser when done importing LDAP Groups. |  |  |
| Notice in the PAM UI the Imported LDAP Groups will appear. |  |  |

# Defining User Access to Server

Prior to providing access to a PAM Device, the PAM Device needs to be defined to the system. The following is a set of steps to define the Linux Target Device. Subsequent steps will define the account.

## Defining Target Device

| **STEP** | **PICTURE/ILLUSTRATION** | **RATIONALE/**  **COMMENTS** |
| --- | --- | --- |
| Connect to IP Address of CA PAM Device.  Use an account with the proper access to perform this function (e.g. “super”) | https://<IP of Device>  or use the PAM Client pointed to CA PAM Device |  |
| Click on the “Devices” Menu.  Click on the “Manage Devices” menu. |  |  |
| In the next window, click on the “ADD” button. |  |  |
| Document the Server Name, Address (FQDN), the OS type.  The Description and Location Information is optional.  The Device Type is important. It determines how PAM will interact with the target device, and eventually how authorized end users/services will access the device type.    Click “OK” Button to save the device into CA PAM. |  | **NOTE**: The Device Type has three options  ***Access*** allows individuals to connect to the device from the PAM appliance.  ***Password Management*** define whether there will be target account(s) on the device that will have their passwords managed by the PAM appliance. Authorized users will then be allowed to use these target account(s) to login to the device from the PAM Appliance (and possibly not see the value of the password).  The ***A2A*** option is to allow individuals the ability to setup “application to application” usage. |

### Defining Policy to Access Device

The following steps will define a policy for an AD Group to be able to access the Device via RDP or SSH.

**NOTE**: The following steps will only allow the authorize user the ability to use the PAM Device the capability to login to the RDP Device. The authorized user will still need to provide the correct credentials to login to the device.

| **STEP** | **PICTURE/ILLUSTRATION** | **RATIONALE/**  **COMMENTS** |
| --- | --- | --- |
| Connect to IP Address of CA PAM Device.  Use an account with the proper access to perform this function (e.g. “super”) | https://<IP of Device>  or use the PAM Client pointed to CA PAM Device |  |
| Click on the “Policy” Menu.  Click on the “Manage Policy” menu. |  |  |
| Click on the “ADD” button to create a new policy.  The policy will appear with additional tabs for access options. |  | NOTE: This field is context sensitive. The list of entries defined below will decrease until you see the specific user or group that will be selected. |
| In the “User (Group):” select the names of the user or group you use to manage. |  | NOTE: This field is context sensitive. The list of entries defined below will decrease until you see the specific user or group that will be selected. |
| In the “Device (Group):” select the name of the device or device group you want to manage. |  |  |
| Now click on the “Access” Tab. |  |  |
| Check the box for protocol being used in Available Access (RDP or SSH)  Click on Arrow to move selection to “Selected Access” side  *Do not add any other values; this field will be leveraged later.* |  | The RDP value will move to the “Selected Access” Side |
| Click on the “Save” button to save the policy. |  |  |
| The policy should appear with the Access enabled. |  |  |
| Goto Access Page to see Windows Devices for access |  |  |

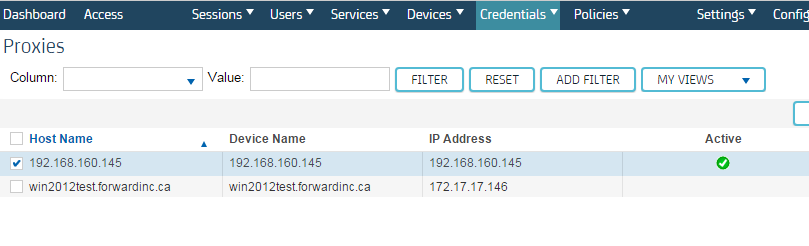
# Proxy Agent

The Proxy Agent is a lightweight application that can be installed on any Windows Server within a network segment that you want to manage accounts on. The Proxy Agent is used to change either Local or Domain based account credentials.

NOTE: If there is no DNS, Windows Proxy must be on every server. If DNS is used, then 1 proxy could be used for all Windows servers on Domain.

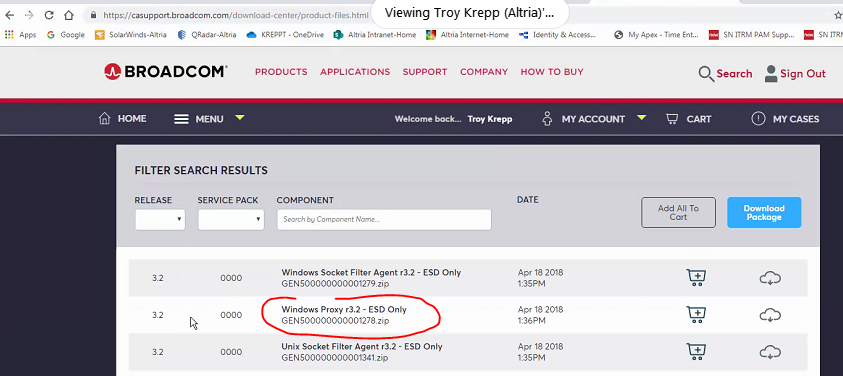
The installation of the Proxy agent does require Admin privileges to install. During the installation, you will be prompted to provide a CA PAM appliance or VIP name to report back into. It is also advised if possible to update the Service after installation to run as the service account that has been authorized to change passwords for CA PAM.

Once a Proxy Agent has been installed and successfully communicated back, it will show as a Proxy Agent under ***Credentials\Managed Targets\Proxies***. It is also important after installing to change the status from Inactive to Active on an Active Proxy by going into a given proxy detail page. This will make it available to be assigned within Target Applications. It is also advisable to deploy at least 2 Proxy Agents within a network segment for redundancy.

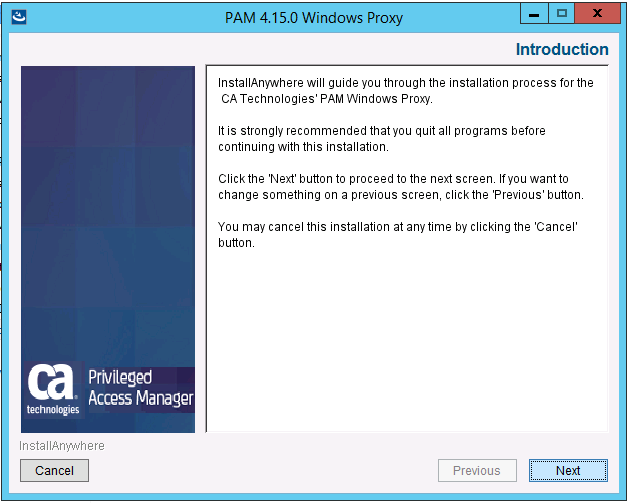


## Installing the Proxy Server on the Windows Server

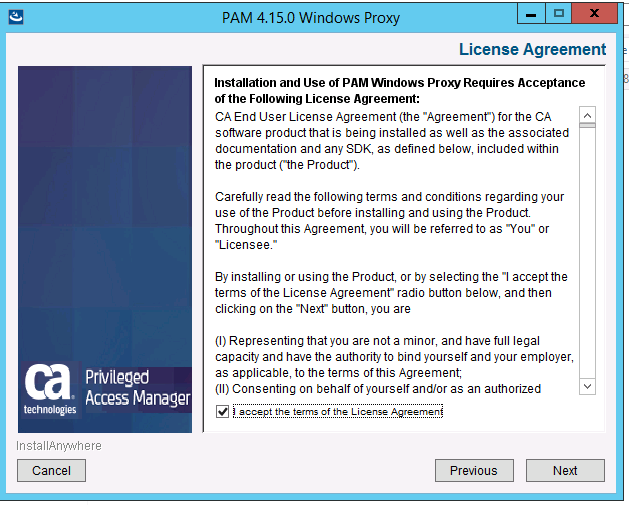
1. Download agent from Broadcom support site



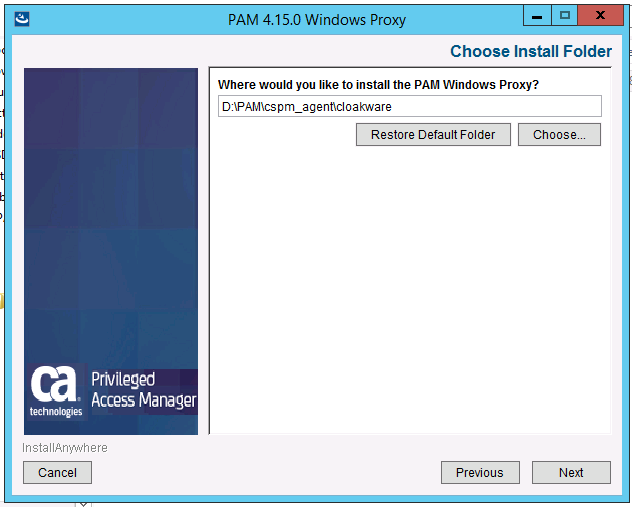
1. Installing proxy by executing the latest Windows Proxy Agent (***setup\_windows\_agent.exe***)
2. On the ***Introduction*** page of the installation, click ***Next***



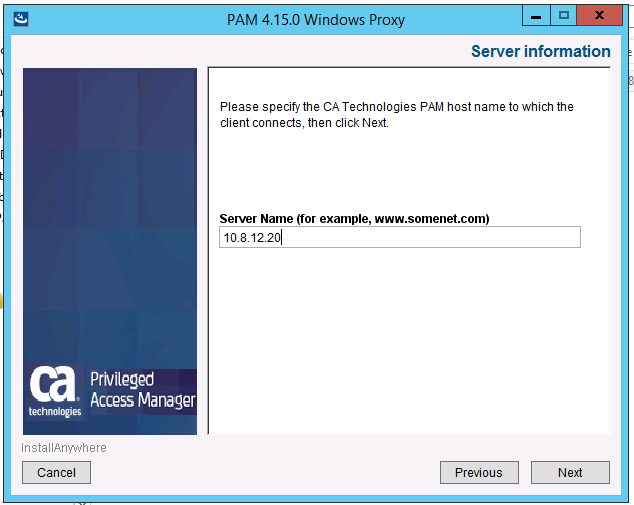
1. On the ***License Agreement*** page of the installation, click ***Next***



1. On the ***Choose Install Folder*** page, click ***Next***, unless you’re required to change the installation folder.



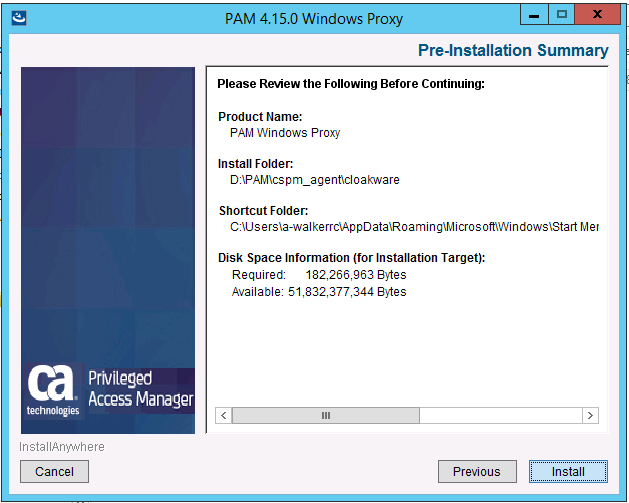
1. On the ***Server Information*** page, enter the CA PAM appliance name in the ***Server Name*** field and click ***Next***. Ensure the name provided here is resolvable.



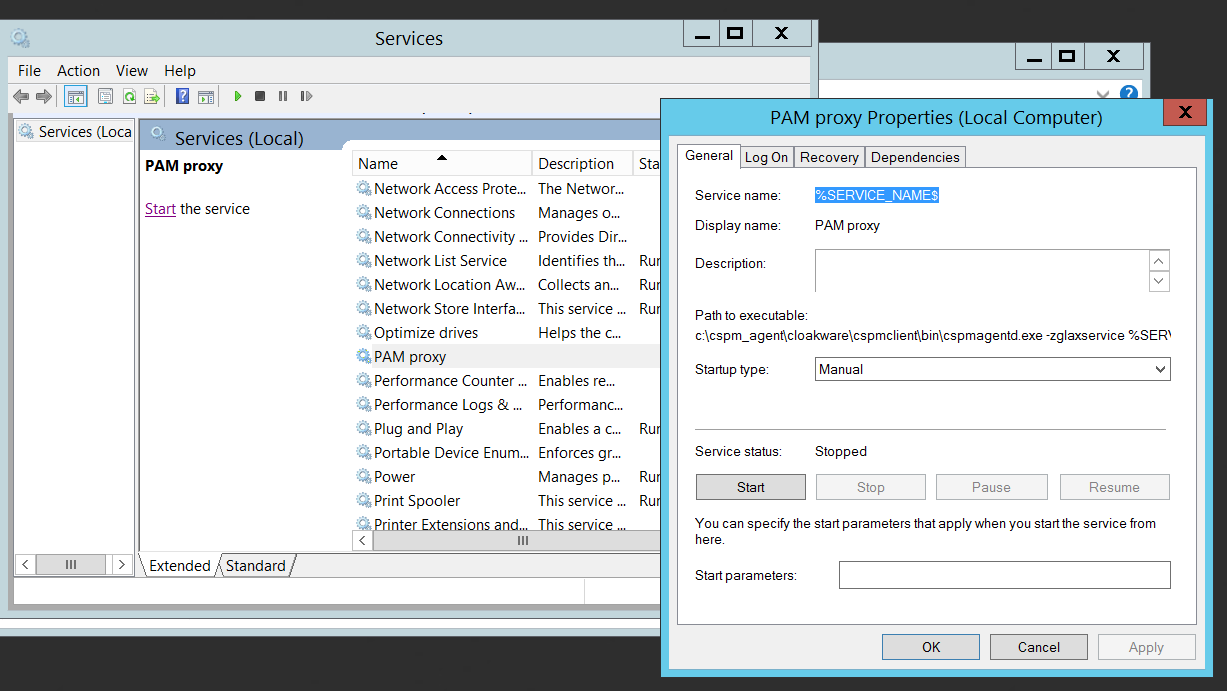
ALCRTPPAMP01 (10.8.12.20 – Bond2 IP only)

Best Practice to use cluster vip (pamrtp.altria.net) – **may re-configure at a later date for HA**

1. On the ***Pre-Installation Summary*** page review the provided information and if everything is correct, click ***Install***

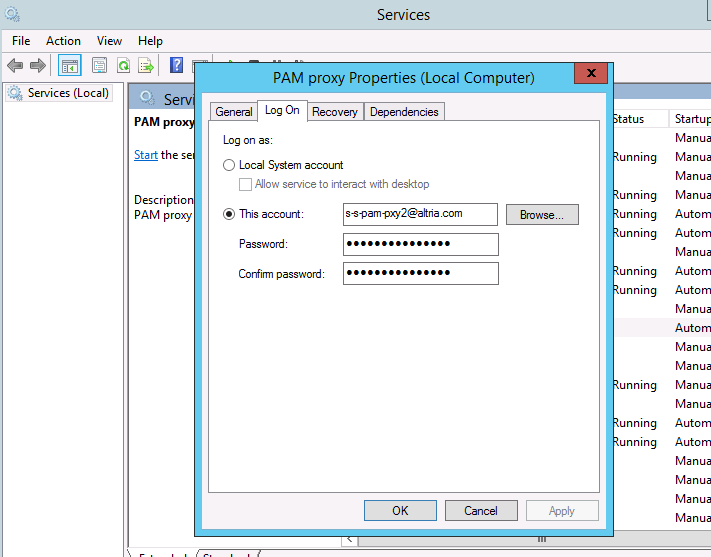


1. Once the installation is completed, open the Services and verify that the PAM Proxy Agent is installed and present. This service is typically not running.
2. Goto ***Services***
   1. Change its startup type to be “Automatic”

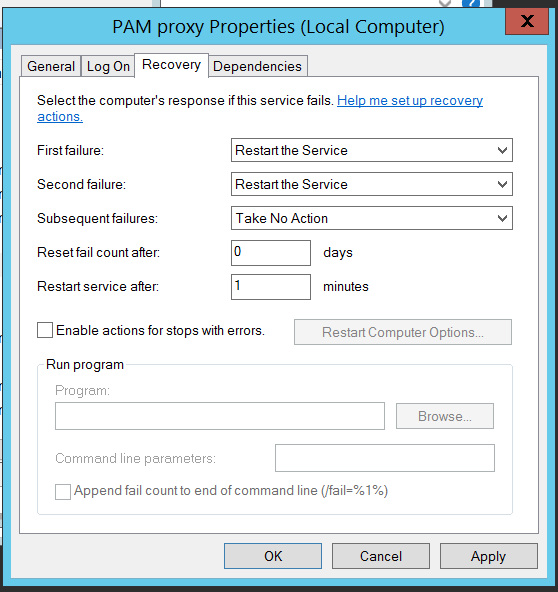


1. Goto Log On tab and set the account
   1. Use **s-s-pam-pxy1 for RTP** or **s-s-pam-pxy2 for RDE**

**\*\* This will allow the Target Accounts to “Use Proxy Credentials to change password”**



1. Goto the ***Recovery*** tab. Change the ***1st*** and ***2nd failure*** fields to ***Restart the Service***. Set the ***Subsequent failures*** to ***Take No Action***.



1. **Dependencies** tab – NO changes
2. Click **OK**
3. Right click on the “PAM Proxy” Service and select “Start” the service
4. If there are any issues with starting and running this service, one of the likely problems could be the Port usage and blockage. Issue the ***netstat –an*** command and review the output for ports 27077

**Note**: **PORT Protocol Source Destination Description**

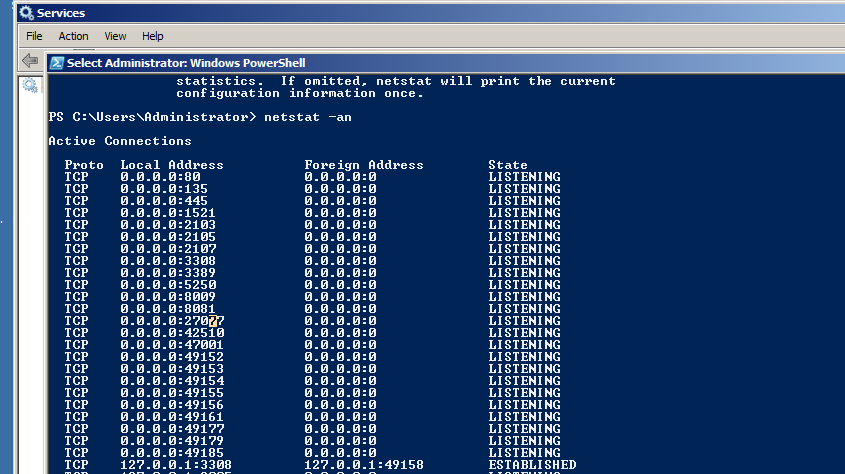
135 TCP PAM Proxy End-Node WMI RPC Negotiation

49154/5 TCP End-Node PAM Proxy End-Node communication

27077 TCP PAM Appliance PAM Proxy Encrypted communication

443 HTTPS PAM Proxy PAM Appliance Encrypted communication

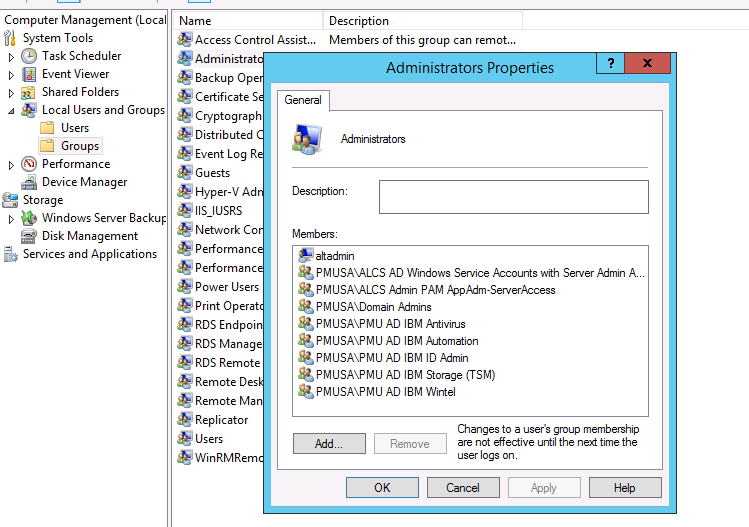
27777 TCP PAM Proxy PAM Proxy Proxy Agent to Server Cache



## Verifying Service Accounts “Group” is on Server

1) On your Windows Proxy Server “Administrative Tools\Computer Management\Local Users and Groups”

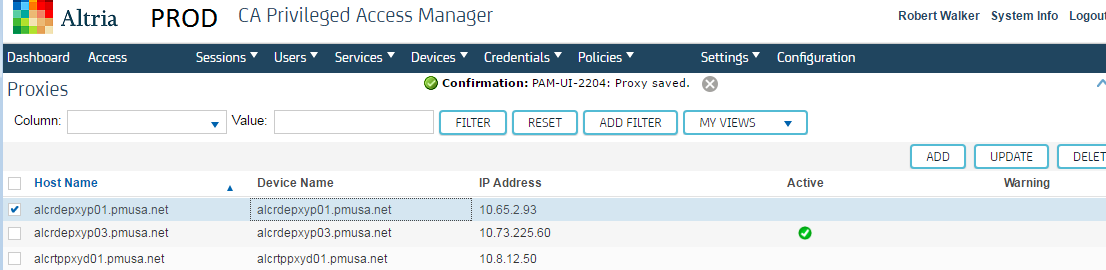
2) Open group ***Administrators*** and verify Service groups are included



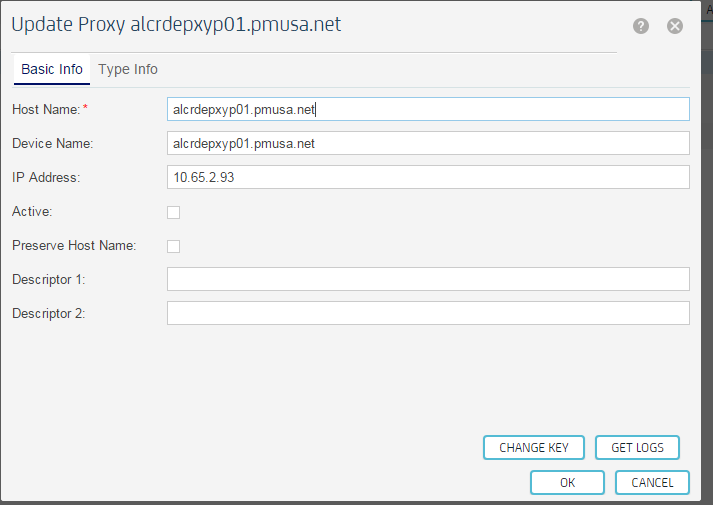
## Steps to enable Proxy

1) Setup the proxy by going to ***Policy*** 🡪 ***Manage Passwords*** 🡪 ***Target*** 🡪 ***Proxies***

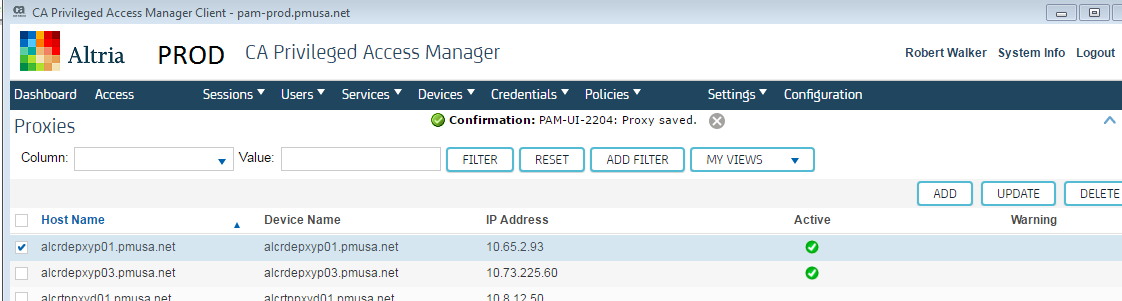
* If Proxy service on Server is started properly, Proxy will be auto-generated
* Click on Proxy and then click the “UPDATE” button



* mark the ***Status*** as ***Active***
* click “OK” button

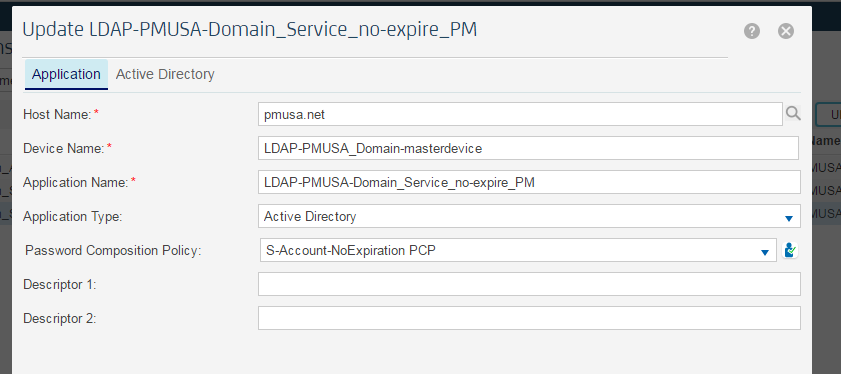


* Proxy will now have a Green “check” mark under the ***Active*** column

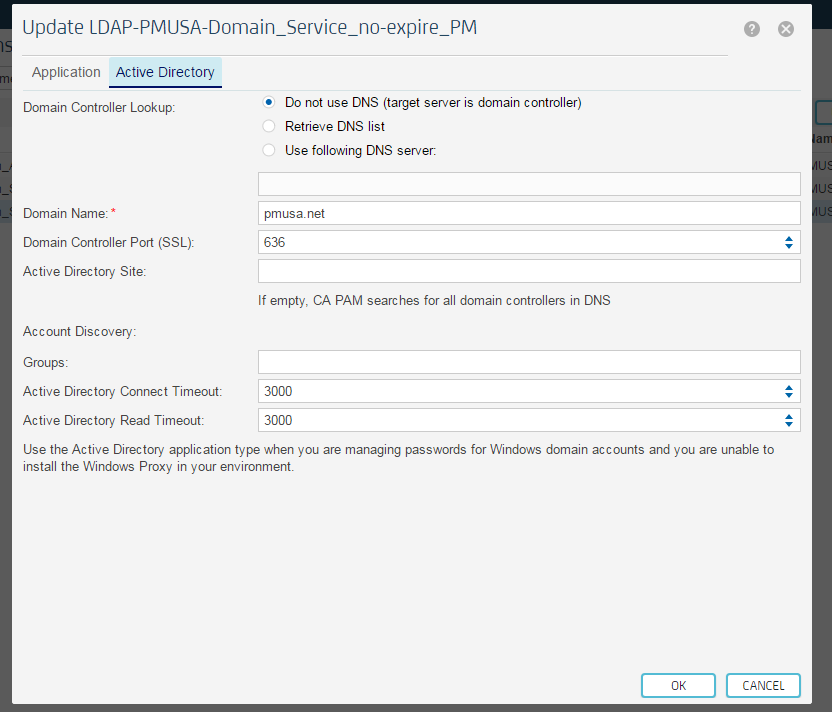


# Setup Proxy target accounts w/ Service Restart

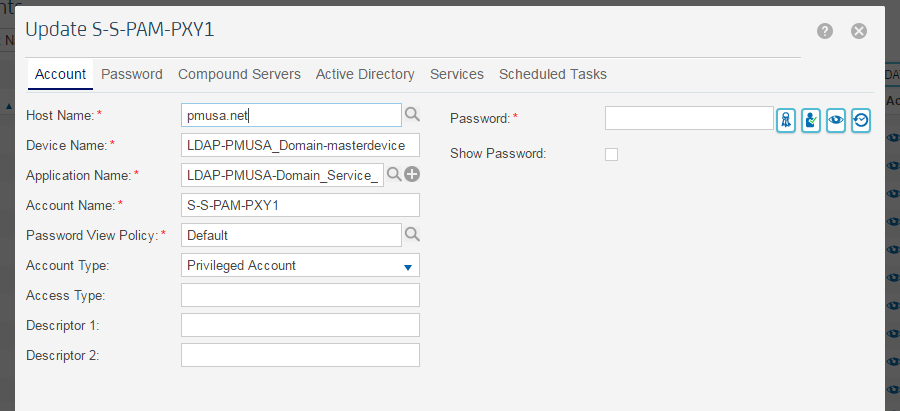
* Setup target application
  1. Select the ***Host Name*** (Domain)
  2. Enter the ***Application Name*** (make descriptive for function)
  3. Select “Active Directory” in the ***Application Type***
  4. Select the PCP, standard policy is ***S-Account-NoExpiration PCP***



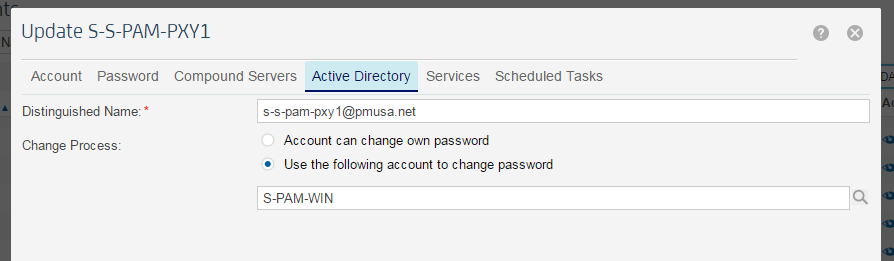
* 1. Enter
     + the Domain to be used > pmusa.net
     + the Port to be used > 636



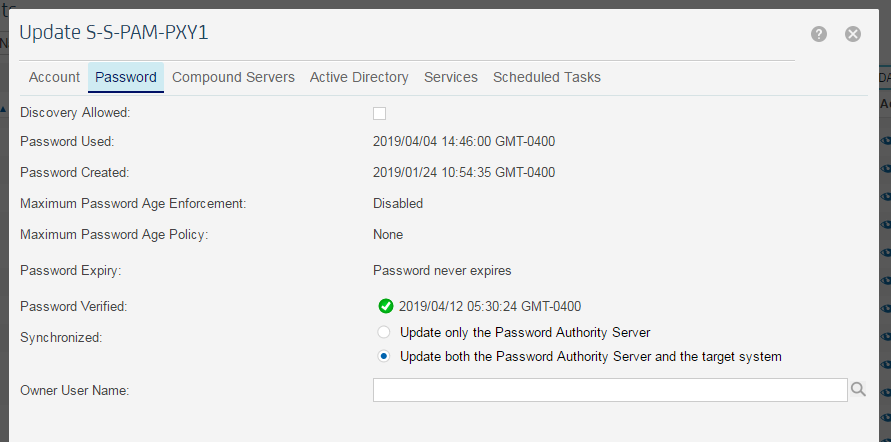
* Setup target account
  1. will use the DN to rotate accounts, NOT Account(sAMAccountName) name
  2. will use Account(sAMAccountName) name for RDP connection
  3. \*\* The sAMAccountName attribute (also known as the pre–Windows 2000 user logon name) is limited to **256 characters** in the Active Directory schema. However, for backward compatibility the limit is **20 characters**
  4. **For instructions on setting up Proxy Server go to section “3.1 Proxy Agent”**
  5. **NOTE: in Tomcat logs, NERR-password too short = password AGE is too short**
  6. Select Application name first (it will populate Host and Device Name fields)
  7. Add the account name > s-s-pam-pxy1
  8. Select a PVP – (these accounts should not be viewed or checked out so default is fine)
  9. This account manages its own password, so you must enter the current password for the account



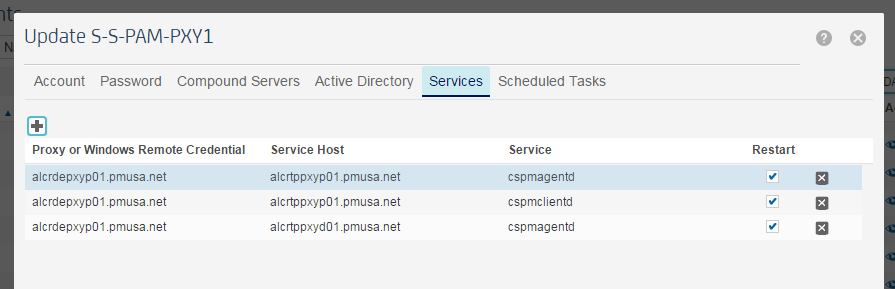
* 1. Enter the email address or full DN name
  2. Select “Use the following account to change password” to have the Master account rotate the password (this overwrites the password, does not need to know current password)



* 1. Go back to ***Password*** tab and select “Update both the PA server and the target system”



* 1. Go back into the Account
  2. Goto the ***Services*** tab
     + Enter the opposite proxy service running on target system
       - When rotating s-s-pam-pxy1 password on RTP server, configure target application to use opposite RDE proxy server
       - When rotating s-s-pam-pxy2 password on RDE server, configure target application to use opposite RTP proxy server
     + Enter the target system where the service is running (RTP proxy server)
     + Enter the service name (get from the Services application on Proxy Server)
     + Enable Checkmark, if you want to restart the service after a password change has been made



\*\* This is showing 3 items

* + - * cspmagentd - 2 Proxy services (PROD & DEV)
      * cspmclientd - 1 A2A service
  1. Go back to ***Account*** tab
     + Click on Generate Password icon
     + Press OK Button
  2. Goto Proxy Server and check password and then check that service restarted

# Managing Passwords

There are a number of steps that needs to be performed in order to have PAM manage passwords.

The first step is to define the target application that will be used to manage the actual target.

The second step is to define the target Account

The third step is to define the target accounts

The last step is to define who has access to the target accounts.

## Defining UNIX Target Application

| **STEP** | **PICTURE/ILLUSTRATION** | **RATIONALE/**  **COMMENTS** |
| --- | --- | --- |
| Connect to IP Address of CA PAM Device.  Use an account with the proper access to perform this function (e.g. “super”) | https://<IP of Device>  or use the PAM Client pointed to CA PAM Device |  |
| Click on “Policy > Manage Passwords”  A New Window/Tab will appear. |  |  |
| Click on the “Targets > Applications”  A window with a list of defined applications appear. |  |  |
| Click on “magnifying glass” icon to search for device |  |  |
| Change Application Type to device OS  UNIX  Enter Application Name  <name\_platform\_ purpose>  ALCRTPEXTP01\_LINUX\_PM/DSCV  Enter PCP  Admin\_LINUX\_30day\_PCP |  |  |
| Select proper UNIX variant  Linux  Click “OK”  No other tabs are altered |  |  |
| Verify Target Application is created |  |  |
|  |  |  |

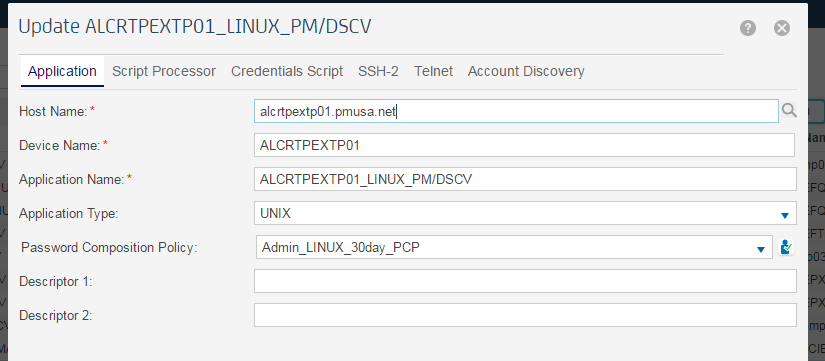
## Defining UNIX Target Account

| **STEP** | **PICTURE/ILLUSTRATION** | **RATIONALE/**  **COMMENTS** |
| --- | --- | --- |
| Connect to IP Address of CA PAM Device.  Use an account with the proper access to perform this function (e.g. “super”) | https://<IP of Device>  or use the PAM Client pointed to CA PAM Device |  |
| Click on “Credentials > Manage Targets > Accounts” |  | A New Window/Tab will appear. |
| Click on “ADD” |  |  |
| Once you select the Host Name, the window will change to proper setup depending on type of OS platform  Select ***Application Name***  alcrtpextp01\_linux\_PM/DSCV |  |  |
| Then fill in the rest of the fields:  Account Name  s-pam-unix  PVP  Pwd Checki-in\_Check-Out |  |  |
| Goto UNIX tab  Select “Use elevated privileges with authentication” |  |  |
| Goto the Password Tab  Select “Update both the Password Authority Server and the target system”  Click “**OK”** |  |  |
| Verify account is Sync’d |  |  |

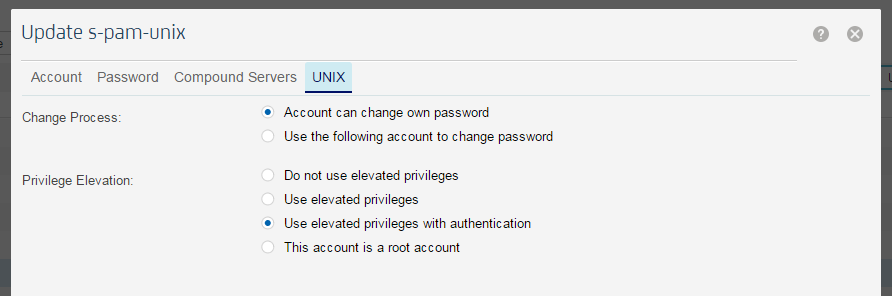
### Using “Admin” account to rotate “root” password

\*\* FYI: a key rotates a key, an account rotates an account, BUT a key CANNOT rotate an account

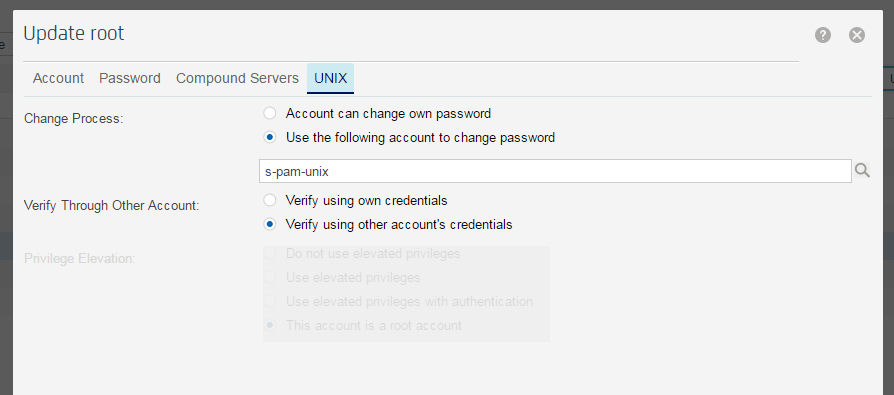
1. Create your Target application for the device (Using the same target application from above)



1. Create your “Admin” account and verify (Using the same target Account from above)
   1. Set account as “Use Elevated Privileged with Authentication”

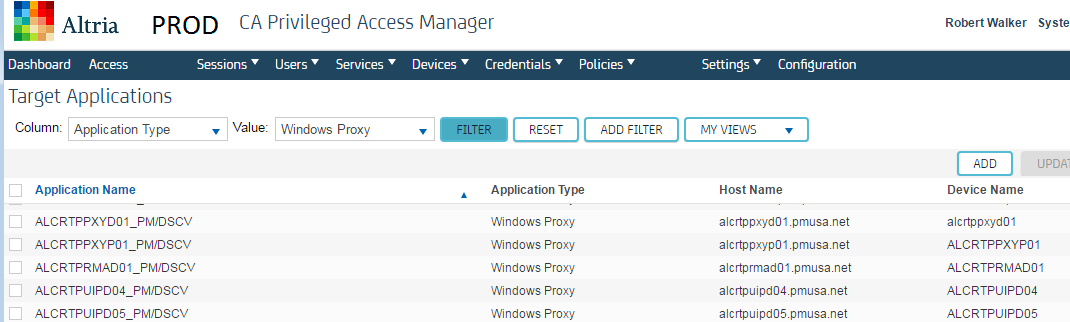


1. Create your “root” account with managed user
   1. Set Privileged Elevation to “This account is a root account”
   2. Set Change Process to “Use the following account to change password”
      1. Root account cannot be logged into directly so the identified account will be used to login to Server and change root’s password
   3. Set the Service Account “s-pam-unix” that is use to manage passwords
   4. Set “Verify through other Account”
      1. This will login as identified account above and verify root’s password

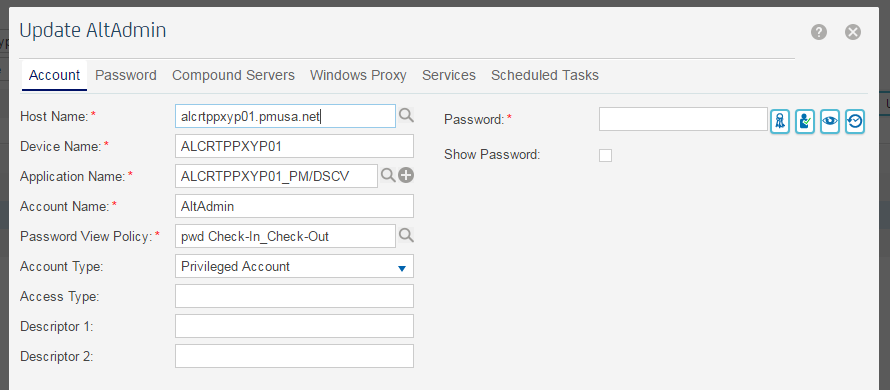


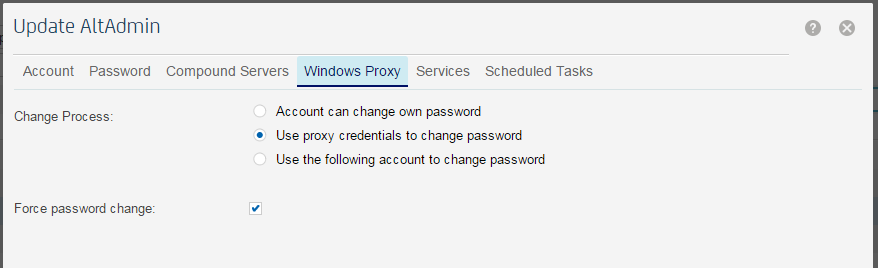
## Win domain Service Account to rotate local users w/ proxy

1. On Windows Server hosting proxy
   1. Click **Start** > **Control Panel** > **Administrative Tools** > **Services**
   2. Right click on cspmagentd and select **Properties**.
   3. Click on the **Log On** tab.
   4. Click the **This Account** radio button.
   5. Type the Domain account name and verify
   6. Restart Service
2. On PAM, setup up Local account
   1. Setup Application
      1. Setup type “Windows Proxy” for local accounts using the proxy server

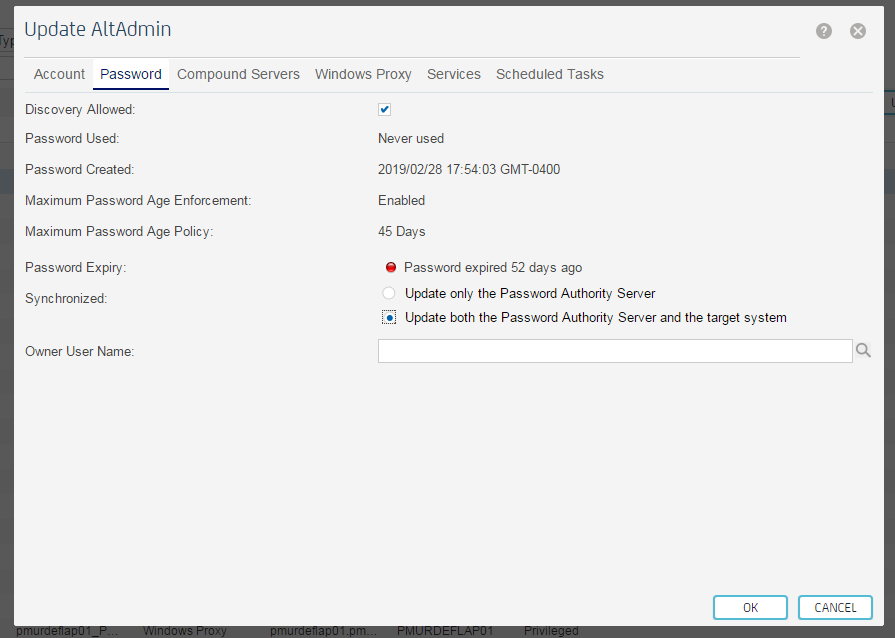


* 1. Setup Account
     1. Setup Local account “AltAdmin” (using Proxy Service credentials to change password)

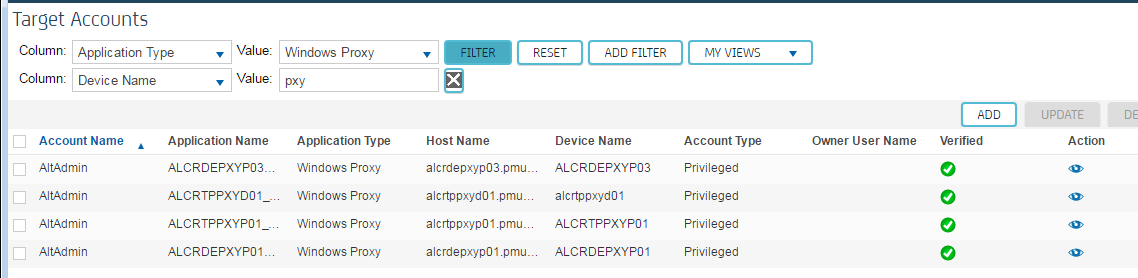




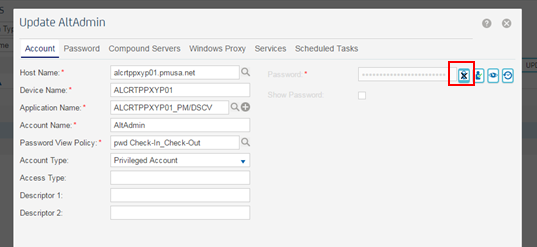
1. Go back to Password Tab
   1. Change synchronized to enable “Update both the Password Authority Server and the target system”
   2. Click OK



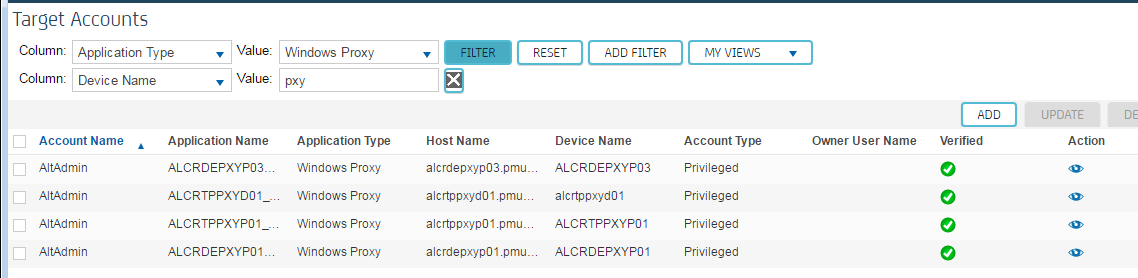
* 1. Check that account is “Verified”



* 1. Re-enter the account and click on the “Generate Credential” and click “OK”



* 1. Account should still be green under “Verify”



# Vaulting “Application” Credentials

There are a number of steps that needs to be performed in order to have PAM vault “Application” credentials.

The first step is to define the target application that will be used to manage the actual target.

The second step is to define the target Account

The last step is to define who has access to the target accounts.

## Defining “Application” Target Application

| **STEP** | **PICTURE/ILLUSTRATION** | **RATIONALE/**  **COMMENTS** |
| --- | --- | --- |
| Connect to IP Address of CA PAM Device.  Use an account with the proper access to perform this function (e.g. “super”) | https://<IP of Device>  or use the PAM Client pointed to CA PAM Device |  |
| Click on “Policy > Manage Passwords”  A New Window/Tab will appear. |  |  |
| Click on the “Targets > Applications”  A window with a list of defined applications appear. |  |  |
| Click on “magnifying glass” icon to search for device |  |  |
| Enter Application Name  <AppName\_UserName\_ purpose>  SAP\_DBAdmin\_Vault  Use default Application Type > Generic  Enter PCP  -- None --  NOTE: No PCP required since PAM will not manage password rotations |  |  |
| Verify Target Application is created |  |  |
|  |  |  |

## Defining “Application” Target Account

| **STEP** | **PICTURE/ILLUSTRATION** | **RATIONALE/**  **COMMENTS** |
| --- | --- | --- |
| Connect to IP Address of CA PAM Device.  Use an account with the proper access to perform this function (e.g. “super”) | https://<IP of Device>  or use the PAM Client pointed to CA PAM Device |  |
| Click on “Credentials > Manage Targets > Accounts” |  | A New Window/Tab will appear. |
| Click on “ADD” |  |  |
| Once you select the Host Name, the window will change to proper setup depending on type of OS platform  Select ***Application Name***  alcrtpextp01\_linux\_PM/DSCV |  |  |
| Then fill in the rest of the fields:  Account Name  s-pam-unix  PVP  Pwd Checki-in\_Check-Out |  |  |
| Verify account is created |  |  |

## Defining Policy to “view” vaulted “Application” credentials

The following steps will define a policy for a User to be able to access the Device via RDP or SSH.

**NOTE**: The following steps will only allow the authorize user the ability to use the PAM Device the capability to login to the RDP Device. The authorized user will still need to provide the correct credentials to login to the device.

| **STEP** | **PICTURE/ILLUSTRATION** | **RATIONALE/**  **COMMENTS** |
| --- | --- | --- |
| Connect to IP Address of CA PAM Device.  Use an account with the proper access to perform this function (e.g. “super”) | https://<IP of Device>  or use the PAM Client pointed to CA PAM Device |  |
| Click on the “Policy” Menu.  Click on the “Manage Policy” menu. |  |  |
| Click on the “ADD” button to create a new policy.  The policy will appear with additional tabs for access options. |  | NOTE: This field is context sensitive. The list of entries defined below will decrease until you see the specific user or group that will be selected. |
| In the “User (Group):” select the names of the user or group you use to manage. |  | NOTE: This field is context sensitive. The list of entries defined below will decrease until you see the specific user or group that will be selected. |
| In the “Device (Group):” select the name of the device or device group you want to manage. |  |  |
| Now click on the “Access” Tab. |  |  |
| Click on the “Save” button to save the policy. |  |  |
|  |  |  |
| The policy should appear with the Access enabled. |  |  |
| Goto Access Page to see Windows Devices for access  Click on Target Applications dropdown  Click on admin account with the correct Application |  |  |
| Enter a reason for viewing password |  |  |
| Password will be displayed |  |  |

# SSH Key

### Setting Up PAM to Utilize/Manage SSH Keys for Authentication to Target Device

*The following steps allow PAM to utilize SSH Keys to login to a target device. PAM will also manage the rotation of those SSH Keys as well. This serves as an alternative form of authentication.*

*NOTE: This is Method 1: The key pair exist on the target account on the target endpoint. This method shows the creation of the pair via ssh-keygen.*

*NOTE: Be aware of which public key | private key pair to utilize. It is possible for PAM to generate its own public key | private key pair. This is shown in Method 2*

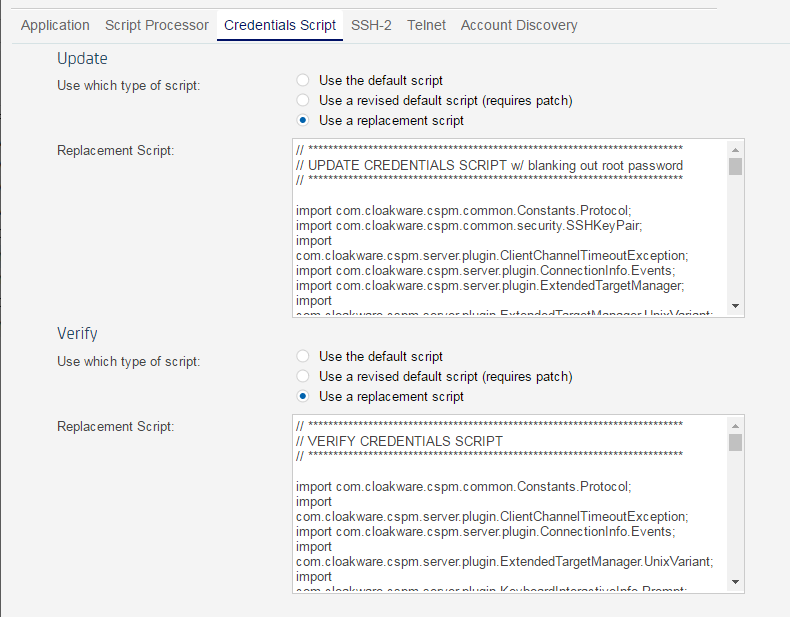
| **STEP** | **PICTURE/ILLUSTRATION** | **RATIONALE/**  **COMMENTS** |
| --- | --- | --- |
| Create “test” Account on target UNIX/Linux endpoint.  In this example, the test account created will be “pamtestxx”  Also set the password for the “test” account. |  |  |
| Login as “test” account. |  |  |
| Create the SSH keys on the target UNIX/Linux endpoint. Use the following command:  ssh-keygen -t rsa -b 2048  Take the defaults.  NOTE: It is possible to set a passphrase. In this example, passphrase was not use. |  | This creates both the private and public key. |
| “cp” or “scp” the “id\_rsa.pub” file to “authorized\_keys” |  |  |
| Login to CA PAM with authorized administrator account.  In this example, the “super” account is used. |  |  |
| If the target device is defined, skip to “**GO TO TARGET APPLICATION**“  If the target device is not already defined, create the device.  Go to “Device” > “Manage Devices”  Click on the “Create Device” Link. |  |  |
| Enter the appropriate Device Name, the Address (IP Address), and the Operating System. |  |  |
| In the “Access” Section, click on the “SSH” link.  The SSH Service should appear below.  Click the “OK” Button to save the device definition. |  |  |
| **GO TO TARGET APPLICATION**  Click on “Credentials > Manage Targets > Applications” |  |  |
| **CREATE TARGET APPLICATION**  Click on the “Add” button to define the new SSHKEY target application. |  |  |
| Click on the “Magnifying Glass” icon to search for the target device that you defined.  In the following pop-up window, select the target device.  It will pre-populate the “Host Name” and “Device Name” text boxes.  In the “Application Name” box, type “SSHKEY-“. Also add the Device Name.  This is to ensure that the solution administrator knows the target application associated with the target device. |  |  |
| Click on the “Devices” > “Manage Passwords” |  | Now that the device is defined, and the target application is defined, the next step is to define the target account that will be managed. |
| Click on the “Add” button at the bottom right of the screen. |  |  |
| In the next screen, click on the “magnifying glass” icon across from “Application Name”. |  | By doing this, select the appropriate Application Name, and the other appropriate text boxes will be filled automatically. |
| Click on the applicable “target application”.  If necessary, click on the buttons below to locate the “target application” |  |  |
| With the top three text boxes auto filled, enter the “target account name”  Click on the radio button for “SSH-2 Public Key Authentication”  Select the appropriate “Password View Policy”  NOTE: The “Public Key”, “Key Options”, and “Private Key” text boxes will appear below. |  | The password view policy will allow an authorized individual the ability to actually view the private key associated with the password.  The password view policy can be set so that if this private key is viewed, it can be automatically changed.  It is recommended that a “password view” policy be created specifically to address ssh-keys |
| On the target machine (using the target account), “cat” the “id\_rsa.pub” file.  Copy the contents and put into the appropriate text box in CA PAM. |  |  |
| Perform a similar function with the “id\_rsa” file.  “cat” the id\_rsa” file. Copy the  NOTE: Ensure to capture all of the private key. The top line begins with:  -----BEGIN RSA PRIVATE KEY-----  The last line should include:  -----END RSA PRIVATE KEY-----  Copy the key into the text box of CA PAM for the “private key” | C:\Users\ifupe01\AppData\Local\Temp\SNAGHTML276a481f.PNG |  |
| Click on the Save Button.  The account will be saved successfully. |  |  |
| To verify the certificate change, click on the newly created account. |  |  |
| Click on the “Generate Key Pair”.  Notice that the public key and private key values change.  Ensure the radio button for “Update both the Password Authority Server and the target system” I selected.  Click on the “Save” button below. |  |  |
| The account is saved successfully. |  | Ultimately, build a policy to allow an end user to login to the machine with this test account via ssh. |

# Password script changes

1. Default script:



1. To make changes insert script into replacement script area
   1. UNIX variance that require replacements:
      1. **AIX**
         1. **Script Update – AIX\_root\_updatescript.txt**
         2. **Script Verify – AIX root uses Default**
         3. **Script Update – AIXAdmin\_updatescript.txt**
         4. **Script Verify – AIXAdmin\_verifyscript.txt**
      2. **HP-UX**
         1. **Script Update – HPUX\_root\_clearpassword\_script.txt**
            1. **Script required to bypass need for old password to be provided**
         2. **Script Update – Admin uses Default**
         3. **Script verify – HPUX\_PROD\_Admin\_verifyscript.txt**
            1. **admin & root use same verify**
            2. **login of root in PROD required logging entries that were bypassed**
      3. **LINUX – using default Script for Admin and root**
   2. UNIX Replacement Scripts for each platform are located here: <https://altriadocs.altria.net/ecm/llisapi.dll?func=ll&objId=85644196&objAction=browse&viewType=1>



# Policy – Composition/View

There are two types of policies that manage passwords within PAM – password composition/view policies.

## Defining Password Composition Policy

A Password Composition Policy defines the password policy that will be leveraged when PAM changes the password policy based on when the password is being managed outside of an end user interaction. A Password View Policy is a password policy that will determine what to do when the password has been viewed by a user, or when to change the password.

It is important to develop an effective password composition policy that will work. Also consider the fact, if using the A2A (application to application) functionality, that some application may not like the password value to contain specific characters as the application may consider them as a control character (i.e. in a shell script).

By default, a password

NOTE: It is recommended to create a password policy that aligns closely or more restrictive than the policy on the target endpoints the policy will be associated.

***Defining Password Composition Policy - Windows***

| **STEP** | **PICTURE/ILLUSTRATION** | **RATIONALE/**  **COMMENTS** |
| --- | --- | --- |
| Connect to IP Address of CA PAM Device.  Use an account with the proper access to perform this function (e.g. “super”) | https://<IP of Device>  or use the PAM Client pointed to CA PAM Device |  |
| Click on “Credentials > Manage Targets > Password Composition Policies” |  |  |
| Click on the “Add” button. |  |  |
| Add a Name to the policy and enter a description for the new password policy that will be created.  BP: Minimum should be at least 8  FYI: PAM will always use Max when it generates a password either manually from icon or when scheduled |  |  |
| You should now see a PCP for use on the Target Application. |  |  |

## Defining Password View Policy

**NOTE:** Password view policies apply only to password administration with the GUI, CLI, or Java API. Requests from A2A clients are unaffected by password view policies.

| **STEP** | **PICTURE/ILLUSTRATION** | **RATIONALE/**  **COMMENTS** |
| --- | --- | --- |
| Connect to IP Address of CA PAM Device.  Use an account with the proper access to perform this function (e.g. “super”) | https://<IP of Device>  or use the PAM Client pointed to CA PAM Device |  |
| Click on “Credentials > Workflow > Password View Policies” |  |  |
| Click on the “Add” button |  |  |
| Enter the name of the password policy.  Add a description.  Click on the “Reason Required for View” (This will prompt the user why the user wants to view the password)  Click on “Change Password on View” (This will change the password when the password is viewed)  Click on “Check-out/Check-in” (This will give the user 60 mins to complete their actions before it forces the check-in and rotates the password)  Click on “OK” |  | If the “Check-out/Check-in” box is selected, then the “Change Password Interval” will be unselected.  **IMPORTANT NOTE**: Selecting “Check-out/Check-in” box will set the target account to be “exclusive” – meaning no one else can check out the account. |
| You will see your newest PVP listed |  |  |

# Transparent Login for UNIX

## “su” to root user

***When someone logs in with their “named” or the “role-based service account”, and now we want them to “su” to root, without knowing root’s password, we perform the following steps.***

***NOTE: Make sure that the account used for transparent login is defined prior to defining***

| **STEP** | **PICTURE/ILLUSTRATION** | **RATIONALE/**  **COMMENTS** |
| --- | --- | --- |
| it is disabled by default, check Configuration/Security/Access > Command String |  |  |
| Need to modify Target Device Definition. Go to “Devices > Manage Devices” |  |  |
| Select the device that will be configured with Transparent Login.  The Manage Device Information Screen will appear. |  |  |
| Enter the commands that will prompt users for the password. |  |  |
| Go to “Policy > Manage Policies” |  |  |
| Click on the “OK” button to save the change. |  |  |

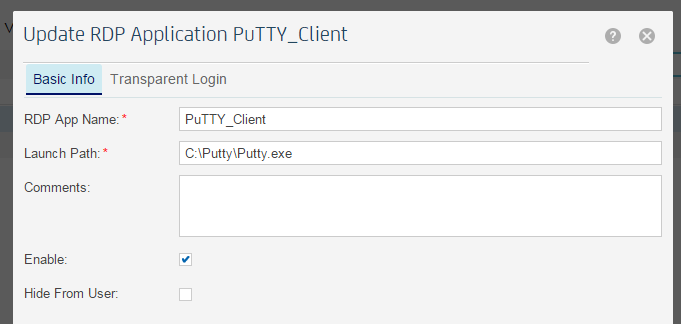
## Auto-login w/Admin account – N/A

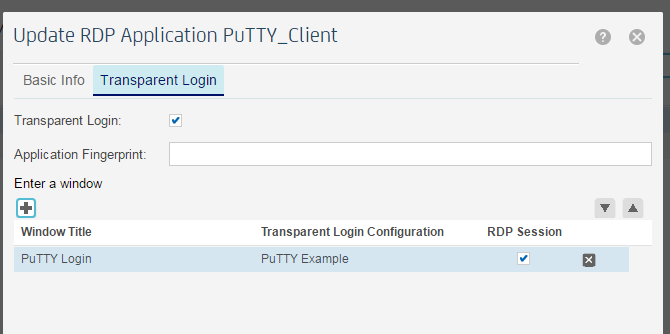
Scenario: Utilizing SSO on for a Group of Unix Servers

When assigning Transparent Login, the option is available on Individual Devices, however when creating a Device Group the Transparent Login option is not shown and subsequently within a Policy you cannot enable TL.

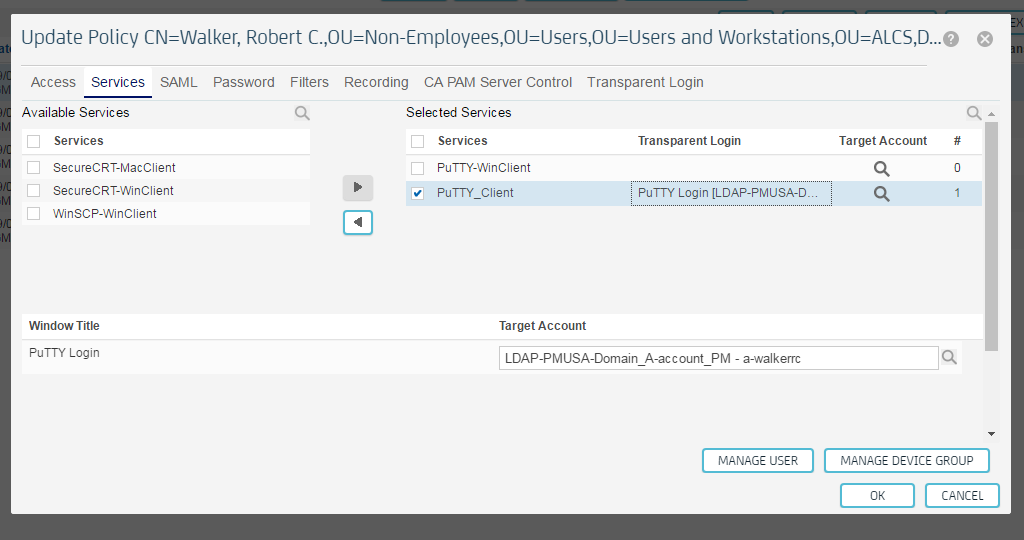
Work Around:

1. Create a RDP Application with Transparent Login enabled. (for the TL config I simply selected one of the OOTB example ones)





1. Assign the “Putty\_Client” Service created for the Device Group. Within your Policy, now you can select Transparent Login



* This “could” use a different account to make the RDP connection and run the application or you can use the same account
* User will not be able to access the RDP session, they will only view the Application window when launched

# Windows RDP Applications – Publishing

First step to configuring CA PAM to publish RDP apps is to ensure that “Remote Desktop Services” is loaded.

\*This may require additional licenses from Microsoft to enable

\*This may require additional licenses for Applications run in Terminal Services

NOTE: This configuration requires the work target endpoint be a member of a domain. The following work was conducted on a Domain Controller

### Enabling Remote Desktop Services – Windows 2012

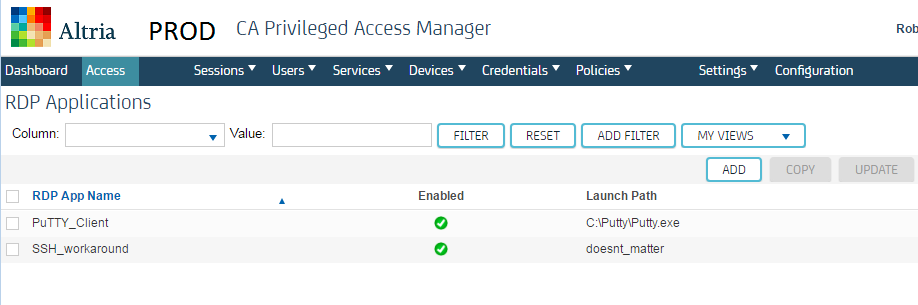
| **STEP** | **PICTURE/ILLUSTRATION** | **RATIONALE/**  **COMMENTS** |
| --- | --- | --- |
| Bring up Server Manager. Move cursor to bottom left hand corner of screen, and click on the “Server Manager” icon. |  |  |
| Click on “Add roles and features” link. |  |  |
| Click on the checkbox “Skip this page by default” and click the “Next” button. |  |  |
| Select “Role-based or feature-based installation”  NOTE: If the work is being done on a domain controller, select the “Remote Desktop Services Installation” |  | NOTE: The Remote Desktop Services Installation is used for VDI (thin clients – and not using a real laptop) |
| Select “Standard deployment” |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| Reboot the server (if not the server did not reboot itself) |  |  |
| Click on the Server Manager Tab |  |  |

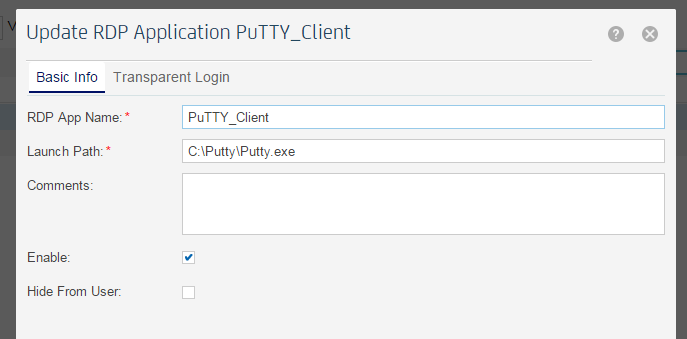
### Defining Applications for Remote Desktop Services – Windows 2012

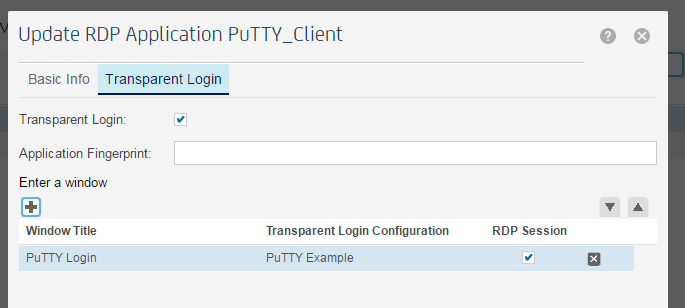
| **STEP** | **PICTURE/ILLUSTRATION** | **RATIONALE/**  **COMMENTS** |
| --- | --- | --- |
| Bring up Server Manager |  |  |
| Click on “QuickSessionCollection”  In the “REMOTEAPP PROGRAMS” section, click on the “TASKS” and select “Publish RemoteApp Programs”  \*\*CMD setup is REQUIRED |  |  |
| Select the Application that will be published.  NOTE: This screen may take a while to populate depending on how many applications are available on the target server. |  | NOTE: If the application does not appear on screen, it is possible to click on the “Add…” button to build one.  This process will need to be used when enabling Learning Mode for Windows Transparent Login. This will involve creating a “cmd.exe” with appropriate switches. |
| Look for the “cmd.exe” command.  Configure the search to look for results in “c:\Windows\System32\”. When the cmd.exe tool is located, select it so that the “File name” field is populated. Click on the “Open” button to continue. |  |  |
| <THERE IS A MISSING STEP – NEED TO MODIFY IT LATER.> |  |  |
| In the “REMOTEAPP PROGRAMS” button, highlight the “cmd” program, and select “Edit Properties” |  |  |
| Click on the “Parameters”.  Click on the “Always use the following command-line parameters”.  Enter the following text into the field:  /C title Initializing RDP session&echo Please wait...&timeout 4 /nobreak>nul&"\\tsclient\virt\xcd\_run.bat"  Click on “Apply” and click on “OK” to continue. |  |  |
|  |  |  |
| Click on “QuickSessionCollection”  In the “REMOTEAPP PROGRAMS” section, click on the “TASKS” and select “Publish RemoteApp Programs” |  |  |
| 1. 1) Click ***Add*** and in center screen work through to windows\system32\cmd.exe and add   \*\* if you work through the left side tree, it will say cannot find application   1. 2) Then select “cmd” and right click to edit properties 2. 3) Select 2nd menu option - **Parameters**, select the **Always use the command-line arguments** option and set its arguments using the string provided in the box below.   ***NOTE*** *Whether you copy-and-paste this string or type it in manually, make sure that you do not introduce any additional hidden characters and/or white space. Otherwise, the command may not work.* | ***/C title Initializing RDP session&echo Please wait...&timeout 4 /nobreak>nul&"\\tsclient\virt\xcd\_run.bat"*** |  |
| Select the Application that will be published.  NOTE: This screen may take a while to populate depending on how many applications are available on the target server. |  | NOTE: If the application does not appear on screen, it is possible to click on the “Add…” button to build one.  This process will need to be used when enabling Learning Mode for Windows Transparent Login. This will involve creating a “cmd.exe” with appropriate switches. |
| Click on the “Publish” button. |  |  |
| Click on “Close” button to complete the process. |  |  |
| The newly publish application should appear. |  |  |
|  |  |  |

### Create RDP Applications setup

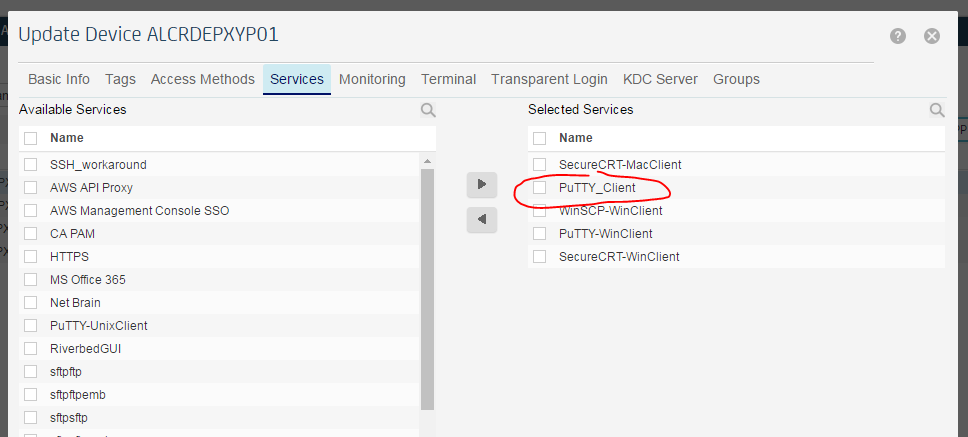
1. To use learn mode, you must have RDP access allowed as well as the RDP service
2. Setup up the RDP application:



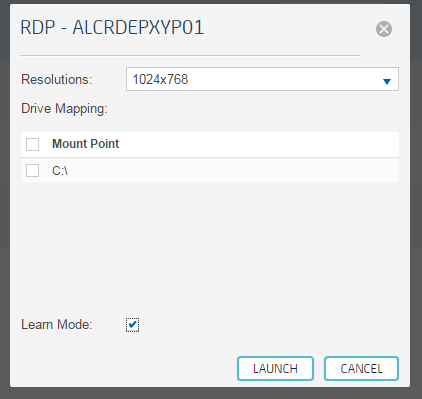




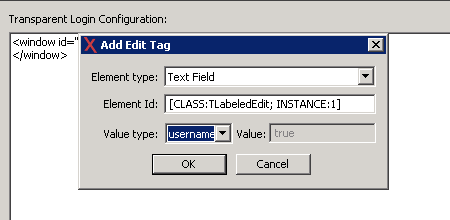
1. Goto Device & Device Group and add the service



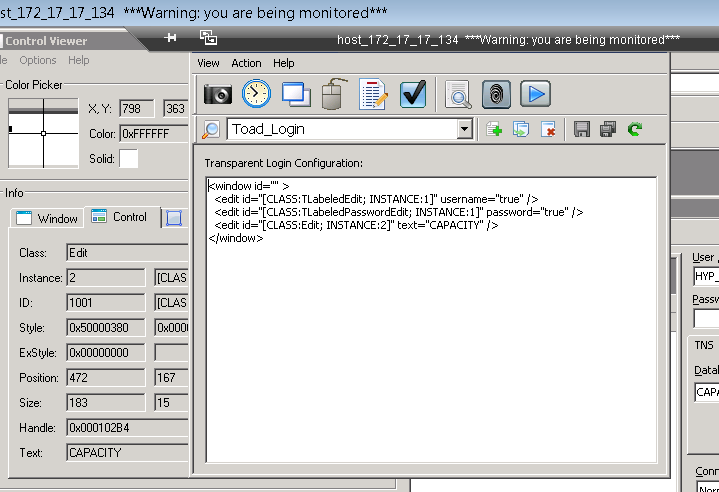
1. Goto Access page and click the black triangle on RDP icon and click “Learn Mode” checkbox and launch



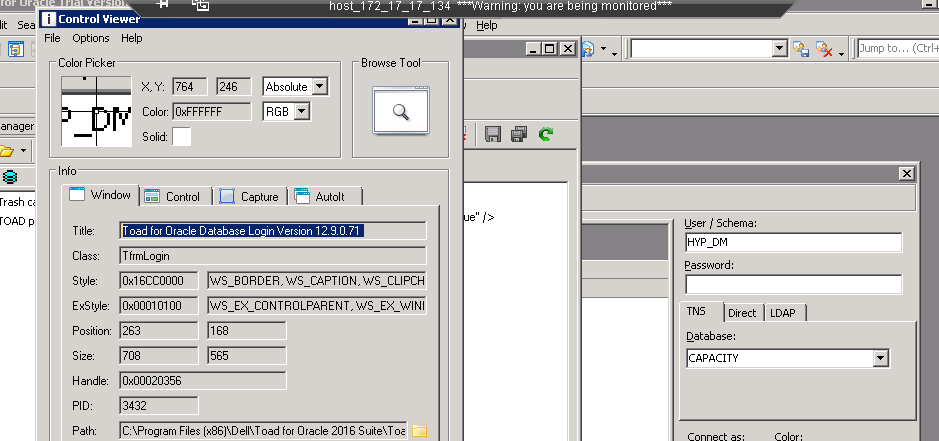
1. Open control viewer switch to control tab
2. Drag the magnifying glass to the field on the application page to be managed
3. Go back to the Control viewer and copy the Instance field



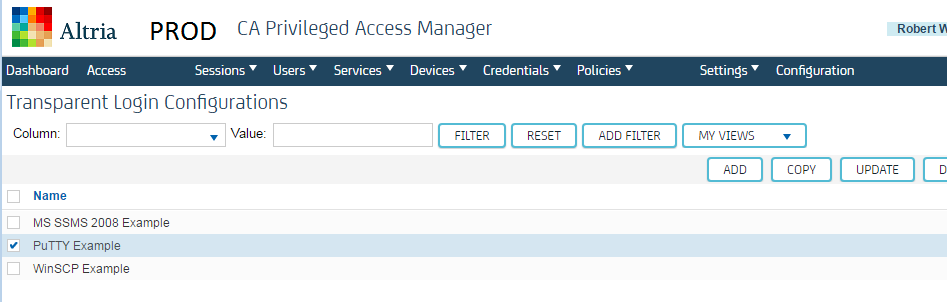
1. After you have added all edits

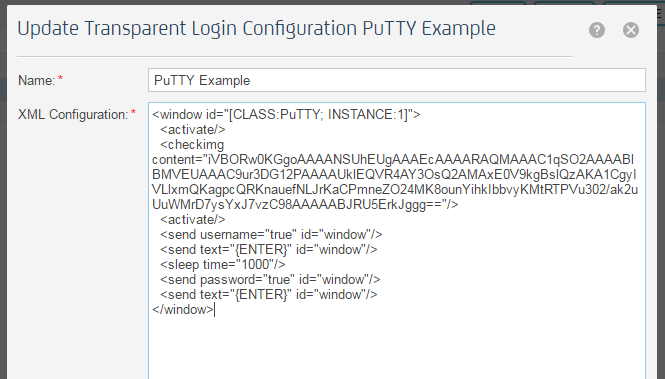


1. To get the Window title go back to Learn Mode and grab the focus window title

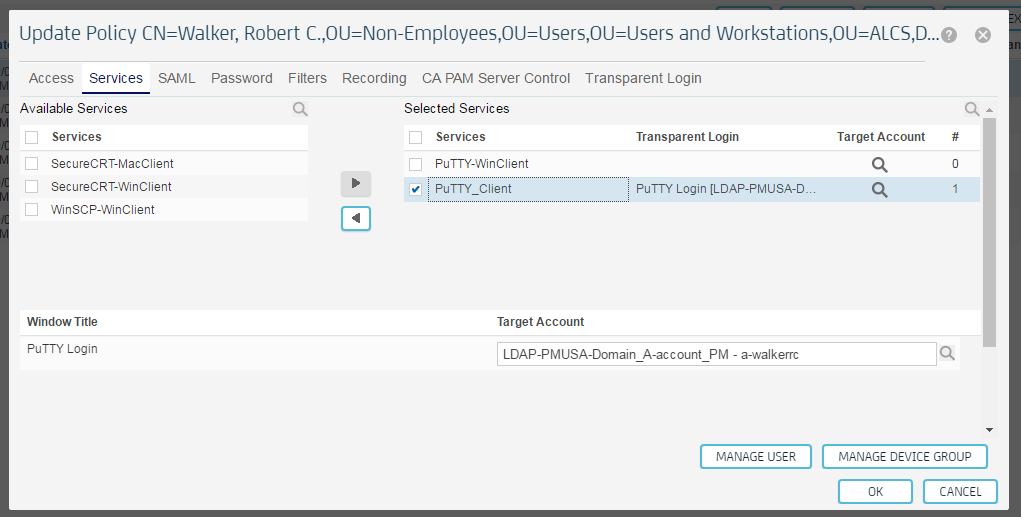


1. Once saved, file will be visible in Transparent Login Config screen

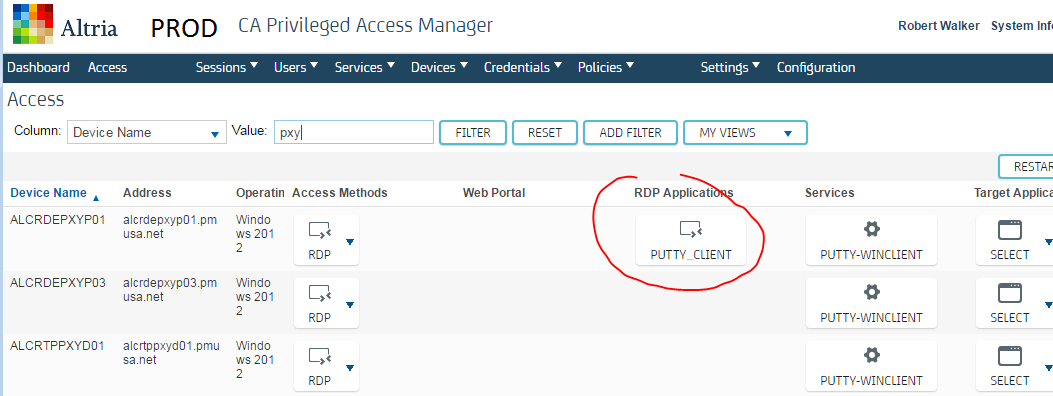




1. Goto Policy and add the Service and Account to be used with Service



1. Click on RDP Application



# Launch Web Applications

For additional information, please refer to <https://docops.ca.com/ca-privileged-access-manager/3-3/EN/implementing/provision-your-server/provisioning-devices/about-access-setup/create-tcp-udp-services/configure-automatic-login-to-web-portals>

| **STEP** | **PICTURE/ILLUSTRATION** | **RATIONALE/**  **COMMENTS** |
| --- | --- | --- |
| Login to CA PAM as authorized end user. |  |  |
| Select Services > Manage TCP/UDP Services |  |  |
| Web Portals ports are how the communication between PAM and Application takes place.  Local IP is ignored for Web Portals |  |  |
| Click on the “ADD” button |  |  |
| In the Basic Info tab click on **Application Protocol** dropdown and select “Web Portal” |  |  |
| In the Basic Info tab click on **Browser Type** dropdown and select “CA PAM Browser” |  | NOTE: CA PAMSC ENTM UI can utilize both 18080 (http) and 18443 (https). Make sure that you utilize the appropriate port and Launch URL are set appropriately. |
| In the **Service Name** Field  enter HTTPS  In the **Ports** Field  enter 443  In the **Protocol** Field  enter TCP  In the **Auto Login Method** Field  Select CA PAM HTTP Web SSO  In the **Launch URL** Field  enter https://<Local IP>  In “Access List”, put an “\*”.  Click “OK” button to continue.  Note: if **Launch URL** doesn’t have <First Port> then it will not use what is entered in the **Ports** field and will use default port, usually 443 |  | NOTE: Modify the Launch URL if the access is http or https. |
| Verify Service is created and enabled |  |  |
| Create the Target Endpoint where the Application runs from. Click on the Devices > Manage Devices |  |  |
| Click on “Add” button to create a Device |  |  |
| Enter the Name  Add the FQDN in the “Address:” field  Select the appropriate Operating system.  Click on “Password Management” button, and populate the Description Field. |  |  |
| In the “Services” Tab, click the service to move  Click on the Arrow button to move Service to “Selected Services” |  | Service will be moved to the “Selected Service” List |
| After clicking on the appropriate service, it should appear in the Selected Services Section.  Click “OK” button to Continue. |  |  |
| Create Policy to allow an authorized end user to bring up the web portal  Click “Add” |  |  |
| Select User that is authorized to use Service  Select Device that has the application running to work with the service |  |  |
| Click on the **Service** tab  Select the Service and hit Arrow button  Verify Service is moved to Selected Service List |  |  |
| Goto Access Page and verify Web Portal is available for user on specified devices |  |  |

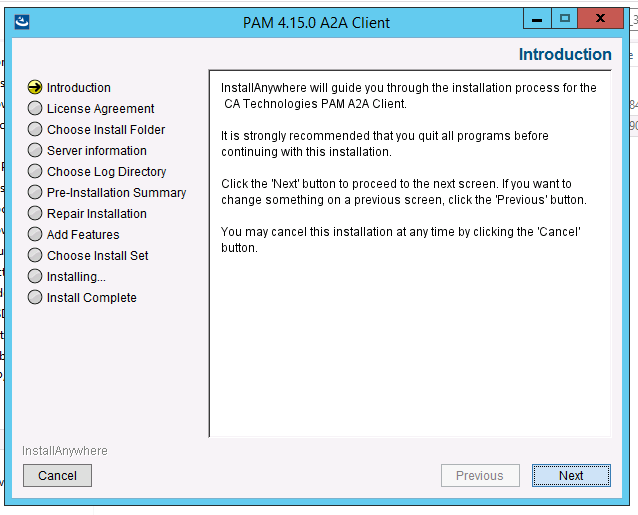
# A2A Client

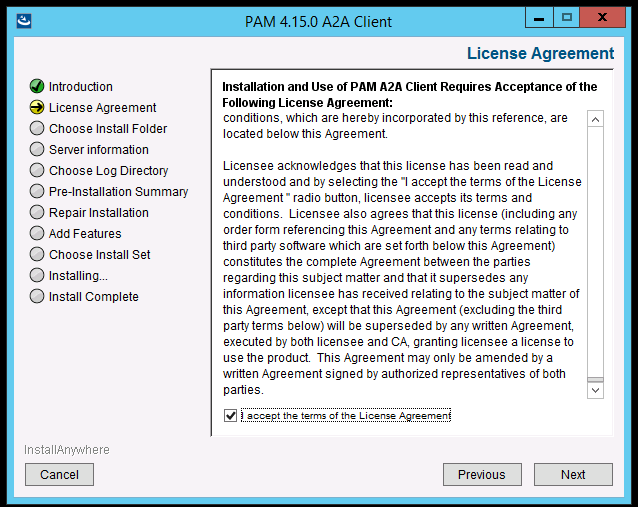
\*\* A2A agents is on Proxy server as an example

\*\* A2A agents need to be installed on Target Application servers

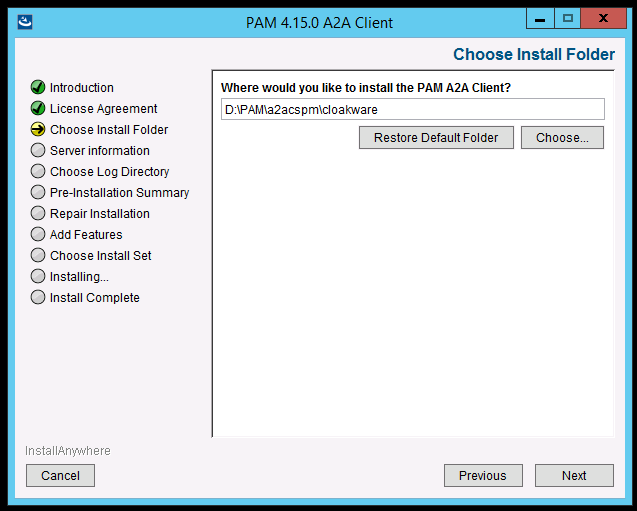
## Install A2A client on the Target Windows Application Servers

1. Installing the A2A client(service) on the Target Windows Application Server ***(where application credential scripts are running)***
   1. Installing proxy by executing the latest Windows A2A Client (***setup\_windows64\_java.exe***)
   2. On the ***Introduction*** page of the installation, click ***Next***

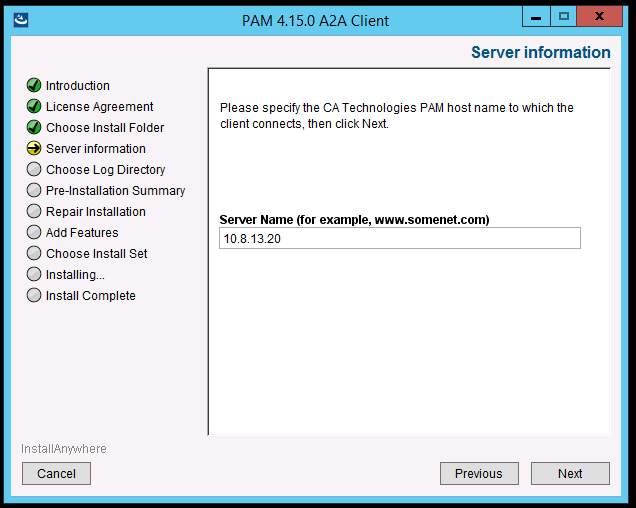




* 1. On the ***Choose Install Folder*** page, click ***Next***, unless you’re required to change the installation folder.



* 1. On the ***Server Information*** page, enter the PAM appliance name in the ***Server Name*** field and click ***Next***. Ensure the name provided here is resolvable.



PROD – 10.8.13.20

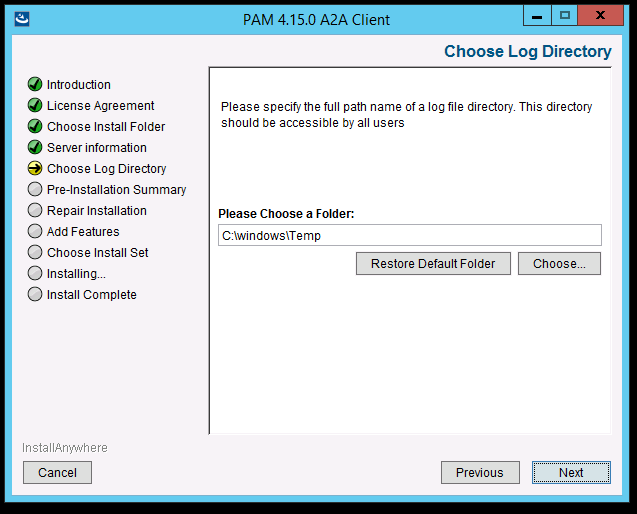
UTS – 10.73.225.110

DMZ – 10.8.58.30

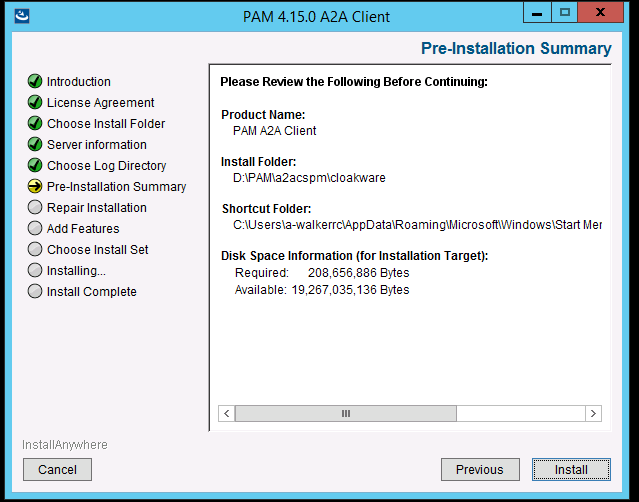
DEV – 10.8.13.25

\*\* may point at any Appliance

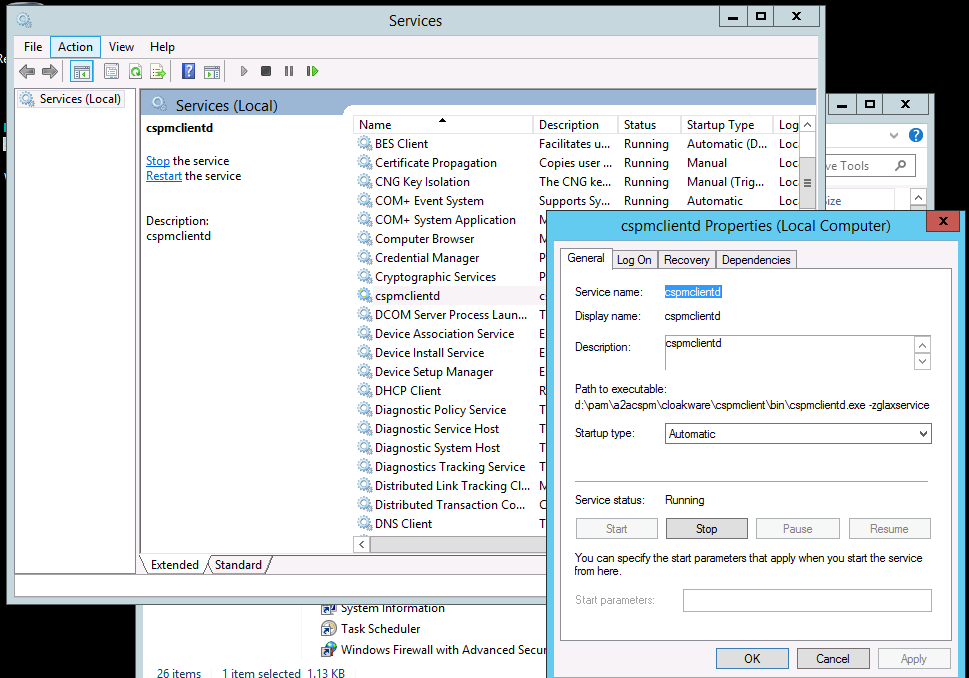
* 1. On the ***Choose Log Directory*** page, use default folder path



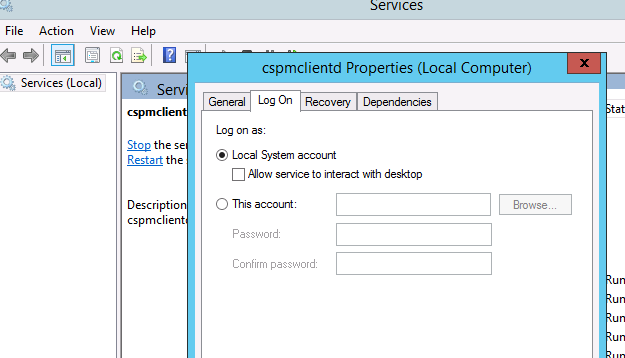
* 1. On the ***Pre-Installation Summary*** page review the provided information and if everything is correct, click ***Install***



* 1. Once the installation is completed, open the Services and verify that the PAM A2A Client (cspmclientd) is installed and present. This service is typically not running. Start it and change its startup type to be automatic.

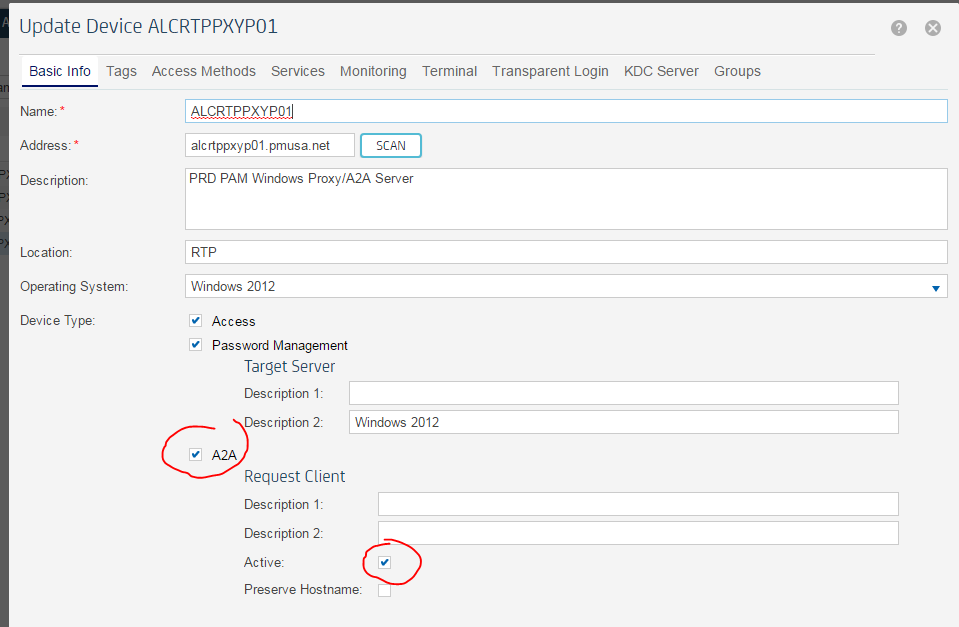


\*\* A2A service can use the “Local System account” to run

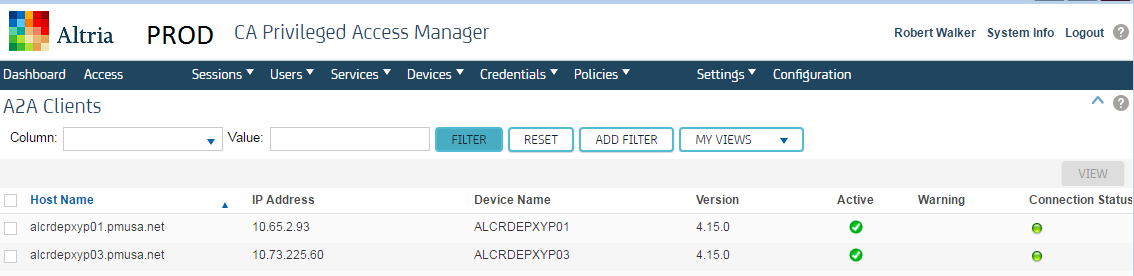


## PAM Steps to enable A2A clients

1. Goto ***Devices*** 🡪 ***Manage Devices***, make sure ***A2A*** and ***Active*** are checked



1. Goto ***Credentials 🡪 Manage A2A 🡪 Clients***, make sure Clients Active icon is “green”



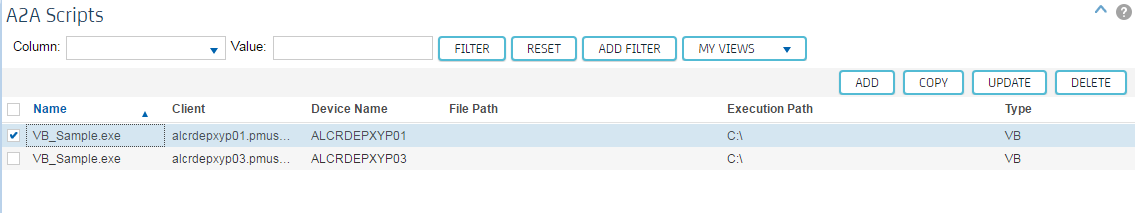
* + 1. Application Users will use A2A template scripts to communicate with PAM

There examples in the A2A folder on both ALCRDEPXYP01 and ALCRTPPXYP01 servers that developers can use to enable their code to request credentials



#### Script

1. Go to ***Credentials*** 🡪 ***Manage A2A*** 🡪 ***Scripts*** and add script info

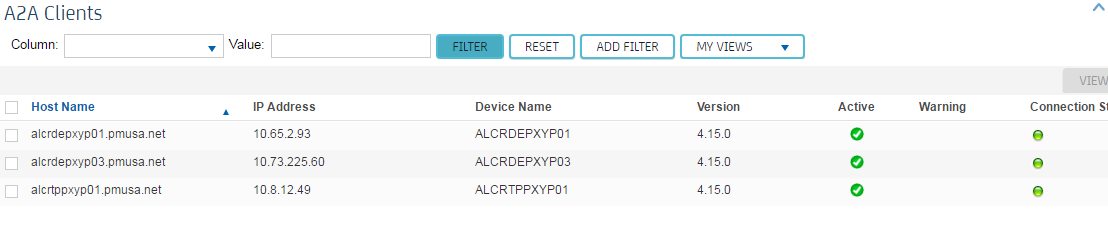


Script/App Name must match exactly with script being run or you get an error “409”

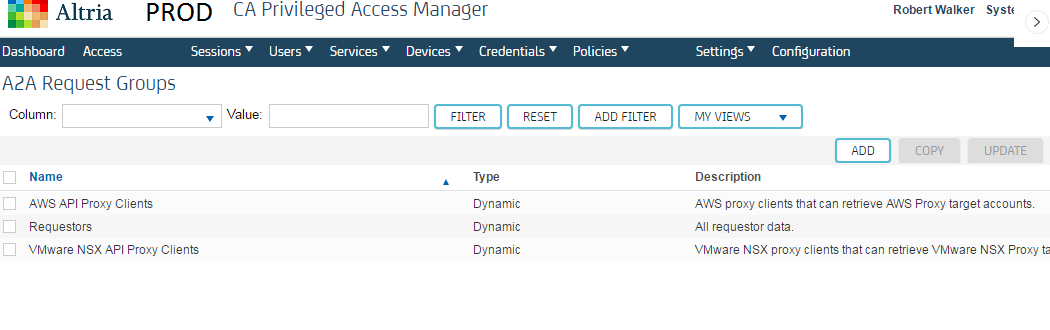
Paths do not have to be correct, depends on mapping options

#### Client

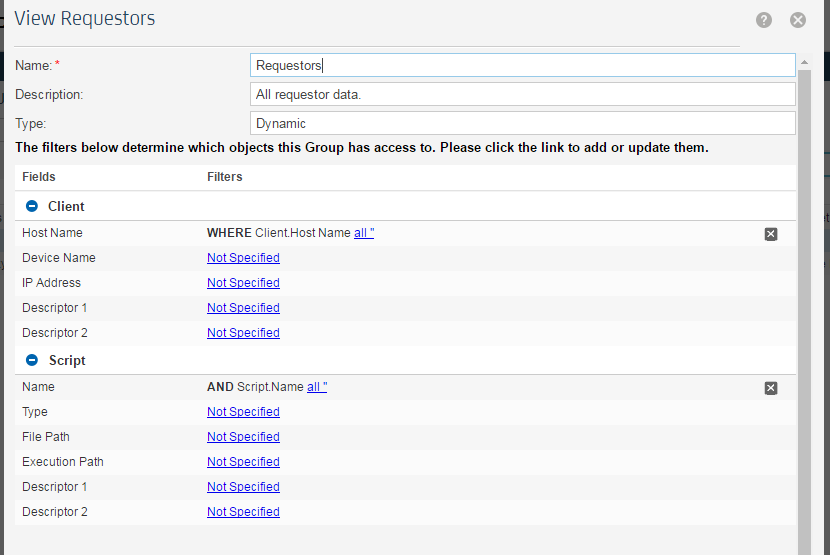
1. Go to ***Credentials*** 🡪 ***Manage A2A*** 🡪 ***Clients*** and you should see ***Requester***



#### Request Group

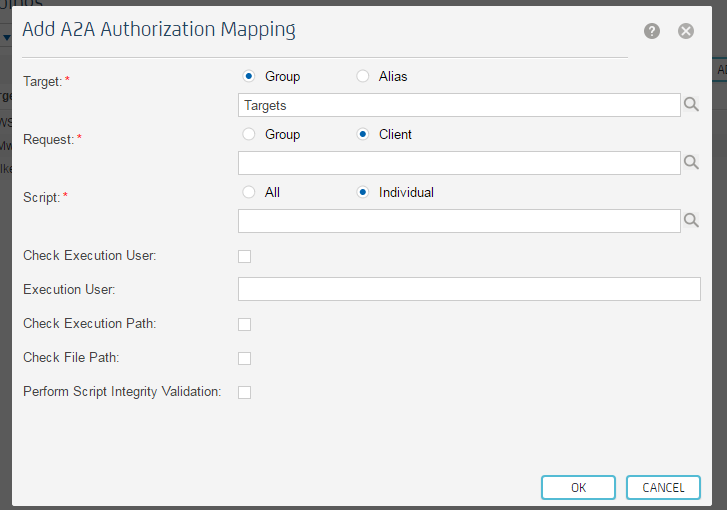


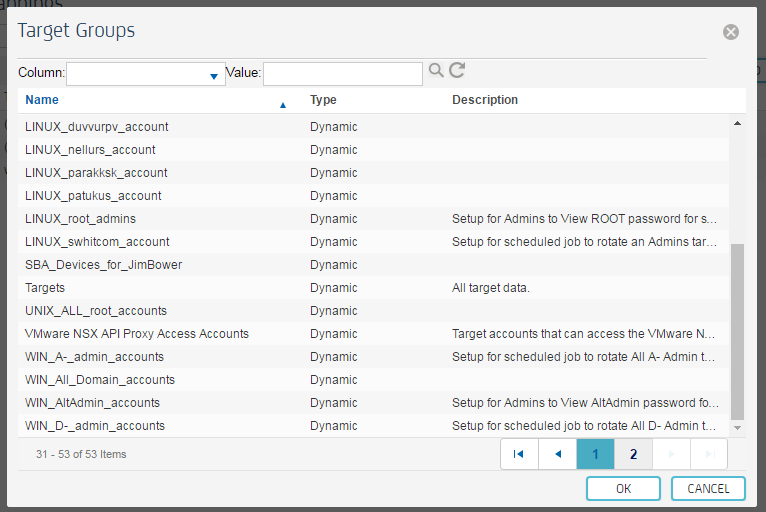
This will combine the Client Agents allowed to make A2A calls and the Scripts allowed to be used by the Agents



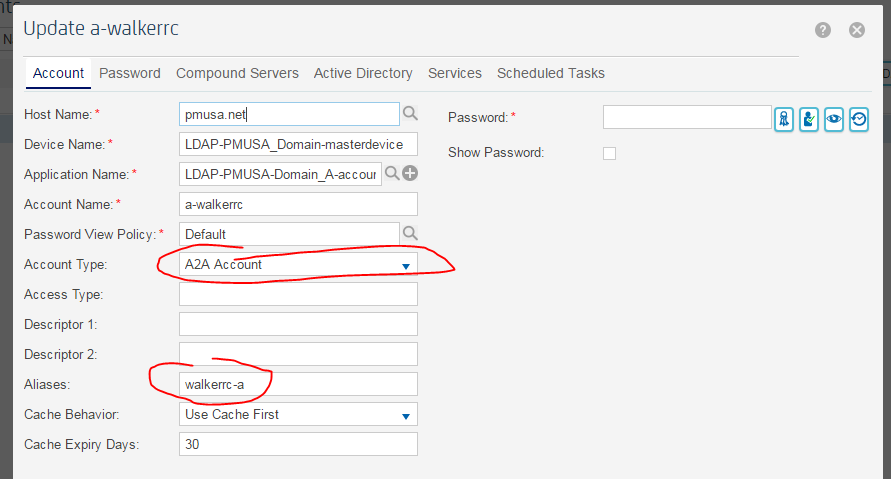
#### Mappings

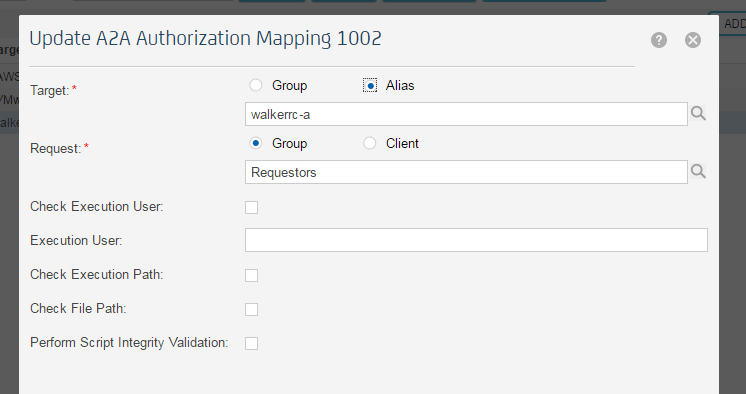
1. Add ***Credentials*** 🡪 ***Manage A2A*** 🡪 ***Mappings*** authorization list item
   1. Target
      1. If using “Group”, select the “Target Group”



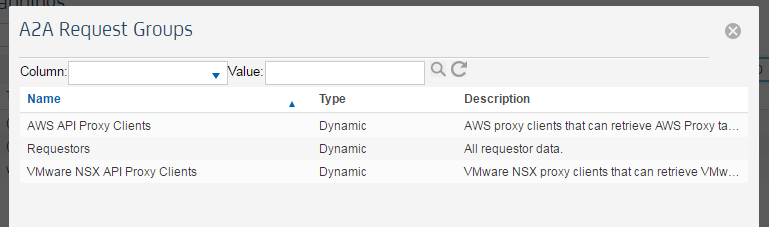


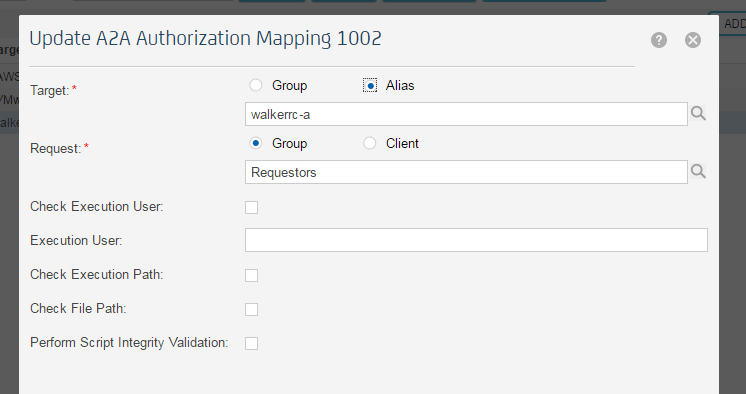
1. If using Alias goto ***Credentials*** 🡪 ***Manage Targets*** 🡪 ***Accounts*** and change account type to A2A Account and add alias name to reference the account credentials



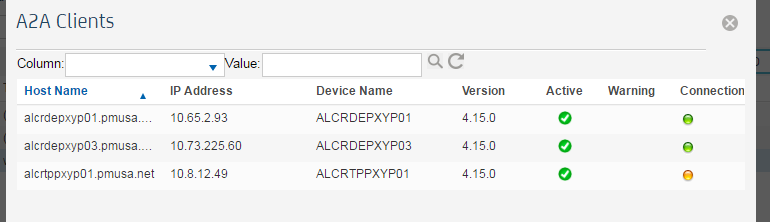


* 1. Request
     1. If you select “Group”, it combines the client agents and the scripts





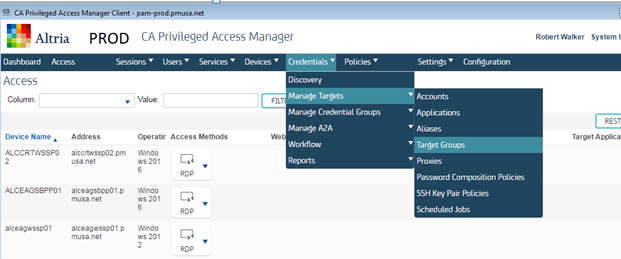
* + 1. If you select “Client”, you are selecting the clients with Agents running



* 1. Script
     1. If you selected the “Request Group” you won’t see this option
     2. If you selected the “Request Client”, you can now select “All scripts OR a single script” setup to run on the Client server you selected

# Schedule Job to rotates local users

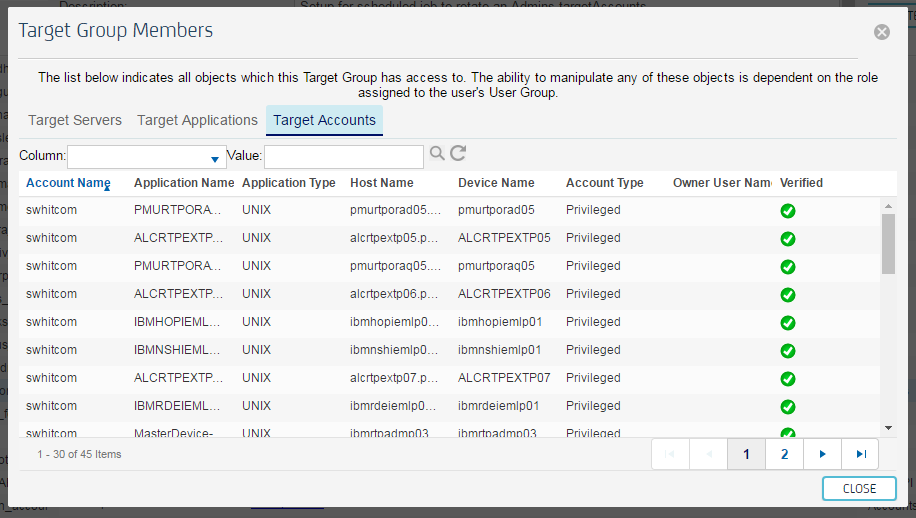
1. Setup a dynamic “Target Group” to list all the accounts to rotate through Scheduled Job



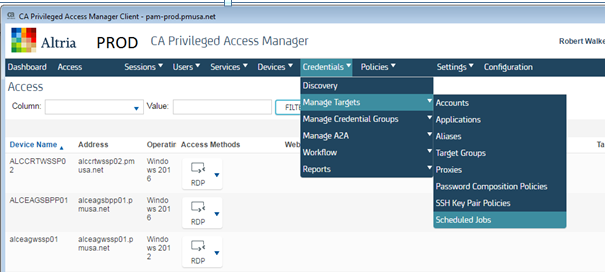
* 1. Add new “Target Group”
     1. Add Name (be descriptive for function of the group)
     2. All Applications Names for a platform (LINUX)
     3. All Application type is “unixII”
     4. Select Admin Account to be rotated (swhitcom)
     5. Click “SHOW”

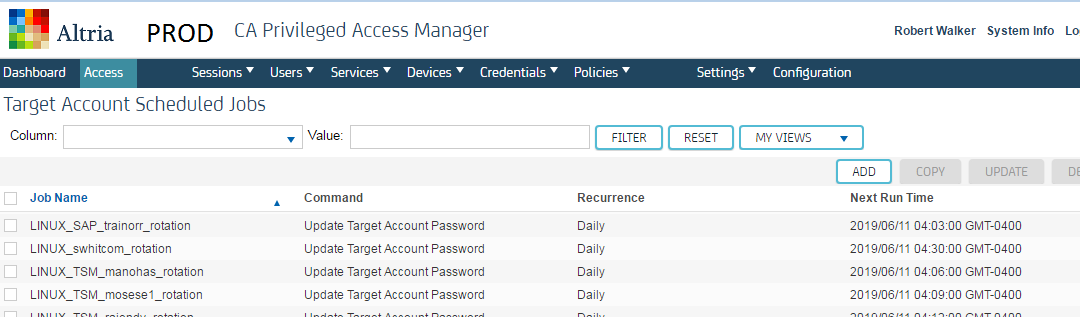


* + 1. Click on “Target Accounts” tab to verify accounts listed

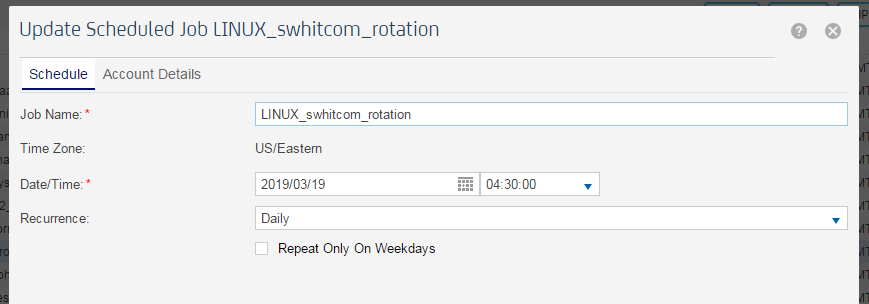


1. Setup a Scheduled Job using the “Scheduled Jobs”



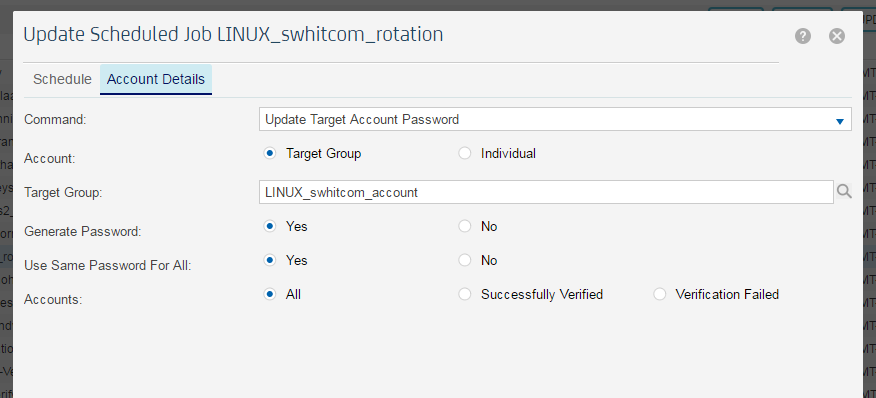


1. Click “ADD”



* 1. Create descriptive name, pick Date/Time and Recurrence

1. Setup a scheduled job using the “Target Group”



* 1. Select Command, Type of Account (Target Group) and select the Group
  2. Choose if you want a “new” password
  3. Choose if you want the same password used for each of the accounts
  4. Choose if you want this applied to all accounts, verified accounts or verify failed accounts

***\*\* You cannot rotate accounts that are unverified (status is none)***

# No Access to Appliance

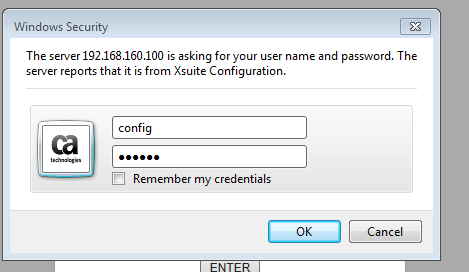
In emergency situations, somehow access to the appliance has been blocked, the only solution is to:

Check to see if config user works?

1. If Physical Appliance
   1. Goto the LED screen on the physical appliance
   2. Click to the “Reset Password” and click <enter>
2. If VM Appliance
   1. Goto the VM Console
   2. Click to the “Reset Password” and <Enter>

This will reset the config user and enable it if it was disabled

1. Goto url (<https://ipaddress/config/> ”
   1. You will get a windows security box



1. Enter reset default credentials > config/config
2. If Super password is unknown, you can enable SSH and have CA Support login and reset the “Super” password