PxM Proof of Concept Configuration

June 2018

Version 3.1

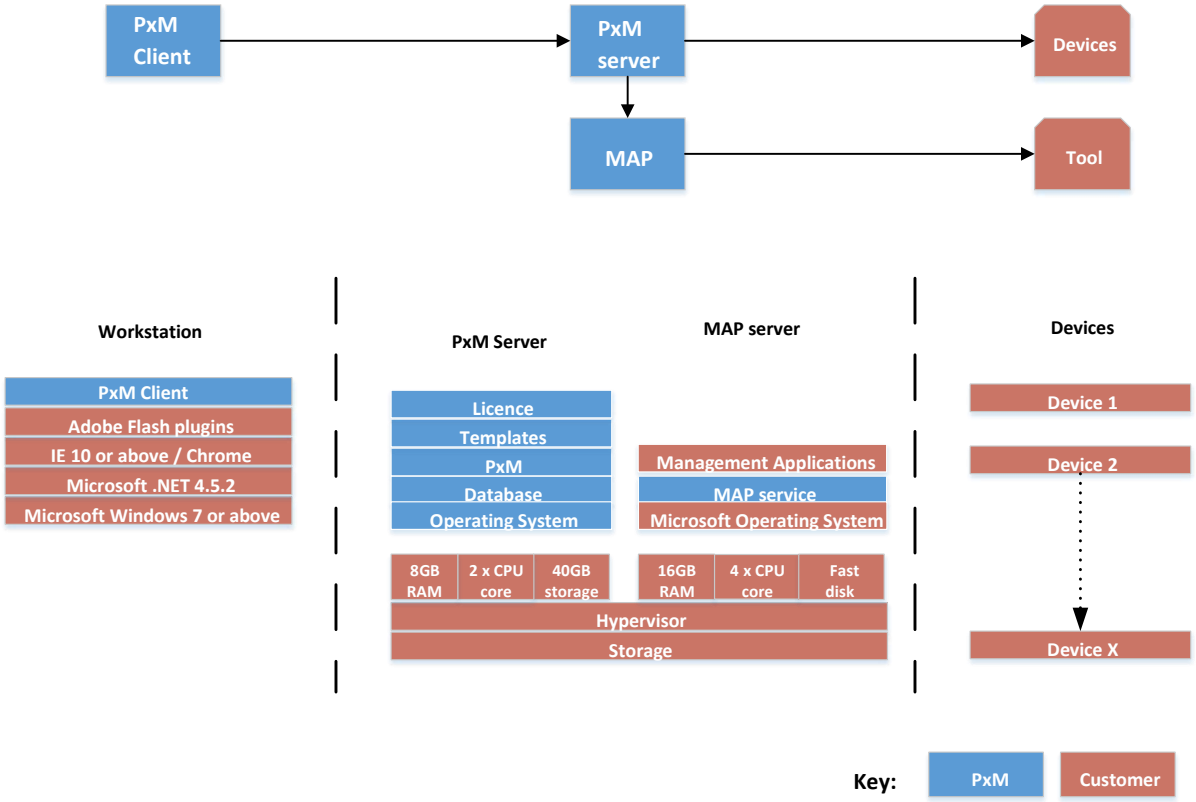
OSIRIUM

Table of Contents

PxM Architecture, Installation & Configuration

This Proof of Concept (POC) Configuration Guide applies to PxM v6.0.x. Before continuing, it is assumed that the PxM Virtual Appliance, MAP server and PxM Client are already installed and configured.

Outlined below are the necessary requirements for this POC.



The following documentation and downloads will allow you to achieve this:

- To request an evaluation license, visit the Osirium Worldwide Locations page to select your region and be directed to the evaluation page.
- The installation and configuration guides for the PxM Virtual Appliance, PxM Client and PxM MAP Server are found on the Osirium Documentation page.
- Register for Support to download the PxM software and the template library bundle.

PxM Proof of Concept (POC) Guide

Introduction

This document is a guide for PxM, a privileged user and infrastructure management solution. It shows how to configure PxM in a 'passive' mode so that it will NOT change any passwords. Several scenarios are covered that you can use to evaluate the PxM product and its features.

Prerequisites

- Access to an Active Directory domain with LDAPS.
- Access to a Windows Domain Member server.
- Access to a command line device (SSH).
- Access to a thick management application.

Objective

At the end of this POC you will be able to:

- Configure PxM to authenticate inbound privileged users via Active Directory using LDAPS.
- Synchronise Active Directory user accounts into PxM.
- Log onto to the PxM Client using a standard user account.
- Single sign on to a Windows Domain Member server through an RDP session.
- Run a task on a Windows Domain Member server.
- Single sign on to a Device through an SSH session.
- Run a task on a device.
- Single sign on to a thick application management tool session via a PxM MAP server.
- Run a task on a thick management application.
- View the device access report.
- Playback a recorded session.
- Search within session recordings to find keywords.
- View the tasks report.

Getting started

The first step is to decide how you want your PxM user to be authenticated, as there are a couple of options:

- **Local authentication:** the PxM user's username/password are checked against the internal PxM database for authentication.

- **External authentication:** Using external authentication allows you to use an existing username/password. Available external authentication options are RADIUS and Active Directory.

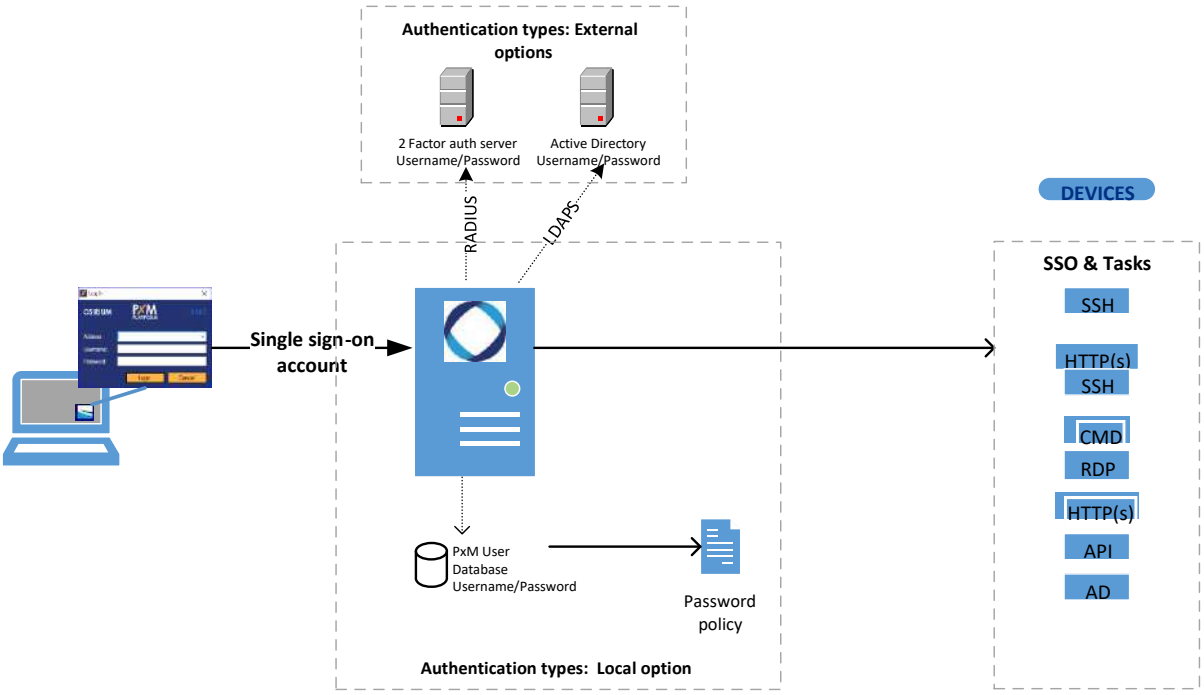
RADIUS: The PxM user created must match the existing username on the external authentication service. PxM will then check with the external authentication service to verify the user before logging the user on to the PxM Client. RADIUS configuration is outside the scope of this POC.

Active Directory: Active Directory users are synchronised using User groups and automatically created in PxM.

PxM uses a two-account model which means:

- **Standard:** Users use a personalised account (username/password) which are used to log onto the PxM Client. This allows them to manage devices and tasks they have been granted permission to. PxM users will know the password for this account.

- **Privileged:** When a PxM user accesses a device through the PxM Client, the appliance uses the privileged account (defined within the profile) to single sign on the device. The user does not know or need to know the credentials because the PxM Platform does the single sign-on to the device.



Creating an Active Directory Service

1. In the left-hand menu, to the right of *Active Directory*, click the icon. The *Manage Active Directory* tab opens and the *New Active Directory* window appears.
2. In the *Create Active Directory* window, fill in the configuration information for your Active Directory service as follows:

Field Name	Description
Name:	Enter the name of your Active Directory to identify it within PxM.

Domain (FQDN):	Enter the fully qualified domain name of your Active Directory. The domain name will be used with a valid username/password to authenticate and provision the Active Directory.
Domain Controller IP/hostname(s):	Enter the IP / hostname of the Domain Controller with Active Directory configured. Multiple Domain Controller IP / hostname(s) can be entered by comma separating them within the field.
UPN Suffixes:	Allows you to enter a list of UPN suffixes PxM should consider when auditing Active Directory. If your domain uses the FQDN as the only suffix, you do not need to specify any here. If you do specify suffixes, you must include the standard FQDN suffix as well.
Container:	Enter the name and location of the Organizational Unit (OU) you want PxM to create. If left blank, the OU will be called Osirium and created in the root of the Active Directory. If the container input field is given a name, for example, *Management Accounts*, then the OU that gets created will be called *Management Accounts* and will be placed in the root of the Active Directory. If the container needs to be placed inside another (or multiple) parent OUs then a DN can be specified to define where to add the PxM OU. For example, for PxM to create an OU called *Management Accounts* inside a parent OU called *Management Tools* then use the following: **OU=Management Accounts, OU=Management Tools** **Note:** The reverse order of OUs in the DN. Do not include any Domain Component attributes (DCs). All parent OUs must already exist, PxM does not create any parent OUs.
Groups of interest:	Enter one or more Active Directory groups, i.e. Domain Admins, Database Admins. For PxM to discover the privileged user accounts in Active Directory, the accounts must be a member of one of the groups of interest listed here.
Control account:	Select **Password known**. (This is what makes it passive.)
User Authentication Service:	Tick the checkbox.

NOTE: All other fields can be left blank.

3. Click **Save**. The *Authentication details* window appears.
4. Within the *Authentication details* window enter a valid **Username/Password.**

   This account will be used as the control account and requires read/write across the domain. PxM will store the account, use it to create the PxM OU on the Active Directory and read the members of the groups of interests, initially and on an ongoing basis.

   NOTE: The PxM OU is only used for Fully Managed accounts, which is outside the scope of this POC.
5. Click **Proceed**. The Active Directory authentication service is added to PxM.

Creating Local PxM Users

Is it important to create individual user accounts, as they are used to monitor user activity and review privileged access through the many PxM reports.

<u>NOTE:</u> To use Active Directory authenticated users, see 'Synchronising Active Directory Users in PxM' below.

1) In the Web Management Interface left-hand menu, to the right of *Users*, click the icon. The *New user* window appears.
2) In the *New* user window, fill in the new user's details.
3) Click **Save**. The *Action queue* window appears and the new user is added to PxM.
4) In the *Manage users* page, click on the new user created. You are navigated to the user's detail page.
5) In the user's detail page, to the right of *PROFILES*, click **Manage**. The *Manager: profiles* window appears.
6) In the *Manager: Profiles* window, in the *Included* column, select the checkbox to the left of 'Osirium Super Admins'.
7) Click **Save changes**. The user now has PxM admin privileges.
8) Log out of the PxM Client and log back in as the user created.

Synchronising Active Directory Users in PxM

1) In the Web Management Interface left-hand menu, to the right of *User groups*, click the icon. The *New user group* window appears.
2) In the *New user group* window:
   a. In the *Source* drop-down, select *Active Directory*.
   b. In the *Name* field, type the name of your user group. The user group name must be identical to the user group name in your Active Directory.
3) Click **Save**. The *Action queue* window appears and the user group is added to PxM.
4) In the *Manage user groups* page, in the *Name* column, click the new user group. You are redirected to the user group detail page. Users belonging to the Active Directory user group will be listed in the *ASSOCIATED USERS* table.

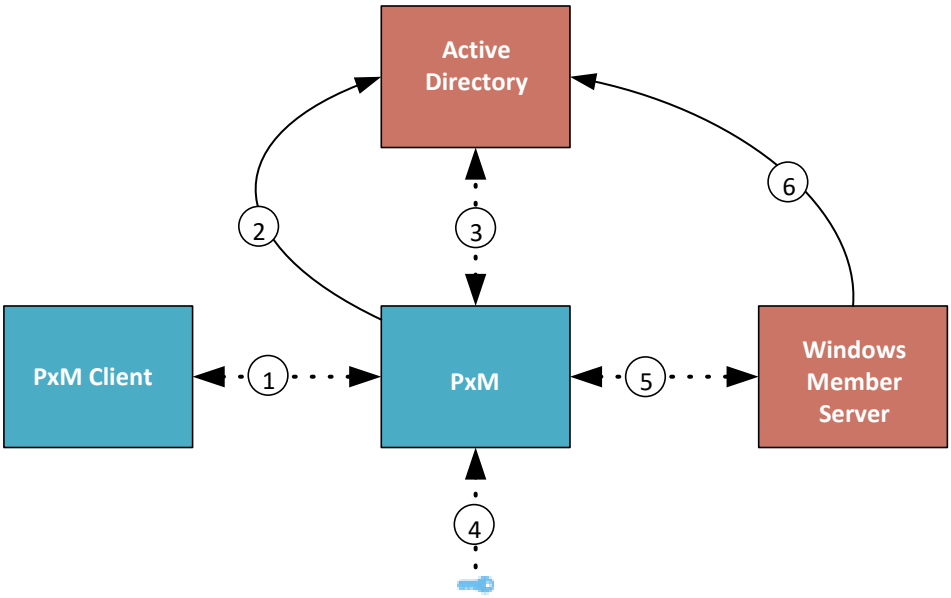
Scenario 1: Using an existing Active Directory account to RDP onto a Windows member server

NOTE: If you do not have an Active Directory available for this POC then skip to Scenario 2.

Having synched an Active Directory user to PxM, we can now provision the Windows member server.

In this scenario, we will be using an Active Directory authentication service to:

- Authenticate users using your normal user.
- Single sign-on to an RDP session using an existing Active Directory account or account mapping.
- Run a task on a device without having to open a session.



1. Logon as a standard user, i.e. fred.smith, and open the remote desktop tool for your Windows Member server.
2. The authentication request for the standard user passes to Active Directory.
3. PxM confirms that the user exists in the Active Directory group of interest.
4. For Password Known, PxM checks the known password against Active Directory.
5. Using the privileged user account, PxM single signs-on the connection to the Windows Member server.
6. The Windows Member server authenticates the privileged user account on the Active Directory service.

Step 1: Auditing the Active Directory user accounts and setting account status

For an Active Directory privileged account to be used to single sign-on to a device, you must tell PxM what the password is of that privileged Active Directory account. This is done by setting the status to Password Known.

1. Click on the Active Directory service added. You will be navigated to the named authentication service page.
2. Within the **Account** column, find the privileged Active Directory account.
3. Right-click the account name and then within the context menu select: **Change status > Set password known**.
4. Enter the existing password and click **Proceed**. The password for this account will be stored in PxM.

Step 2: Using Account mappings

Account mappings allow the management of privileged user access to be simplified within PxM by allowing users to be mapped through profiles to their existing privileged account. Account mappings are typically used within Active Directory two account model but can also be used with local accounts, if they exist on each device.

To create an account mapping:

1. Within the Web Management Interface, click the icon next to *Account mappings* in the left-hand menu.
2. Within the *New account mapping* window, add the account mapping pattern. Example:
   If the existing privileged accounts in Active Directory have the format john.smith_admin.
   Then the account mapping pattern would be: %username%_admin
3. Click **Save**.

Step 3: Adding a Windows Member server

Before privileged device access can be granted to PxM users, the device must be provisioned in PxM. Provisioning allows the device to be administered by PxM.

Device templates are used to provide the necessary access control and language for PxM to communicate with the device.

1) Within the PxM Web Management Interface, click the icon next to *Devices* in the left-hand menu.
2) Within the *New device* window, select the device template called: **Windows Domain Member** 3) Within the *Connection details*, enter the Windows member server configuration information.
4) Within the *Create device* window, enter a name for your device and then select the following and create.

Field Name	**Description**
Device name:	Enter the name of your Windows Member server to identify it within PxM.
Authentication Service	Select the Active Directory service added.
Control Account:	Password known
Select Control Account:	Select the same account that was entered when provisioning the Active Directory authentication service.

Step 4: Create a Profile

Up until now, we have only created PxM users and provisioned devices which can be managed by a PxM SuperAdmin through the Web Management Interface.

To assign privileged access for PxM users to single sign-on to devices and run tasks, profiles need to be created.

Profile are like job description, they allow you to operate on a least privileged model so only giving the necessary access to users to allow them to carry out their job role activities, rather than full admin access.

Profiles are used to connect devices, tools, tasks and users. Any user that is linked to a given profile will be able to run tasks and single sign-on to devices with the granted access level.

1) Click on the icon next to *Profiles* in the left-hand menu.
2) Within the *New profile* window configure the following and save.

Field Name	Description
Name:	Enter the name of the profile to identify it within PxM.
Enabled	Leave as default.
Session Recording:	Tick the checkbox.
Change ticket required	Leave unchecked.

NOTE: Change Ticket Management Tool is possible but outside the scope of POC, please can sale representative for information on this feature.

3) Click on the new profile. Within the *Profile detail* page, add the following by clicking **manage** next to each of the headings within the **Profile members** section:

Devices	Tick the checkbox next to the Window member device.
Access level	There are several options for selecting and granted access levels for a device but for this POC we recommend selected either of the following: **Account:** These are existing accounts on the device but only those accounts that have a **'Password known'** status in PxM will be listed. Select the account that was set as Password known earlier. The account will now be listed as an access level in the '**Manager: devices' 'Access level'** list. Or **Mapping:** Select an account mapping which will map each user's PxM account to their privileged in the Active Directory auth service. For example: Mapping: %username%_admin PxM username: m_wood Active Directory account mapped to: m_wood_admin

Tools **Options**	Tick the checkbox next to Remote Desktop Select the following options: ✦ Allow RDP Drive mapping ✦ Allow RDP clipboard
Tasks	✦ ARP Flush ✦ Check FIPS mode
Users or **User groups**	If selecting a *User*, check the PxM user that you want to give access through this profile. If selecting a *User group*, select the Active Directory user group from the list.

Step 5: Using the PxM Client to single sign-on to an RDP session

Now that we have told PxM to give users privileged access to the RDP tool for the Windows Member server, it will be listed in your PxM Client list.

1. Log onto the PxM Client using the normal user. PxM passes your credentials to the Active Directory for authentication. Once verified, the user will be logged into the PxM Client.
2. Within the PxM Client window, the device access list will dynamically update.
3. Click the arrow in front of the Windows member sever device to see the tools and tasks available.
4. Double-click on the RDP tool. The normal user is single signed onto the Windows Member server using the Password known credentials stored in PxM as defined in the profile. The normal user does NOT see the account password that is being used to log them onto the device. The password is never sent down to the client and only injected by the PxM proxy on the way through.
   As Session Recording was enabled on the profile earlier, a red banner will appear around the RDP session. Everything that is done during this session will be recorded and can be played back.
5. Once logged into the RDP session, open the Notepad application, type a message and save it. This will allow you to view a Session Recording later in the POC.

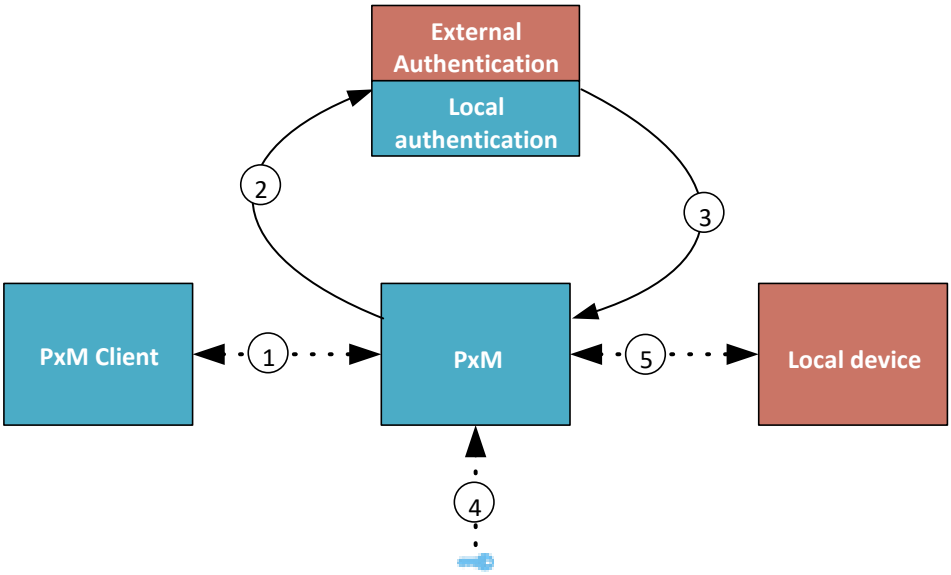
Step 6: Run a task on the device

1) Within the PxM Client, under Windows member server device, double-click on the **ARP Flush** task.
2) Within the *Execute task ARP Flush* window, select the device the task will be executed on. If you had multiple Windows Member servers, you could select them all and run the task on all the servers with the click of a button. This saves a lot of time as you wouldn't have to log onto each individual server and run the task.
3) Click **Execute**.
4) In the *Question* window, click **Yes**.
5) The task is executed on the windows server.
   The device template tells PxM how to run the task on the device and uses the control account to execute the task on the device.

Scenario 2: Using local accounts to SSH onto a device

In this scenario, we will be using local accounts on the device to run an SSH session

- Authenticate users using an existing account already present on the device or an account created by PxM.
- Single sign-on to an SSH device session.
- Run a task on a device without having to open a session.



1. Logon as a standard user, i.e. fred.smith.
2. User authenticated locally or externally.
3. PxM user verified.
4. For Password known, PxM uses the stored device password.
5. PxM single signs-on the connection to the local device.

Step 1: Add a local device

Before privileged device access can be granted to PxM users, the device must be provisioned in PxM. Provisioning allows the device to be administered by PxM.

Device templates are used to provide the necessary access control and information for PxM to communicate with the device.

1) Within the PxM Web Management Interface, click the icon next to *Devices* in the left-hand menu.
2) Within the *New device* window, select the device template for the device you will be using.
3) Within the *Connection details*, enter the Device configuration information.
4) Authentication
5) Within the *Create device* window, enter a name for your device and then select the following and create.

Field Name	Description
Device name:	Enter the name of your device to identify it within PxM.
Control Account:	Password known
Select Control Account:	Select the account that was provided during the *'Test connection'* phase.

[Optional] Step 2: Change device account states

NOTE: The following only applies to the vendor specific device templates and not the generic access templates.

When a device is provisioned as 'Password known', PxM audits all accounts that exist on the device and marks them as 'Unapproved' as they are not known to PxM. Only the device account selected as the control account will have a state of 'Password known'.

Before PxM can assign an account (as an access level within a profile) to single sign-on to a device, the account on the device must be known to PxM and have a state of Password known.

To change the state of a device account:

1) Within the PxM Web Management Interface, click the icon next to *Devices* in the left-hand menu.
2) Click on the device name. You will be navigated to the named device page.
3) Click on the *Account management* tab. All the accounts that have been audited on the device will be listed here.
4) To change the state of an account, right-click the account. From the context menu click on 'Change state' and select 'Password known'. You will be asked to enter the existing password of the account.

Step 3: Create a Profile

Up until now, we have only created PxM users and provisioned devices which can be managed by an PxM SuperAdmin through the Web Management Interface.

To assign privileged access for PxM users to single sign-on to devices and run tasks, profiles need to be created.

Profile are like job description, they allow you to operate on a least privileged model so only giving the necessary access to users to allow them to carry out their job role activities, rather than full admin access.

Profiles are used to connect devices, tools, tasks and users. Any user that is linked to a given profile will be able to run tasks and single sign-on to devices with the granted access level.

1) Click on the icon next to *Profiles* in the left-hand menu.

2) Within the *New profile* window configure the following and save.

Field Name	Description
Name:	Enter the name of the profile to identify it within PxM.
☑ Enabled	Leave as default.
☑ Session Recording:	Tick the checkbox.
☐ Change ticket required	Leave unchecked.

NOTE: Change Ticket Management Tool is outside of this POC, please call sale representative for information on this feature.

3) Click on the new profile. Within the *Profile detail* page, add the following by clicking **manage** next to each of the headings within the **Profile members** section:

Devices	Tick the checkbox next to the device.
Access level	You now need to decide the access level that will be granted for the device when a user logins in. **Account:** For this POC select an account from the list.
Tools **Options**	Tick the checkbox next to the tool i.e. SSH. Leave blank
Tasks	**Optional: select a task valid for the device provisioned.**
Users	Check the PxM user that you want to give access through this profile.

Step 4: Using the PxM Client to single sign-on to a tool

Now that we have told PxM to give your user access to device tool, it will be listed in your PxM Client list.

1. Log onto the PxM Client using your normal user. Once verified, you will be logged into the PxM Client.
2. Within the PxM Client window, your device access list will dynamically update.
3. Click the arrow in front of the device to see the tools and tasks available for the device.
4. Double-click on the tool i.e. SSH. Normal user is single signed onto the device using the Password known credentials stored in PxM. The normal user never needs to know the account password that is being used to log them onto the device.
   As Session Recording was enabled on the profile earlier, a red banner will appear around the RDP session. Everything that is done during this session will be recorded and can be played back.
5. Within the device SSH session type in a simple command i.e. show users etc. This will allow you to view a Session Recording later in the POC.

Step 5: Run a task on the device

1) Within the PxM Client, under device, double-click on a task.
2) Within the *Execute task* window, select the device the task will be executed on.

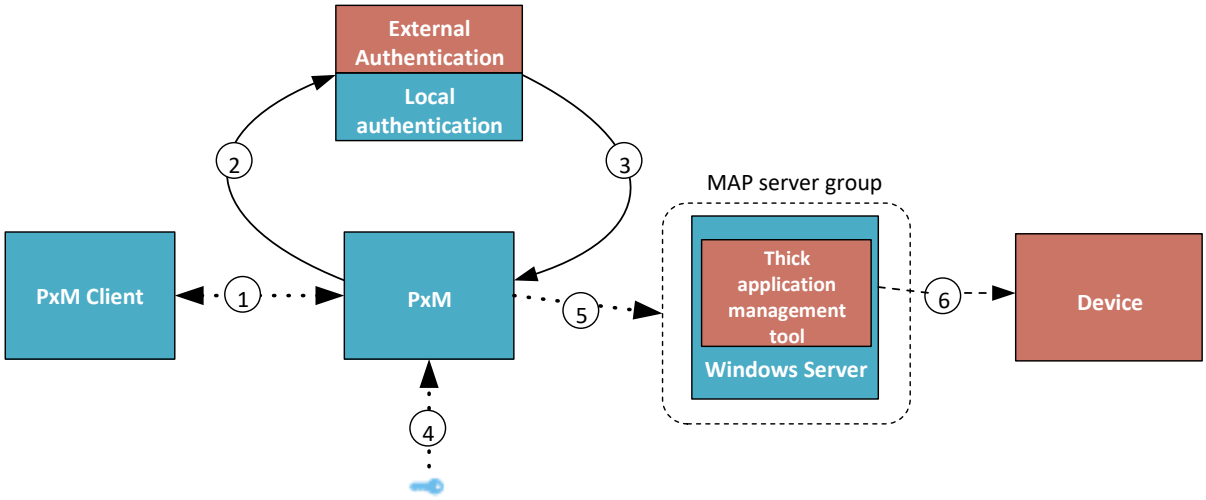
If you had multiple devices, you could select them all and run the task on all of them with the click of a button. This saves a lot of time as you wouldn't have to log onto each individual device and run the task.

3) Click **Execute**.
4) In the *Question* window, click **Yes**.
5) The task is executed on the device.
   The device template tells PxM how to run the task on the device and uses the control account to execute the task on the device.

Scenario 3: Using MAP server to launch a remote application tool

In this scenario, we will be using PxM created MAP server user accounts to connect to the MAP server and run a tool.

- Single sign-on to a tool running a MAP server.



1. Logon as a standard user i.e. fred.smith.
2. Authenticate standard user (local or external)
3. 3. PxM user verified.
4. For Password Known, PxM needs to told the password
5. A connection is established to the MAP server.
6. The MAP server uses the privileged account to single sign onto the thick application management tool.

Step 1: Add a remote application device

NOTE: Ensure the remote application tool has been installed on the MAP server and the end device available.

Before privileged device access can be granted to PxM users, the device must be provisioned in PxM. Provisioning allows the device to be administered by PxM.

Device templates are used to provide the necessary access control and information for PxM to communicate with the device.

1) Within the PxM Web Management Interface, click the icon next to *Devices* in the left-hand menu.
2) Within the *New device* window, select the device template for the device you will be using.
3) Within the *Connection details*, enter the Device configuration information.
4) Within the *Create device* window, enter a name for your device and then select the following and create.

Field Name	**Description**
Device name:	Enter the name of your device to identify it within PxM.
Control Account:	Password known
Select Control Account:	Select the account that was provided during the *'Test connection'* phase.

Step 2: MAP server groups

Each MAP server needs to belong to a MAP server group. MAP server groups are a collection of MAP servers that PxM can use to load balance connections to tools. Each tool is assigned a MAP server group when it is added to a profile.

Create a MAP server group:

1) Within the PxM Web Management Interface, click the icon next to *MAP servers* in the lefthand menu.
2) Within the *Manage MAP servers* window, click *New MAP server groups* button.
3) In the New *MAP server group* window, give the group a name and click **Save**.
4) Click on the new group create, you will be navigated to the *MAP server group detail* page.
5) Click **Manage** next to *MAP servers*.
6) Within the *Manager: MAP servers* window, select the provisioned MAP server you want to add to the group.
7) Click **Save** changes.

Step 3: Create a Profile

Up until now, we have only created PxM users and provisioned devices which can be managed by a PxM SuperAdmin through the Web Management Interface.

To assign privileged access for PxM users to single sign-on to the remote application devices and run tasks, profiles need to be created.

Profile are like job description, they allow you to operate on a least privileged model so only giving the necessary access to users to allow them to carry out their job role activities, rather than full admin access.

Profiles are used to connect devices, tools, tasks and users. Any user that is linked to a given profile will be able to run tasks and single sign-on to devices with the granted access level.

1) Click on the icon next to *Profiles* in the left-hand menu.
2) Within the *New profile* window configure the following and save.

Field Name	Description
Name:	Enter the name of the profile to identify it within PxM.
☑ Enabled	Leave as default.
☑ Session Recording:	Tick the checkbox.
☐ Change ticket required	Leave unchecked.

NOTE: Change Ticket Management Tool is outside of this POC, please can sale representative for information on this feature.

3) Click on the new profile. Within the *Profile detail* page, add the following by clicking **manage** next to each of the headings within the **Profile members** section:

Devices	Tick the checkbox next to the device.
Access level	You now need to decide the access level that will be granted for the device when a user logins in.
	Account: For this POC select an account from the list.
Tools **Options**	Tick the checkbox next to the tool i.e. SSH. Leave blank
Users	Check the PxM user that you want to give access through this profile.

Step 4: Using the PxM Client to single sign-on to a tool

Now that we have told PxM to give your user access to device tool, it will be listed in your PxM Client list.

1. Log onto the PxM Client using your normal user. Once verified, you will be logged into the PxM Client.
2. Within the PxM Client window, your device access list will dynamically update.
3. Click the arrow in front of the device to see the tools and tasks available for the device.
4. Double-click on the tool. Normal user is single signed onto the device using the Password known credentials stored in PxM. The normal user never needs to know the account password that is being used to log them onto the device.

Reporting

There are many reports within the PxM Web Management Interface that allow you to monitor, manage and analyse devices and device activity.

For this POC we will only be looking at a subset of the reports available.

Device access report

The device access report provides an audit of the PxM users that have logged into the PxM Client and device connections they have made.

Session recording screenshots captured can also be viewed here and recordings can be played back.

To playback a session recording:

1) Within the PxM Web Management Interface, click *Device access* in the left-hand menu.
2) Within the *Device access report* window, ensure the *Device connections* checkbox is ticked.
3) Within the *Device connections* table, click on play button next to an entry. A Session player window will open. Use the controls to play the session recording.

Searching for keywords

The 'Fuzzy Filter' feature enables you to search for keywords within the recorded sessions.

The search term is matched against:

- The keystrokes made within a connection.
- The titles of the recorded connection window.

To create a search:

1) Within the *Device access report* window, click the *Fuzzy Filter* checkbox.
2) Within the *Fuzzy filter* search term window, type in a word you used when creating the Notepad file during your RDP session.
3) Click *Apply filter*.
4) View the recording that contains your search.

Task reporting

The tasks report provides visibility of the most recent tasks executed on a device by PxM users.

To view the task report:

1) Within the PxM Web Management Interface, click *Tasks* in the left-hand menu.
2) Within the *Tasks reports* window, the tasks executed on your devices will be listed. The report tells you when the task was executed on the device, whether the task was successful, the device the task was executed against and who ran the task.
3) If any tasks have failed you can view the log file, right click on the task and select *View log*.

POC acceptance checklist

User

Proof of concept objectives	Yes	No	N/A	Comments
Able to successfully log onto the PxM Client using a standard user (if using Active Directory LDAPS)				
Able to successfully log onto the PxM Client using a PxM local user				
Once logged into the PxM Client, user could see a list of available devices with the granted access level				
Once logged into the PxM Client, user could see a list of available tasks for each of the devices				
Used the PxM Client search to find a device or task				
User successfully single signed on to a Windows Member server RDP session without having to enter or know the username/password of the device.				
User could see the session recording red box around the RDP session				
User successfully used the clipboard function within a Windows Member server RDP session				
User could successfully use the drive mapping function within a Windows Member server RDP session				
User could successfully run a task on the Windows Member Server without having to log onto the server or know the command to run the task				
User could successfully single sign on to a SSH session without having to enter or know the username/password of the device.				
User could successfully run a task on the local device without having to log onto the device and know the task command				
User could see the session recording red box around the SSH session				
User could successfully single sign on to a thick application management tool without having to enter or know the username/password of the device.				
User could see the session recording red box around the thick application management tool session				

Administrator

Proof of concepts objectives	Yes	No	N/A	Comments
Easily configured PxM to use Active Directory user authentication when logging users onto the PxM Client				
Could successfully create PxM user accounts to match the users Active Directory user accounts				
Successfully added an Active Directory authentication service to manage Windows Member servers				
Successfully provisioned a Windows Member server using an existing Device Template				
Successfully created a profile for a Windows Member server device				
Successfully added a Windows Member Server device and selected an access level within the Windows Member Server profile				
Successfully added an RDP tool with clipboard and drive mapping options to the Windows Member Server profile				
Successfully added tasks to the Windows Member Server profile				
Successfully added users to the Windows Member Server profile				
Successfully provisioned a local device using an existing Device Template				
Successfully create a profile for a local device				
Successfully added a local device and selected an access level within the Local device profile				
Successfully added an SSH tool within the Local device profile				
Successfully added tasks to the Local device profile				
Successfully added users to the Local device profile				
Successfully create a profile for a thick application management tool				
Successfully added a thick application management tool and selected an access level within the thick application management tool profile				
Successfully added a tool within the thick application management tool profile				
Successfully added users to the thick application management tool profile				
Successfully view a recording of an RDP session				
Successfully search an RDP session recording using the Fuzzy Filter search				
Successfully view a recording of an SSH session				
Successfully search an SSH session recording using the Fuzzy Filter search				
Successfully view a recording of a thick application management tool session				

Successfully search a thick application management tool session recording using the Fuzzy Filter search				
Successfully view the Task reports and see the task that have been run on the Windows member server by the user				
Successfully view the Task reports and see the task that have been run on the Local device by the user				