Xton Access Manager

INSTALLATION GUIDE (UNIX/LINUX)

UPDATED APRIL 2018

Contents

Introduction 2

Technical Support 2

Xton Access Manager 3

Privileged Account Management 3

Privileged Session Management 3

Privileged Job Management 3

Software Components 3

Architectural Diagram 3

Services 5

Active Directory or LDAP Integration 5

Planning your Installation and Deployment 5

Installing Xton Access Manager 5

System Requirements 6

Software Requirements 6

External Database 6

Installation 7

License Agreement 7

Components 7

System Administrator 10

SSO Connect 10

External Database 10

Active Directory Integration 11

Installation Complete 12

Logging into Xton Access Manager 13

Browser SSL Certificate 13

Initialize 13

License Registration 14

Manual Registration 15

Uninstalling Xton Access Manager 15

Uninstaller 15

Database Cleanup 15

Appendix 16

Remote Session Manager Configuration 16
Web Server 17

Introduction

This guide is designed to show system administrators how to install, initialize and run Xton Access Manager on a Unix computer. For administration and user guide documentation, please visit our support section. https://www.xtontech.com/resources

Technical Support

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

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.

The target audience is system administrators with knowledge of computer administration, Active Directory and (optionally) database connectivity.

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.

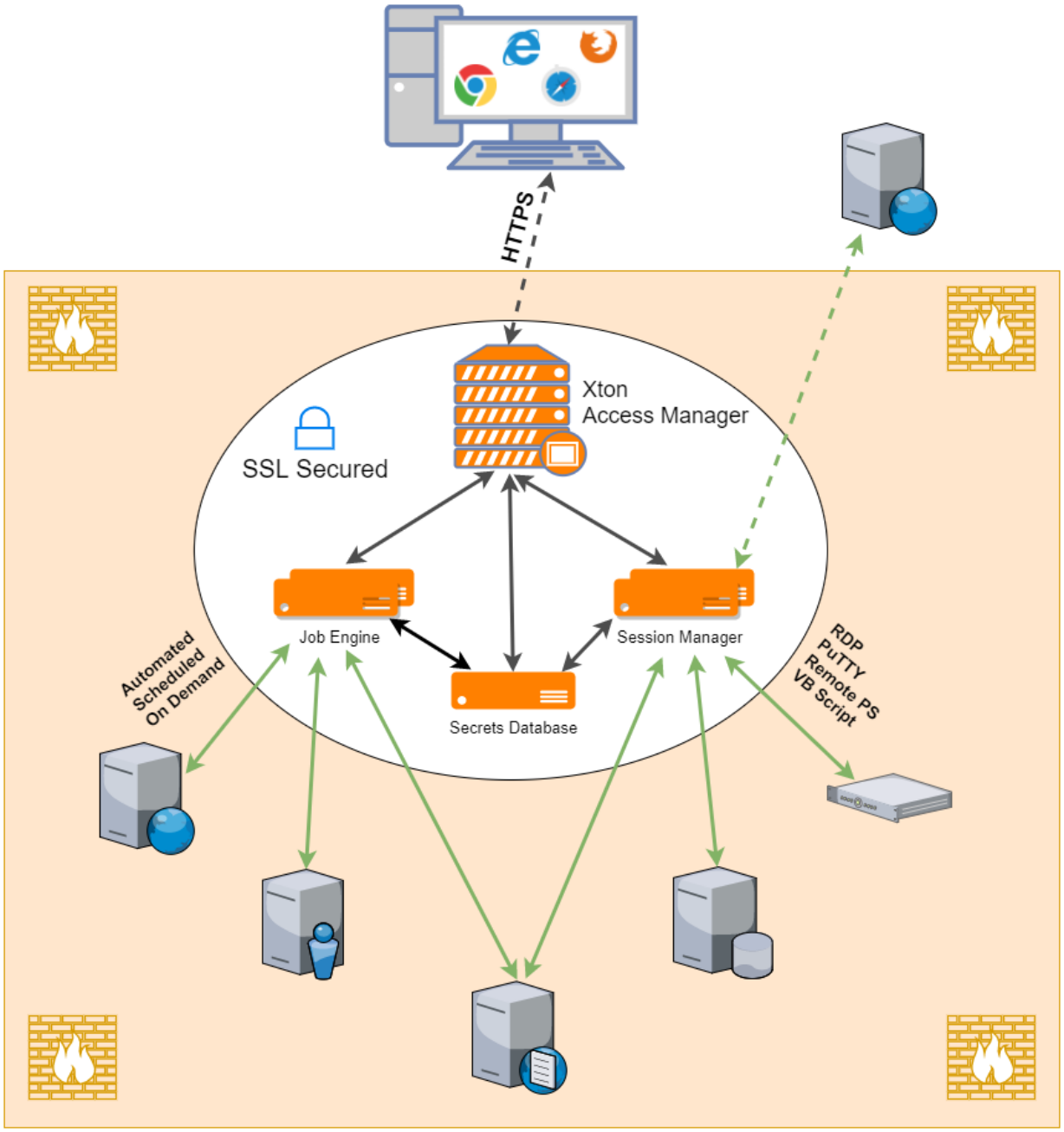

Figure 1: Xton Access Manager Architectural Diagram

Services

Depending on your installation, the following services may be deployed to Automatically startup on your computer.

Service	Function
pamdirectory	Provides the directory service to manage local users and groups in XTAM.
pammanager	Provides the service to manage the XTAM system.
pamsession	Provides the service to establish, maintain, control and record privileged sessions via a user's web browser.

Table 1: XTAM Services

Active Directory or LDAP Integration

Integration with Active Directory or LDAP provides the ability to add Active Directory Users or Groups to XTAM to manage or use the system. XTAM will use this Active Directory integration to

- Authenticate user logins
- Read Active Directory group membership
- Reset Active Directory passwords

Planning your Installation and Deployment

The key to a successful deployment is proper planning. Before you begin the installation process, please understand the following.

- The full scope of your user base. How many individual users will be working with XTAM and of those how many will be accessing the system at the same time. This will help in planning the amount of resources and servers that are required to run the system efficiently.
- Setup a test environment. This could be a basic single server VM or a dedicated workstation, but ensure XTAM is configured and running in your test environment before deploying to production. This can also act as a test bed for future software releases.
- Decide if you want to integrate with Active Directory or LDAP for users, groups and authentication or to maintain a local directory for users and groups.
- If you want to use a SSL certificate to ensure a secure connection between the client computers and XTAM, then it is highly recommended to obtain and deploy the certificate prior to installation.
- Create a new user (non-root) with su or sudo privileges and a new directory (not /tmp) for the XTAM software. Neither the root account nor the /tmp location should be used for installation.

Installing Xton Access Manager

This section will work through the process of installing Xton Access Manager to a Unix computer.

System Requirements

The following are minimum requirements to use XTAM for Single Server and medium use Production farms. Please contact us to discuss architecture and system recommendations for large scale farm deployments.

NOTE: Do not install XTAM using a *root* account. This is not recommended nor best practices for installing or configuring any software in a Unix environment. The recommendation is to create a new user and give it *su* or *sudo* (or add to the sudo group) privileges to perform the installation.

	Single Server, Test or Quick Trial	**Medium Use Production Farm**
Windows O/S (64-bit only)	Windows Server 2008 R2+ / Windows 7+	Windows Server 2008 R2+
Other O/S (64-bit only)	Red Hat, Ubuntu, Debian, CentOS	Red Hat, Ubuntu, Debian, CentOS
Database	Included *	MS SQL, MySQL, Oracle, PostgreSQL
Servers	1	5 (1 database, 2 job engines with session manager role, 1 user directory, 1 load balancer)
Memory	2GB+	4GB+
Disk Space	10GB+	10GB+

Table 2: System Requirements

*For Single Server, Test or Quick Trial deployments the recommendation is to use the included, internal database however you can use any of the other supported databases that are available to you.

Software Requirements

- Web Browsers *(latest version is recommended if not specified)*
    - Internet Explorer 10+, Windows Edge, Google Chrome, Mozilla Firefox or Apple Safari

External Database

The default installation includes an internal database that can be deployed. If you would prefer to use an existing database in your environment, the following are supported. Please be prepared to supply a valid connection string to your database as well as an appropriate user and password to successfully establish this connection. *Please contact your Database Administrator if you need assistance.*

NOTE: The installation process does **not** create its own database or tablespace but rather makes use of an existing one. With that in mind, please ensure one with the name "PamDB" already exists as this will be used by the application.

- Apache Derby version 10.12.1.1+

- Microsoft SQL version 2008+
- MySQL Community or Enterprise Edition version 5.7+
- Oracle version 11.2+
- PostgreSQL version 9.5+

Installation

The following section will describe each option that is available when executing the Unix installation shell script. To begin, run the shell script from the location where you want to install the software. Depending on the options selected, the following configuration parameters may be available.

TIP: Rather than using the Unix /tmp folder to perform the installation, create a new folder because background processes on the host may attempt to "clean" this directory during this process. Suggested locations would be either /opt/xtam or /urs/local/xtam.

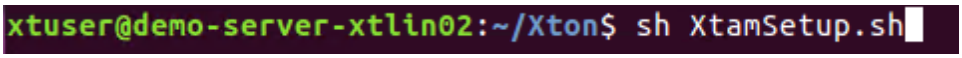

Figure 2: Execute Installation Shell Script

License Agreement

Press **<ENTER>** to read the license agreement and enter **<Q>** when complete. When prompted, accept the license agreement by entering **<Y>** to continue. The license agreement must be accepted to install the software.

Figure 3: Read and Accept the License Agreement

Components

Choose from the available list of components to install on this computer. If you are looking to deploy a quick test environment, the recommendation is to accept the default options by pressing the **<Enter>** for each component. If you would like to customize the installation, then please review the following sections to understand the purpose of each component and enter the **<N>** key to exclude a component.

Please note that while you can choose to not install some components on this computer, they may still be required for proper software operations. For example, you may wish to install the Session Manager service on another system for performance optimization. In this situation, you would choose to not deploy this service on your primary host and then after this initial installation is complete, you would then run this same script on your other host and only choose the Session Manager option. Later on in the configuration of the software, you will have the ability to define which workstation is running each service.

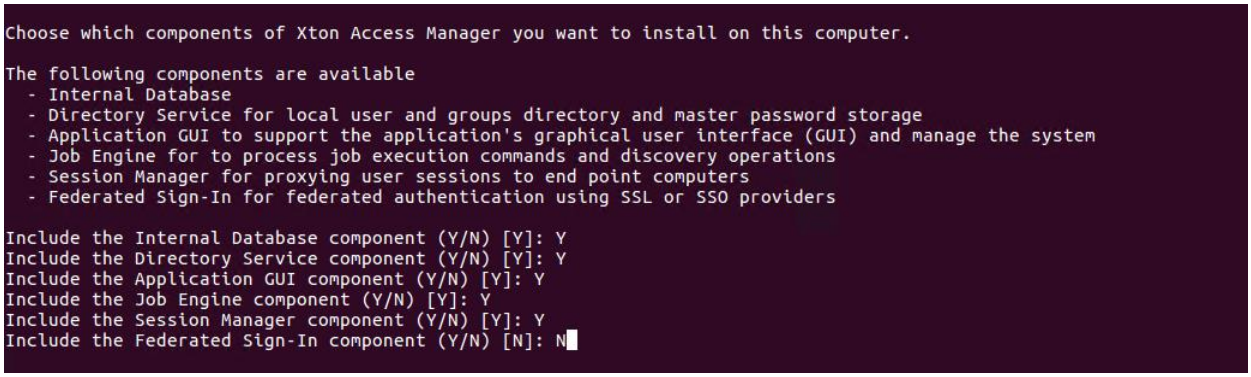

Figure 4: Choose Components

Internal Database

This option will define which database to use. When included (**<Y>**) the installation will deploy, configure and use its internal database. If excluded (**<N>**), you will be prompted to supply an existing database in your environment to use (connection string, user and password). Please review the requirements section for more information about External Database support.

*For single server or test environments, the recommendation is to include (**<Y>**) this option to use the included database.*

Directory Service

This option will define which user store to use. When included (**<Y>**) the installation will include a local user store that can be used to create users and groups and a database to secure the master password. When excluded (**<N>**) the installation will not deploy this component to the computer; however, this is a required component so it must be deployed to only one other computer and configured post installation in XTAM.

To install this component on another host, simply run the script on that system and include (**<Y>**) this option.

*The recommendation is to include (**<Y>**) this option during installation.*

Application GUI

This option will define the deployment of the XTAM interface (GUI). When included (**<Y>**) the installation will include the manager interface (GUI) to this host computer. When excluded (**<N>**) the installation will not deploy the GUI requirements to this host computer.

To install this component on another host, simply run the script on that system and include (**<Y>**) this option.

*The recommendation is to include (**<Y>**) this option during installation.*

Job Engine

The Job Engine is required to execute background operations like discovery queries and password resets. This option defines the deployment of a worker role to this host computer. When included (**<Y>**) a Job Engine role will be deployed. When excluded (**<N>**) a Job Engine role will not be deployed to this computer.

To install this component on another host, simply run the script on that system and include (**<Y>**) this option.

Please note that at least one job engine should be present in the farm to execute password reset, remove script execution or discovery queries.

*The recommendation is to include (**<Y>**) this option during installation.*

Session Manager

The Session Manager component is required to establish, control and record privileged sessions. This option defines the deployment of a session manager service to this host computer. When included (**<Y>**) a session manager service will be deployed, configured and run from this host. When excluded (**<N>**) a session manager service will not be deployed.

To install this component on another host, simply run the script on that system and include (**<Y>**) this option. Review the following section if you intend to install Session Manager on a remote computer(s): Remote Session Manager Configuration

Please note that if a session manager service is not defined during installation, you will need to add one during system configuration before sessions can be established.

*The recommendation is to include (**<Y>**) this option during installation.*

Federated Sign-In

This option defines the deployment of a federated sign-in component that can be used to establish user authentication. When included (**<Y>**) you will need to supply your federated sign-in server connection parameters. When excluded (**<N>**) a SSO server will not be configured and the default login authentication will be used.

To install this component on another host, simply run the script on that system and include (**<Y>**) this option.

*This is an advanced option and should only be included if necessary. For single server or test environments, the recommendation is to not include (**<N>**) this option.*

NOTE: The Federated Sign-In component requires the use of a properly trusted (not self-signed) SSL certificate which is used to communicate over a secure HTTPS connection. This ensures that both the client browsers and server side components trust the certificate. If you do not want to deploy and configure a trusted certificate, then do not include this component during installation.

System Administrator

Enter the required parameters to create your default System Administrator login to XTAM. The account specified here may be used as the first System Administrator, so be sure to choose a memorable login (default login is "xtamadmin") with a strong password (maximum of 30 characters). Both the user login and password will be displayed later when they can be saved to a file for safe keeping. Press the **<Enter>** key after each field to continue.

```
Create system administrator by specifying login, first name, last name and password

Please enter the Administrator Login [admin]: pamadmin
Please enter the Administrator First Name [System]: System
Please enter the Administrator Last Name [Administrator]: Administrator
Please Enter Password:
Please Repeat Password:
```

Figure 5: Create XTAM System Admin Account

SSO Connect

To define a managed path to be used with federated sign in, select (**<Y>**) the SSO option and then enter that valid path in the **Managed Path** field. If XTAM is to be used with an SSL certificate, then this option should be enabled and the managed path needs to be defined with a secure path (for example, https://host.example.com). Press the **<Enter>** key to continue.

```
Do you want to access this server using SSO Service (Y/N) [N]: Y
Please Enter Managed Path []: https://host.example.com
```

Figure 6: Enable and Define Federation Connection (optional)

External Database

If the Internal Database option was excluded (**<N>**) earlier, then you will now need to define your connection to your external database. Choose your database type by entering the number to the left of its name and then press **<Enter>**. You will then be required to enter the database host, connection and

a user and password to establish a successful connection. If further assistance is required, please contact your database administrator.

NOTE: The installation process does **not** create its own database or tablespace but rather makes use of an existing one. With that in mind, please ensure one with the name "PamDB" already exists as this will be used by the application.

Example strings are listed below.

- Remote Embedded Database [1]
  - Example connection string: db-host or db-host:port
- Microsoft SQL Server [2]
  - Example connection string: db-host or db-host:port
    - A database with the name "PamDB" must already exist and will be used for the application. Ensure the supplied account is the "owner" of this database.
- Oracle [3]
  - Example service: db-host/db-service
  - Example instance: db-host:port:SID
    - Grant *(at a minimum)* "CONNECT, RESOURCE, UNLIMITED TABLESPACE" to the supplied user account.
- MySQL [4]
  - Example connection string: db-host or db-host:port
    - A schema with the name "pamdb" must already exist and will be used for the application. Ensure the supplied account has ALL schema privileges assigned.
- PostgreSQL [5]
  - Example connection string: db-host or db-host:port
    - A database with the name "PamDB" must already exist and will be used for the application. Ensure the supplied account is the "owner" of this database or has been provided with "ALL" privileges to it (CTc).

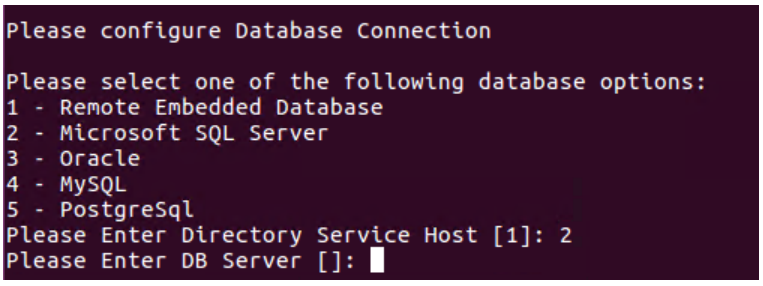

Figure 7: Connect to an External Database (optional)

Active Directory Integration

Optionally, you may choose to integrate XTAM with your existing Active Directory or LDAP server. Enter your **LDAP Server** FQDN, your Active Directory or LDAP **User** (user@domain.com or domain\user), its

Password, Repeat the Password and then the **<Enter>** key. If the connection is successful, this user may become a System Administrator in XTAM and you may continue. If you cannot or do not want to integrate with Active Directory or LDAP, simply enter **<N>** at the prompt and **<Enter>** to continue with the setup.

```
Do you want to configure access to Microsoft Active Directory or LDAP (Y/N) [N]: Y
Please enter LDAP Server []: ad.example.com
Please enter User []: user@domain.com
Please enter a Password:
Please repeat Password:
Connecting to AD... Ok
Successfully configured connection to your Microsoft Active Directory or LDAP Server: ad.example.com
```

Figure 8: Active Directory or LDAP Server Integration

Installation Complete

When the installation is complete and all services are started, the following summary will appear. The summary will display the services, accounts and passwords that were created during installation. It is **extremely** important that the example information highlighted in the yellow box below be saved to a file and kept in a safe location. The Master Password displayed will be required in a "break glass" or database transfer scenario and no one will be able to identify nor update this password if it is ever lost.

```
Generating Session Manager certificate... Ok
Archive:  /home/xtuser/Xton/certbundle.zip
  inflating: session.crt
  inflating: session.key
Creating environment file
Import session manager certificate from ADS... Ok
Successfully imported session manager certificate from ADS
Xton Access Manager installation had been successfully completed.
Below is the information about the system to remember.  It is important to save this information to a file and store it
 in a safe location.

System Admin:  pamadmin/Mq7bl6
Master Password:  Ok: uiCvb6UBAQGa83AYvPHtEBc2YAyMkCau
DB Password:  Ok: 0L4yEBTDpIr3Y3
Directory Admin Password:  Ok: SU8Qwtpn4qDpKl
Copy certificate bundle file /home/xtuser/Xton/certbundle.zip to the Session Manager components.
xtuser@demo-server-xtlin02:~/Xton$
```

Figure 9: Summary Screen with Passwords (save this information to a file for safe keeping)

If you do not see these passwords or receive any errors in this Summary screen the installation was not successful. Complete the installation and then uninstall to try again. Do not initialize Xton Access Manager without a successful deployment and a safe and secure copy of the logins and passwords shown in the example Summary screen.

Xton Access Manager is now installed and ready for initialization. You can now exit the installation session and login to XTAM at http://localhost:8080/xtam.

NOTE: It is extremely important that all the passwords displayed in this section are saved to a file and this file is stored in a safe location. These passwords cannot be retrieved by Xton Technologies or anyone else once the installation is complete.

Logging into Xton Access Manager

Open your web browser and navigate to the login screen of XTAM or double click the shortcut on your desktop.

- Non-secured login: http://localhost:8080/xtam
- Secured login: https://localhost:6443/xtam
    - (Click here to understand your browser certificate warning)

At the login prompt, you can sign in with one of the following system administrator logins:

- The System Administrator account that was created during the installation process.
- The Active Directory or LDAP account that was (optionally) used to establish integration during the installation process.

Enter the System Admin user and password and click the Login button. Upon successful login, you will be directed to the initialization page of XTAM. The account used as the first login will become a System Administrator.

Browser SSL Certificate

A default installation of XTAM comes with a pre-created XTAM Self-signed SSL certificate to encrypt traffic. Because this SSL certificate is self-signed and therefore not trusted by your browser or certificate authority, a security warning will appear when the login page opens.

It is safe to accept the security warning for this self-signed certificate only; however, you may consider these options:

1. You may use the non-secured login at this location: http://localhost:8080/xtam to avoid the browser warning and continue using the software without encrypting your traffic.
2. You may accept the warning, install the certificate and use it as supplied. Although it is self-signed, it will still encrypt the traffic.
3. You may substitute our non-trusted, self-signed certificate with your own trusted, signed certificate by following the procedure described in this FAQ article.

While our self-signed SSL certificate is acceptable for trial or PoC deployments, they should not be used for any production deployments. We **strongly** recommend the use of a well-known trusted SSL certificate or one generated by your own Certificate Authority.

Initialize

The first login (and only the first) after a new installation will require a system initialization. When logged in for the first time, click the Initialize button to begin this process. During this time, the system will create all its needed configuration in the database and services. Depending on the complexity of your configuration, this process may take anywhere from a few seconds to 1-2 minutes to finish.

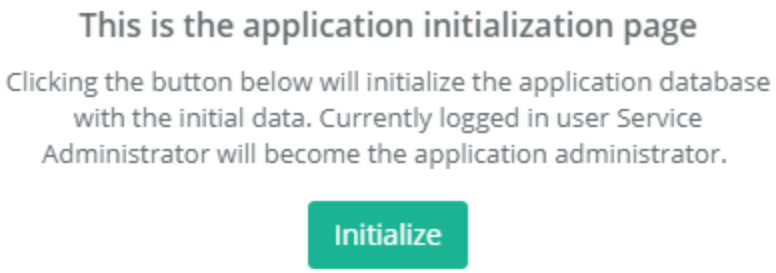

Figure 10: XTAM "first-time" Initialization

When the initialization is complete, the system will redirect you to the landing page. You should see a few menu headings on the left side including Records, Administration and Management indicating that the process is complete.

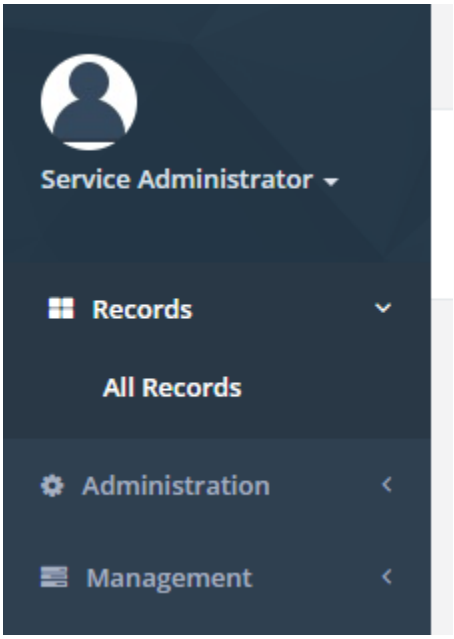

Figure 11: Initialization Complete

License Registration

If you have a license key, then you should activate it now. Navigate to Administration > Settings > Registration. On the registration screen, copy and paste your key into the "Activation Code" field and then click **Automatic Registration**. When the license is retrieved successfully (status should display "License is Valid"), click the **Save License** button to finalize. The software is now activated and ready for use.

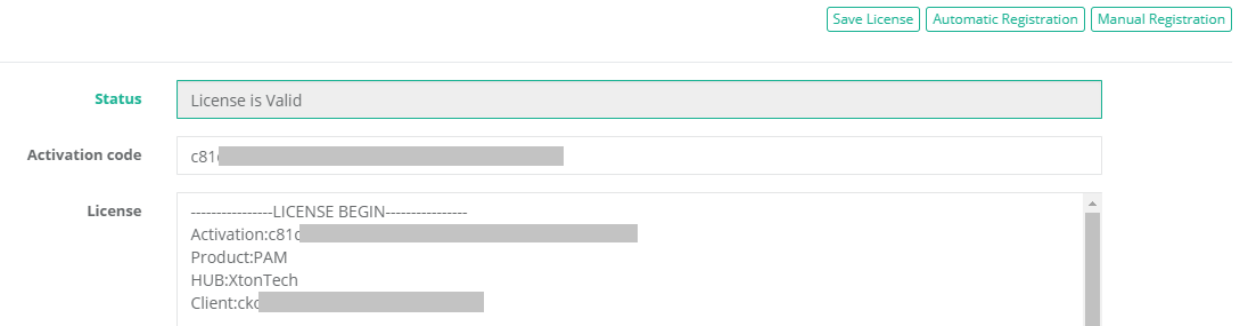

Figure 12: License Activation

Manual Registration

If the computer is not connected to the internet or cannot establish a connection to the license server for registration, then the following procedure will register the software manually.

1. Click the Manual Registration button. A new browser window will appear.
2. Copy or transfer this URL to a computer with an internet connection and load the page.
3. Select the copy the license information between and including the LICENSE BEGIN header and LICENSE END footer.
4. Save this information to a file or paste it directly into the "License" field in XTAM.
5. Click the Save License button.
6. The license status will read "License is Valid" and the software is now registered.

Uninstalling Xton Access Manager

You can uninstall XTAM by simply running the uninstall shell script located in its installation directory.

Uninstaller

First, logout and close any open Sessions in XTAM as well as any open sessions in your Web Browser. Execute the uninstall script and follow the prompts. When the script completes, the software and its services will be removed from your computer.

NOTE: The uninstall script is ./uninstall.sh and should be executed from the <XTAM_HOME> directory.

If you deployed additional services to other servers, then you will need to run the uninstall script on each of these computers to remove the components.

Database Cleanup

If you have configured XTAM with the use of an external database, then you will need to manually remove these database objects. Please contact your database administrator for assistance.

Appendix

Remote Session Manager Configuration

When installing the Session Manager component on a remote Unix or Linux computer(s), then the following steps should be taken.

1. Ensure that XTAM is Installed and configured on your master computer.
2. Run the install script on the remote computer where Session Manager is to be deployed.
3. Read and accept the License Agreement by pressing **<ENTER>** to display the agreement, **<Q>** when finished and finally **<Y>** to accept it and continue.
4. Enter **<N>** to exclude each component except for the "Session Manager component" which you will include **<Y>**.

```
Include the Internal Database component (Y/N) [Y]: N
Include the Directory Service component (Y/N) [Y]: N
Include the Application GUI component (Y/N) [Y]: N
Include the Job Engine component (Y/N) [Y]: N
Include the Session Manager component (Y/N) [Y]: Y
Include the Federated Sign-In component (Y/N) [N]: N
Downloading components...
```

Figure 13: Select the Session Manager component

5. Next, enter the location of the certificate bundle that was deployed to your master computer where XTAM was installed earlier and press **<ENTER>** to continue.

```
Configuring components...
Provide certificate bundle location: /home/xtuser/Xton/certbundle.zip
```

Figure 14: Enter the Certificate Bundle file location

   a. The certificate bundle is in the root XTAM installation directory on your master computer. The default file location is /certbundle.zip
   b. You may select the zip file from this default location (if possible), copy it to a shared network location or simply copy the zip file to this remote computer and select it locally.

NOTE: This step is optional, so if you wish to <u>not</u> supply the certificate you may simply click Next to continue. By skipping this option, you are acknowledging that the communication between XTAM on the master computer and this remote Session Manager computer will not be secured. Because of this, it is recommended that you supply the certificate when prompted and do not skip this step.

6. The Session Manager service will now startup on this computer and the installation script will finalize the operation.

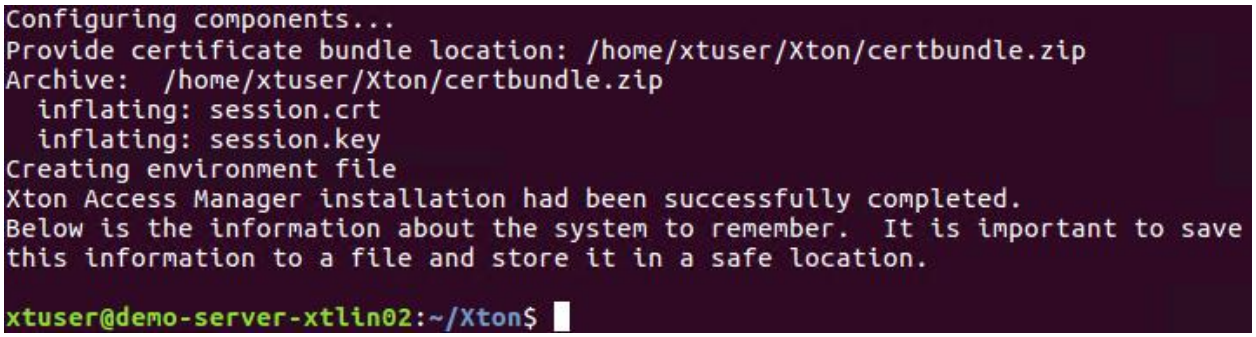

Figure 15: Session Manager Component Deployed

Web Server

If you are configuring XTAM using a trusted SSL certificate or exposing it to external traffic, then a web server will need to be deployed and configured. The XTAM installation process does not include web server deployment and configuration and therefore should be performed by a knowledgeable Unix administration. Popular web servers include Apache HTTP or NGINX.

The purpose of the web server is to act as a reverse proxy. Its forwarding rules should process the certificate secured HTTPS 443 inbound port and route it to the XTAM port (default 8080) inside the server.

Since the trusted SSL certificate is applied to a specific domain (i.e. https://host.example.com) this URL becomes the managed path for XTAM's Federated Sign-In server.