Xton Access Manager

GETTING STARTED GUIDE

Contents

Introduction

This guide is designed to show system administrators and power users how to begin configuring and using Xton Access Manager (XTAM). It will provide an introductory walkthrough of some features and functionality that will be used to gain a baseline understanding of the software.

The below list is our recommendations to follow the exercises in this guide:

- Access to an XTAM system that is currently running.
- User and password of the XTAM System Administrator.
- Access to a remote Windows (RDP) or Unix (PuTTY or VNC) session
    - Authorized Host, User and Password will be required
- A non-production test account that can successfully connect to your Windows or Unix session to be used for the password reset exercise.
- 60 minutes of time to read the guide and complete the exercises.

By the end of this short guide, you will have created a folder and record, secured it with unique permissions, established and recorded a session, setup a baseline system configuration and developed a working knowledge of the software.

Technical Support

If at any time you encounter an issue, have questions, need guidance or would like to see a demonstration walkthrough, please contact us using the information provided in our Help section. https://www.xtontech.com/company/contact-us/

What is Xton Access Manager?

Xton Access Manager (XTAM) is an agentless solution that provides a secured database to manage privileged accounts and secrets, establishes secure sessions for users through a standard web browser and automates the execution of jobs or tasks without disclosing or sharing access.

The purpose of this guide is to perform a new installation and first time system initialization. At the conclusion of this guide, XTAM will be ready for system configuration and use.

XTAM is installed to a Windows or Unix computer (physical or virtual), with optional connection to Active Directory or LDAP. The system consists of several modules; a database that contains secrets, configuration, passwords and audit events, a service to establish, monitor and record privileged sessions, a user directory to maintain local users and groups and a job engine to execute scripts and tasks.

Privileged Account Management

A secure AES 256-bit encrypted database that contains records which can be stored, shared and used without disclosing the actual privileged account or its secrets (passwords, certificates or keys).

Privileged Session Management

The ability to establish a privileged session to an underlying system (Windows, Unix, Linux, Mac) through a standard web browser while providing the means to monitor, join, record or terminate this session.

Privileged Job Management

Schedule, automate or execute on demand jobs to privileged systems without embedding the secrets in scripts or sharing them with untrusted users.

Software Components

To accomplish the requirements above, XTAM needs to install, configure and run the following software and services. These components are deployed during the installation process (single server deployment) or they can be distributed to multiple servers (farm deployment) to scale performance. Single server deployments can be scaled to farm deployments when additional resources become needed.

Architectural Diagram

XTAM sits within the firewall in its own SSL secured network. Client computers make requests, establish sessions and run jobs from inside or outside the firewall to computers also located inside or outside the firewall using only their native web browser of choice. The Database of Secrets secures all records using an AES 256-bit encrypted protocol and only delivers these secrets to authorized remote requests.

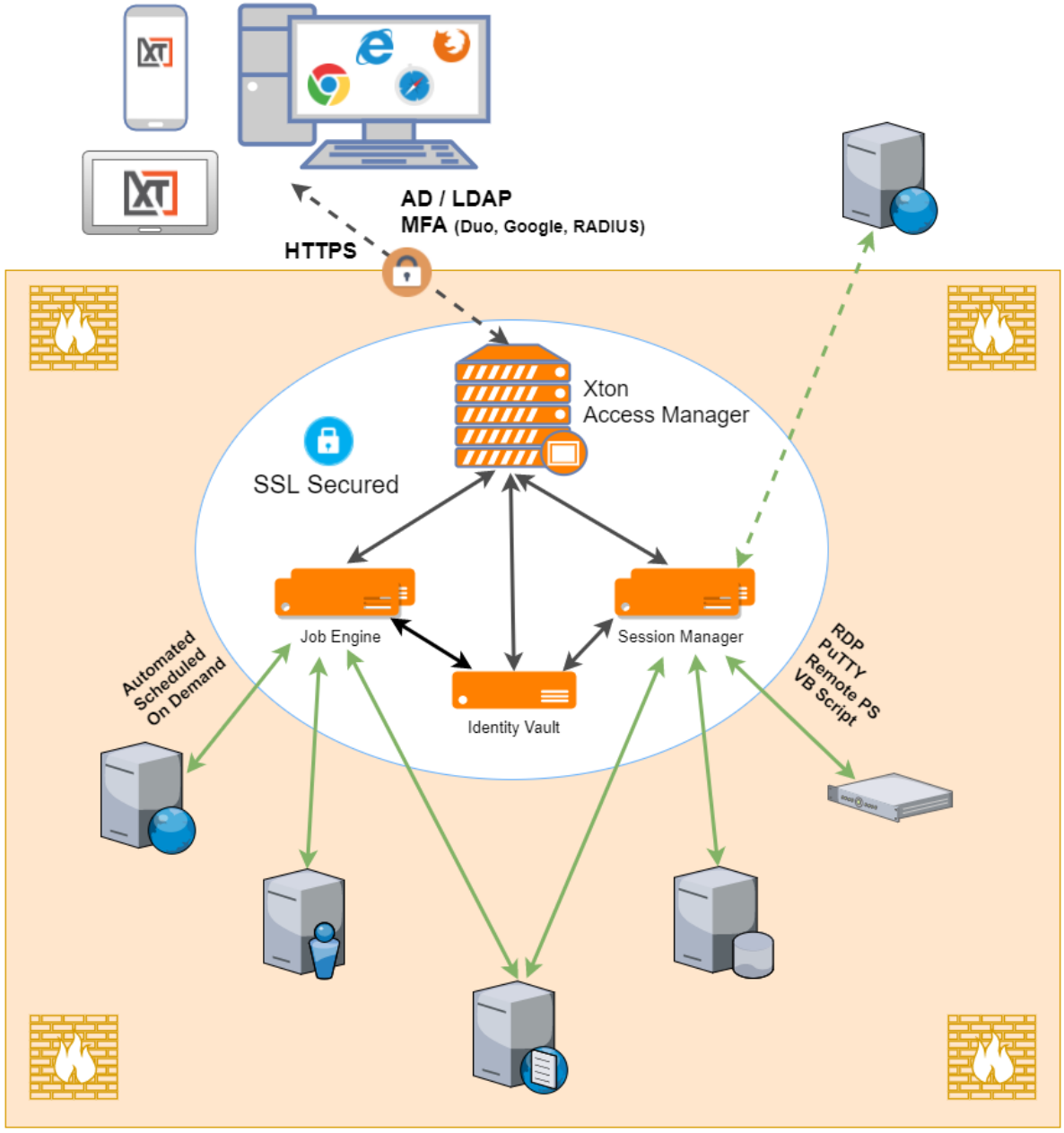

Figure 1: Xton Access Manager Architectural Diagram

Navigating the Graphical User Interface (GUI)

Before we dig into the functionality, let's begin the guide by introducing the Xton Access Manager's graphical user interface (GUI). This will get you aquatinted with the layout so you can learn to navigate and efficiently locate specific functionality.

Login to Xton Access Manager (XTAM) by opening the following link in your browser and use the System Administrator account that was created during installation.

XTAM (default) login page: http://localhost:8080/xtam

The XTAM GUI is divided into three principal areas:

1. Left Navigation Menu
2. Display Page
3. Top Bar

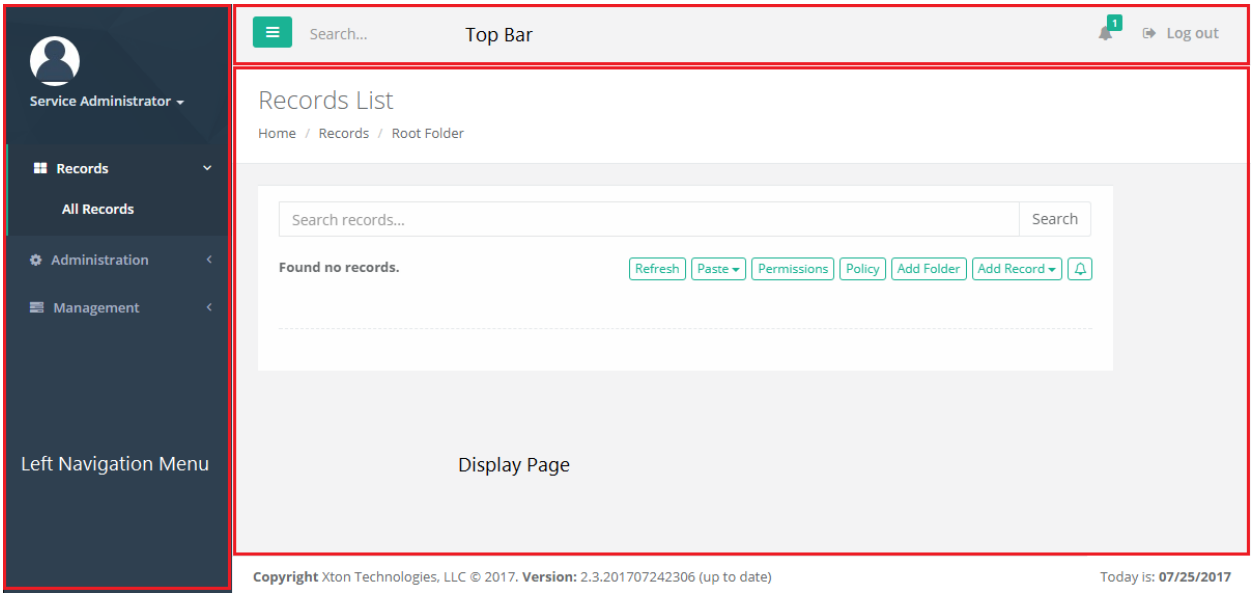

Figure 2: XTAM Graphical User Interface

Left Navigation Menu

The left navigation menu in XTAM provides an effortless way to quickly navigate through the different sections of the software. It is security trimmed and some areas may be hidden and inaccessible by users with varying levels of permissions.

The menu is grouped into three sections:

- Records
  - This section contains access to all objects related to records. This includes folders, host records, passwords, certificates and keys.
- Administration

    - This section contains links to areas that are used to configure and maintain the use and management of the XTAM system.
        - Only users with the System Administrator role will have access to this menu section.
- Management
    - This section contains useful links specific to the user account that is logged into the system. These objects are configured by the user and are only accessible by them when they log in to XTAM.

Display Page

The Display Page is the large section to the right of the left navigation menu that will be used to interact with XTAM. This area will display all objects, configuration, views, records, logs and actions that are used by the logged in user.

Top Bar

The Top Bar along the top of XTAM is visible from all areas of the software and contains quick access to the following objects:

- Search to quickly locate objects in the Left Navigation Menu
- Notifications that are triggered while you are logged into the system
- Log out button to log out of XTAM

Now that we have a quick overview of the software, let's dive into some examples and use cases.

Working with Folders

Folders provide a straightforward way to organize and more easily share records. We will begin this guide's feature walkthrough with folders.

Creating Folders

To create our first folder:

1. On the left navigation menu, expand the Records section and click **All Records**.

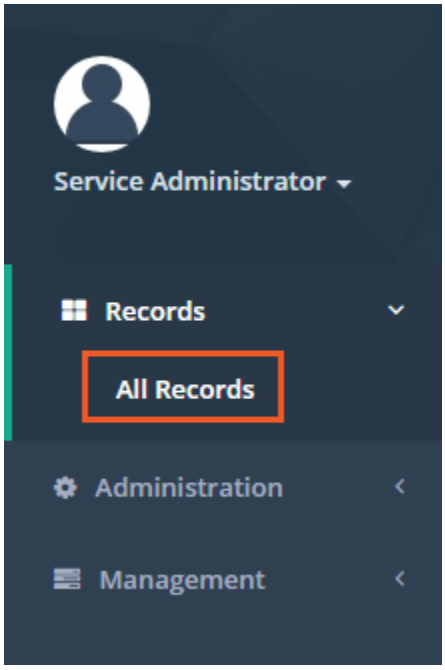

Figure 3: All Records Menu Option

2. From the Records List page, click the **Add Folder** button.

Figure 4: Add Folder

3. For the new folder, enter:
   a. *Name*: IT Records
   b. *Description*: Use this folder to organize and share records within the IT department
4. Click **Create**.

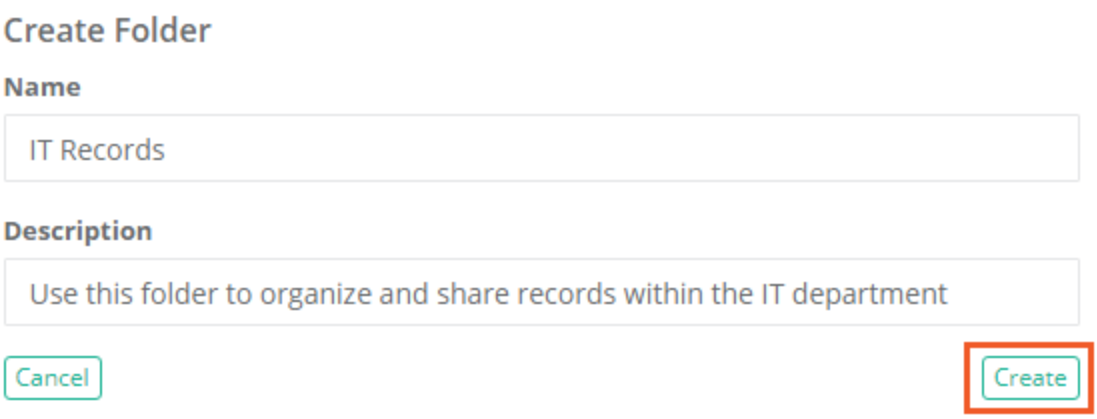

Figure 5: Creating a New Folder

5. Your new folder will now appear in the root Records List page view. The folder Name and Description will display in this view as well as Action menus located to the left and right side of this folder.

Folder Options

Folders can contain or be associated to several custom objects which we will cover throughout this guide. For now, let's begin with two basic options; *Alerts* and *Favorites*.

Alerts configured on a folder will notify the user to specific events that take place on and within this container. To setup your alert:

1. Open the "IT Records" folder by clicking on the folder name in the list or by using the folder dropdown or Action menu and selecting **Open**.
2. When *in* the IT Records folder, click the **Alerts** icon along the top row.

Figure 6: Subscribe to Alerts

3. On the **Subscribe to Alerts** dialog, select
   a. *Category*: Permissions
   b. *Level*: All
   c. *Event Filter*: can be left empty
4. Click **Select**. The alert is now saved to your profile and will trigger when any permission events are generated for this folder.

Favorites can be assigned to folders to make them more easily accessible when navigating throughout the software. Favorited folders will appear in the Records section of the left navigation menu. To favorite your folder:

1. Open the IT Records folder by clicking on the folder name in the list or by using the folder dropdown or Action menu and selecting **Open**.

2. Click the **Favorites** button along the top row.

Figure 7: Add to Favorites

3. The GUI will refresh and in a few moments your favorited folder <IT Records> will appear in the left navigation menu.

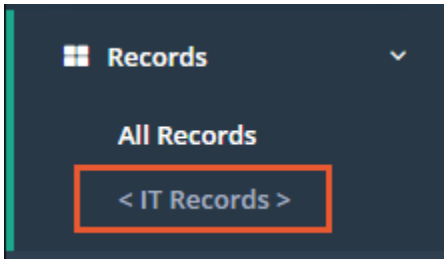

Figure 8: Favorites Menu

NOTE: To unfavorite a folder, simply click this same button a second time.

Folders are configurable containers within XTAM to organize records. We will revisit these options later in the guide. For now, we have this basic building block configured, so we can move on to Records.

Creating Records

Records are the objects that store session host connection parameters, secured passwords, certificate and key files as well as several other secrets. Much like folders, many configurable objects are associated to records to facilitate their sharing and use in XTAM. To better understand Records, we will begin by first creating one.

Your First Record

To create a new record:

1. Open the IT Records folder by clicking on the folder name in the list or by using the folder dropdown or Action menu and selecting **Open**.
    a. If you still have it in your Favorites, then you can click <IT Records> in your left navigation menu for quick access to this folder.
2. Click the **Add Record** button and select the Record Type "Windows Host". This will create a record that will be used to establish a browser based remote desktop connection to the configured Windows host.
    a. This example will use a simple Windows Host record type, however if you would prefer to use the Unix Host type, the process will be similar.
    b. To learn about the other standard Record Types or how-to custom create a new Record Type, please review the User Manual located on our website's Documentation page.

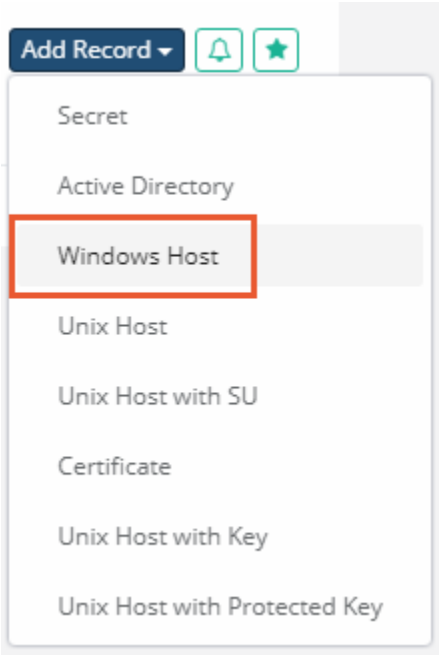

Figure 9: Create a "Windows Host" Record

3. We'll begin by giving this new record a name and description
    a. *Name*: Production Web Server
    b. *Description*: Record for our production web server
4. Now the connection details will need to be supplied.

a. *Host*: Enter the computer host that will be used for a remote desktop connection.
b. *Port*: Define the port that is open and available on this host for remote desktop. Default port for Windows is 3389. Unix or Linux is 22.
c. *User*: Enter the username (user@domain.com or domain\user) that has remote access to the host.
d. *Password*: Enter the password for this user account.

5. Click **Save and Return** when the fields have been populated.

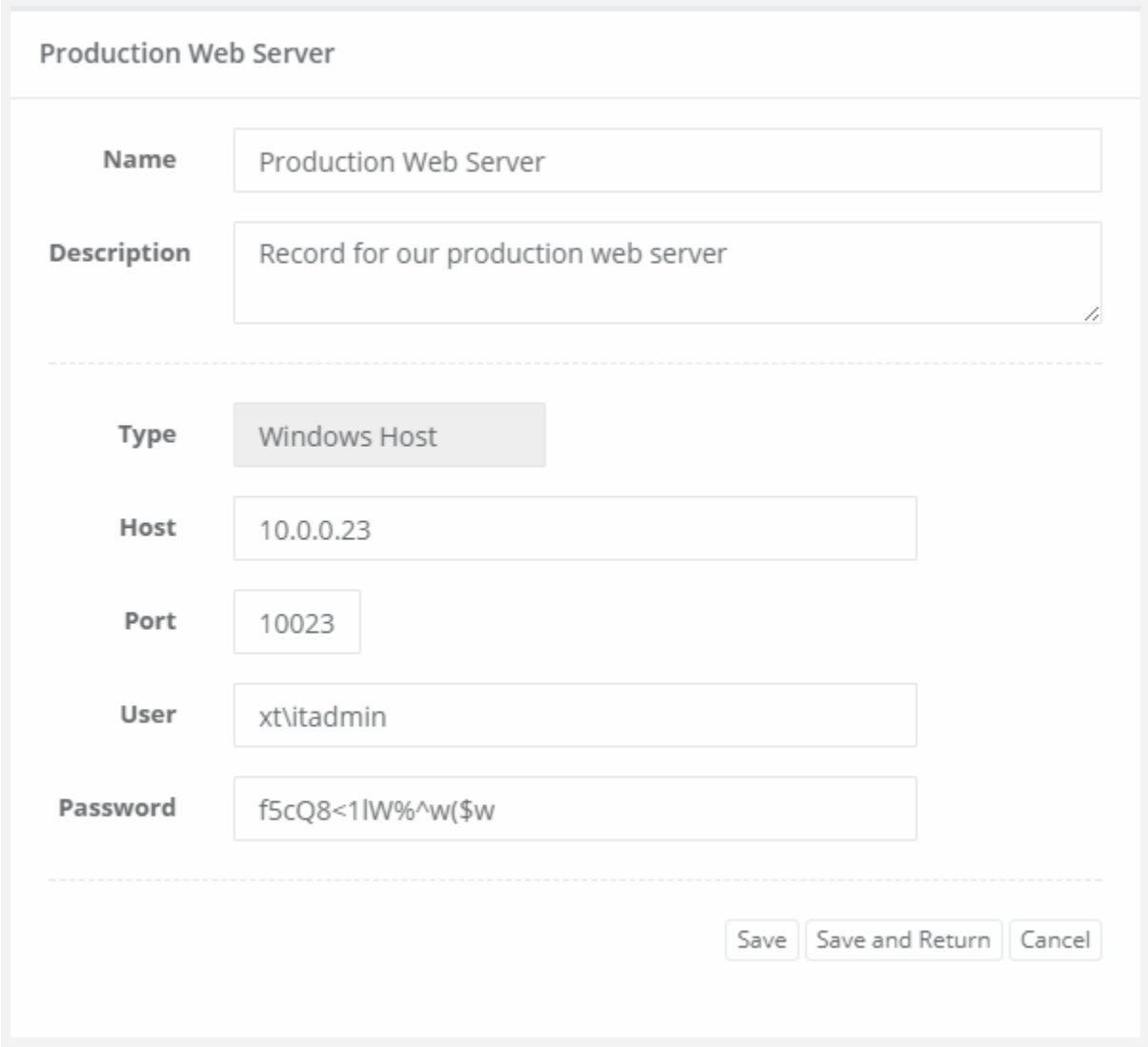

Figure 10: "Windows Host" Record

Your first record is now created and can be viewed and edited within the IT Records folder. We will return to explore some of the other options within Records later in the guide.

Connecting to Sessions

One of the many features of Records is the ability to use them to establish a secured session. Sessions themselves can be established with or without recording enabled, which we will discuss further in another section of this guide. For now, let's use our recently created "Production Web Server" record to create a secure session.

Establishing your First Secure Session

To establish your first session:

1. Open the IT Records folder by clicking on the folder name in the list or by using the folder dropdown or Action menu and selecting **Open**.
    a. If you still have it in your Favorites, then you can click <IT Records> in your left navigation menu for quick access to this folder.
2. Open the "Production Web Server" record by clicking on the record name or by using the record dropdown or Action menu and selecting **View**.
3. Once in this record's View page, you will see several options both in the top and bottom rows. Locate the Connect button along the top, click it to expand the dropdown menu and then select the **Connect** option.

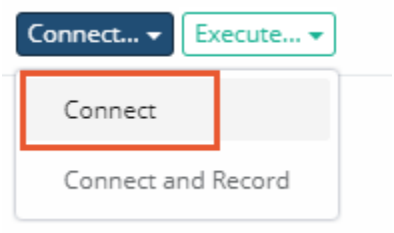

Figure 11: Connect to a Session

4. A new browser window or tab will appear with the message "Connecting to Session Manager". This message will change to "Connecting to Host" after a few seconds and then finally, the remote desktop connection to your host will appear in your browser.

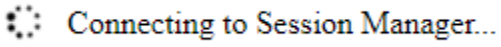

Figure 12: Session Manager Browser Connecting Message

    a. This is a full remote desktop connection so feel free to explore the session's functionality and responsiveness for a bit.
5. When you are ready to complete the session, you may do so by logging out of Windows (or Unix) as you normally would in a remote session or you could simply close this browser window.

Your first secure session is now complete. Before we proceed with establishing a recorded session, let's take a quick look at the record's Session History.

Record's Session History

Within XTAM, every record's session history is captured and made available throughout the system for quick and easy review. The session history will capture valuable information about each established session including who created the session, session start and end times, current activity status and whether it was recorded. In this section, we are going to look specifically at the session history associated to our "Production Web Server" record.

To view our record's Session History:

1. Open the IT Records folder by clicking on the folder name in the list or by using the folder dropdown or Action menu and selecting **Open**.
    a. If you still have it in your Favorites, then you can click <IT Records> in your left navigation menu for quick access to this folder.
2. Open the Production Web Server record by clicking on the record name or by using the record dropdown or Action menu and selecting **View**.
3. Locate and click the **Sessions** button along the bottom row of options.

Figure 13: Record's Session History

4. A new view will load that provides details for all sessions (active or completed) associated to this specific record. You will notice that our previously established session is listed and as expected it displays your System Administrator account, the start and end time of the session, status as "Completed" and Recording as "Not recorded".

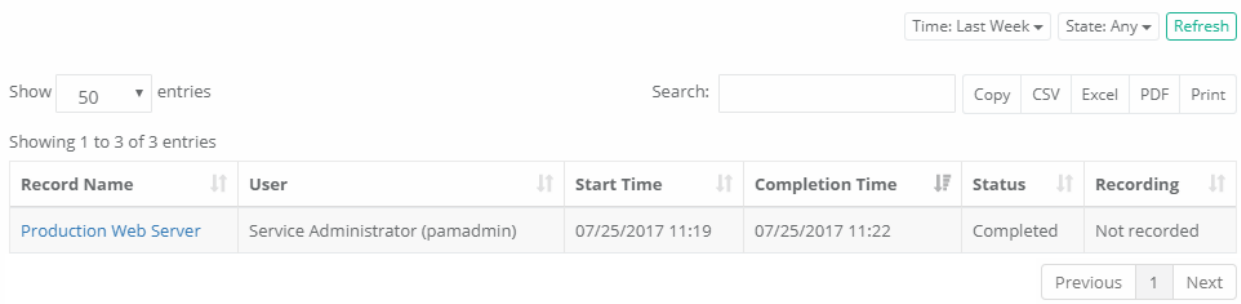

Figure 14: Session History

5. At this time, please explore the assorted options that are available in this view including
    a. Filter options along the top to help filter based on time or state
    b. Number of display entries to load
    c. Search box to quickly locate specific events
    d. Export options to download and share the session history with others
6. When you are ready to return, simply click your browser's Back button. This will navigate you back to the record's View page.

Secure Session with Recording

Our first secure session was established without recording enabled. This allowed the user to securely connect to the session and fully interact with the host using their browser without it being recorded, but now we want to introduce the option to add recording to this same session. Recording is a great option to have because it maintains a record of everything that happened during the session beyond just the basic session history events of "who" and "when". Using our same "Production Web Server" record, we are now doing to connect with recording enabled.

To establish a secure session with recording:

1. Open the IT Records folder by clicking on the folder name in the list or by using the folder dropdown or Action menu and selecting **Open**.
    a. If you still have it in your Favorites, then you can click <IT Records> in your left navigation menu for quick access to this folder.
2. Open the Production Web Server record by clicking on the record name or by using the record dropdown or Action menu and selecting **View**.
3. Locate the **Connect** button along the top, click it to expand the dropdown menu and then select the **Connect and Record** option.

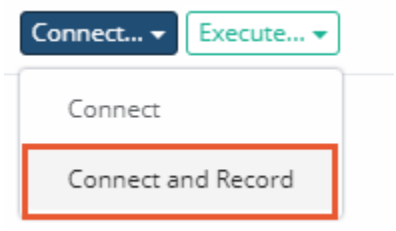

Figure 15: Connect to and Record a Session

4. As was with the earlier, non-recorded session, a new browser window or tab will appear and in a few seconds, you will be logged into the remote desktop session again.
    a. Please note that the message above the session states "(with Recording)" to indicate to the user that this secure session is being recorded.
    b. Feel free to use the session for a bit to perform some operations so that activity is recorded and can be reviewed later.
5. Unlike earlier, when you are ready to continue with the exercise do not complete this session. Instead, return to your record view still open in another browser window. On the records' view, open the Session history by clicking the **Session** button at the bottom of the record's View page.
6. When the Session page loads, you will see our earlier non-recorded session at the bottom and at the top of the list you will see our current Active session still running. Notice that this current session status is displayed as "Active" and recording shows "Recording". Take a moment to explore some of the other options available in the view. Stay on this page when you are ready to continue.

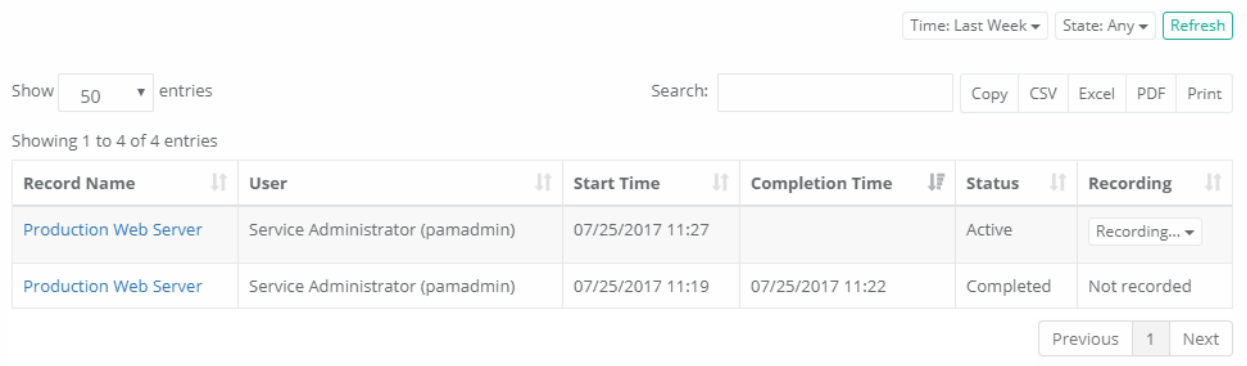

Figure 16: Session History with Active Session

7. Return to the secure session currently running in your other browser window and complete the session as you did previously. You will receive a session completed message when this is done. You may now close this window or tab.
8. Back in the Session History page, click the Refresh button. You will now see that the previously Active session is now "Completed" indicating that this session was closed. You should also note that the Recording status has changed to "Access" and has a dropdown menu.

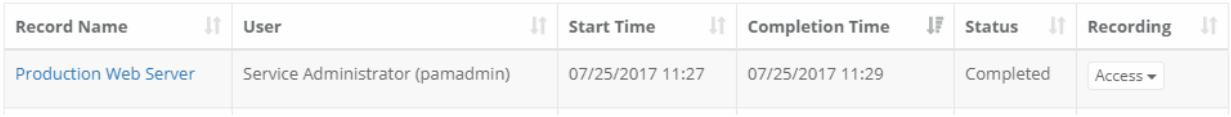

Figure 17: Completed Session with Recording

9. All completed and recorded sessions will have this Access option to convert and download previously recorded secure sessions. Click the Access recording dropdown and select either **Convert to AVI** or **Convert to MOV**. Our recording will now be converted into the selected video format. Depending on the length of the session, the conversion process can take a few seconds or several minutes to complete.

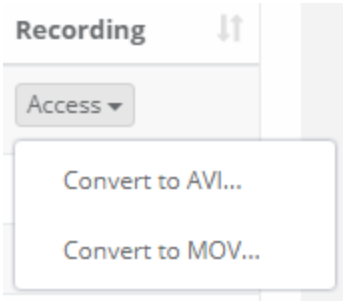

Figure 18: Recorded Session Video Conversion

10. When the conversion is complete and ready for viewing, a Download button will appear in this column. Click **Download** to download the video file to your computer to be viewed locally. Open this video file in your local media player to review the session that was just recorded.

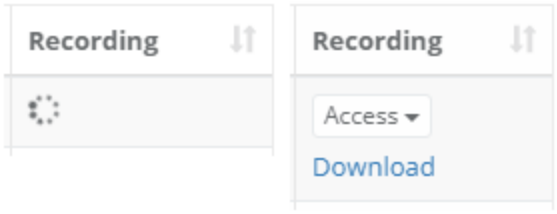

Figure 19: Video Processing and Download

This concludes the steps required to establish a connection to a record with and without recording. You may establish more sessions if you wish to further test the connections or even create additional records to test other types. When satisfied with this exercise, please continue to the next section of this guide.

Resetting Privileged Passwords

Creating records, securing access and establishing sessions is a great first step to securing your privileged accounts. We are now doing to take it one step further and introduce the concept of automated (or on demand) password resets.

This functionality takes security another step forward because it allows XTAM to not only secure accounts but to also update their passwords in cases where events or triggers occurred.

In this section, we will configure and run an example of on demand password reset. Because we will be resetting an account password, it is highly recommended to use a test account for this exercise. If you do use an alternate test account, please be sure to update your "Production Web Server" record in XTAM with this test account's user and password.

To start and eventually validate the results, let's establish a baseline use case.

1. Outside of XTAM, open a standard Remote Desktop session and connect to the Windows host we have been using in our "Production Web Server" record.
2. When prompted, enter the user and password of your test account.
3. Ensure that Remote Desktop connects successfully.
4. Sign out and close Remote Desktop.

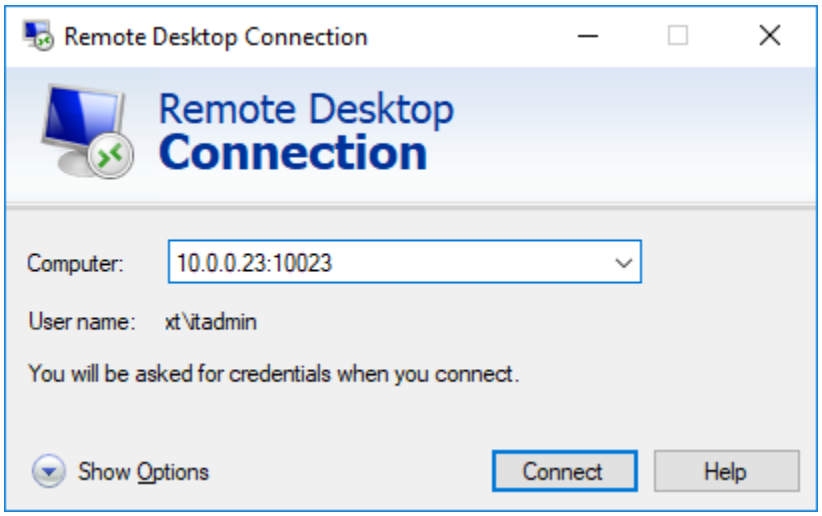

Figure 20: RDP Baseline Test Connection

Before we continue with the password reset exercise, we will take a few moments to examine the components that can be configured to execute this or other jobs in XTAM.

Password Formulas

Formulas are configured to determine the strength and complexity of an automated or on demand password. It is here that you can configure password complexity to include such options as character length, include upper or lower case, numbers or special characters as well as history. To open and configure a formula:

1. Open the IT Records folder by clicking on the folder name in the list or by using the folder dropdown or Action menu and selecting **Open**.
    a. If you still have it in your Favorites, then you can click <IT Records> in your left navigation menu for quick access to this folder.
2. Open the Production Web Server record by clicking on the record name or by using the record dropdown or Action menu and selecting **View**.
3. Locate and click the **Formula** button along the bottom of the record view.

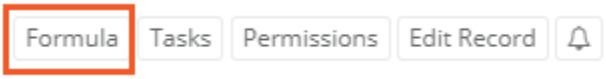

Figure 21: Formula Button

4. The Password Formula page will load and display the default configuration. It is here where changes to this configuration can be made, but first we must decide if we want to change the inherited Formula (default) or to make it unique to this object and then change it as needed.
    a. To learn more about inheritance throughout XTAM, please review What is Inheritance? .
5. For this exercise, we are going to make this Formula unique to this record. Continue by clicking the **Make Unique** button and then accepting the message that appears. The Formula will refresh and it is now unique to this record only.
6. Now we can change the Formula without it affecting any other records in the system.
    a. Change the following settings:
        i. *Password Length*: 25
        ii. *Special Characters* "!@#$%^&*()-_+=": Disable (uncheck)

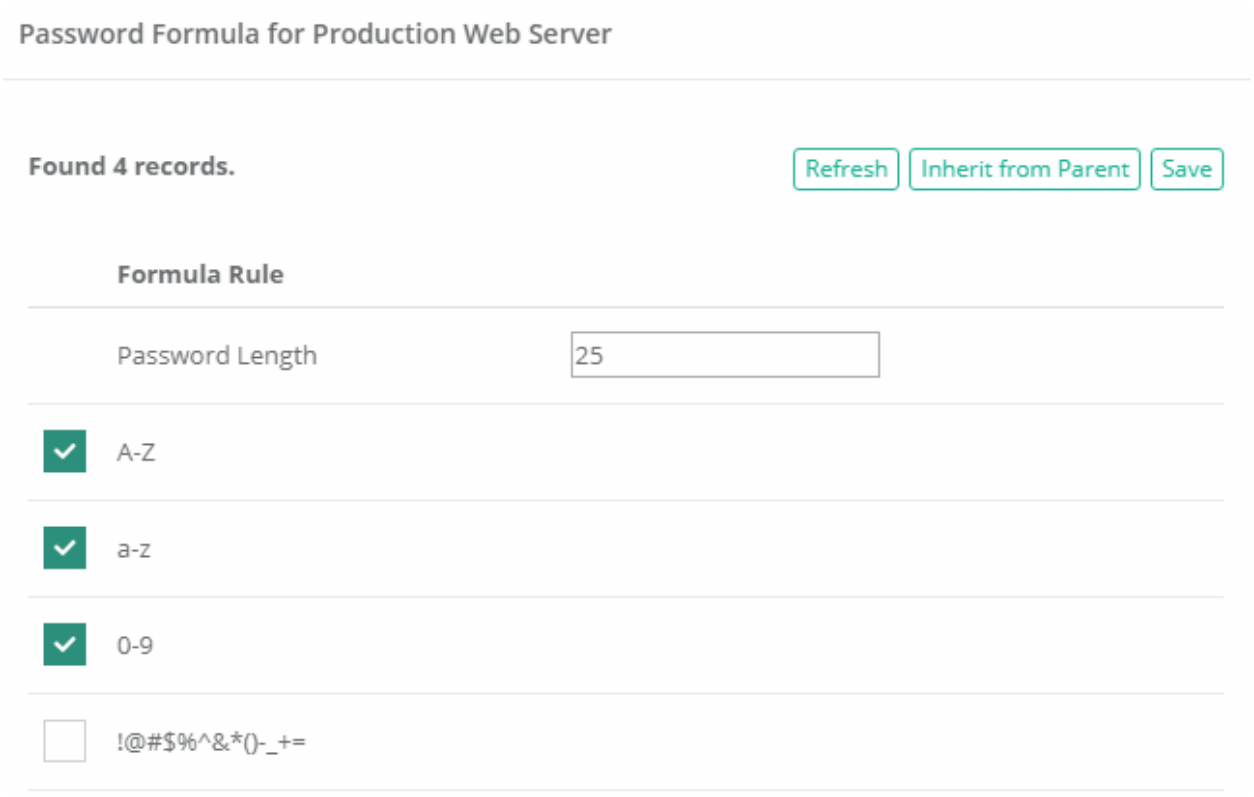

Figure 22: Creating a Unique Formula

7. Click **Save**.
8. Click your browser's Back button to return to the record.

The Formula is customized and has been saved to this record only (*made unique*).

Record Tasks

A Record's Task consists of two elements, a Script and a Policy. The Script component is what will be executed against the record (password reset or custom written) and the Policy is when it will be executed. In our example, we will be executing the default "out of the box" Password Reset script for our Windows Host record type. Since this task is already available for our Windows Host record type (via inheritance), we do not have to make any changes, we can simply proceed to the next component in our Task which is the Policy.

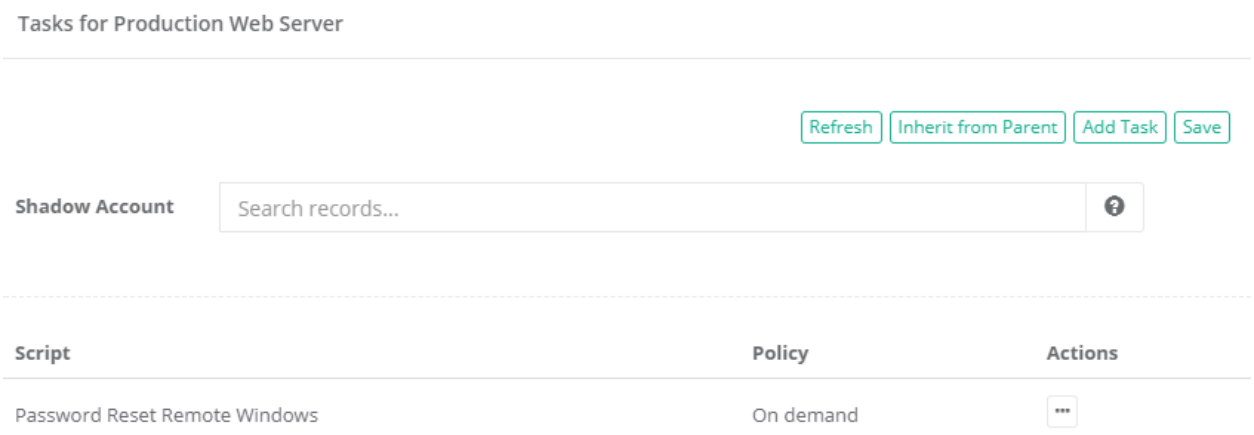

Figure 23: Record Task View

Record Policies

The next area of job execution is the schedule or trigger that causes the script execution which are called Policies. This can be associated to specific events detected on a record like an edit operation, it could be a trigger on a specific day or it can be configured as an "on demand" action. To access the Policies:

1. Open the IT Records folder by clicking on the folder name in the list or by using the folder dropdown or Action menu and selecting **Open**.
    a. If you still have it in your Favorites, then you can click <IT Records> in your left navigation menu for quick access to this folder.
2. Open the Production Web Server record by clicking on the record name or by using the record dropdown or Action menu and selecting **View**.
3. Locate and click the **Tasks** button along the bottom of the record view.

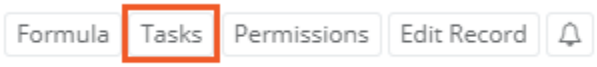

Figure 24: Tasks Button

4. The Tasks page will load and display the default configuration. It is here where changes to this configuration can be made, but first we must decide if we want to change the inherited Policy or to make it unique to this object and then change it as needed.
    a. To learn more about inheritance throughout XTAM, please review What is Inheritance? .
5. For this exercise, we will be executing the Password Reset Task using the Policy "On demand" and because the inherited default policy already includes this option we will not be making it unique like we did with the Formula. However, if you want to experiment with a unique Policy, click Make Unique and customize as needed. To continue along with this exercise, be sure "On demand" is enabled and the Task is saved.

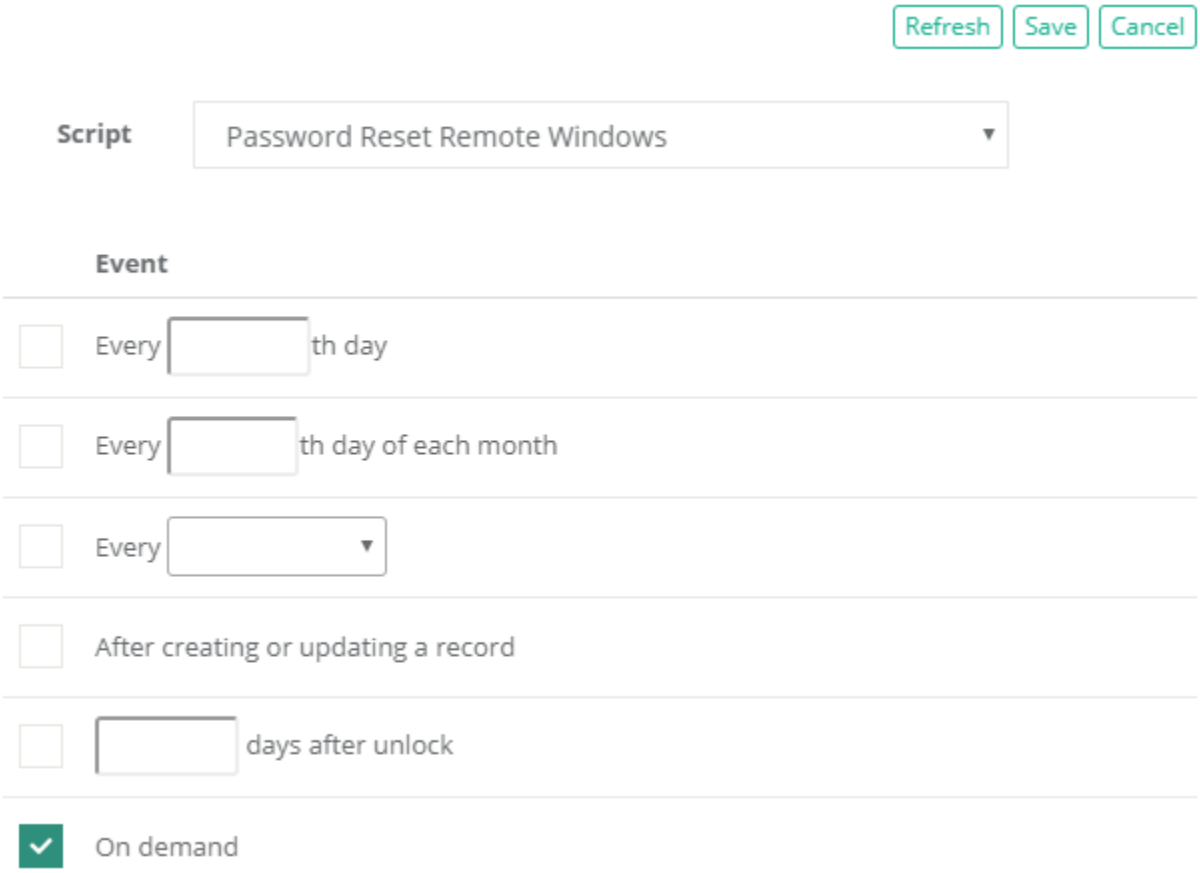

Figure 25: Unique Policy on Task

6. Click your browser's Back button to return to the record.

Our task already included the On Demand policy option, so we are going to continue without making any changes to it.

Password Resetting

We have configured our basic password reset job (more complex formula and on demand policy in our task), so our next step is to run it. To run this password reset job:

1. Open the IT Records folder by clicking on the folder name in the list or by using the folder dropdown or Action menu and selecting **Open**.
    a. If you still have it in your Favorites, then you can click <IT Records> in your left navigation menu for quick access to this folder.
2. Open the Production Web Server record by clicking on the record name or by using the record dropdown or Action menu and selecting **View**.

3. Locate and click the **Execute** button along the top of the record view and then select our *Password Reset* task.

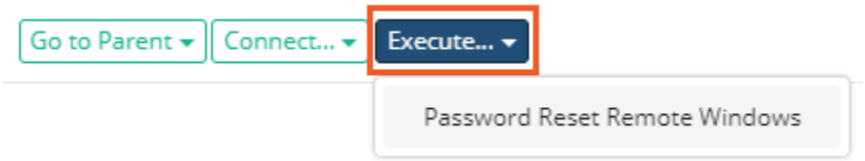

Figure 26: Execute Password Reset

4. The Schedule Job page will now display. Before we continue, let's look at the information and options on this page.
    a. Along the top, an automatically generated password will appear in the Password field that satisfies the formula we defined earlier. If you were to continue now, the password displayed in this field will become the new password for the account associated to this record when the reset job completes.
    b. You can click the **Generate** button to its right to cycle through randomly generated passwords that also satisfy the formula.
    c. You can also manually type in a password if you prefer but it must satisfy the formula rules before you can continue. Use the **Validate** button to ensure your password meets these requirements and adjust as necessary.

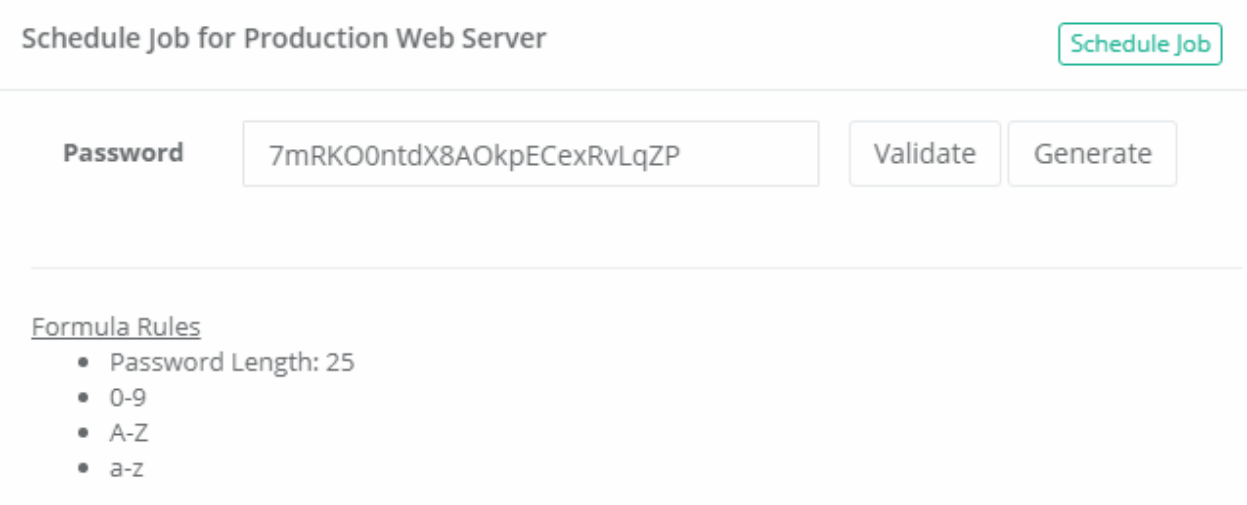

Figure 27: Password Generation

5. When you are happy with the password, click **Schedule Job** to execute the reset.
    a. On demand jobs like this will be immediately added to the Job Queue and processed based on availability and XTAM's queue. In this newly installed system, this job should begin processing almost immediately.
6. The system will navigate you back to the record's View page. The Job Queue field will show that the job has been generated and set to process.

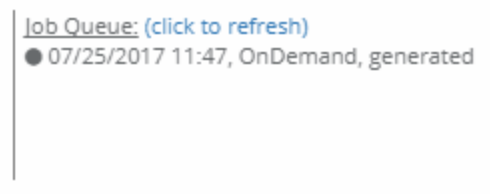

Figure 28: Record's Job Queue

7. Locate and click the **Job History** button. It will be in this view where you can view information about any currently running or scheduled jobs associated to this record.
8. You will see our "On Demand" job displayed with a specific state. Navigate around the page to explore the options that are available for Job History and after a minute or two, click **Refresh**.
9. When the job completes, the State will be shown as "Completed".

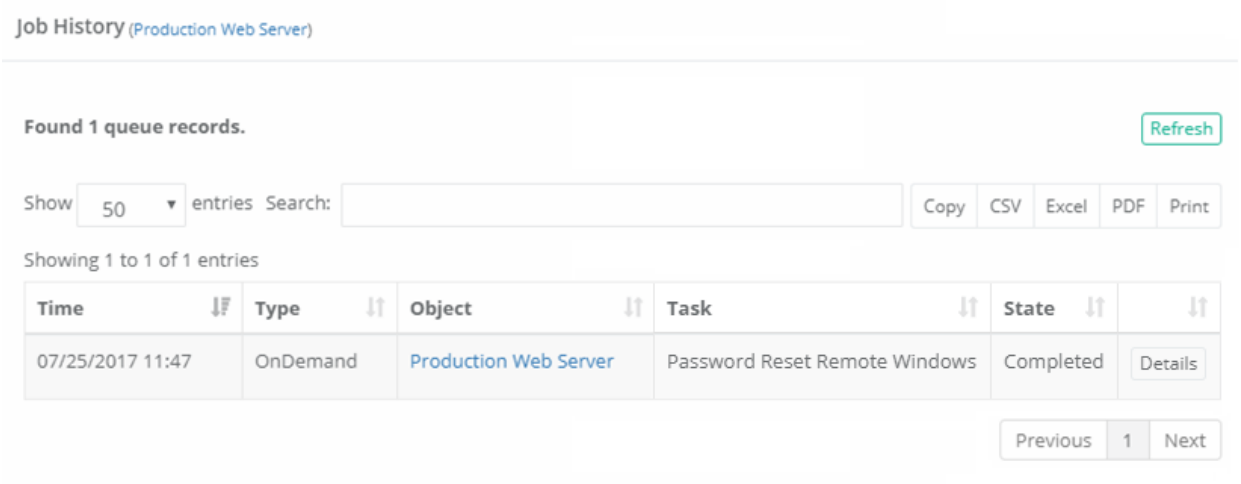

Figure 29: Job History Completed

The password reset job is now complete, but we need to validate our results before we continue. To do this, let's repeat our baseline test from the beginning of this section. Outside of XTAM, open your Remote Desktop session and attempt to connect using the original test account's user and password. Now, unlike earlier, you should fail to connect because either the username or password is wrong. We know it is the password because we just changed it.

At this point in the exercise, we have totally secured this connection. The only way to connect to this host is by using a secure privileged session in XTAM because the password to the account is not known to anyone besides the system.

With that stated, there are very valid reasons when the password must be shown or shared between users, so you are still able to expose (unlock) it when needed. The process is quite simple and we demonstrate that now.

Password Unlocking

Unlocking a password is the act of exposing a password to the user of XTAM. A couple of points to highlight before we begin the exercise:

- The user must be granted the appropriate permission to unlock a password. Permissions will be discussed in the next section.
- Secured passwords are never stored on any client computer. Passwords remain secured in the database of secrets until and only when they are required. In this example, the user requests an unlock and it is delivered to their browser where it is stored temporarily for this browser session only.
- All password *Lock* and *Unlock* events are captured in XTAM's Audit Log.

Now let's try out a password unlock. Using our recently password reset "Production Web Server" record as our example, to unlock a password:

1. Open the IT Records folder by clicking on the folder name in the list or by using the folder dropdown or Action menu and selecting **Open**.
    a. If you still have it in your Favorites, then you can click <IT Records> in your left navigation menu for quick access to this folder.
2. Open the Production Web Server record by clicking on the record name or by using the record dropdown or Action menu and selecting **View**.
3. Locate the Password field. To its right, click the **Unlock** button.

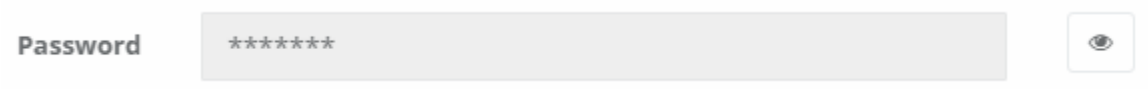

Figure 30: Password Locked

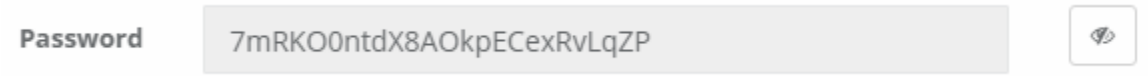

Figure 31: Password Unlocked

4. The password is requested by the client and is delivered to your web session from the secured database of secrets.
    a. Observe that it is no longer the password that we used in our baseline Remote Desktop test and that it validates against the unique Formula rule we created in the previous exercise.
5. You can click the Unlock button again or refresh your browser to return this field to its default Locked state.

And there it is. A fully automated (on demand) password reset job to a complexity (formula) you defined and secured in such a manner that most users will only be able to connect to the host using a secure, recorded session in XTAM.

Securing Objects with Permissions and Sharing

Permissions and sharing are concepts applied to both Folder and Records. The act of granting permissions is providing a user or group (of users) the ability to access folders and records with a pre-

determined set of security levels. Permissions can range from the low end "Viewer" up to "System Administrator" at the top and several steps in between.

Throughout this section, we will discuss these core permission concepts and perform a few exercises to help illustrate how they are applied to users.

User and Groups

Permissions are granted to specific users or groups of users. If you have connected XTAM with your Active Directory or LDAP server, then most likely these permissioned users or groups will originate from there. If you did not, then the users and groups will be created locally in XTAM's Directory Service component.

If you will use your Active Directory or LDAP connections solely in XTAM, then you may jump to the next topic Grant Permissions, otherwise let's continue with creating your first users and groups locally in the system.

To create a new user in XTAM:

1. If not already, login to XTAM as a System Administrator
2. Expand the Administration section of the left navigation menu and select **Local Users**
3. Click the **Create** button

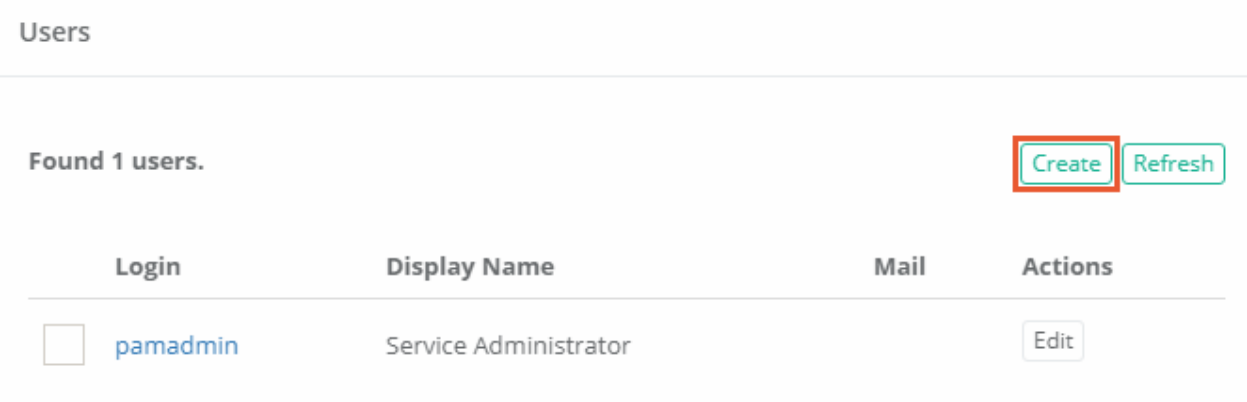

Figure 32: Create Local Users

4. Enter the following information into the User fields
    a. *Login*: ituser
    b. *First Name*: IT
    c. *Last Name*: User
    d. *Mail*: leave empty *(used to send alerts and notifications when configured)*
    e. *Password*: choose a password
    f. *Repeat Password*: reenter the password
5. Click **Save** to create this new user.

If you also want to organize local users into local groups:

1. If not already, login to XTAM as a System Administrator

2. Expand the Administration section of the left navigation menu and select **Local Groups**
3. Click the **Create** button
4. Enter the following information into the Group fields:
    a. *Name*: IT Department
    b. *Description*: IT Department Group

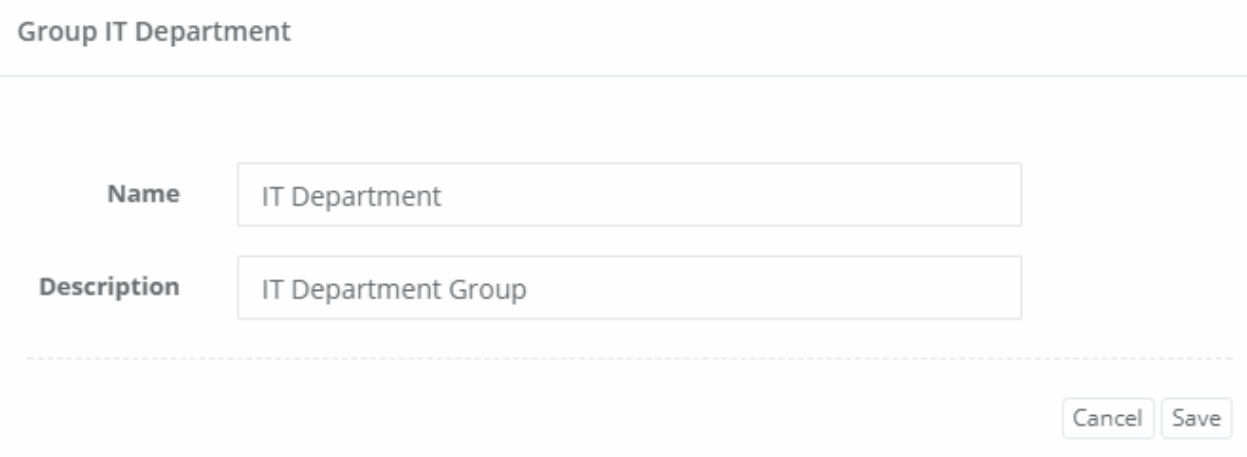

Figure 33: Create Local Groups

5. Click **Save** to create this new group.
6. Click on the new IT Department group to open it and then click **Add** to add a new member.

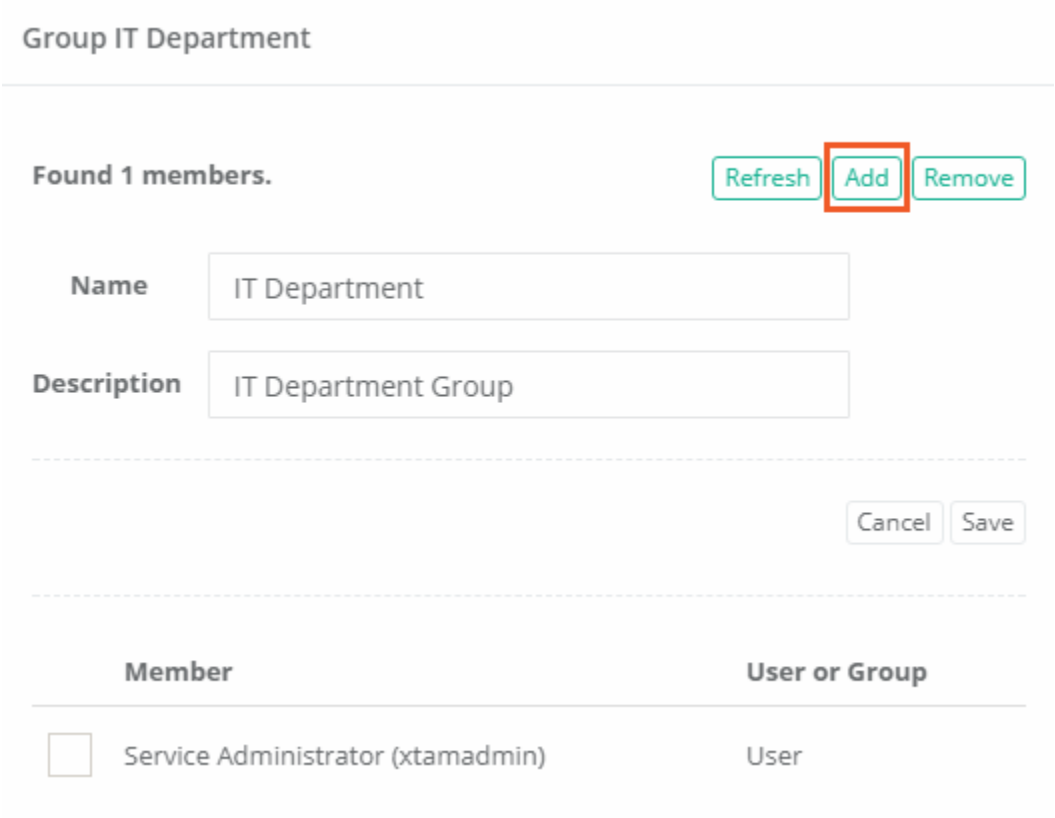

Figure 34: Add New Group Members

7. In the principal field, type “ituser” and then click **Add.**
8. When “IT User” appears as a Selected Principal, click **Select** to add this user to the group. IT User is now a member of the IT Department group.

Please note that the user who creates the local group will automatically become its first member. In this exercise that is our Service Administrator.

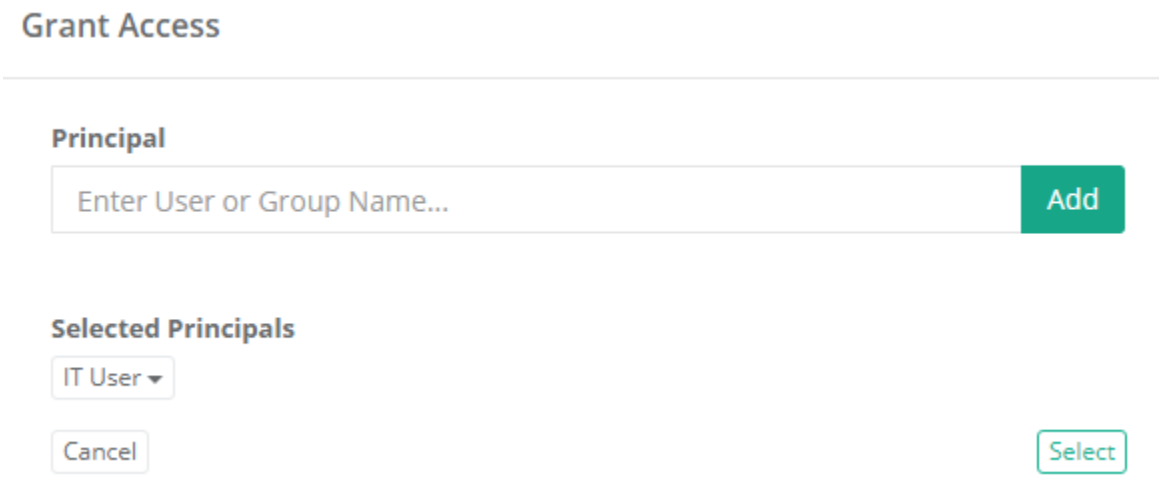

Figure 35: Add Local User to Local Group

Please note that local users and groups cannot be mixed with Active Directory or LDAP users and groups. Specifically, this means that AD users cannot be added to Local Groups and Local Users cannot be added to AD Groups.

Grant Permissions

Once users and/or groups (local or AD) have been added to XTAM, you can begin to grant permissions to folders and records. The act of granting permissions will give this user or group varying levels of access to this object, so it is important for you to understand the following points in your system:

- What are the XTAM permission “roles”?
- What options do these roles grant to users and groups?
- Who do you want to assign these roles?
- How granular do you wish to control permissions (inheritance vs unique)?

A user or group giving the wrong permissions can result in inappropriate access to privileged accounts, sessions or jobs.

For this scenario, let’s return to our original “IT Records” folder and begin granting permissions.

1. Open the IT Records folder by clicking on the folder name in the list or by using the folder dropdown or Action menu and selecting **Open**.

a. If you still have it in your Favorites, then you can click <IT Records> in your left navigation menu for quick access to this folder.

2. Once you are inside the IT Records folder, locate and click the **Permissions** button along the top.

Figure 36: Permissions Button

3. The IT Records permissions page will load. Before proceeding, it is good practice to always confirm that you are looking at the correct object before modifying permissions. In our example, you will see this:
   a. "Permissions for IT Records / inherited from Root Folder"
      i. This means we are working on the Permissions of the object "IT Records" which currently inherits permissions from its parent "Root Folder". *Root folder is simply the home or root of the All Records view.*
      ii. You will also notice the Make Unique button. When the option to Make Unique is available, that implies this object is currently inheriting from its parent.

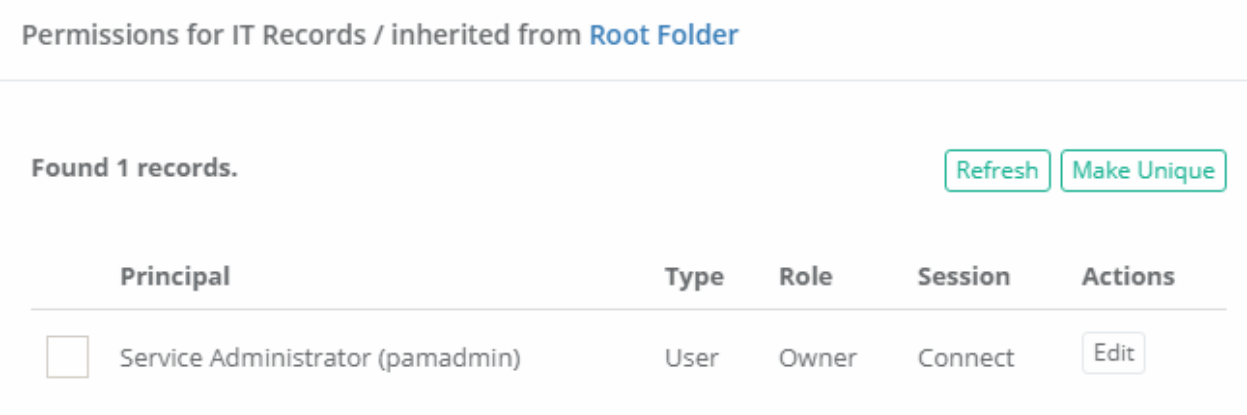

Figure 37: Inherited Permissions on our IT Records Folder

4. Now that we are certain about the object, click the **Make Unique** button so we can modify the folder's permission. Click **OK** to accept the confirmation message.
   a. To learn more about inheritance throughout XTAM, please review What is Inheritance?
5. The permissions view will refresh and display "Permissions for IT Records" correctly indicating that it has unique permissions now and is no longer inheriting from its parent Root Folder.

If you want to revert and go back to inheriting permissions, simply click the **Inherit from Parent** button. However, for this exercise, we are going to proceed with unique permissions.

6. Click **Grant Permissions**

Figure 38: Grant Permissions

7. In the Principal field, enter “IT Department” and click **Add**. The group IT Department will be listed under Selected Principals.
    a. If you want to grant additional permissions, you could add more users or groups during this operation by simply repeating this step as often as needed.
8. Choose the Permissions options:
    a. *Role*: Viewer
    b. *Session Control*: None
9. Click **Select** to complete the operation and grant the selected permissions to the IT Department group.

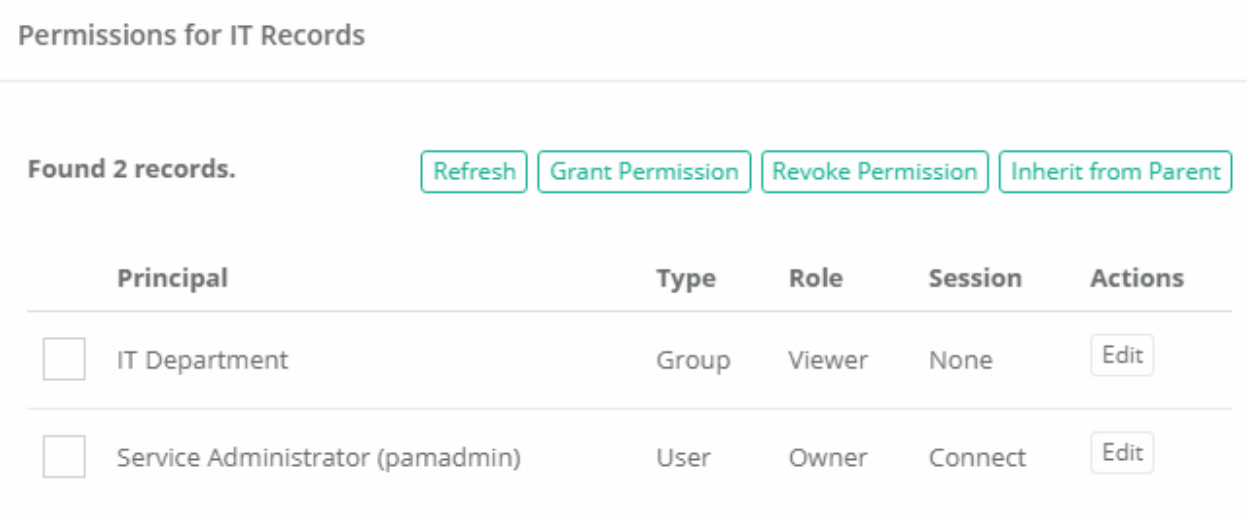

Figure 39: Unique Permissions

You have now granted the group “IT Department”, and subsequently all its members, with the Viewer role and No session control to this folder. Something very important to remember is that inheritance is enabled by default for all records and folders in XTAM, so whatever child objects reside in this folder (now or in the future) the IT Department group also automatically has the same View role and No session control to them as well. To illustrate this point, let’s look at the permissions to the record “Production Web Server” currently residing in the IT Records folder where inheritance is enabled.

1. Open the IT Records folder by clicking on the folder name in the list or by using the folder dropdown or Action menu and selecting **Open**.
    a. If you still have it in your Favorites, then you can click <IT Records> in your left navigation menu for quick access to this folder.
2. Open the Production Web Server record by clicking on the record name or by using the record dropdown or Action menu and selecting **View**.
3. Locate and click the **Permissions** button along the bottom of the record’s View.
4. When the record’s permissions load, you will notice two things:
    a. As expected, “Permissions for Production Web Server / inherited from IT Records” appears along the top. This record inherits permissions from its parent IT Records because that is the default mode and we never made the permissions unique (Make Unique button).
    b. The group IT Department therefore has permission (Viewer and None) to this record.

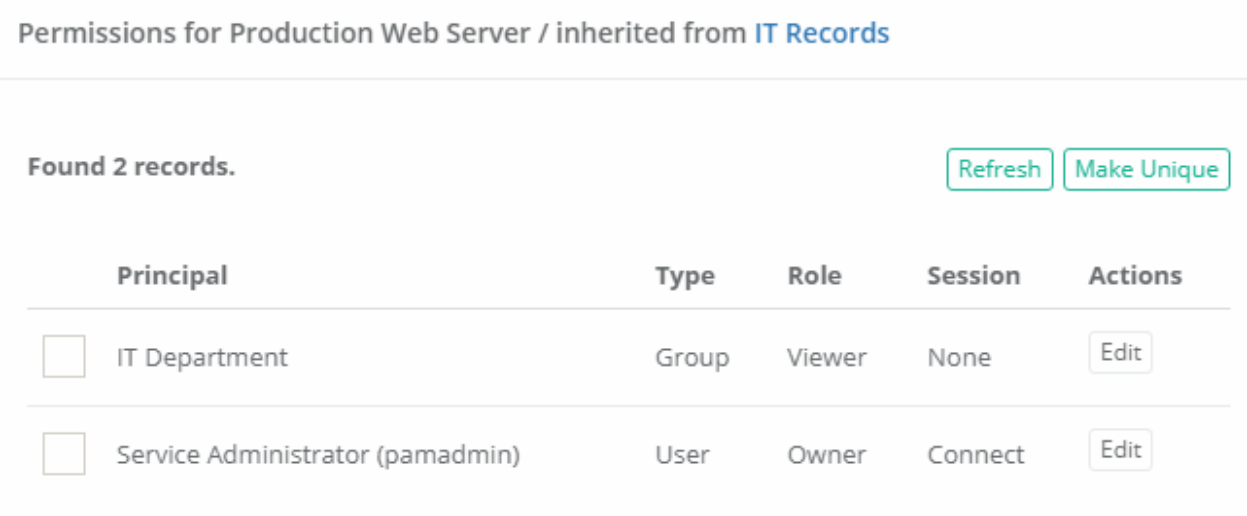

Figure 40: Inherited Permissions on a Child Record

This highlights the ease of use and flexibility of working with permission inheritance throughout the XTAM system. On the other hand, it also highlights the importance of truly understanding all parent-child relationships and ensuring only the required users or groups have the base level of permissions to all required objects.

Permissions in Action

Now that we have completed the exercise and implemented some basic level of object permissions, let's see how that looks from an end user's perspective.

1. Open a new browser or a new private/incognito browser session
2. Login to XTAM using the user account "ituser" that was created in the previous section.
3. A few observations to note when you first login with this account:
    a. This is not a System Administrator account so the entire Administration section of the left navigation menu is hidden and inaccessible.
    b. Under the Records section, the favorite <IT Records> is not displayed because Favorites are specific to a user and are not shared globally across the system.

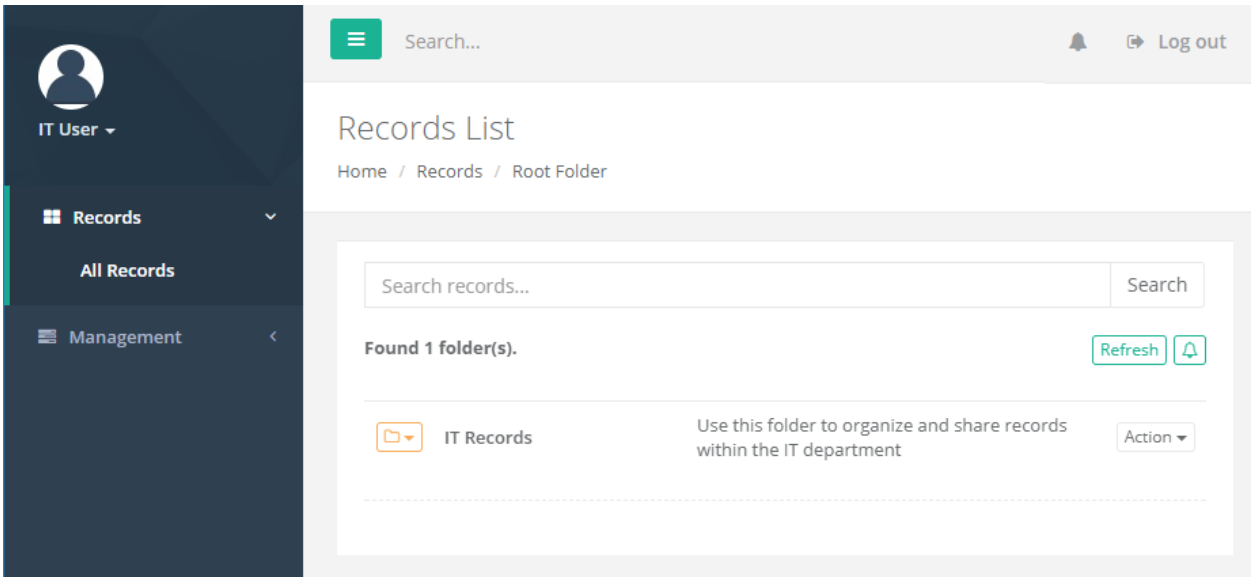

Figure 41: "IT User" Logged In View (non-Admin)

4. Open the IT Records folder by clicking on the folder name in the list or by using the folder dropdown or Action menu and selecting **Open**.
5. Within this folder, observe that all the options along the top are hidden and inaccessible. Compare this view with that of the System Administrator in your other browser session.
6. Open the Production Web Server record by clicking on the record name or by using the record dropdown or Action menu and selecting **View**.
7. Within this record, observe again that all the options along the top and bottom are hidden and inaccessible by this user. Compare against your System Administrator view and take special note that the edit, configuration, unlock and connect buttons are not available. This user has minimum permissions to View this folder and record only.

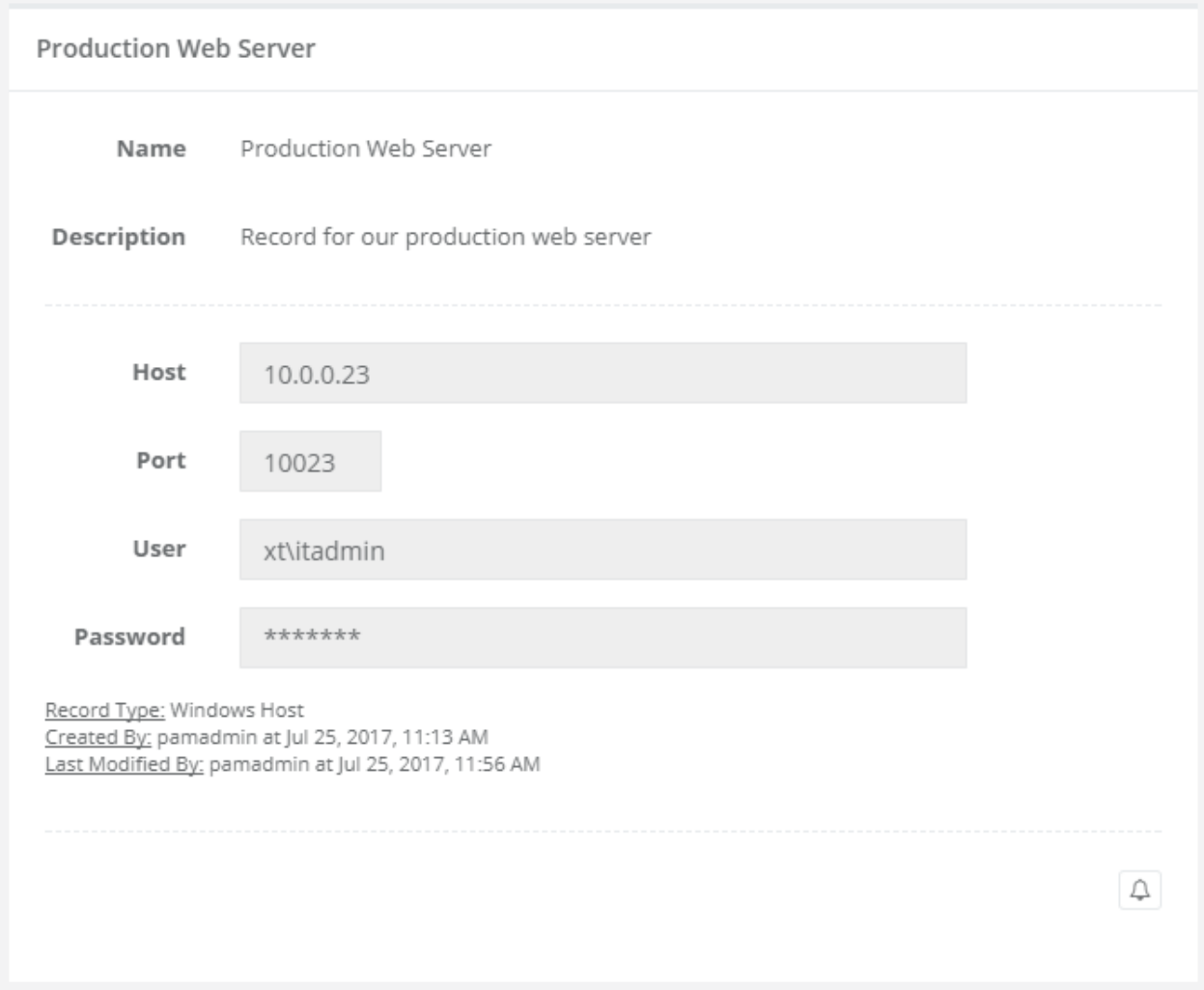

Figure 42: Record with Viewer Only Permissions

Let's modify the permissions of "ituser" slightly to see how permissions can be adjusted to grant or revoke specific functionality in real-time.

1. Back in your System Administrator's XTAM session, modify the permissions on the IT Records folder.
2. Select the permission record for IT Department (the group 'ituser' is a member of) and click **Edit**
3. Make the following changes:
    a. *Role*: Editor
    b. *Session Control*: Recording
4. Click **Select** to save the change.

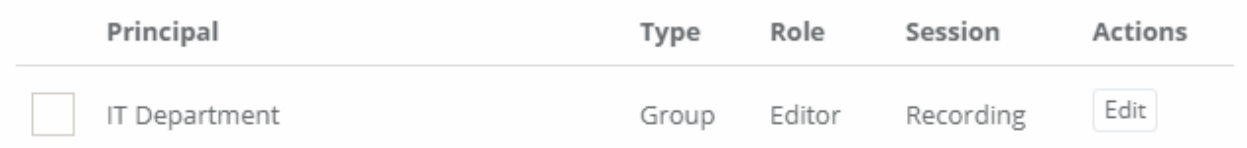

Figure 43: IT Department Permissions after Modification

5. Return to ituser's browser session and refresh your browser.
6. Open the IT Records folder by clicking on the folder name in the list or by using the folder dropdown or Action menu and selecting **Open**.
7. Within this folder, observe the options along the top that are visible and accessible by this user.
8. Open the Production Web Server record by clicking on the record name or by using the record dropdown or Action menu and selecting **View**.
9. Within this record, observe that the options along the top and bottom are visible and accessible by this user now. Including both the Unlock button for the password field and the Connect button to establish a secure session.

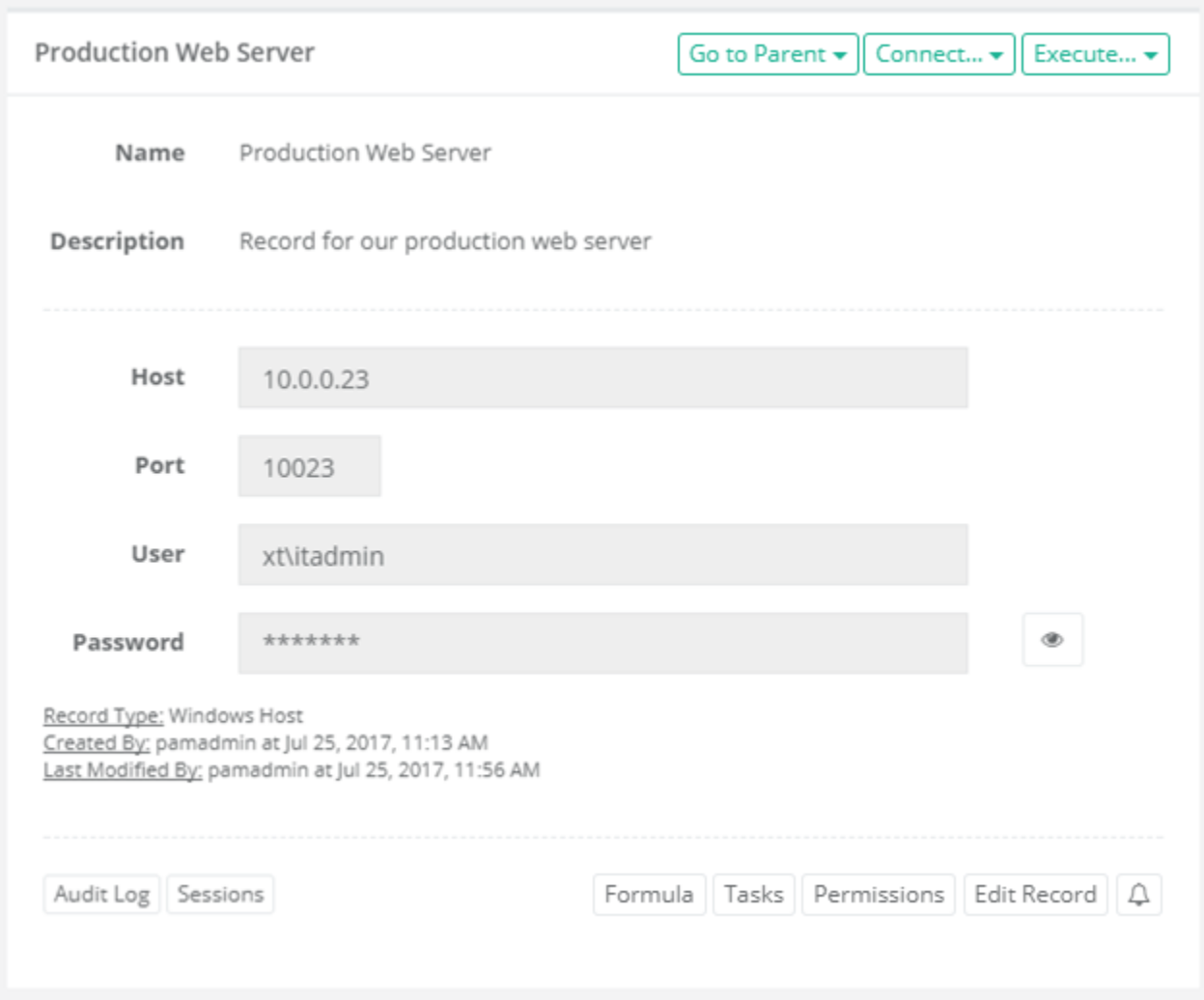

Figure 44: Record with Edit and Connection Permissions

To recap, we covered the relationship between users and groups, how permission inheritance is defined by default and when making them unique as well as how permissions can be modified and what that means to the end user's access to the system.

Revoke Permissions

Revoking permissions is quite simply removing permissions to an object that was originally granted to a user or group or users. To demonstrate this principle, let's revoke "ituser" from the permissions we just granted it.

1. From the System Administrator's session, modify the permissions on the IT Records folder.
2. Locate and select the box next to IT Department.
3. Click the **Revoke Permissions** button. IT Department is immediately removed from the permissions of this folder and all child objects that are set to inherit from it (our "Production Web Server" record in this folder).

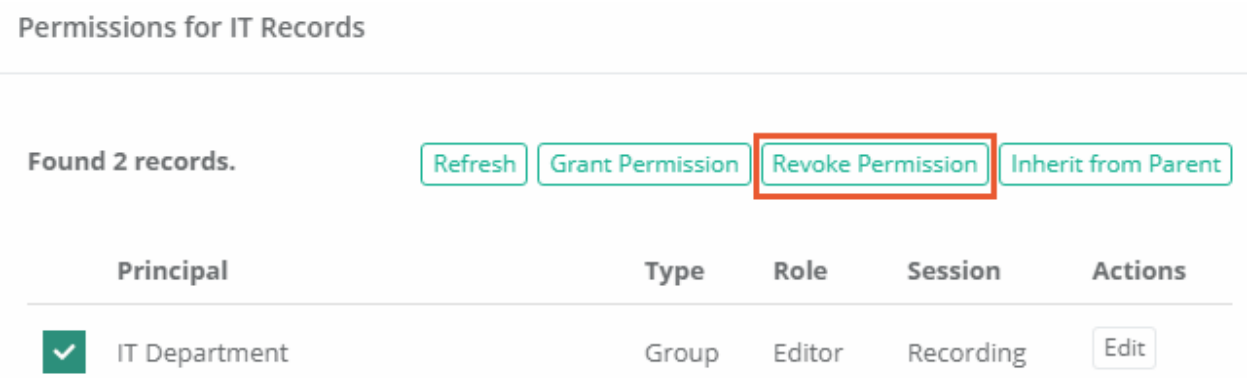

Figure 45: Revoke Permissions

4. Refresh the browser that ituser is logged in and you will notice that they can no longer see nor access the IT Records folder or any object that inherits from it.

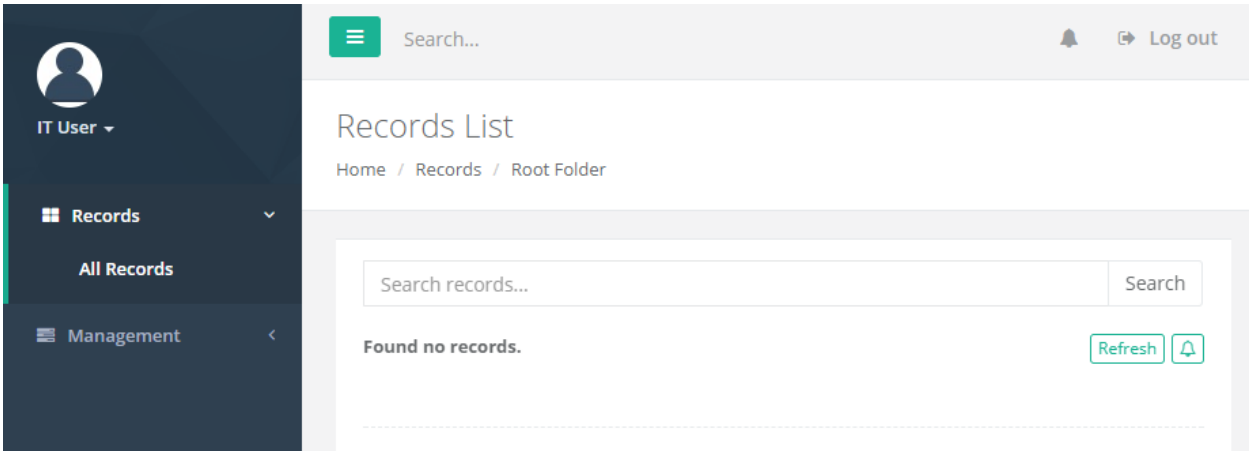

Figure 46: "IT User" with Revoked Permissions

System Administrators

The System Administrator role is defined as the top most permission any user or group can be granted in XTAM. The default installation account will become the first System Administrator and from this starting point, other users and groups can be given this role. It is extremely important to know that this

role has complete and total control over all objects including folders, records, password unlocks, sessions, deletion, XTAM configuration and view access to all logging. They also can grant AND remove any other users as System Administrators. Please only grant this permission to trusted users.

To grant a user or group the System Administrator role:

1. If you are not already, login to XTAM as a System Administrator
2. Navigate to and expand the Administration section of the left navigation menu and select **Global Roles.**
3. Click the **Add** button
4. Enter the user "ituser" and click **Add.** IT User will appear as a Selected Principal.
5. Choose "System Administrator" from the Global Role dropdown.
6. Click **Select** to complete the operation.

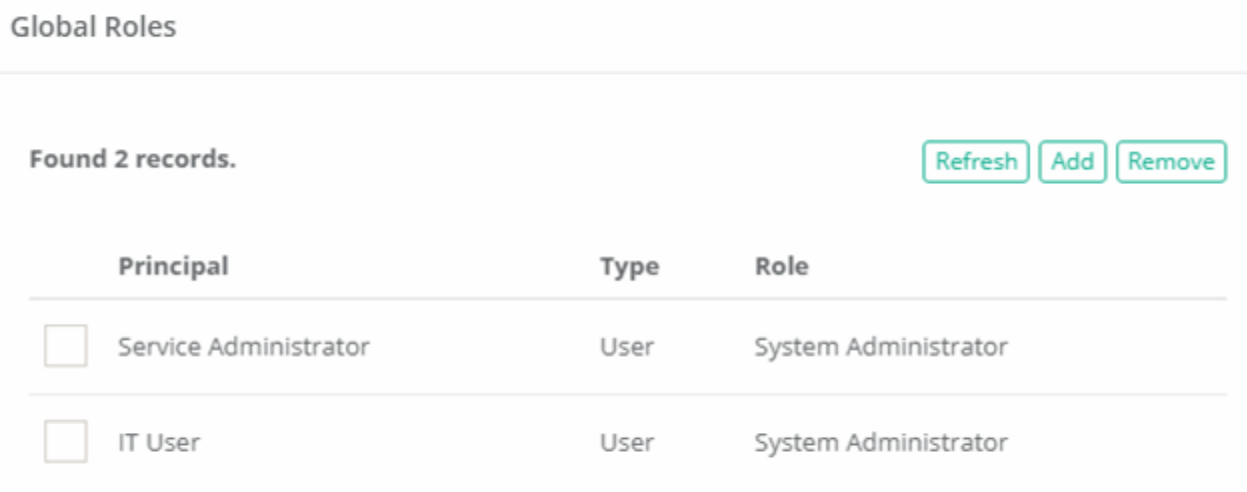

Figure 47: System Administrators

7. Refresh the browser that "ituser" is logged in and you will notice that the Administration section is now visible and accessible. Also, this user can now view, access, connect and has full control over the IT Records folder and all other records and folders regardless of the specific permissions assigned to the object's permissions.

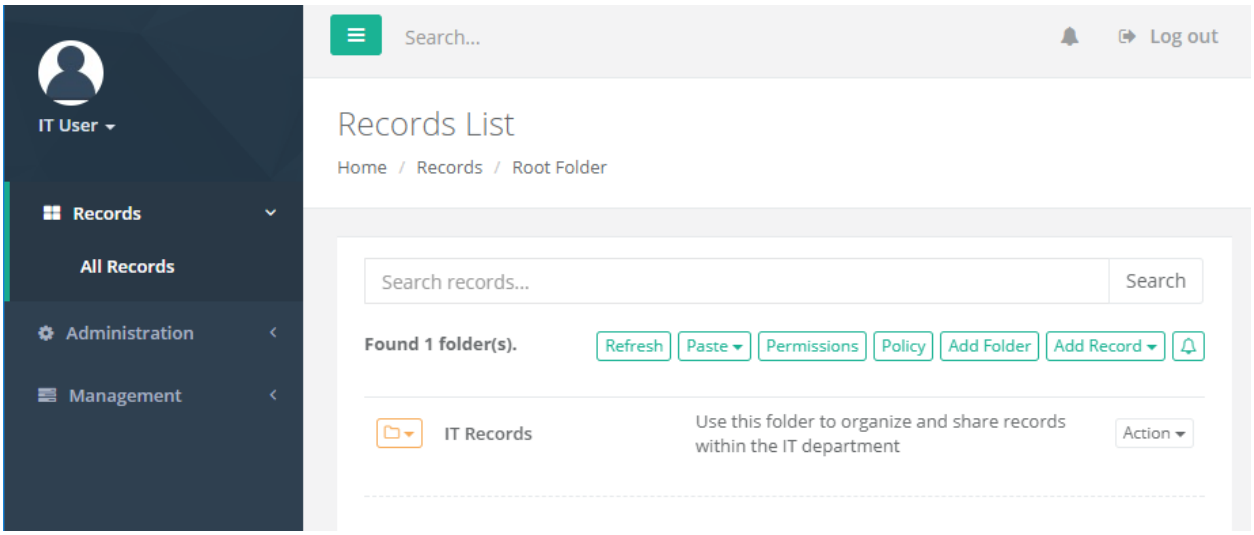

Figure 48: "IT User" with System Administrator Permissions

System Administrator has full control over all components within the XTAM system and should only be granted to trusted users.

Please revoke the System Administrator role from the user “IT User” before continuing with this guide. It’s good practice to always revoke untrusted, outdated or test accounts from this permission role.

Reviewing the Audit Log

One of the most important sections of the XTAM system is the Audit Log. The System's Audit Log is accessible only by users who have been given the System Administrator role.

The System Audit Log contains captured events that have taken place across the entire XTAM system. These events include record creation, modifications, session connections, system configuration and more.

To access the Audit Log:

1. If you are not already, login to XTAM as a System Administrator
2. Navigate to and expand the Administration section of the left navigation menu and select **Audit**
3. Wait a few moments for the Audit Log to load the most recent events
4. When the events appear, scroll down through the list and observe all the activities that we have performed during this walkthrough.
5. Please also explore the options available along the top that include filtering, search and export.

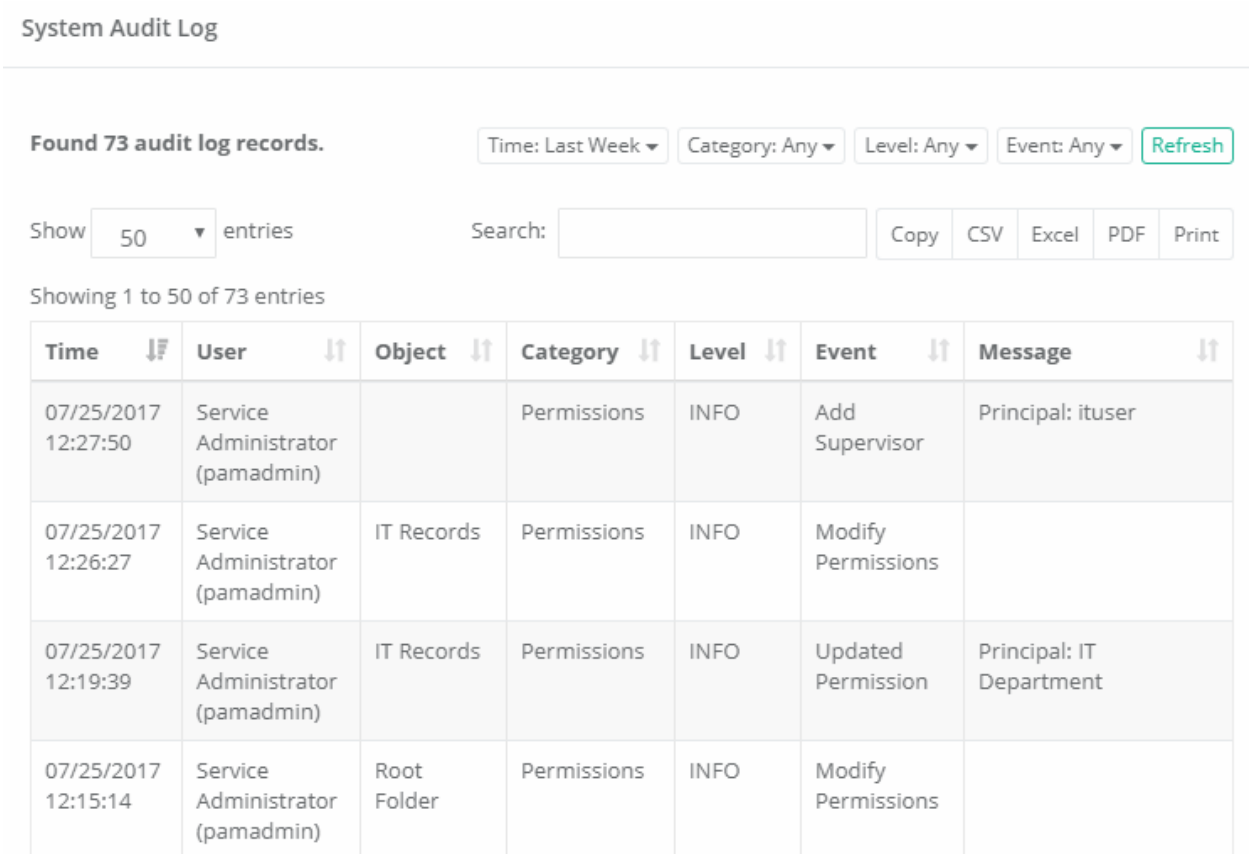

Figure 49: System Audit Log

Notifications and Alerts

If you remember back to the beginning of this guide, when we first created our IT Records folder we started with setting up an Alert to notify on permission events. We did this so our permission modifications in the previous section would be captured.

User alerts can be accessed in two locations and will display the event that triggered the notification. Let's look at our Alerts from today:

1. Along the top of the XTAM interface, accessible from any view, click the **Alert** button. If you followed along closely, you should see a badge indicating several alerts have been generated.

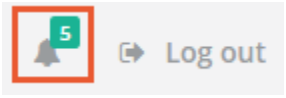

Figure 50: Top Bar Alert Notifications with Badge

2. Clicking the Alerts button will open the dropdown menu displaying a handful of recent notifications, sorted from the most recent to the oldest. In this dropdown, you will see several notifications related to the permissions we updated on the IT Records folder during earlier exercises.
3. At the bottom of this dropdown, click the **See All Alerts** option.

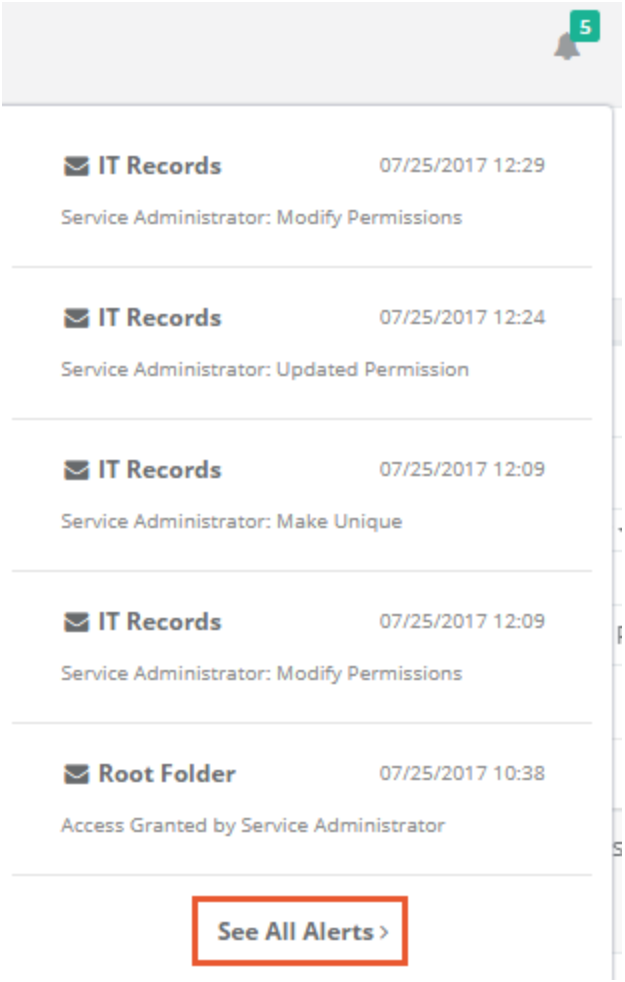

Figure 51: Open My Alerts

4. This will open the full list of all Alerts including some additional information and descriptions.

As with most event based views in XTAM, there are many options to explore including filters, search and export. Look around and continue to the next section when you are ready.

Unsubscribe to Alerts

When you no longer want, or need to receive Alerts about an object, you can very easily unsubscribe from it and these notifications will no longer be generated for you. Let's quickly unsubscribe from the IT Records folder:

1. Navigate to and expand the Management section of the left navigation menu and select **My Profile**
2. When My Profile loads, click over to the **Subscriptions** tab.
3. Locate and select the IT Records object by clicking its checkbox.
4. Click **Unsubscribe.**
5. The view will refresh and IT Records will be removed from the list.

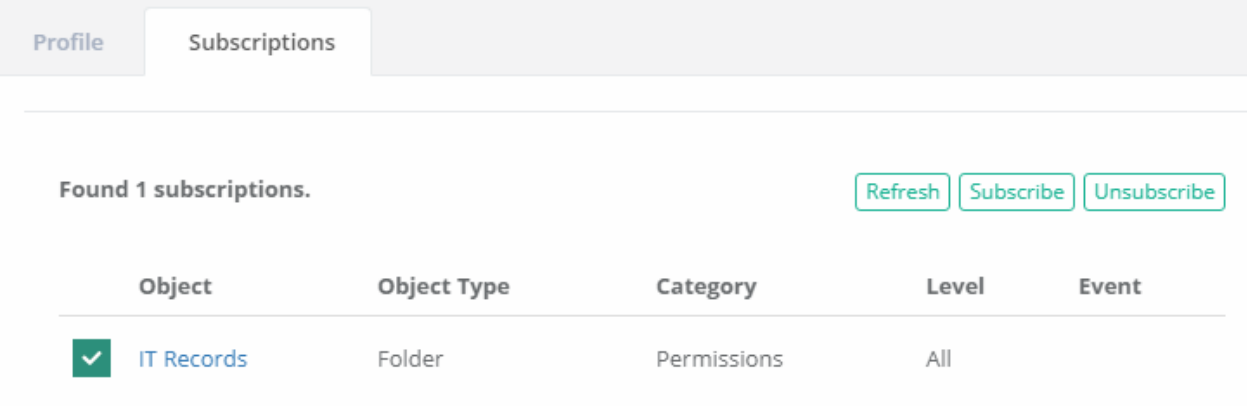

Figure 52: Unsubscribe from Alerts

You have successfully unsubscribed from receiving notifications related to this object.

Logging Out of Xton Access Manager

When you are done working with XTAM, it is highly recommended to securely log out of the system. You should never walk away from your computer when logged into a session of XTAM as anyone could walk by and have control of the software.

To securely log out of XTAM:

1. Click the **Log out** button located in the upper right corner of XTAM or **Logout** located under the User Profile located in the upper left.

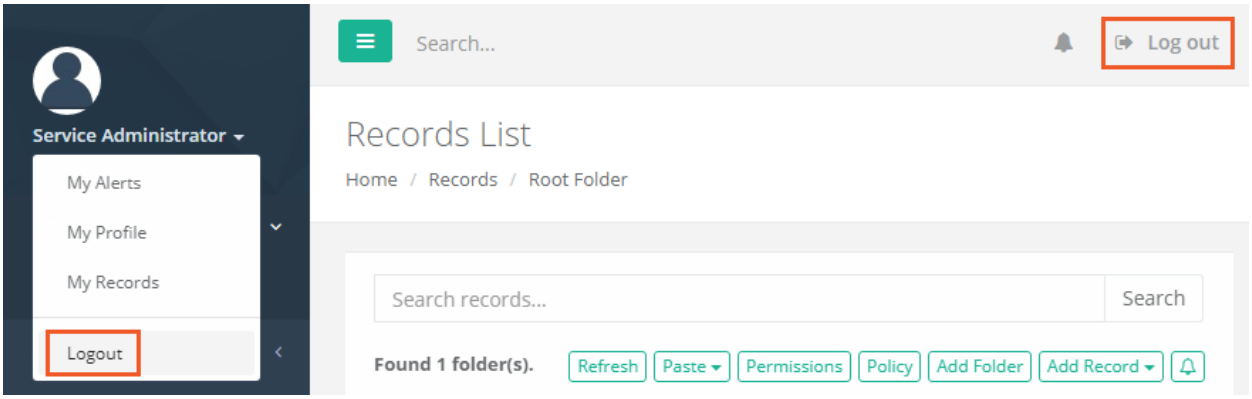

Figure 53: Logout Options

2. The application will log your account out.
3. Exit your web browser to ensure the session is completely logged out.

If you have not already, logout and exit your browser that was used for our “IT User” exercises too.

Wrapping Up

That concludes this Getting Started Guide. If you followed along through each section, you should now feel more comfortable with Xton Access Manager and have an introductory working knowledge of its features and functionality. We encourage you to revisit each section and try new options and configurations. Also, explore the many areas that were not included in this guide like Discovery Queries, Custom Record Types and Reports at your own pace.

Additional Information

To read additional documentation, watch some walkthrough videos or read our FAQ and How-To articles, please visit our Resources page located at https://www.xtontech.com/resources/.

If you have any questions, feel free to contact us at any time.

Appendix

What is Inheritance?

XTAM utilizes the concept of inheritance is several areas to make the management and configuration of objects more streamlined and easily organized. Inheritance defines the relationship between a parent and child object and specifically what is inherited down from the parent to the child which resides beneath it.

Inheritance in XTAM can be found in the following areas:

- Permissions
  - Permissions are inherited by default from parent folder to child objects (subfolders or records). If permissions are modified on the parent folder, then all child objects will reflect this change.
  - To make permissions unique means to stop this parent to child inheritance and instead have the child contain its own set of permissions which may in turn inherit down to its own children.
- Formulas
  - Formulas are inherited by default from Record Types. If the formula on a parent record type is modified, then all child types will reflect this change.
  - To make formulas unique means to stop this parent to child type inheritance and instead have the child contain its own formula which may in turn inherit down to its own children.
- Strategies
  - Strategies are inherited by default from Record Types. If the strategy on a parent record type is modified, then all child types will reflect this change.
  - To make strategies unique means to stop this parent to child type inheritance and instead have the child contain its own strategy which may in turn inherit down to its own children.
- Policies
  - Policies are inherited by default from parent folder to child objects (subfolders or records). If a policy is modified on the parent folder, then all child objects will reflect this change.
  - To make policies unique means to stop this parent to child inheritance and instead have the child contain its own policy which may in turn inherit down to its own children.

The “pros” of inheritance is that it allows for ease of use and flexibility when configuring and using the system while the “cons” are that the more *unique* objects you create, the more difficult and cumbersome it becomes to understand and manage the structure of your system.