Akkadian Provisioning Manager Administration Guide

4.14 — Last update: 2019/07/29

Table of Contents

Introduction

Akkadian Provisioning Manager™ brings the "unified" to provisioning in Cisco Unified Communications. No other solution makes it easier or faster to provision across multiple applications, all from a single, secure web interface. This manual will guide you through the process of deploying and configuring Akkadian Provisioning Manager.

1. Requirements and Limitations

The following sections provide information about the requirements that your system must meet, and limitations that apply when you install or upgrade Akkadian Provisioning Manager.

1.1. Virtual Machine Requirements

Akkadian Provisioning Manager 4.14 is a Linux based Virtual Appliance supported on VMware ESXi.

Supported Versions of VMware vSphere ESXi = 5.0 U1, 5.1, 5.5, 6.0, and 6.5

The recommended server requirements for Akkadian Provisioning Manager depend on several variables.

- **Applications Severs** – number of integrated UC Servers
- **Devices** – number of devices supported by Cisco Unified Communications Manager
- **Users** – number of concurrent users provisioning via Provisioning Manager

To assist with allocating the proper resources for Provisioning Manager 4.14, use the Table below to determine the appropriate system resources.

Size	Application Servers	Devices	Users	vCPU	vRAM	vDISK	vNIC
Small	10	15000	10	2	8	1 × 110 GB	1
Medium	11+	30,000+	30+	2	12	1 × 110 GB	1
Large	20+	60,000+	60+	4	16	1 × 110 GB	1

- Applications servers are defined as configured applications servers in Provisioning Manager and are not related to the number of servers with a cluster.
- Minimum of 2000 MHz reserved

1.2. Application Support

Provisioning Manager provides support for the following applications:

Application	Versions
Cisco Unified Communications Manager	10.x – 12.x
Cisco Unity Connection	10.x – 12.x
Cisco Unified Contact Center Express	10.x – 11.x
Cisco Packaged Contact Center Enterprise	10.5 – 11.x
Cisco WebEx Meetings	WBS31+
Cisco Meeting Server	2.2.3+

1.3. Browser Support

Provisioning Manager supported browsers:

- Microsoft Internet Explorer 11+
- Microsoft Edge 39+
- Mozilla Firefox 53+
- Chrome 50+

1.4. Network Requirements

Akkadian Provisioning Manager communicates on the following ports:

| Traffic	Port	Direction
Application Web Access	HTTPS:443	Inbound —> Provisioning Manager
Communication to Cisco Communications Manager	HTTPS:8443	Outbound Provisioning Manager —> CUCM
Communication to Cisco Unity	HTTPS:8443	Outbound Provisioning Manager —> CUC
Communication to WebEx	HTTPS:443	Outbound Provisioning Manager —> WebEx
Communication to Cisco Spark	HTTPS:443	Outbound Provisioning Manager —> Cisco Spark
Communication to UCCE	HTTPS:443 / TCP 1443	Outbound Provisioning Manager —> UCCE
Communication to Cisco Meeting Server	HTTPS:443 by default	Outbound Provisioning Manager —> CMS
FTP between application and backup server	TCP Port 21	Outbound Provisioning Manager —> SFTP Server
Secure FTP between application and backup server	TCP Port 22	Outbound Provisioning Manager —> SFTP Server
SMTP to mail server	TCP Port 25	Outbound Provisioning Manager —> SMTP Server
LDAP	TCP/UDP Ports 389/ 3268	Outbound Provisioning Manager —> LDAP Server
SSO (SAML)	TCP Port 443	Outbound Provisioning Manager —> SSO Server
Network Time Protocol (NTP)	UDP Port 123	Outbound Provisioning Manager —> NTP Server

2. Virtual Appliance Deployment

Akkadian Provisioning Manager is deployed as a virtual appliance on VMware ESXi versions 5.x and above. The steps below will help guide you through the process of deploying the virtual appliance; however, you should understand VMware or contact your VMware administrator for assistance.

1. Download the latest akkadian Provisioning Manage Express OVA to a location accessible by the vSphere client.
2. From the vSphere client select **Deploy OVF Template** from the **File** menu.
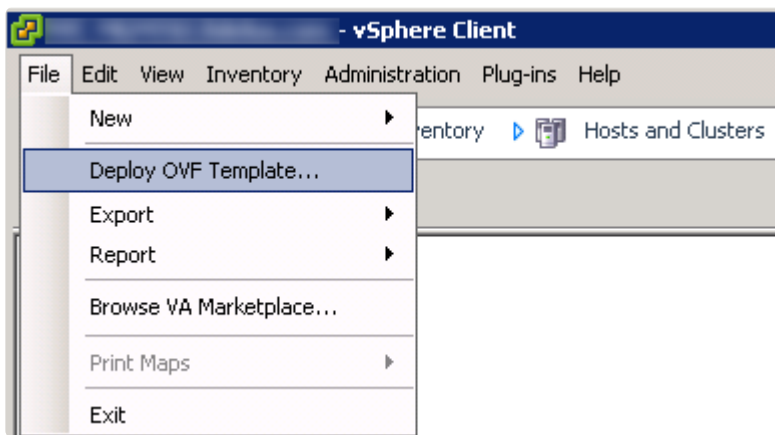
3. Select the OVA from computer or network location and click Next to continue.
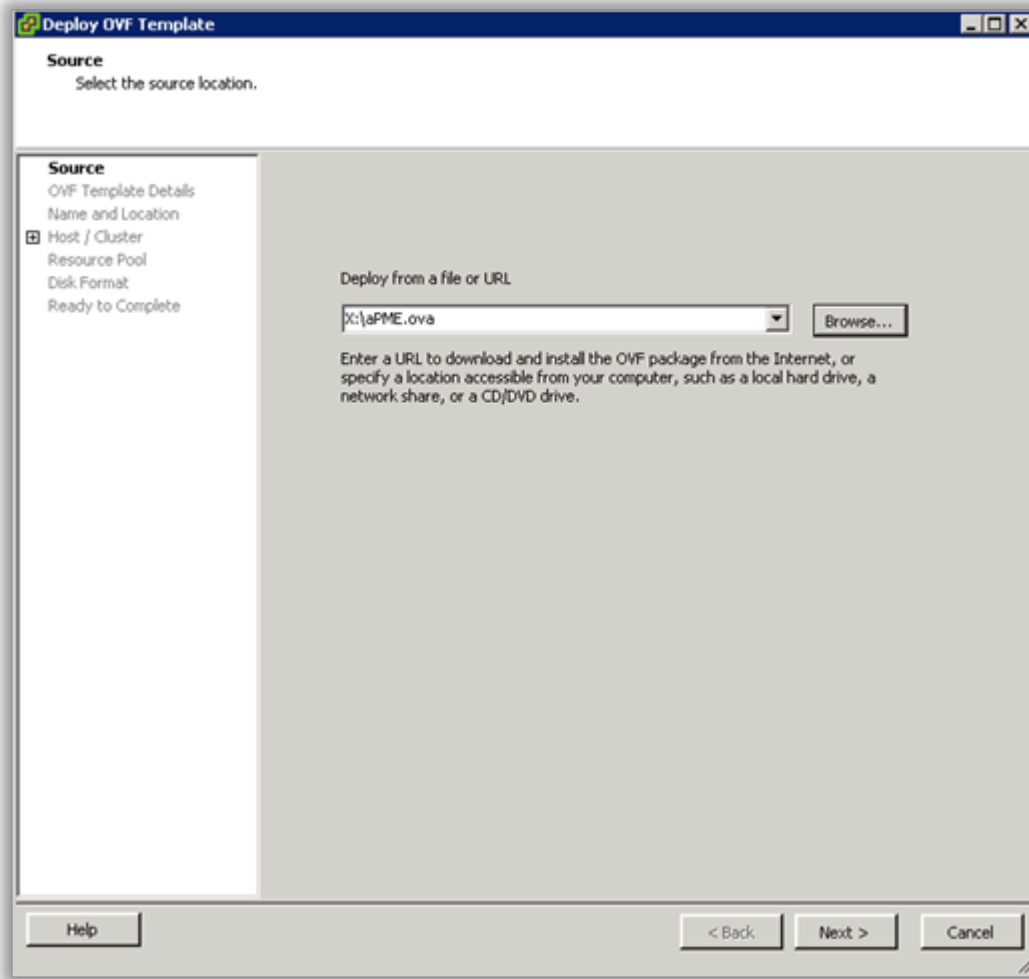
4. Review the License Agreement and click **Next** to continue.
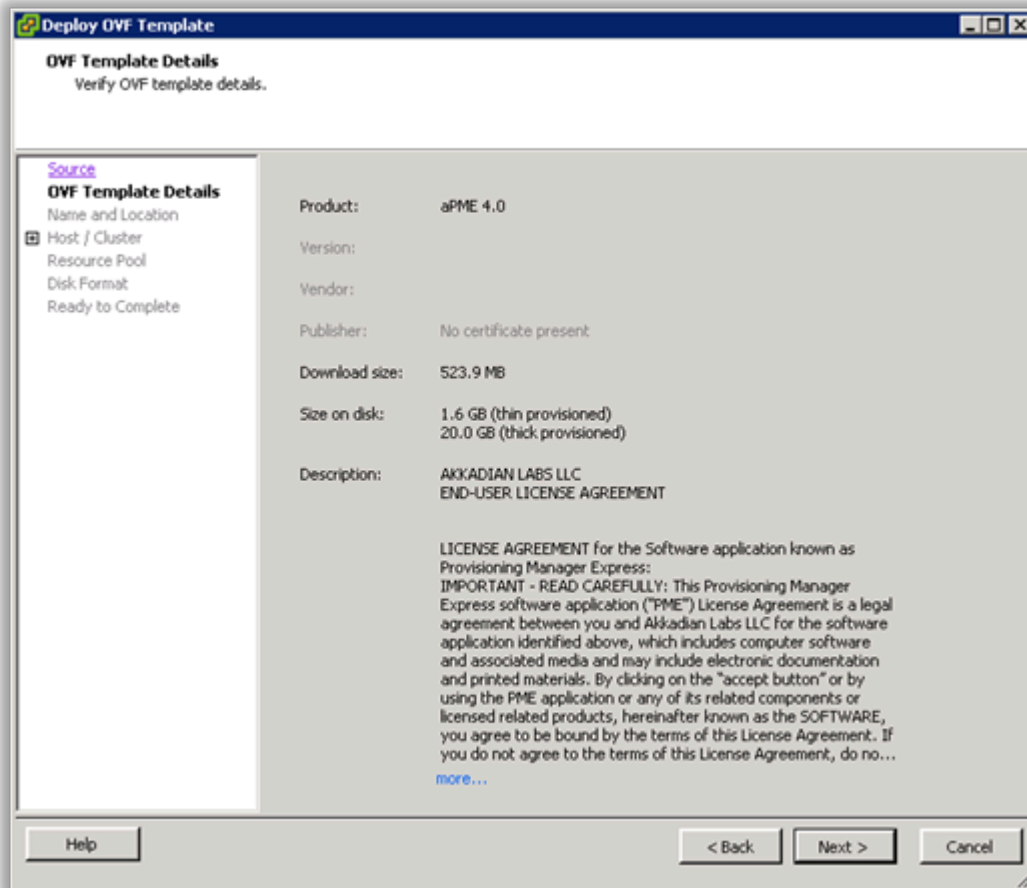
5. Specify the name and location for the VMware machine and click Next to continue.

6. Specify the VMware Host / Cluster and click **Next** to continue.
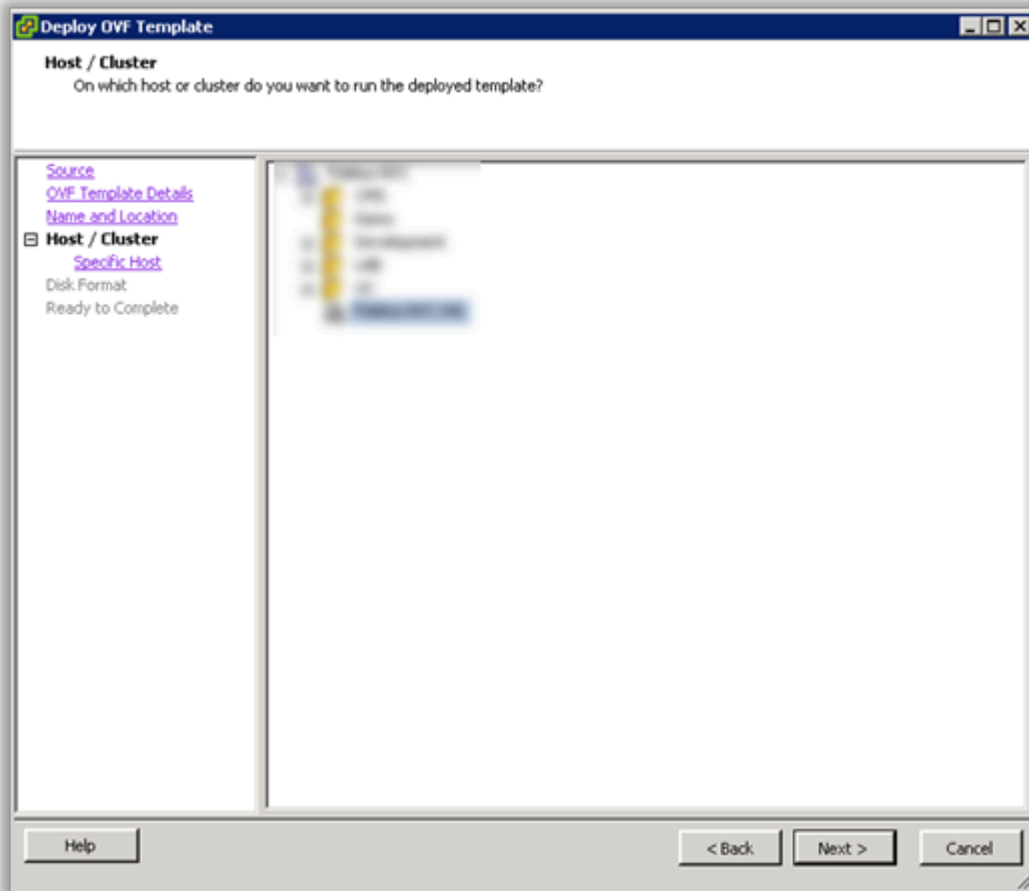
7. Specify a host within the cluster and click Next to continue.
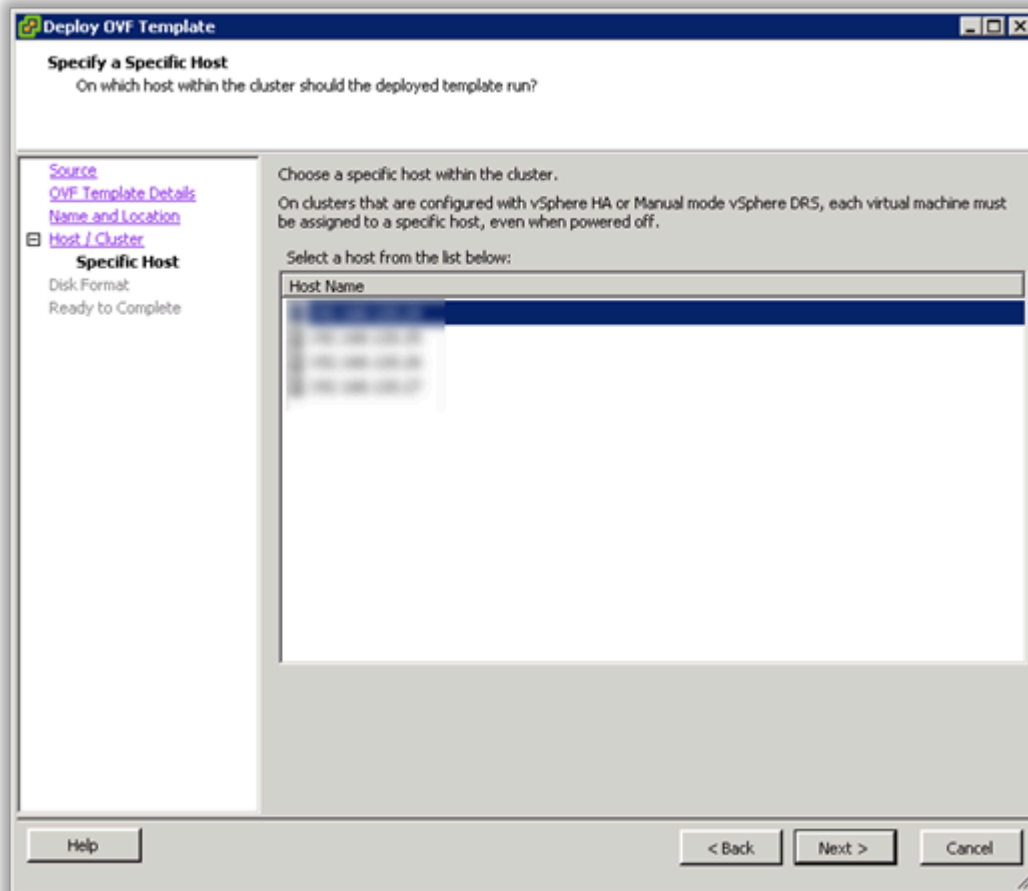
8. Specify the storage location for the virtual machine and click Next to continue.
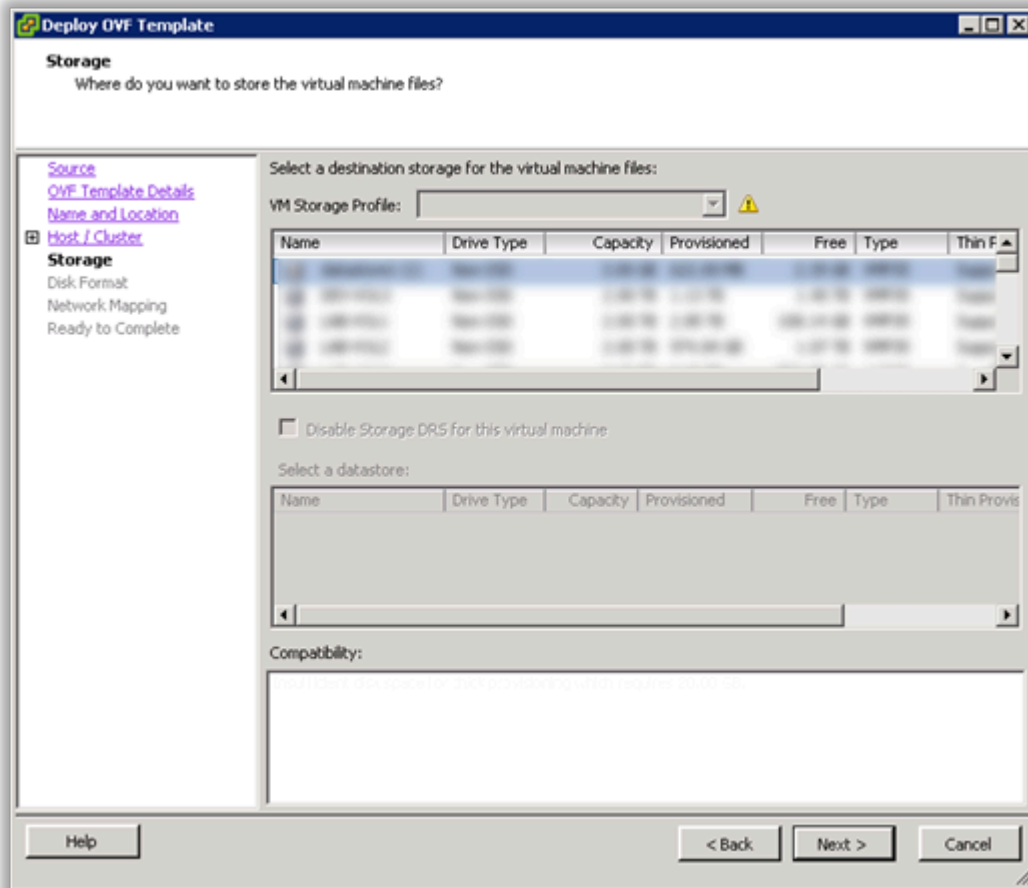
9. Select Thick Provision Lazy Zeroed and click Next to continue.
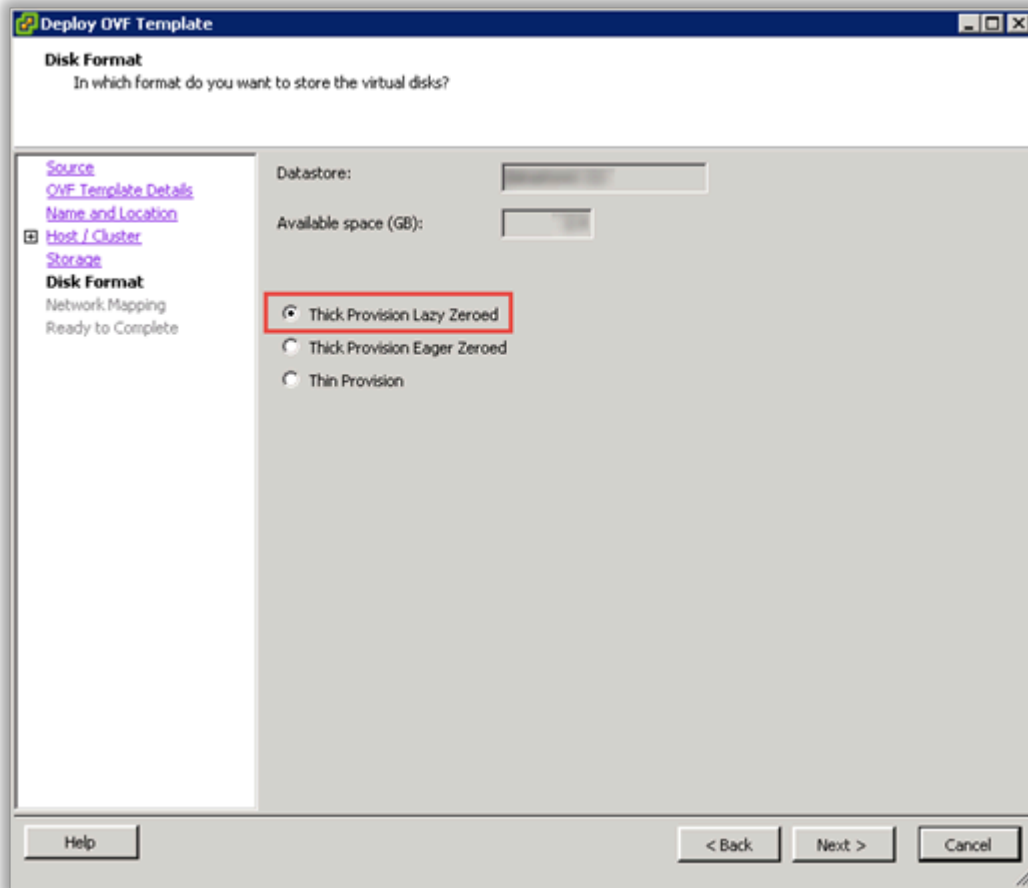
10. Select the Destination Network for the virtual machine and click Next to continue.
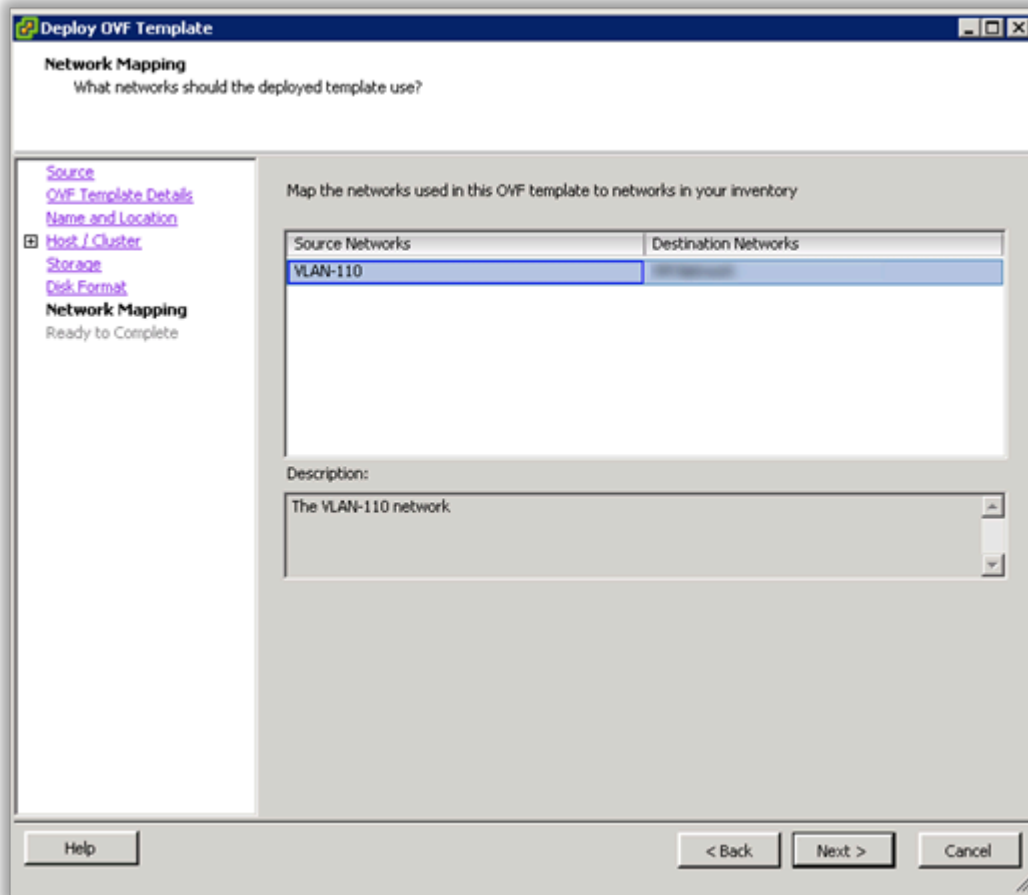
11. Verify the virtual machine settings. The initial OVA deploys with 2 vCPU and 8GB Memory. Depending on your system requirements, you may need to adjust the virtual CPU and Memory settings. Please refer to the virtual machine requirements to determine the appropriate settings for your environment.
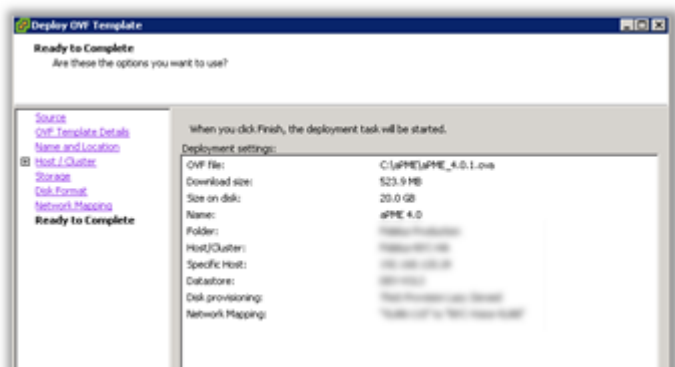
12. Click OK to complete the deployment.

Deployment Completed Successfully

Deploying aPME 4.0

Completed Successfully

Close
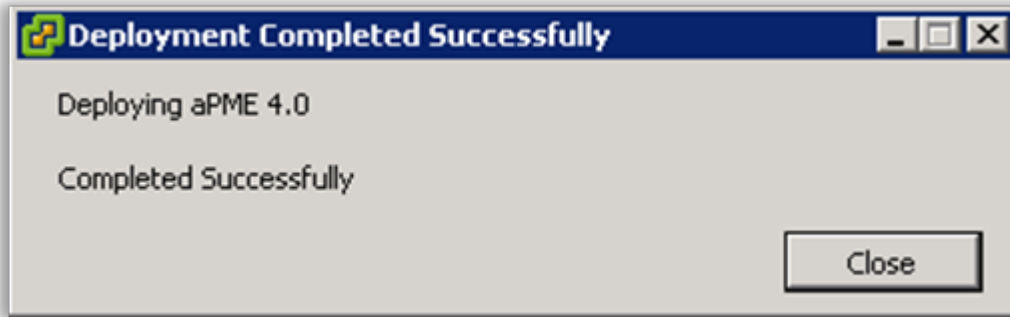
13. To adjust the virtual machine CPU and Memory, locate the newly deployed virtual machine in vCenter, right click on the virtual machine and select Edit Settings.

Power ▸
Guest ▸
Snapshot ▸
Open Console
Edit Settings...
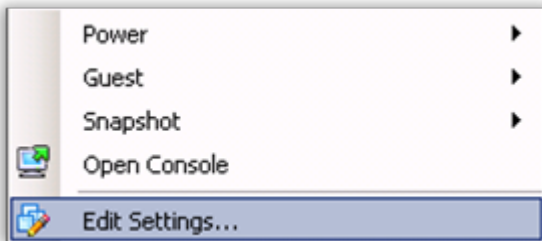
14. On the Hardware tab, select CPU and adjust the setting to provide the required number of cores for your environment.

Hardware	Options	Resources	Profiles	vServices		Virtual Machine Version: 4

☐ Show All Devices   Add...   Remove   Number of virtual sockets: 1 ▾

Hardware	Summary
Memory	4096 MB
CPUs	1

Number of cores per socket: 1 ▾

Total number of cores: 1
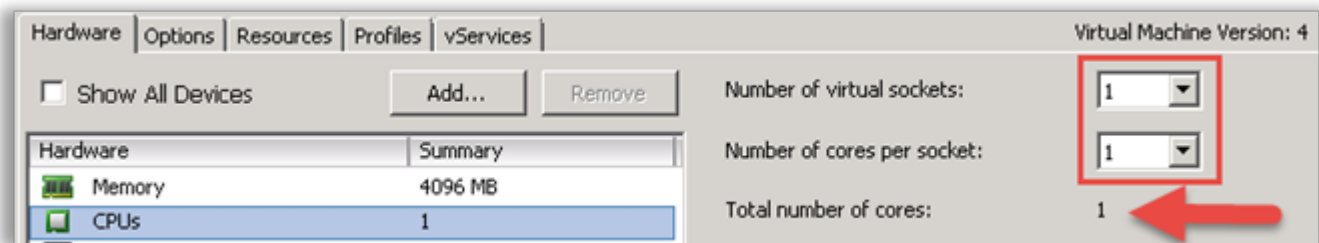
15. After adjusting the CPU, click on Memory and adjust the settings to provide the required resources for your environment. When completed, click OK to commit the changes.

16. Power on the virtual machine and proceed.

17. Locate the virtual machine in vSphere and open a console.

18. When the server boot process is complete, the system will arrive at a login prompt. Login using:

Username – **akkadianuser**
Password – **akkadianpassword**
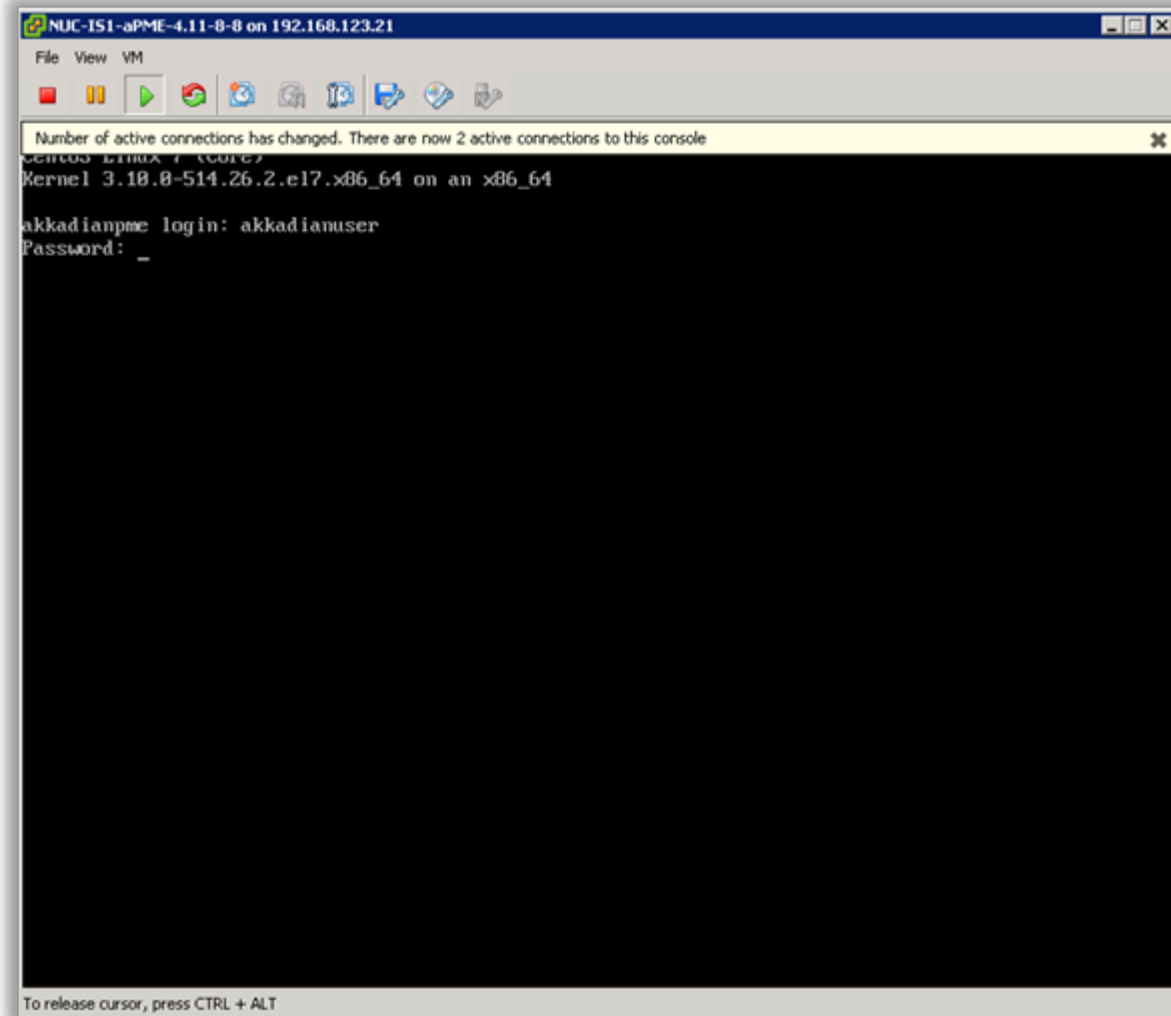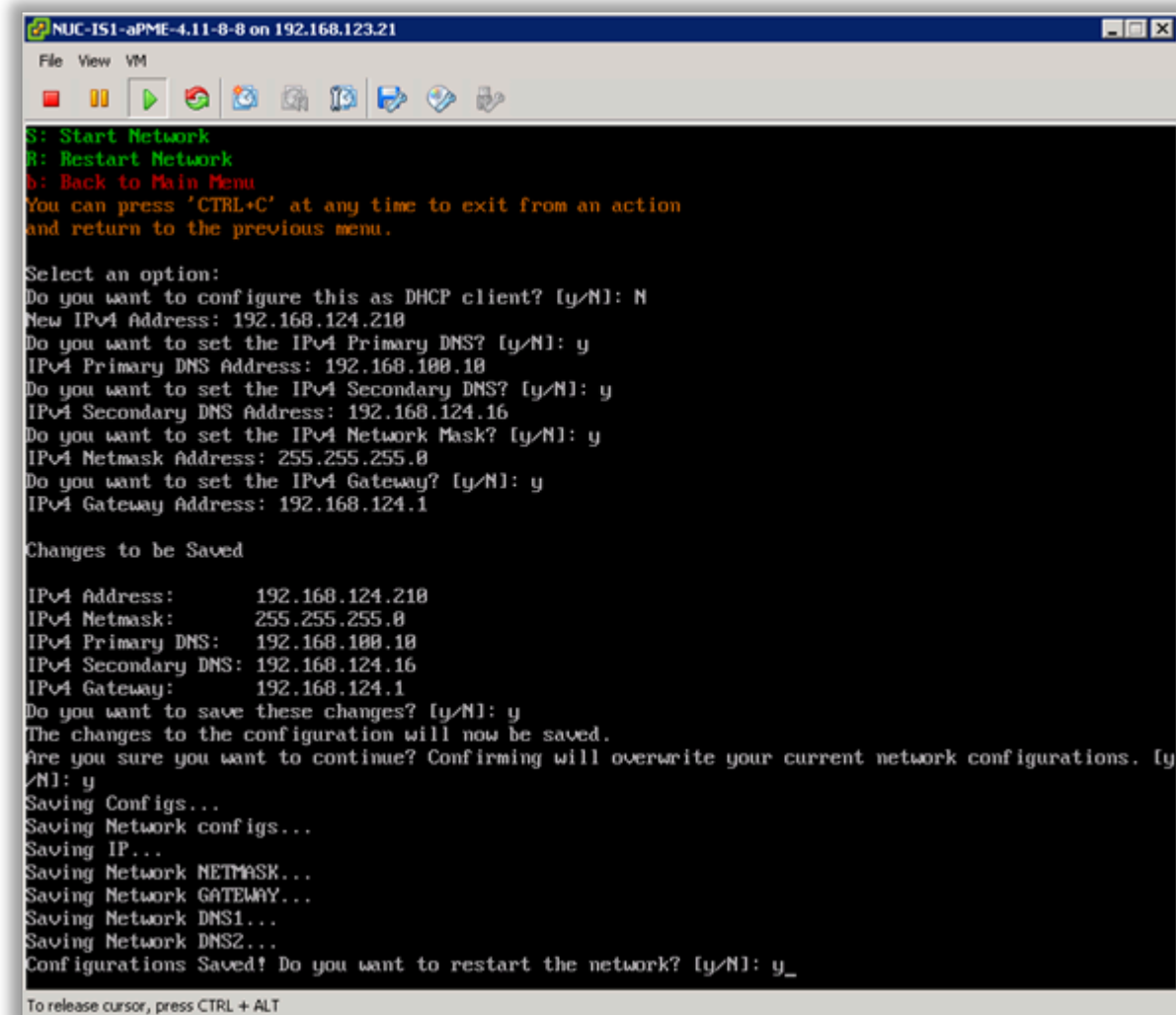
19. From the Akkadian Appliance Manager main menu, select option 1 to Configure Network.
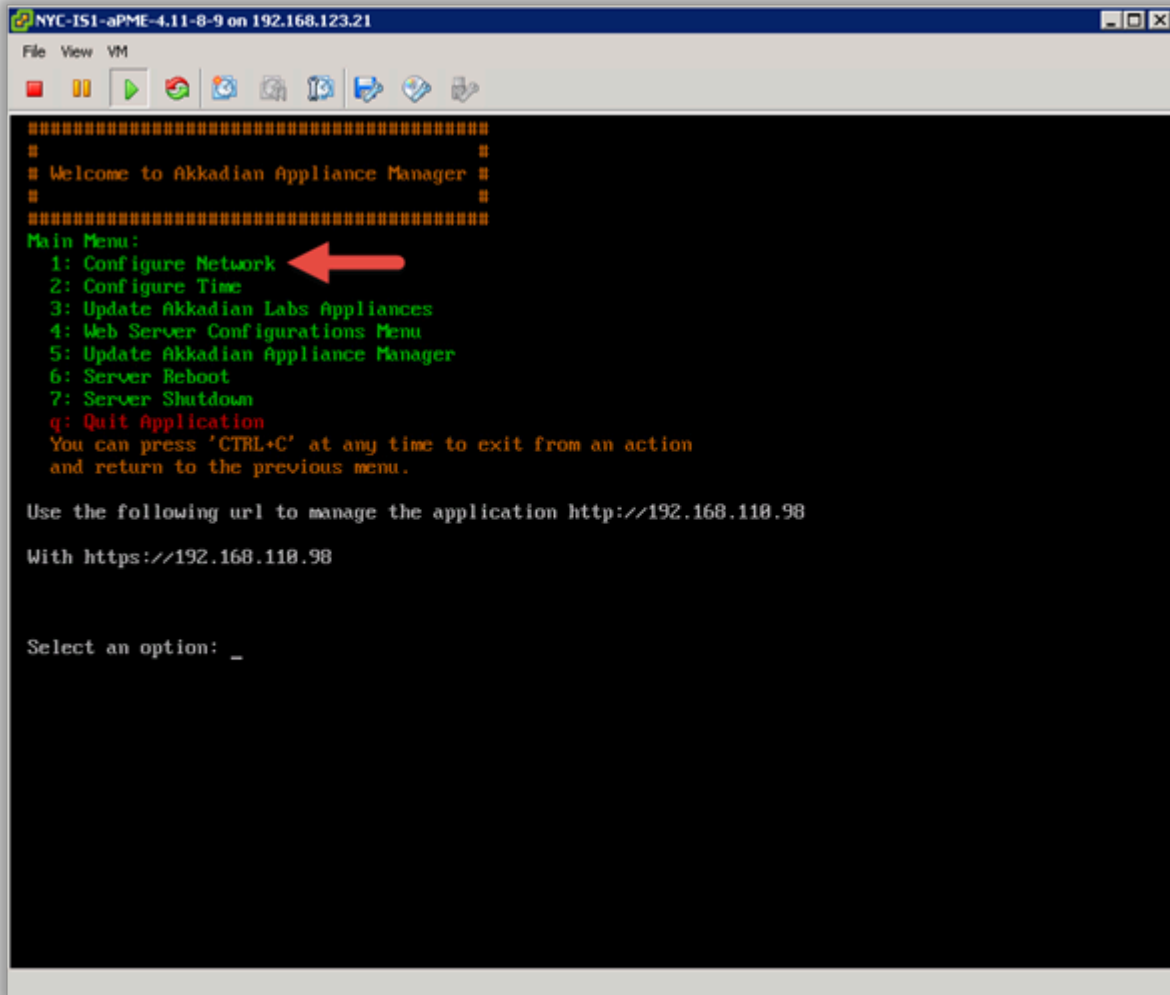
20. Select option 1 to configure the network setting.
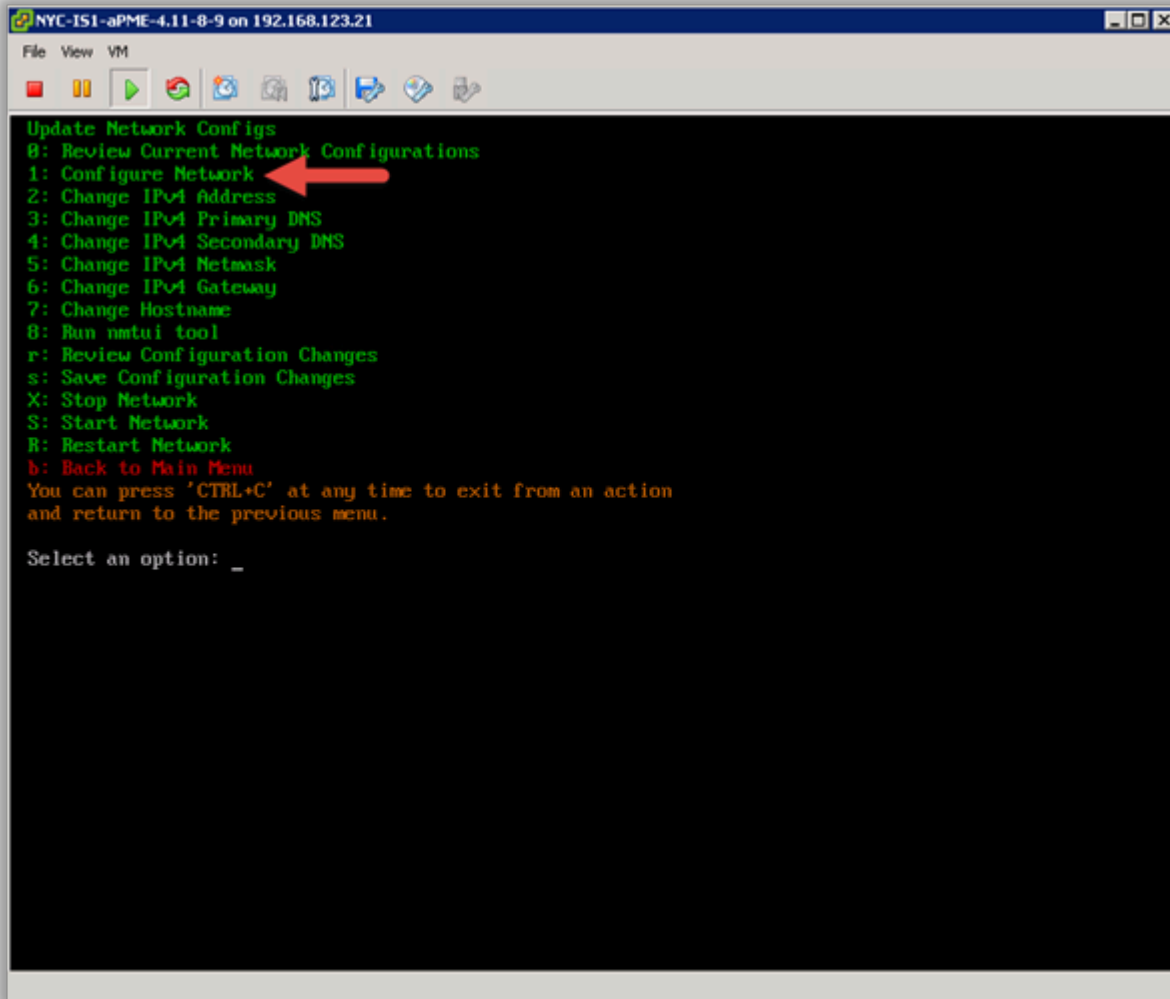
21. Follow the prompt to configure the network settings for your environment.

```
NUC-IS1-aPME-4.11-8-8 on 192.168.123.21                              _ □ ✕
File  View  VM

■  ‖  ▶  ⟳  ▣  ▣  ▣  ➡  ◈  ➡

S: Start Network
R: Restart Network
b: Back to Main Menu
You can press 'CTRL+C' at any time to exit from an action
and return to the previous menu.

Select an option:
Do you want to configure this as DHCP client? [y/N]: N
New IPv4 Address: 192.168.124.210
Do you want to set the IPv4 Primary DNS? [y/N]: y
IPv4 Primary DNS Address: 192.168.100.10
Do you want to set the IPv4 Secondary DNS? [y/N]: y
IPv4 Secondary DNS Address: 192.168.124.16
Do you want to set the IPv4 Network Mask? [y/N]: y
IPv4 Netmask Address: 255.255.255.0
Do you want to set the IPv4 Gateway? [y/N]: y
IPv4 Gateway Address: 192.168.124.1

Changes to be Saved

IPv4 Address:       192.168.124.210
IPv4 Netmask:       255.255.255.0
IPv4 Primary DNS:   192.168.100.10
IPv4 Secondary DNS: 192.168.124.16
IPv4 Gateway:       192.168.124.1
Do you want to save these changes? [y/N]: y
The changes to the configuration will now be saved.
Are you sure you want to continue? Confirming will overwrite your current network configurations. [y
/N]: y
Saving Configs...
Saving Network configs...
Saving IP...
Saving Network NETMASK...
Saving Network GATEWAY...
Saving Network DNS1...
Saving Network DNS2...
Configurations Saved! Do you want to restart the network? [y/N]: y_

To release cursor, press CTRL + ALT
```

22. Select option 7 from the network configuration menu to configure the hostname. It is recommended the hostname is entered using the fully qualified domain name.

Example – Provisioning Manager.yourdomain.com
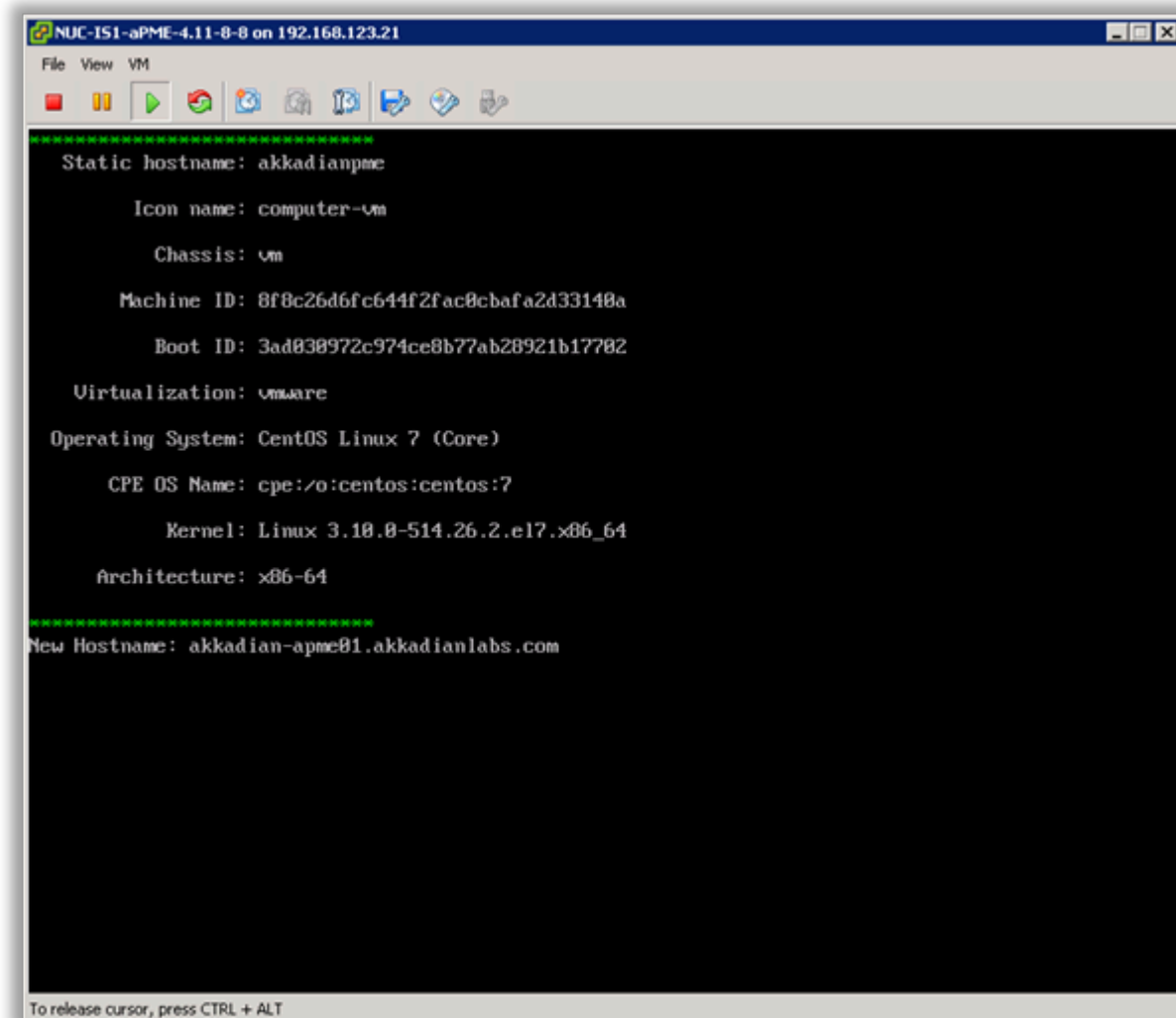
23. Optionally you may configure the server time by selecting option 2 form the configure network menu.

24. It is recommended you change the default Akkadian Appliance Manager password by selecting option 4 (Web Server Configuration Menu) from the main menu and then selecting "p" (Change Current AAM Password").
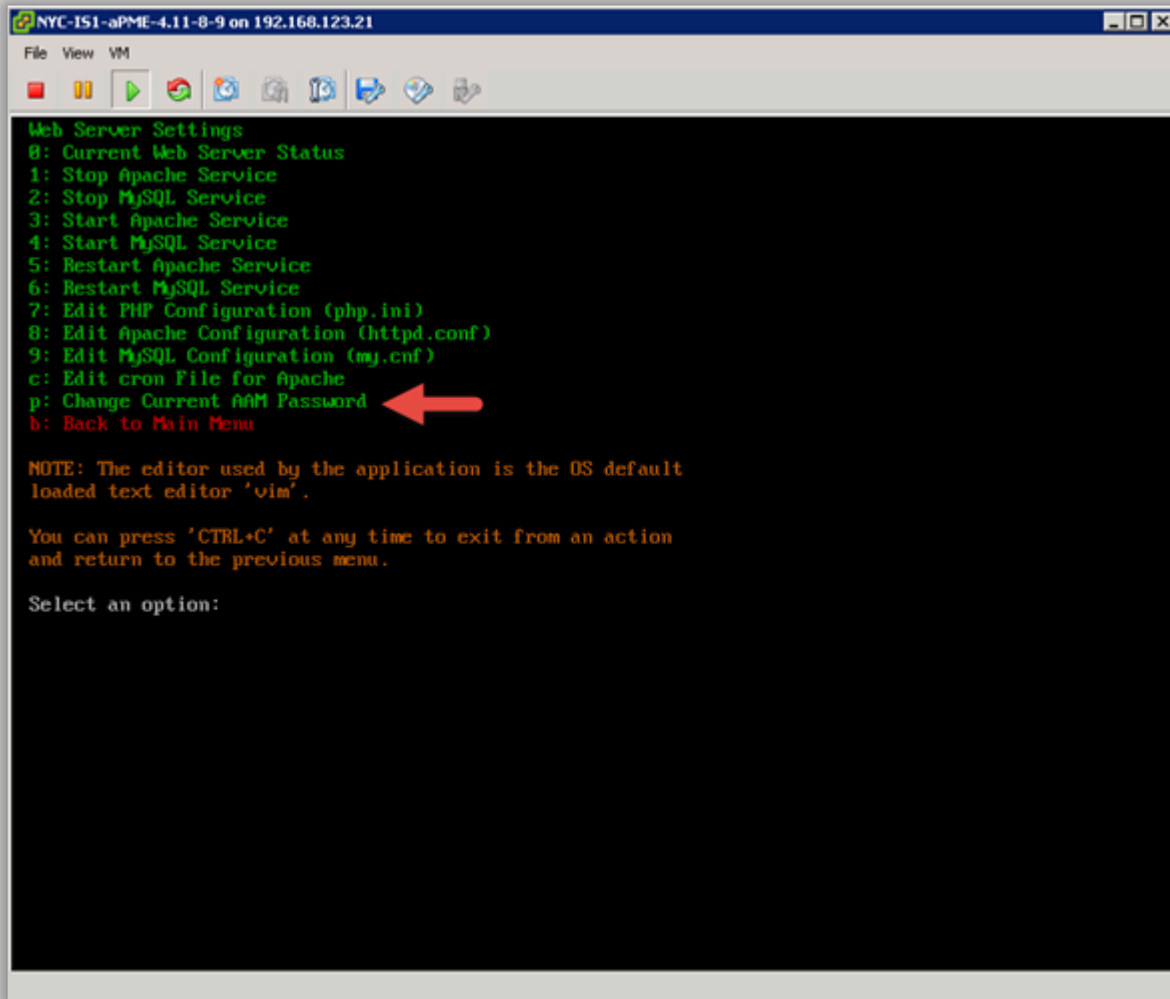
25. When all configurations are complete, select "s" from the network configuration menu to save the configuration and restart the network.

26. From the main menu, select Reboot Server to finalize the configuration.

27. When the system returns to the login prompt, the Akkadian Provisioning Manager virtual appliance deployment is complete and can be accessed by going to https://{Server IP or Name}/pme.

3. Initial Configuration

After completing the installation, Akkadian Provisioning Manager requires some basic configuration before you can begin provisioning. This section will guide you through the configuration process.

3.1 Logging in for the First Time

1. In a browser, navigate to HTTPS://{Server IP or NAME}/pme

> ✳ During the initial login process, Provisioning Manager will attempt to contact the Akkadian Labs licensing server. If Provisioning Manager does not have Internet access, this process may take 15-30 seconds.

2. Before accessing Provisioning Manager, a license must be applied. There are 3 options to license Provisioning Manager:

- **Trial License** – Apply a 30-day trial license
- **Off-line activation** – Upload a license file
- **On-line activation** – Enter a license key for on-line activation

3. Log in using the default credentials:

Username – PMEAdmin

Password – PMEAdmin (Case sensitive)
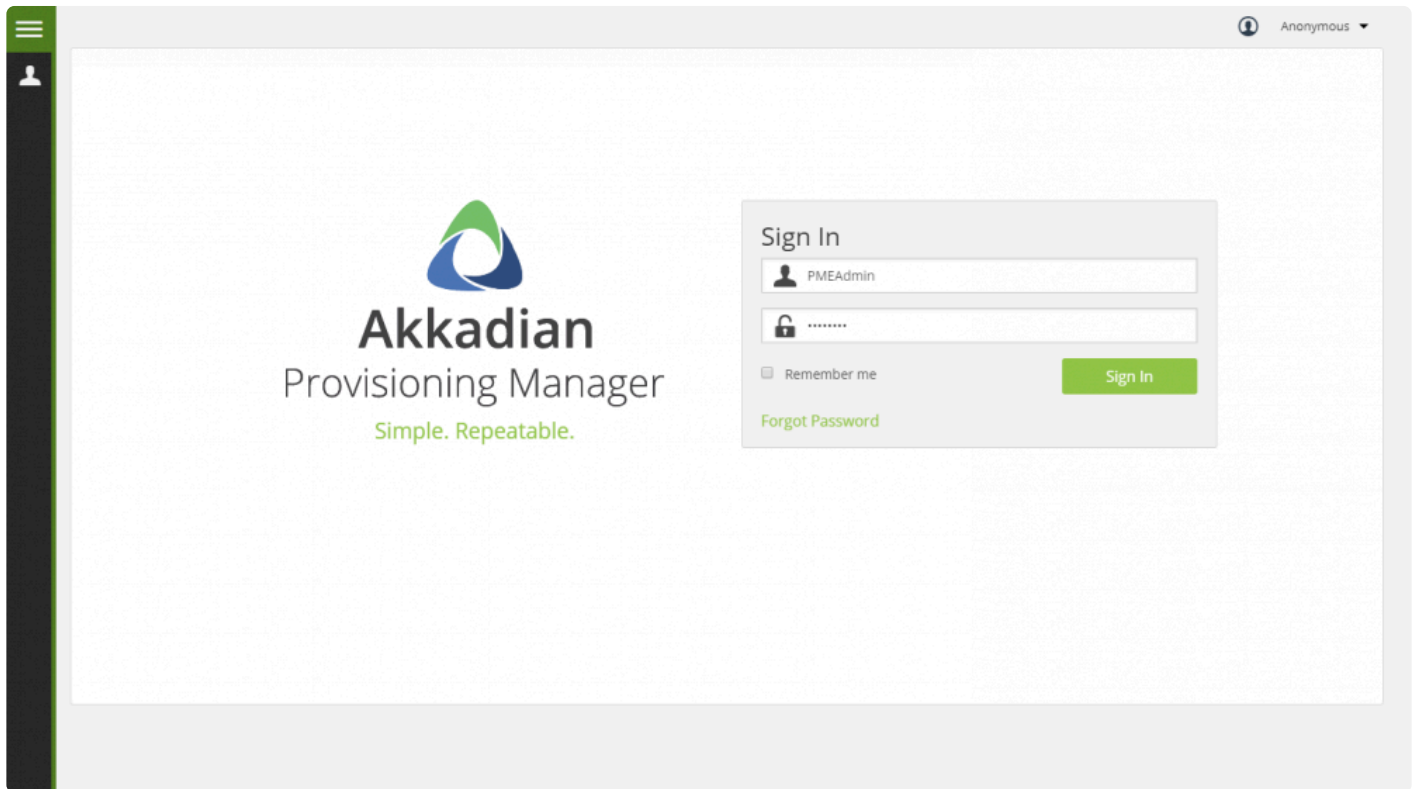
4. By default, the Menu Bar is collapsed. The menu bar may be expanded and locked.
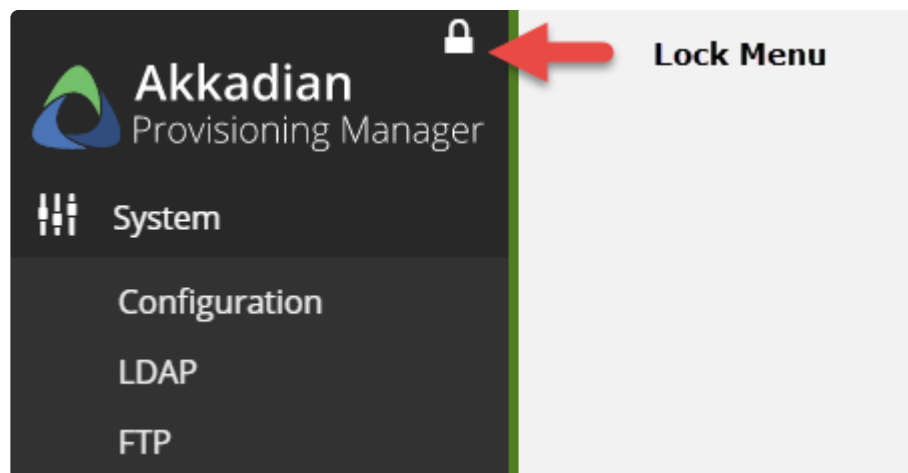
3.1.1 Changing the PMEAdmin Password

It is highly recommended that you change the default PMEAdmin password and set a valid email address for password recovery.

1. Click on "Hi Default" to open the PMEAdmin profile
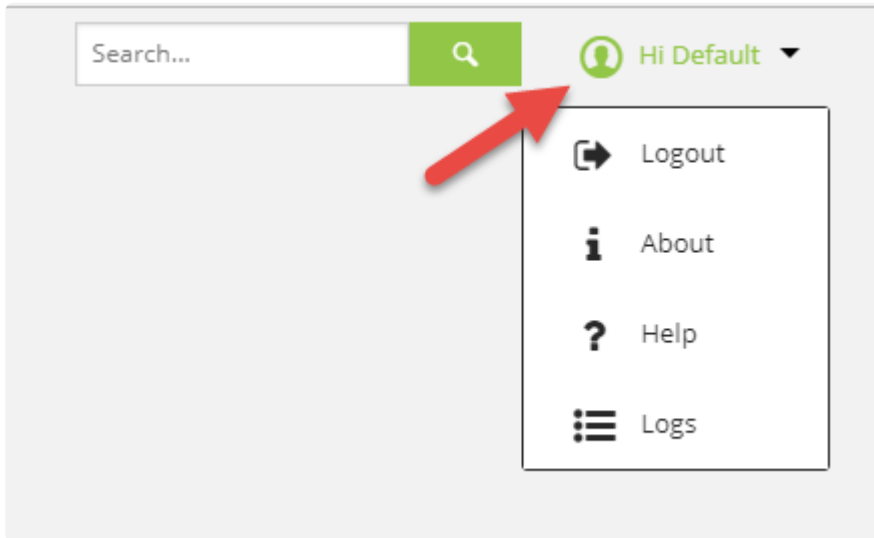
2. Update the PMEAdmin users profile with a valid email address and password. You may also update the first and last name.

! Please ensure the PMEAdmin email address is valid for a successful password recovery!

Search...

Hi Default

Profile

* First Name	Default
* Last Name	Admin
* Email Address	admin@company.com

Password

Current Password	
New Password	
Confirm Password	

⊘ Save

3.2 System Configuration

After licensing Provisioning Manager and successfully logging in, there are few system configuration items which should be completed before setting up provisioning. This System Configuration section will guide you through configuring the necessary items for your environment.

3.2.1 Email Configuration

Email configuration is optional, but is required for several Provisioning Manager features, such as notifications and password recovery.

1. Select **Configuration** from the **System** menu
2. Click the **Email Configuration** Tab
3. Enter the information for your SMTP server
4. When complete, click **Save**

3.2.2 Single Sign-on

Provisioning Manager supports Single Sign-on (SSO) using Security Assertion Markup Language (SAML). The configuration is optional and only one SSO configuration is supported.

1. Select **Configuration** from the **System** menu
2. Click the **Single Sign-on** Tab
3. Enter the information for your SSO provider
4. When complete, click **Save**

Email Configuration	Single Sign-on	Branding	Bulk Provisioning Configuration

Single Sign-on

☑ Activate SSO Service

* IDP Name (Label)

Configure Using   ○ Metadata URL   ○ Metadata file   ◉ Manual Settings

* IDP Entity Id

* Single Sign-on Endpoint (IDP URL)

Single Log-out Endpoint

* X509 Certificate (public key)

SP Entity Id   https://192.168.124.227/pme/index.php/user/metadata

SP Meta-data URL   https://192.168.124.227/pme/index.php/user/metadata

SP Assertion Consumer URL   https://192.168.124.227/pme/index.php/user/login?acs

SP Single Logout URL   https://192.168.124.227/pme/index.php/user/logout?sls

Save

3.2.3 Branding

Optionally, Provisioning Manager can be branded with your organization's name, logo an colors.

1. Select **Configuration** from the **System** menu
2. Click the **Branding** Tab
3. Set desired customer branding attributes
4. Optionally you may specify a custom help URL for the system, which will replace the standard administration guide
5. When complete, click **Apply**

3.2.4 Bulk Provisioning Configuration

The Bulk Provisioning Configuration controls the batch processing size for the bulk provisioning process. The default is 500, which means bulk jobs will be divided into batches of 500 items. This setting should not be updated without guidance from Akkadian Labs technical support.

1. Select **Configuration** from the **System** menu
2. Click the **Bulk Configuration** Tab
3. Enter the Batch Processing Size value
4. When complete, click **Save**

Email Configuration	Single Sign-on	Branding	Bulk Provisioning Configuration

Bulk Provisioning Configuration

* Batch Processing Size   500

Save

3.2.5 LDAP

LDAP configuration is optional, but is required for several Provisioning Manager features including LDAP authentication and Active Directory integration.

Provisioning Manager supports creating multiple LDAP agreements in order to support multiple domains as well as configurations for Active Directory updates.

1. Select **LDAP** from the **System** menu
2. Click on **Default** edit the default LDAP agreement or click **Add** to create a new agreement

> ✳ It is recommended to update the default LDAP configuration for the initial LDAP configuration

3. Enter the information for your LDAP configuration

Field	Description
LDAP Config Name	Enter a name to identify this specific LDAP configuration
Base	Enter the LDAP search base
Server	The LDAP server IP address or DNS name
Port*	Enter the LDAP server port number
Username	Enter the LDAP Username used to authenticate to the LDAP server
Password	Enter the LDAP Password used to authenticate to the LDAP server
Username Bind Attribute	Enter LDAP Attribute to bind to Username during authentication

> ✳ Provisioning Manager support connecting to Active Directory on ports 389 and 3268. Please note that only port 389 is supported for Active Directory LDAP updates as 3268 is read-only.

4. When complete, click **Save**

LDAP Authentication

		Edit LDAP
* LDAP Config Name	Default	
* Base	dc=company,dc=com	
* Server	ldap://127.0.0.1	
* Port	389	
* Username	cn=service account,ou=Users,ou=IT,dc=company,dc=com	
* Password	••	
* Username Bind Attribute	sAMAccountName	

3.2.6 FTP

Configuring an FTP server is optional, but is highly-recommended and required to support scheduled backups.

1. Select **FTP** from the **System** menu
2. Click *Add *to create a new FTP connection
3. Enter the information for your FTP server
4. When complete, click **Save**

3.2.7 Certificate

Provisioning Manager is deployed with a self-signed SSL certificate, but optionally can be configured with a certificate from a private or public certificate authority.

Provisioning Manager supports SSL certificates generated using its own private key or using an external private key.

Method 1 – Use Provisioning Manager's private key

1. Select **Certificate** from the System menu
2. Select the **Generate CSR** tab
3. Complete the Certificate Signing Request

> ❗ The common name must match the fully qualified domain name of the server.

1. When complete, click **Generate CSR**
2. Download the CSR file
3. On your Certificate Authority, generate a certificate using the downloaded CSR

1. Select the **Upload Certificate** tab
2. Click **Choose File** to the right of **Certificate** and upload the certificate generate by your certificate authority

> ✱ Uploading a Private Key is not necessary as the certificate was generated using Provisioning Manager's private key

3. If the certificate was generated using a Public Certificate Authority, click **Upload Certificate** to complete the process
4. If the certificate was generated using an Internal Certificate Authority, select the **Use Internal Certificate Authority (CA)** check box
5. Upload the Root Certificate from your Internal CA

6. Click **Upload Certificate** to complete the process

> ✳ Provisioning Manager must be restarted for the changes to take affect. This can be done using the Appliance Manager CLI or using VMWare tools.

Method 2 – Use an external private key

1. Select **Certificate** from the System menu
2. Select the **Generate CSR** tab
3. Complete the Certificate Signing Request

> ❗ The common name must match the fully qualified domain name of the server.

1. When complete, click **Generate CSR**
2. Download the CSR file
3. On your Certificate Authority, generate a certificate using the downloaded CSR
4. Select the **Upload Certificate** tab
5. Click **Choose File** to the right of **Certificate** and upload the certificate generate by your certificate authority
6. Click **Choose File** to the right of **Private Key** and upload the private key from your certificate authority
7. If the certificate was generated using a Public Certificate Authority, click **Upload Certificate** to complete the process
8. If the certificate was generated using an Internal Certificate Authority, select the **Use Internal Certificate Authority (CA)** check box
9. Upload the Root Certificate from your Internal CA
10. Click **Upload Certificate** to complete the process

Upload Certificate	Generate CSR

Upload Certificate

Certificate   [Choose File] No file chosen

Private Key   [Choose File] No file chosen

☑ Use Internal Certification Authority (CA)

Root Certificate [Choose File] No file chosen

[Upload Certificate]

Self-signed Certificate

Will generate a new private key and create a self-signed certificate which will be valid for one year.

Please note this will replace the existing certificate.

[GENERATE!]

View Current Certificate

Note: After making changes to the certificate you will need to restart the server for the changes to take effect.

3.2.8 Backup and Restore

The Backup and Restore feature is used to run manual backups, schedule recurring backups and restore backups.

3.2.8.1 Manual Backup

To run a manual backup:

1. Select **Backup and Restore** from the **System** menu
2. Click **Backup**
3. Save the backup file to a safe location

Generate and download backup	Restore database backup	Schedule backup

Generate and download backup
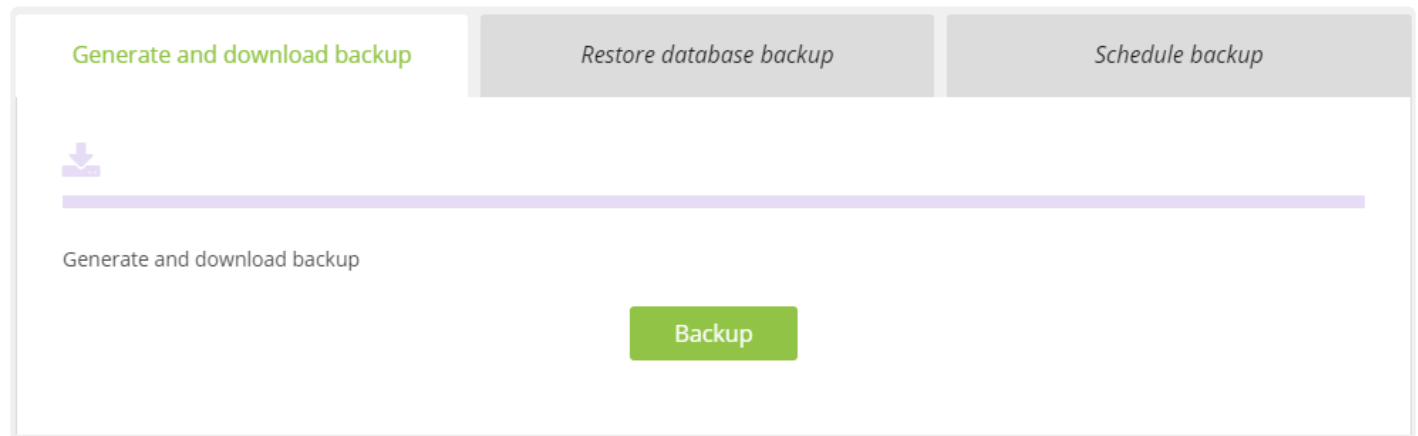
Backup

3.2.8.2 Schedule Backup

To schedule a backup:

> ❗ Scheduled backups cannot be configured without an FTP location.

Scheduled backups cannot be configured without an FTP location.

1. Select **Backup and Restore** from the **System** menu
2. Click the **Schedule Backup** tab
3. Click **Add** to configure a scheduled backup
4. Configure the schedule and click **Add**

> ✳ Maximum number of backups files specified the number of backup files that will be maintained before they are removed.

Generate and download backup

Restore database backup

Schedule backup

+
Add

−
Delete

Backup Location

User

Status

Add new schedule

* Location

Backup

* Frequency

Daily

* Starting Date

03/25/2018

* Time

1

00

AM

* Notification Email

email@yourcompany.com

Maximum number of backup files
(leave empty for no maximum)

7

Close

Add

3.2.9 Log Configuration

By default, Provisioning Manager logging and reporting data is maintained for six month before it is locally archived. Though archiving significantly reduces the storage requirements, it is recommended the data is archived off box.

1. Select Log Configuration from the System menu
2. Update the Log Archiving configuration
3. Click **Save**

1. Select the Report Archiving tab
2. Update the Report Archiving configuration
3. Click **Save**

| Log Archiving | Report Archiving |

Archiving Settings for Reporting Records

✓ Save   🗄 Archive List   ⟳ Archive

Reporting Records Archiving

☑ Enable Archiving

* Mode   Time Based ▾

* Archive Records Older than   6 × ▾   Month ▾

* Storage Location   Local ▾

* Archive Every (Frequency)   1 × ▾   Month ▾

* Starting Date   03/23/2018

/edit?group=logconfig#report-archiving

4. Application Servers

Application Servers provide the necessary configuration for Provisioning Manager to integrate with the Cisco Unified Communication Applications. Currently Provisioning Manager supports the following Cisco UC applications:

- Cisco Unified Communications Manager
- Cisco Unity Connection
- Cisco Contact Center Express
- Cisco Packaged Contact Center Enterprise
- Cisco Meeting Server
- Cisco WebEx
- Cisco Spark

This section will guide you through the process of configuring applications servers in Provisioning Manager.

✳ The first Applications Servers will be added using the PMEAdmin account. Additional Application Servers may be added using another account with Administrator privileges.

4.1 Cisco Unified Communication Manager

Akkadian Provisioning Manager requires integration to at least one Cisco Unified Communications Manager (CUCM), but supports provisioning across multiple CUCM clusters. Integration to a CUCM cluster only requires access to one node running the AXL Web Service, which is typically the publisher, but also be any Subscriber running the service.

This section will guide you through the process of preparing CUCM for integration and configuring CUCM as an Application Server in Provisioning Manager.

4.1.1 Preparing CUCM

Two items are required on Cisco Unified Communications Manager to allow access via the AXL API:

1. The Cisco AXL Web Service must be activated and started
2. An Application user with with required privileges

The Cisco AXL Web Service is disabled by default on some versions of Cisco Unified Communications Manager. The service must be activated to enable AXL API access.

*To activate the AXL Web Service: *

1. Browse to the CUCM **Serviceability** page on https:///ccmservice
2. **Tools > Service Activation**
3. Select the Publisher node

> ✳ Provisioning Manager also supports integrating with a CUCM Subscriber running the Cisco AXL Web Service.

1. Scroll down to **Database and Admin Services**
2. Check the box for **Cisco AXL Web Service** and click Save

Database and Admin Services	
Service Name	Activation Status
☑ Cisco AXL Web Service	Activated

To create Provisioning Manager CUCM Application User:

1. From the Cisco Unified Communications Manager Administration Web page, select Application User from the User Management menu, and then click Add New.
2. In the User ID field, type PMEAXL.
3. In the Password and Confirm Password fields, type a password for the new user and then click Save.
4. Navigate down the page to Permissions Information.
5. Click Add to Access Control Group and then click Find.
6. Select the following Groups:

- **Standard TabSync User**
- **Standard EM Authentication Proxy Rights**
- **Standard CCM Server Monitoring**
- Click **Add Selected**
- Click **Save**

4.1.2 CUCM Integration

To add a Cisco Unified Communications Manager Application Server:

1. Select **Application Servers** from the **System** menu
2. Select the **Communications Manager** tab to add a Cisco Communications Manager server
3. On the menu, click **Add**
4. Complete the required fields
5. Click **Verify AXL** to validate the connection
6. Click **Save**
7. Click Back, select the CUCM server and click **Sync**
8. Repeat this process for additional integrations

✱ Please note the same credentials may be used for **Phone Control**. You also have the option of using a different CUCM Application user, but the account must have AXL and Server Monitoring privileges.

Communication Manager Information

* Application Server Name   CUCM01

* CUCM Server   192.168.124.225

Version   11.5.1.12900(21)

Communication Manager Authentication

* Username   PMEAXL

* Password   ········

* Confirm Password   ········

Verify AXL

Phone Control Information

Phone Control Username   PMEAXL

Phone Control Password   ········

Confirm Phone Control Password   ········

	CUCM	Unity Connect...	UCCX	UCCE	WebEx	Spark	Cisco Meeting...	Schedule Sync

Add   **Delete**   **Sync**   **Refresh**

Show 15 entries

Search Licensing Usage	Search Address		Search Last Processed	Search Status

Licensing Usage

	Name	Address	UBL	DBL	Last Processed	Status	
☐	CUCM01	192.168.124.225	-	-	2018-03-26 10:59:08	✔	

Showing 1 to 1 of 1 entries

First   Previous   **1**   Next   Last

4.2 Cisco Unity Connection

Akkadian Provisioning Manager supports provisioning across multiple Cisco Unity Connection (CUC) clusters. Integration to a CUC cluster only requires access to the Publisher node.

This section will guide you through the process of preparing CUC for integration and configuring CUC as an Application Server in Provisioning Manager.

4.2.1 Preparing CUC

Akkadian Provisioning Manager communicates with Cisco Unified Connection using the REST API. The built-in Cisco Unity Connection application administrator account can be used for access, but for security purposes a separate account should be created.

To configure a new user:

1. From the Cisco Unity Connection Web page, select **Users** from the User section, and then click **Add New**
2. In the User Type drop-down menu, select **"User Without Mailbox"**
3. In the Based-on Template drop-down menu, select **"administratortemplate"**
4. In the Alias field, type a username (Example – PMEREST) and click **Save**
5. From the Edit Menu select Password Settings and uncheck **"User Must Change at Next Sign-In"** and click **Save**
6. From the **Edit Menu** select **Change Password**.
7. In the **Password** and **Confirm Password** fields, type a password for the user and click **Save**.
8. From the Edit Menu select Roles.
9. Verify the user has the **"System Administrator"** under **Assigned Roles**

> ✳ The default CUC authentication rule expires passwords in 120 days. For service accounts, we suggest password are set not to expire.

Edit Roles

User   Edit   Refresh   Help

[Save]

Roles

Assigned Roles | System Administrator

˄ ˅

Available Roles

Audio Text Administrator
Audit Administrator
Greeting Administrator
Help Desk Administrator
Mailbox Access Delegate Account

[Save]

4.2.2 CUC Integration

To add a Cisco Unity Connection Application Server:

1. Select **Application Servers** from the **System** menu
2. Select the **Unity Connection** tab
3. On the menu, click **Add**
4. Complete the required fields
5. Click **Verify Unity Connection** to validate the connection
6. Click **Save**
7. Click Back, select the CUC server and click **Sync**
8. Repeat this process for additional integrations

Unity Connection Server Information

* Application Server Name   CUC01

* CUC Server   192.168.124.226

Version   11.5.1.1459

Unity Connection Server Authentication

* Username   PMEREST

* Password   ....

* Confirm Password   ....

Verify Unity Connection

CUCM	Unity Connec...	UCCX	UCCE	WebEx	Spark	Cisco Meeting...	Schedule Sync

Add **Delete** **Sync** **Refresh**

Show 15 entries

	Search Name	Search Address	Search Last Processed	Search Status
	Name	**Address**	**Last Processed**	**Status**
☑	CUC01	192.168.124.226	2018-03-26 11:32:29	✔

Showing 1 to 1 of 1 entries

First   Previous   **1**   Next   Last

4.3 Cisco Contact Center Express

Akkadian Provisioning Manager supports provisioning across multiple Cisco Unified Contact Center Express Clusterd (UCCX) clusters. Integration to a UCCX cluster only requires access to the primary node.

This section will guide you through the process of preparing UCCX for integration and configuring UCCX as an Application Server in Provisioning Manager.

4.3.1 Preparing UCCX

Akkadian Provisioning Manager communicates with Unified Contact Center Express (UCCX) using the REST API.

Two items are required on UCCX to allow access via the API:

1. The "Cisco Unified CCX Configuration API" service must be activated and started
2. User with Cisco Unified CCX Administrator capability

> ✳ Before configuring the user account in UCCX, it must be created in CUCM and synchronized.

Creating a Cisco Unified CCX integration account:

1. From the Cisco Unified CCX Administration web interface, select **Tools** -> **User Management** -> **Administrator Capability View**
2. Locate the user from the **Available Users** list or using the Search tool
3. Move the user from* Available Users* to **Cisco Unified CCX Administrators**
4. Click **Update** to save the changes

4.3.2 UCCX Integration

To add a Unified Contact Center Express Application Server:

1. Select **Application Servers** from the **System** menu
2. Select the **UCCX** tab
3. On the menu, click **Add**
4. Complete the required fields
5. Click **Verify UCCX Server** to validate the connection
6. Click **Save**
7. Click Back, select the UCCX server and click **Sync**
8. Repeat this process for additional integrations

UCCX Server Information

* UCCX Server Name	UCCX01
UCCX Server	192.168.124.190

UCCX Server Authentication

UCCX Username	admin
UCCX Password	....
Confirm UCCX Password	....

Verify UCCX Server

	CUCM	Unity Connect...	UCCX	UCCE	WebEx	Spark	Cisco Meeting...	Schedule Sync

Add **Delete** **Sync** **Refresh**

Show 15 entries

	Name	Address	Last Processed	Status
Search Name		Search Address	Search Last Processed	Search Status
☑	UCCX01	192.168.124.190	2018-03-26 11:39:06	✔

Showing 1 to 1 of 1 entries

First Previous **1** Next Last

4.4 Unified Contact Center Enterprise

Akkadian Provisioning Manager supports provisioning across multiple Cisco Packaged Contact Center Enterprise Clusters (PCCE) clusters.

This section will guide you through the process of preparing PCCE for integration and configuring PCCE as an Application Server in Provisioning Manager.

4.4.1 Preparing PCCE

Requirements:

1. Version 10.5+ of Cisco Packaged Contact Center Enterprise (PCCE).
2. PCCE account with the Administrator role.
3. SQL user account with read access to the AWDB database. This account is only used for database reads.

> ✱ Administrators who are in the Active Directory Config Security Group or Setup Security Group have full access to the Cisco Packaged Contact Center Enterprise APIs, unless that access has been limited by the Feature Control Set List Tool and the User List Tool. These tools are Unified CCE Configuration Manager tools, used together to establish and limit access to the Cisco Packaged Contact Center Enterprise administration tools—both the user interface and APIs—and to Unified CCE Configuration Manager. Note that the Administrator user name should be in the form of a Fully Qualified Domain Name (FQDN).

4.4.2 PCCE Integration

To add a Unified Contact Center Enterprise Application Server:

1. Select **Application Servers** from the **System** menu
2. Select the **UCCE** tab
3. On the menu, click **Add**
4. Enter the CCE server name or IP address (AW/Logger Server)
5. Supply the necessary authentication credentials
6. Enter the AW database name as configured in your system
7. Enter the database user credentials (User must have database read access)
8. Click **Verify UCCE Connection** to validate the connection
9. Click **Save**
10. Click Back, select the UCCE server and click **Sync**
11. Repeat this process for additional integrations

* Application Server Name	PCCE01
* UCCE Server	192.168.124.240
Deployment Type	Packaged CCE: CCEPACM1 Lab only
Version	10.5

Ucce Server Authentication

* Username	administrator@akkadianlabs.com
* Password	••••••••
* Confirm Password	••••••••
* SQL Server Database Name	dev_awdb
* SQL Server User	pme1
* SQL Server Password	••••••••

Verify Ucce Connection

+	—	↻	↺
Add	**Delete**	**Sync**	**Refresh**

Show 15 ▾ entries

☐	**Name** ⇕	**Address** ⇕	**Last Processed** ⇕	**Status** ⇕
	Search Name	Search Address	Search Last Processed	Search Status
☐	PCCE01	192.168.124.240	2018-03-24 23:06:16	✔

Showing 1 to 1 of 1 entries

First   Previous   **1**   Next   Last

4.5 Cisco WebEx

Akkadian Provisioning Manager supports provisioning users in Cisco WebEx.

This section will guide you through the process of preparing WebEx for integration and configuring WebEx as an Application Server in Provisioning Manager.

> ✳ Because WebEx is a cloud service, Provisioning Manager will required outbound access to your WebEx site.

4.5.1 Preparing WebEx

Akkadian Provisioning Manager communicates with Cisco WebEx using the REST API. There are several requirements for Provisioning Manager to integrate with Cisco WebEx.

Requirements:

1. Provisioning Manager must have access to the Cisco WebEx cloud servers, which includes a valid DNS server for name resolution
2. The WebEx site must be enabled for API access and you must have access to the Site ID and Partner ID
3. Must have a WebEx account with Site Administrator privileges

> ✱ If you don't see the Site ID and Partner ID on your WebEx account settings page, the API is most likely not enabled and you will need to contact your WebEx account manager.

4.5.2 WebEx Integration

To add a Cisco WebEx Application Server:

1. Select **Application Servers** from the **System** menu
2. Select the **WebEx** tab to add a Cisco WebEx site
3. On the menu, click Add
4. Complete the required information
5. Click **Save**
6. Repeat this process for additional integrations

WebEx Site Information

* WebEx Site Name

* WebEx Site URL yourserver.webex.com

* Site ID

* Partner ID

Version

WebEx Site Authentication

* Username

* Password

* Confirm Password

Verify Webex

4.6 Cisco WebEx Teams

Akkadian Provisioning Manager supports provisioning users in Cisco WebEx Teams.

This section will guide you through the process of preparing Spark for integration and configuring Spark as an Application Server in Provisioning Manager.

> ✳ Because Spark is a cloud service, Provisioning Manager will required outbound access to your Cisco Spark site.

4.6.1 Connecting to WebEx Teams

Akkadian Provisioning Manager communicates with Cisco WebEx using the REST API. There are several requirements for Provisioning Manager to integrate with Cisco WebEx Teams.

Requirements:

1. Provisioning Manager must have access to the Cisco WebEx cloud servers, which includes a valid DNS server for name resolution
2. Must have a WebEx Teams account with Administrator privileges

To connect to Cisco WebEx Teams:

1. Select **Application Servers** from the **System** menu
2. Select the **WebEx Teams** tab
3. On the menu, click Add
4. Enter a name for the WebEx Teams site
5. Enter the WebEx Teams URL – api.ciscospark.com
6. Enter the username of the user with administrative privileges
7. Click the **Request access to WebEx Teams** button to obtain a token
8. Follow the prompts to log into WebEx teams
9. Copy the token into the **Authorization Token** field
10. Click **Save**
11. Repeat this process for additional integrations

WebEx Teams

Hi Tom ▼

| Back | Save | Add | Copy | Delete |

WebEx Teams Site Information

Edit WebEx Teams

* WebEx Teams Site Name
Akkadian WebEx Teams

WebEx Teams Information

* WebEx Teams Site URL
api.ciscospark.com

WebEx Teams Authentication

WebEx Teams Site Authentication

* Username
admin@akkadianlabs.com

Please click on this button to authorize the Webex Team integration on your selected account.
You will be directed to an external page where you would need to select a code to be entered in the field provided below.

Request access to WebEx Teams

* Authorization Token
••

4.7 Cisco Meeting Server

Akkadian Provisioning Manager communicates with Cisco Meeting Server using the REST API.

This section will guide you through the process of preparing Cisco Meeting Server for integration and configuring Cisco Meeting Server as an Application Server in Provisioning Manager.

4.7.1 Preparing CMS

Requirements:

1. HTTPS via the same TCP ports as you would use to access the Web Admin Interface – typically port 443
2. Meeting Server user account with Admin privileges

4.7.2 CMS Integration

To add a Cisco Meeting Server Application Server:

1. Select **Application Servers** from the **System** menu
2. Select the **CMS** tab
3. On the menu, click **Add**
4. Complete the required fields
5. Click **Verify Cisco Meeting Server** to validate the connection
6. Click **Save**
7. Repeat this process for additional integrations

Cisco Meeting Server Site Information

* Server Name	
* IP Address	
* Port	

Cisco Meeting Server Site Authentication

* Username	
* Password	

Verify Cisco Meeting Server

5. Service Groups

Provisioning Manager Service Groups provide the following functions

- Assemble Applications Servers into a logical container for provisioning
- Provide configuration settings for Service Group based features

This section will focus on basic settings required to configure a Service Group. Other Service Group based feature configuration will be covered in their respective sections.

❋   The initial Service Group must be created using the PMEAdmin account.

To add a Service Group:

1. Select **Service Groups** from the **System** menu
2. On the menu, click **Add** to create a new **Service Group**
3. Configure the **Service Group** by selecting the application servers
4. When finished, click **Save**

Service Group Information

* Group Name	SG1
Group Description	Service Group 1
* Communications Manager	CUCM01
Unity Connection	CUC01
UCCX	Please Select Item
UCCE	Please Select Item
WebEx Site	Please Select Item
Spark	Please Select Item
Cisco Meeting Server	Please Select Item

6. Security

The Provisioning Manager Security section provides the ability to configure and manage:

- Group Permissions
- Service Groups
- Group Membership
- Provisioning Job Access
- Filter Template Assignment
- Site Template Access

This section will cover configuring security within Provisioning Manager.

6.1 Groups

Groups are used to provide a common class of users with permissions and access to items within Akkadian Provisioning Manager.

The system is configured with four default groups:

- Administrator
- Editor
- Provision
- Template Manager

✱ These built-in groups cannot be modified, but additional groups may be added.

To add a Group:

1. Select **Security** from the **System** menu
2. Select the **Groups Permissions** tab
3. On the menu, click **Add** to create a new Group
4. Enter the Group **Name** and configure the appropriate permissions
5. When finished, click **Save**
6. Repeat the process to create additional Groups

Groups Permissions	Service Group	Group Membership	Jobs	Filters	Site Templates

✚ Add	✎ Edit	➖ Delete	✔ Save

Show 15 ▾ entries   ▼ Filter…

Name ▲	Actions											
	Provision	Bulk	Edit	Delete	Extension Mobility	Device Swap	End User Swap	CMC/FAC Edit	Phone Editor	Phone Control	Templates	System
Help Desk	☑	☐	☑	☑	☐	☑	☐	☐	☑	☑	☐	☐
*Administrator	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
*Editor	✔	✔	✔	✔	✘	✘	✘	✘	✘	✔	✘	✘
*Provision	✔	✔	✘	✘	✘	✘	✘	✘	✘	✔	✘	✘
*Template Manager	✘	✘	✘	✘	✘	✘	✘	✘	✘	✔	✔	✘

Showing 1 to 5 of 5 entries   First   Previous   1   Next   Last

6.2 Service Groups

Service Groups provide the ability to assemble Applications Servers into a logical container for provisioning, but to begin using Service Groups, security permissions must be granted.

To assigned access to a Service Groups:

1. Select **Security** from the **System** menu
2. Select the **Service Group** tab

Method 1 – Associating Multiple Groups to a Service Groups

1. Select the **Service Group**
2. Click the **Edit** button
3. Select the **Groups**
4. Associate the **Groups**
5. When finished, click **Save**
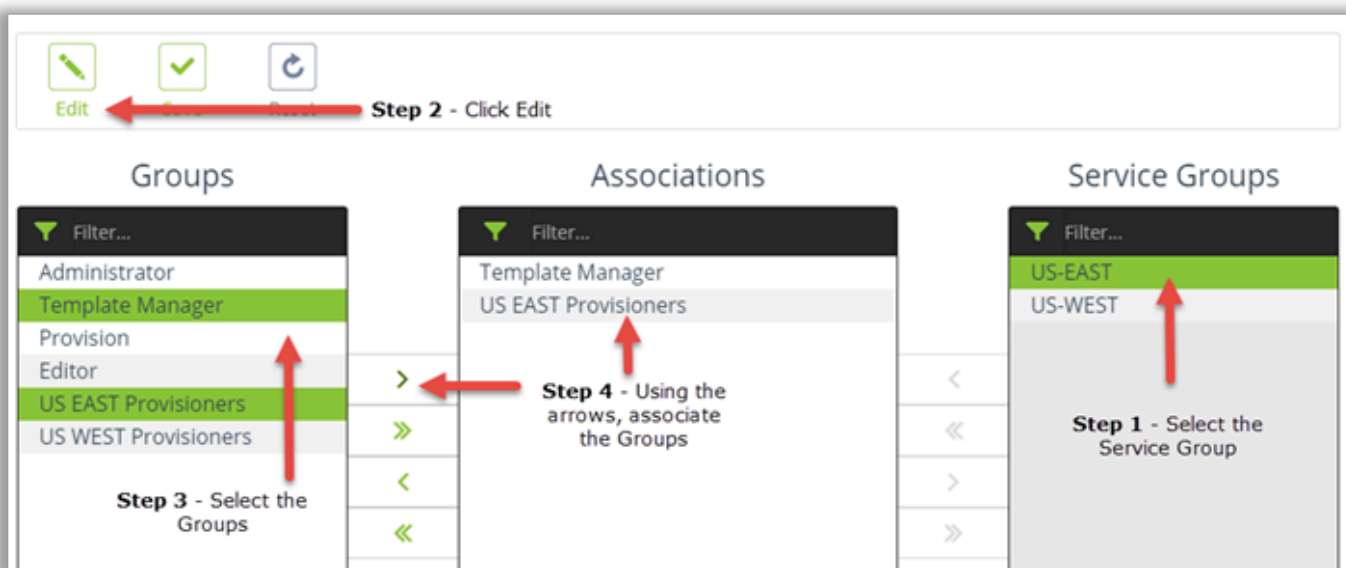
Method 2 – Associating Multiple Service Groups to Group

1. Select the Group
2. Click the **Edit** button
3. Select one or more **Service Groups**

4. Associate the **Service Groups**

5. When finished, click **Save**
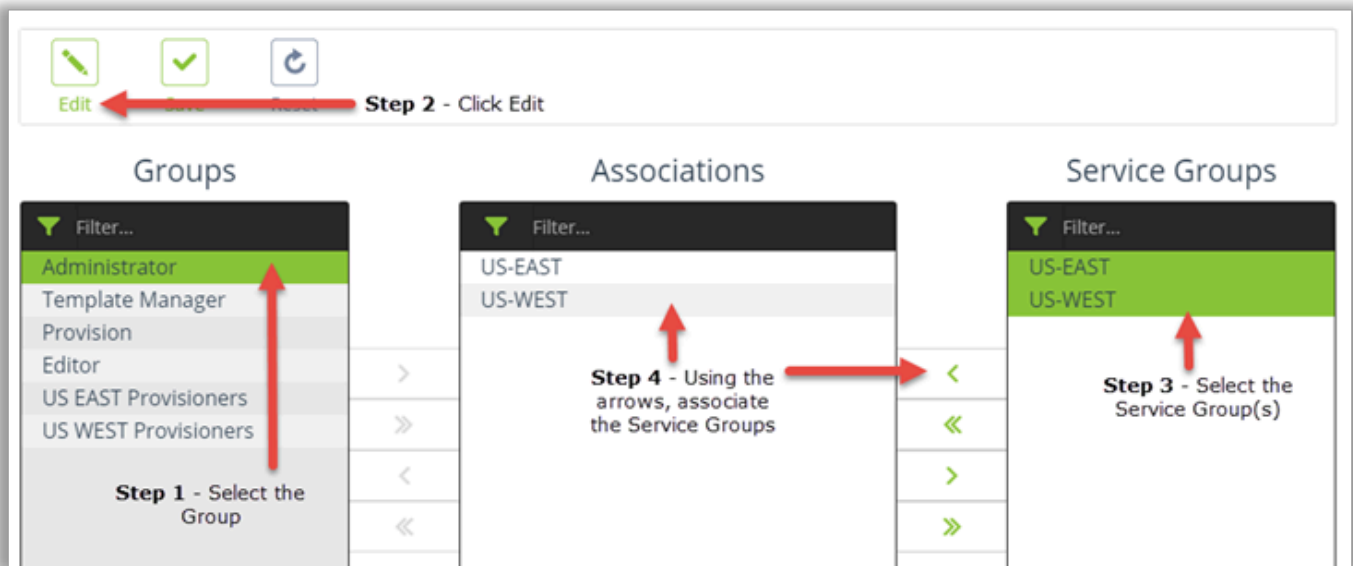
6.3 Group Membership

The Group Membership section provides the ability to manage users membership to Groups within Provisioning Manager.

To assigned users to a Group:

1. Select **Security** from the **System** menu
2. Select the **Group Membership** tab
3. Select the **Group**
4. Click the **Edit** button
5. Select the **Users**
6. Use the arrow to move the users to the **Members** box
7. When finished, click **Save**
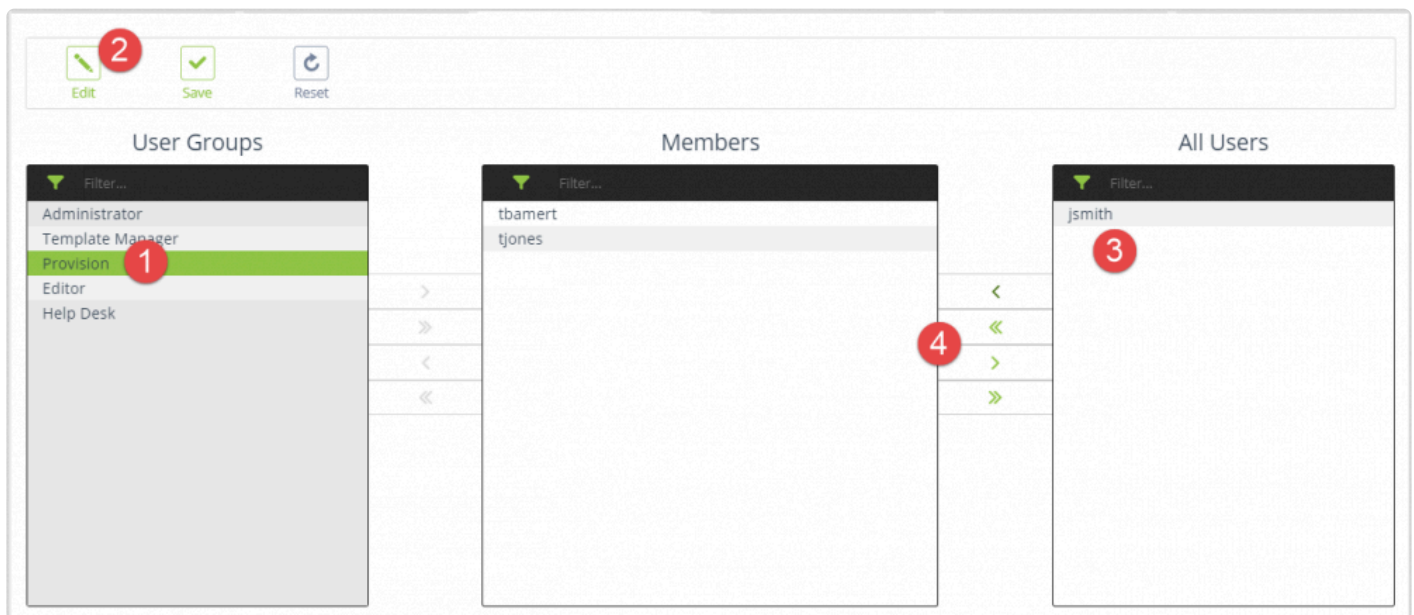
6.4 Jobs

The Jobs sections provides the ability to manage Groups access to provisioning Jobs within Provisioning Manager.

To assigned Groups access to Jobs:

1. Select **Security** from the **System** menu
2. Select the **Jobs** tab
3. Select the **Group**
4. Click the **Edit** button
5. Select the **Jobs**
6. Use the arrow to move the Jobs to the **Associations** box
7. When finished, click **Save**

6.5 Filters

The Filters section provides the ability to apply filters to Groups within Provisioning Manager.

Filter Templates are an optional security component used to restrict user's access to objects and field data within a Service Group.

To apply a Filter to a Group:

1. Select **Security** from the **System** menu
2. Select the **Filters** tab
3. Select the **Group**
4. Click the **Edit** button
5. Select the **Filter(s)**
6. Use the arrow to move the Filters to the **Associations** box
7. When finished, click **Save**

6.6 Site Templates

The Site Template sections provides the ability to manage Group access to Site Templates within Provisioning Manager.

To apply a Site Template to a Group:

1. Select **Security** from the **System** menu
2. Select the **Site Template** tab
3. Select the **Group**
4. Click the **Edit** button
5. Select the **Site Templates**
6. Use the arrow to move the Site Templates to the **Associations** box
7. When finished, click **Save**

7. Users

The PMEAdmin account is a built-in system administrator account and has no ability to provision. At least one user account must be created with Administrator rights to complete the initial Provisioning Manager configuration.

> ✳ Before creating LDAP authenticated users, the LDAP authentication configuration must be configured.

> ✳ It is recommended Groups be configured before adding the users.

To add a User:

1. Select **Users** from the **System** menu
2. On the menu, click **Add** to create a new User
3. Populate the required fields
4. For local authentication, the email address is required
5. For LDAP authentication, set the User Type to LDAP and select the LDAP agreement
6. Add the **Group Association(s)** to assign permissions
7. When finished, click **Save**
8. Repeat the process to create additional users

7.1 AD Group Mapping

Provisioning Manager also offers the ability to automatically import users from Active Directory. This feature works by mapping Active Directory Groups to Provisioning Manager Groups. When users in the mapped AD Groups login, there account is created in Provisioning Manager with corresponding security Group.

> ✱ Before configuring AD Group Mapping, an LDAP agreement must be configured with access to AD LDAP users.

To Configure AD Group Mapping:

1. Select **Users** from the **System** menu
2. On the menu, click the **AD Group Mapping** tab
3. Select the appropriate LDAP agreement and click **Set LDAP Server**
4. The screen will refresh and you will need to navigate back to the **AD Group Mapping** tab
5. In the **Associative Information** section, choose the AD Group and the Provisioning Manager Group to which these users should be assigned
6. Click **Associate** to add the association
7. Repeat this process to add additional group mappings

LDAP server * LDAP Authentication × ▾   Set LDAP server

✓
Associate

↻
Refresh

━
Disassociate

Associative Information

Active Directory Group Help Desk × ▾

aPME Group Help Desk ▾

Show 15 ▾ entries

Search Active Directory Group

Search aPME Group

☐	**Active Directory Group**	**aPME Group**
☐	Help Desk	Help Desk

Showing 1 to 1 of 1 entries

First Previous **1** Next Last

8. Preparing for Provisioning

This section will guide you through the process of preparing Provisioning Manager to provision in your environment. Please ensure the following initial configuration has been completed before proceeding:

1. Initial configuration has been completed as outlined in the Initial Configuration section
2. At least one CUCM application server and Service Group has been created as outline in the Application Servers and Service Groups sections
3. At least one user with the Administrator role has been created and outline in the Users section

If these tasks are complete, login to Provisioning Manager as a user with Administrator role to begin the configuration.

8.1 Global Variables

Global Variables (GVs) are placeholders used to provide key information required to provision. GVs are used to capture data such as used ID, First Name, Last Name etc…
Global Variables can be repeated within templates, but only requires single input at provision. For example, first and last name may be required multiples times when provisioning an end user with multiple devices, lines and voicemail. Global Variables can reduce this input to a single entry.

There are three types of Global Variables:

Default – captures provisioning data using a validated input field
List – creates drop-down list for selection at provision
System – Used to capture the provisioned Directory Number and apply it as a Global Variable

To add a Global Variable:

1. Select **Global Variables** from the **System** menu
2. On the menu, click **Add** to create a new **Global Variable**
3. Select the **Global Variable** type
4. Configure the options as described in the table:

Field Name	Description
Global Variable Type	Default, List or System
Variable Name	Enter the variable name
Tooltip	Enter a tool-tip to help users understand the variable
Description	Enter a description
Optional (Checkbox)	By default, Global Variables are required fields. Check Optional to make these optional fields.
Input Validation	Enter a validation method. Example, if you only want users to enter a numeric value, choose "numeric".
Appearance Index	Set the appearance index value. This will determine in which order the Global Variable will be displayed on the provisioning screen
Use Custom Regular Expression	As an alternative to choosing a validation method, a custom regular expression can be used

Enable Lookup (Checkbox)	Converts the field from input to lookup during provision. This is required when CUCM is LDAP integrated and Global Variable is created for enduser ID.
CUCM Validation	Specifies the target validation field in CUCM
CUCM Field Association	Choose the filed from which Provisioning Manager will automatically pull data. This only applies to LDAP integrated endusers.
Enable Product Type Prefix Mapping (Checkbox)	For edit jobs, this allows Provisioning Manager to automatically apply the appropriate product prefix. For example, if you were running a name change job, Provisioning Manager can automatically apply the proper Device Name prefix.

Global Variable Information

*Global Variable Type	Default
* Variable Name	
Tooltip	
Description	
☐	Optional
* Input Validation	Please Select Item
Appearance Index	< NONE >
Custom Regular Expression	
Custom RegEx Fail Message	
☐	Enable Lookup
CUCM Validation	Please Select Item

Global Variable Information

*Global Variable Type	List ▾
* Variable Name	
Tooltip	
Description	

☐ Optional

☐ Enable "type-in" data

* Custom List		Value	Display Name
	1		

Global Variable Information

*Global Variable Type | System   ▼ |

System Global Variable Configuration

* Directory Number System Global Variable Name

* Directory Number System Global Variable Instances

☐ Enable System Global Variables

* Service Groups

8.2 DN Pools

Provisioning Manager DN Pools provide real-time directory number management. They can help simplify the provisioning process by automating directory number assignment.

DN pools are predefined number ranges between which Provisioning Manager Express can search for available DNs.

To add a DN Pool:

1. Select **DN Pool** from the **System** menu
2. On the menu, click **Add** to create a new **DN Pool**
3. Select a **Service Group**
4. Configure the **DN Pool** options as described in the table
5. When finished, click **Save**
6. To add another **DN Pool**, repeat the process

Field Name	Description
Service Group Name	Select the Service Group
DN Profile Name	DN Pool Name
DN Profile Description	DN Pool Description
Route Partition	Select the Route Partition for the DN Range
Search Across Clusters (Checkbox)	Enables DN management to search across multiple CUCM clusters when DNs are disturbed across multiple clusters.
Search All Partition (Checkbox)	Check this box to search all CUCM partitions when performing a DN lookup.
Include Unassigned DNs (Checkbox)	Check this box to include unassigned CUCM DNs in the DN lookup.
Enable DN Aging	Check this box to enable DN aging on the DN Pool. Deleted DNs will be excluded from reassignment according the DN aging period configured on the Service Group.
External Phone Number Mask	Enter a phone number mask to be applied when allocating a DN from this pool
AAR Destination Mask	Enter a AAR destination mask to be applied when allocating a DN from this pool

DN Prefix	Enter digits common to the range, such as are code and exchange
Directory Number Pool Ranges From/ To	Enter start and end of the DN Range. The range must be contiguous. The range cannot start with 0.

DN Pools

Back	Save	Add	Copy	Delete

* DN Profile Name   Boston

DN Profile Description   Boston

Route Partition   Boston_Internal_RTP

☐ Search Across Clusters
☑ Search All Partitions
☑ Include Unassigned DN
☑ Enable DN Aging

External Phone Number Mask   617545XXXX

AAR Destination Mask

DN Prefix   \+1617545

Directory Number Pool Ranges

From	To	Exceptions List ?
7500	7599	7560,7575,7590-7595

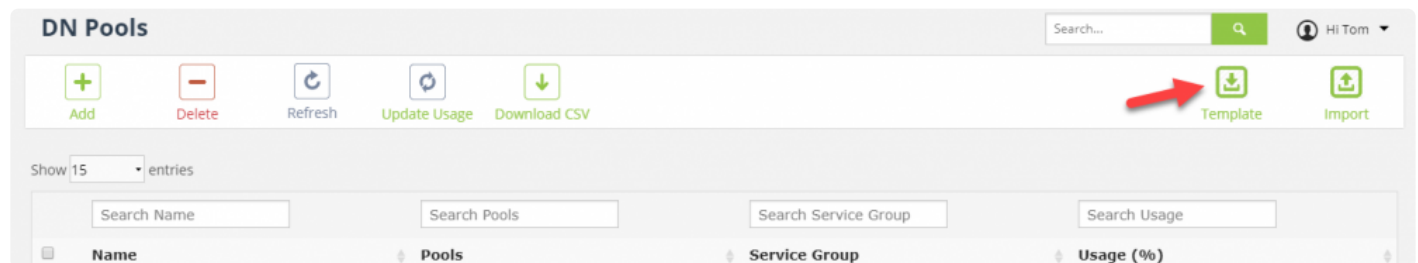+ Add Row

8.2.1 Importing DN Pools

If a large number of DN Pools need to be created, importing the data may be more effective.

To import a DN Pool:

1. Select **DN Pool** from the **System** menu
2. On the menu, click **Template** to download a sample CSV template.
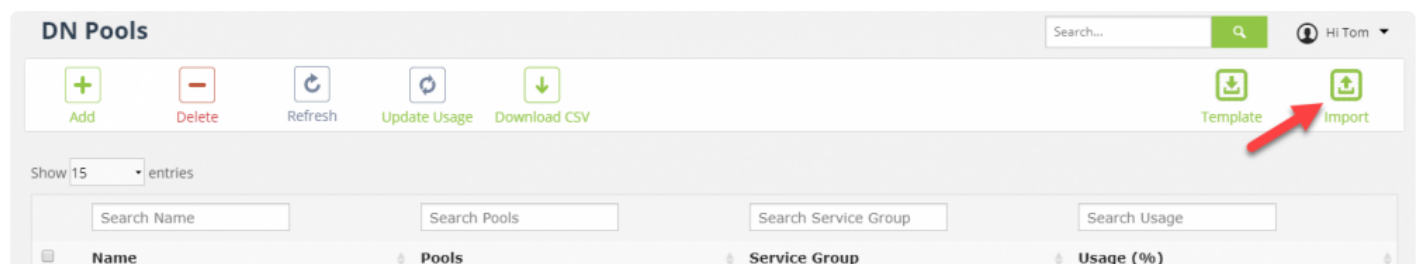

3. Populate the template with the DN Pool information.

> ✱ If the DN Pool requires multiple DN ranges per pool, use multiple rows with the same DN Pool name. Multiple exceptions can be included using comma separated values. Examples – "1200,1299" or "1200-1205,1299". In excel, this string usually begins with a single quote.

4. Upload the CSV to import the DN Pools.

8.3 License Pools

License Pools simplify the provisioning process by helping manage the licensing process. In Cisco CUCM, it may be necessary to assign an Owner User ID to devices in order to effectively leverage Cisco User Workspace Licensing. When devices are not directly associated to user, this process can be challenging. License Pools help alleviate this challenge by automatically creating local end users and associated devices strictly for licensing purposes.

To add a License Pool:

1. Select **License Pool** from the **System** menu
2. On the menu, click **Add** to create a new **License Pool**
3. Select a **Service Group**
4. Configure **License Pool** options as described in the table
5. When finished, click **Save**
6. To add another **License Pool** Template, repeat the process

Field Name	Description
Service Group Name	Select the Service Group
License Pool Name	License Pool Name
License User Prefix	Username prefix for license user. Username format will be Prefix_Licensing_XXXX
Max Number of Devices per User	Maximum number of devices to which the license user will be assigned as the Owner User ID before the next license user will be created. Max = 2000
End User Template	End User Template used to provision the license end user. Template should not contain any global variables and fields requiring unique values, such as Mail ID & Directory URI should not be configured.

License Pool Information

* License Pool Name	
* License User Prefix	
* Max Number of Devices per User	
* End User Template	Please Select Item ▾

8.4 Device Pools

Device Pools provide the ability to create a group of CUCM Device Pools across which Provisioning Manager will load balance devices. When the Device Pool features is used in a provision, Provisioning Manager will look at the number of devices in each CUCM Device Pool assigned to the group and provision the device in the Device Pool with the fewest number of devices and will always attempts the keep the number of devices distributed as evenly as possible across the CUCM Device Pools.

Device Pools will override any Device Pool settings on Device Templates and Site Templates.

To add a Device Pool:

1. Select **Device Pools** from the **System** menu
2. On the menu, click **Add** to create a new Device Pool group
3. Select a Service Group
4. Configure filter options as described in the table
5. When finished, click **Save**
6. To add another **Device Pool**, click **Add**
7. To use the Device Pool, it must be added to the Device Pool(s) section located at the bottom of the Device Template or Site Template.

Field Name	Description
Service Group	Select the Service Group
Template Name	Enter a name for the template
Device Pools(s)	Add 2 or more Device Pools to the group

Device Pool Information

* Template Name

* Device Pool(s)   Please Select Item

8.5 Email Templates

Email Templates can be used to send automated notifications to end users upon the completion of a provision. Variables are used to pull data provisioning job and populate the email template. Please note, email templates can only be used in conjunction with Site Templates.

To add an Email Template:

1. Select **Email Templates** from the **System** menu
2. On the menu, click **Add** to create a new **Email Template**
3. Select a Service Group
4. Configure options as described in the table below.
5. When finished. Click **Save**.
6. Repeat the process for additional **Email Templates**
7. Assign the Email Template to the appropriate **Site Template(s)**

Email Template Information

* Template Name   Default Email Template

* From   helpdesk@yourcompany.com

* To   {{Email Address}}

Bcc

* Subject   Welcome aboard!

* Content

Welcome|

Insert Provision Var ▸	Remote Destinations
🔗 Insert/edit link	CTIs
	Username
	First Name
	Last Name
	User PIN
	User Password
	Email Address
	Self Service ID
	Unity User Alias
	Unity User Password
	Webex User Id
	UCCE Agent Name
	SPARK Emails

Right-click to select variable

Email Template Information

* Template Name	Default Email Template
* From	helpdesk@yourcompany.com
* To	{{Email Address}}
Bcc	
* Subject	Welcome aboard!

* Content

Welcome {{First Name}},

Welcome aboard. We are excited to have you as a part of our team. Below is all the information you will need to get started using your Unified Communications devices.

Username	{{Username}}
PIN	12345
Extension	{{Line1}}

8.6 Filter Templates

Filter Templates are an optional security component used to restrict user's access to objects and field data within a Service Group.

Scenario: Help desk personnel at Company X are divided into groups: support for the New York and Atlanta offices. The challenge is help desk personnel should only see devices and field data specific to their location, but they share CUCM and CUC clusters. Filter templates overcome this challenge by providing a mechanism to filter views of devices and field data at a Service Group level.

To add a Filter Template:

1. Select **Filter Templates** from the **System** menu
2. On the menu, click **Add** to create a new Filter Template
3. Enter the Filter Template Name and select a Service Group
4. Configure filter options as described in table
5. When finished, click **Save**
6. To add another **Filter Template**, repeat the process

Field Name	Description
Name	Filter Template Name
Service Group Name	Select the Service Group
Device Pools	Select the CUCM Device Poos(s)
Calling Search Space	Select the CUCM Calling Search Space(s)
Route Partitions	Select a CUCM Route Partition(s)
Device Profile Filter	Applies to the Device Profile Description Field. Matches using "contains".
Telephone Number	Applies to the CUCM End User Telephone number field. Matches using "begins with".
Department	Applies to the End User Department Field. Matches using "contains".
Email (mailid)	Applies to the End User Mail ID Field. Matches using "contains".
Apply CUCM End User filter to Unity Connection	Applies CUCM End User filter to Unity Connection
Filter Field	Select the Unity Connection filter field
Filter Starts With	Specify the filter criteria

8.7 Voice Mail Scheduled Delete

Provisioning Manager has the ability to scheduled Cisco Unity Voice Mail account deletions. By default, the CUC VM delete function in Provisioning Manager complete deletes the user's VM account and all messages in Unity Connection. Alternatively, you may delay the deletion process by enabling the scheduled deletion feature and setting the number of days to retain the VM account before it is deleted.

To enable VM Scheduled Delete Service:

1. Select **Service Group** from the **System** menu
2. From the list, click on a **Service Group**
3. Navigate to the "**CUC Voice Mailbox Scheduled Delete Service**" section
4. Check the box to enable the service
5. Set the number of days to retain the VM account before being deleted
6. Check the box to enable email notifications when VM accounts are deleted
7. Click **Save**
8. Repeat the process for any other **Service Groups** where the feature should be enabled

CUC Voice Mailbox Scheduled Delete Service

☑	Enable CUC Voice Mailbox Scheduled Delete
* Number of days (to delete)	30
☑	Send Email Notification notify@mycompany.com

To enable VM Scheduled Delete on the Delete Template:

1. Select **Editing Templates** from the **Templates** menu
2. Select an existing Unity Voicemail Delete template or create a new one
3. On the Unity Voicemail Delete template, select the "Enable CUC Voicemail Schedule Delete" checkbox
4. Click **Save**

Editing Template Information

* Template Name	Delete VM
* Template Type	Delete
* Editing Item Type	Unity Voicemail
	☑ Enable CUC Voice Mailbox Scheduled Delete

✳ The Voice Mail Scheduled Delete process can be monitored at any time by going to **Voice Mail Schedule** in the **System** menu. You may also cancel a scheduled delete for any job that has not been processed.

8.8 Templates

Templates are the building blocks in Provisioning Manager used to create provisioning jobs.

There two major Template categories in Provisioning Manager:

- Add Templates
- Editing Templates

Add Templates are used to provision new items, where editing templates are used to change existing items.

There are three types of editing templates:

- Edit Templates – edit existing items
- Delete Templates – delete existing items
- Edit/Delete Templates – edit and delete existing items

This section will cover the process of creating each template type in Provisioning Manager.

8.8.1 Add Templates

Add Templates are used to provision new items in the Cisco UC applications. This section will cover the process of creating an Add Templates in Provisioning Manager. Because there are numerous types of Add Templates, this section will provide general instructions that can be applied to create any add template.

To add a Template:

1. Expand **Templates** from the left navigation menu
2. On the menu, select the desired Template type

> ✳ Call Routing & Device menu options contains multiple templates types

3. Click **Add** to create a new template
4. Select a Service Group
5. Configure the template options for your environment
6. When finished, click **Save**
7. To add another Template, click **Add**

Video – Planning for Templates



Video – Creating Add Templates

8.8.2 Editing Templates

Editing Templates are used to manipulate existing items in the Cisco UC applications. This section will cover the process of creating an Editing Templates in Provisioning Manager.

To create an Editing Template:

1. Expand **Templates** from the left navigation menu
2. On the menu, select Editing Templates
3. Click **Add** to create a new template
4. Select a Service Group
5. Provide a Template Name
6. Select the Template Type
7. Select the Editing Item Type
8. Configure the template options
9. When finished, click **Save**
10. To add another Template, click **Add**

Video – Creating Editing Templates
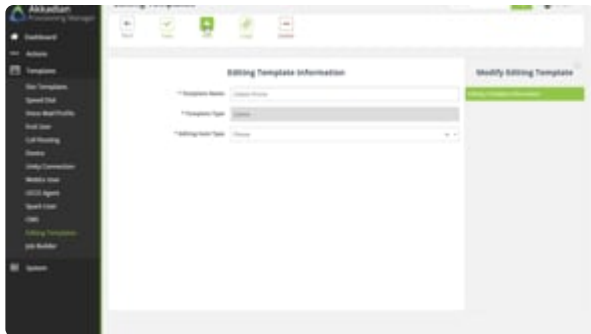
8.9 Site Templates

Site Templates are used to apply site based settings to provisioning jobs, drastically reducing the number of required templates and jobs in Provisioning Manager.

To add a Site Template:

1. Select **Site Templates** from the **Templates** menu
2. On the menu, click **Add** to create a new **Template**
3. If required, select a **Service Group**
4. Configure the Template based on your requirements
5. Assign **User Groups**
6. Click **Save**

Video – Site Templates

8.10 Jobs

Jobs are responsible for performing the provisioning tasks within Provisioning Manager. Jobs are made up of one or more templates to create a desired provisioning result. Provisioning Manager Jobs are very flexible and will vary depending on an organizations needs. This sections will provide general instructions and examples that can be applied to building Jobs in Provisioning Manager.

To add a Job:

1. Select **Job Builder** from the **Templates** menu
2. On the menu, click **Add** to create a new **Job**
3. If required, select a **Service Group**
4. Provide a Name for the Job
5. Choose a **Template Category**
6. Drag the first **Template** to the Job Builder pane

7. Add the placeholder(s)

Set Placeholders

Phone templates to add:

| 0 | ▾ |

Device Profile templates to add:

| 0 | ▾ |

Remote Destination Profile templates to add:

| 0 | ▾ |

Unity Voicemail templates to add:

| 0 | ▾ |

Line / Intercom templates to add: ☐ Group Lines

| 1 | ▾ |

WebEx User templates to add:
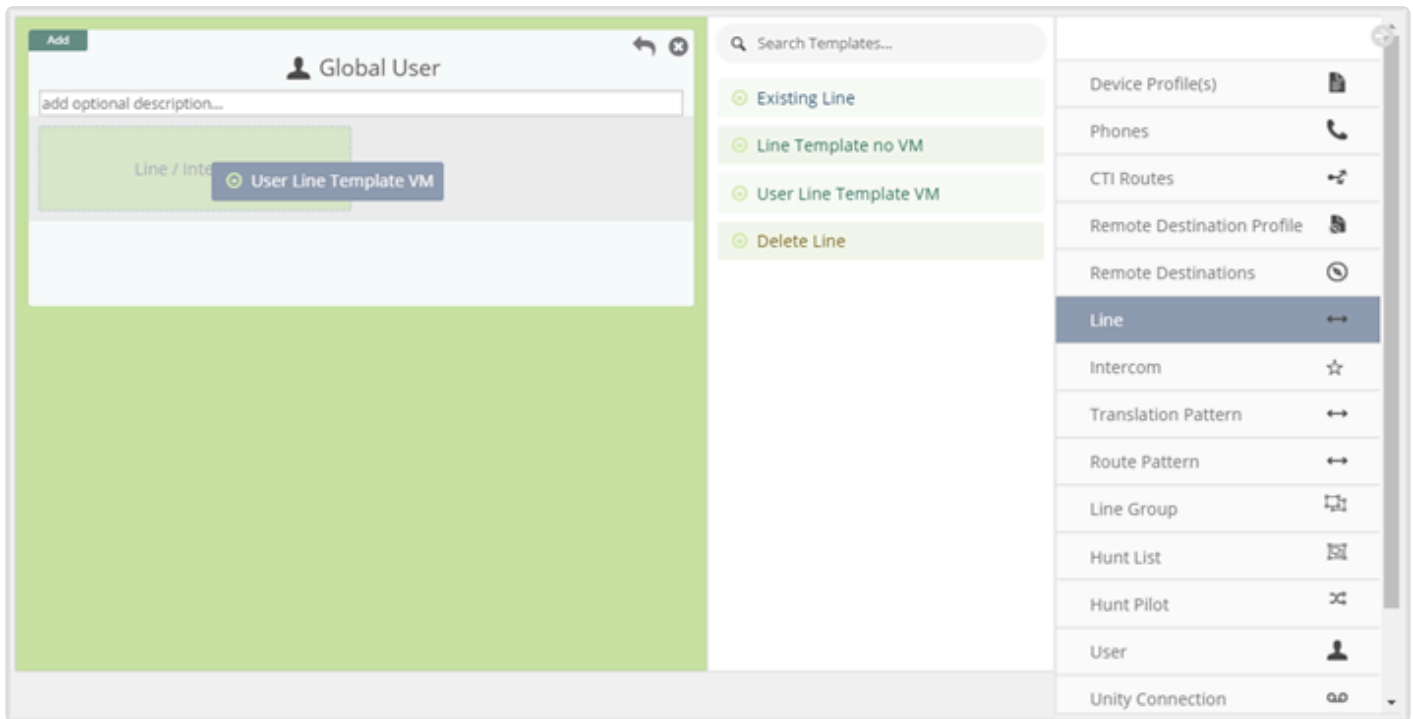
| 0 | ▾ |

Ucce Agent templates to add:

| 0 | ▾ |

Spark User templates to add:

| 0 | ▾ |

Translation Pattern templates to add:

| 0 | ▾ |

Route Pattern templates to add:

| 0 | ▾ |

User Profile templates to add:

| 0 | ▾ |

Delete   Continue

8. Drag the appropriate template(s) into the placeholder(s)

9. If required, set additional placeholder(s) or click Continue to skip adding additional Placeholders
10. Add any additional templates in the open placeholders
11. When complete, assign **User Groups** in the **Job Access** field
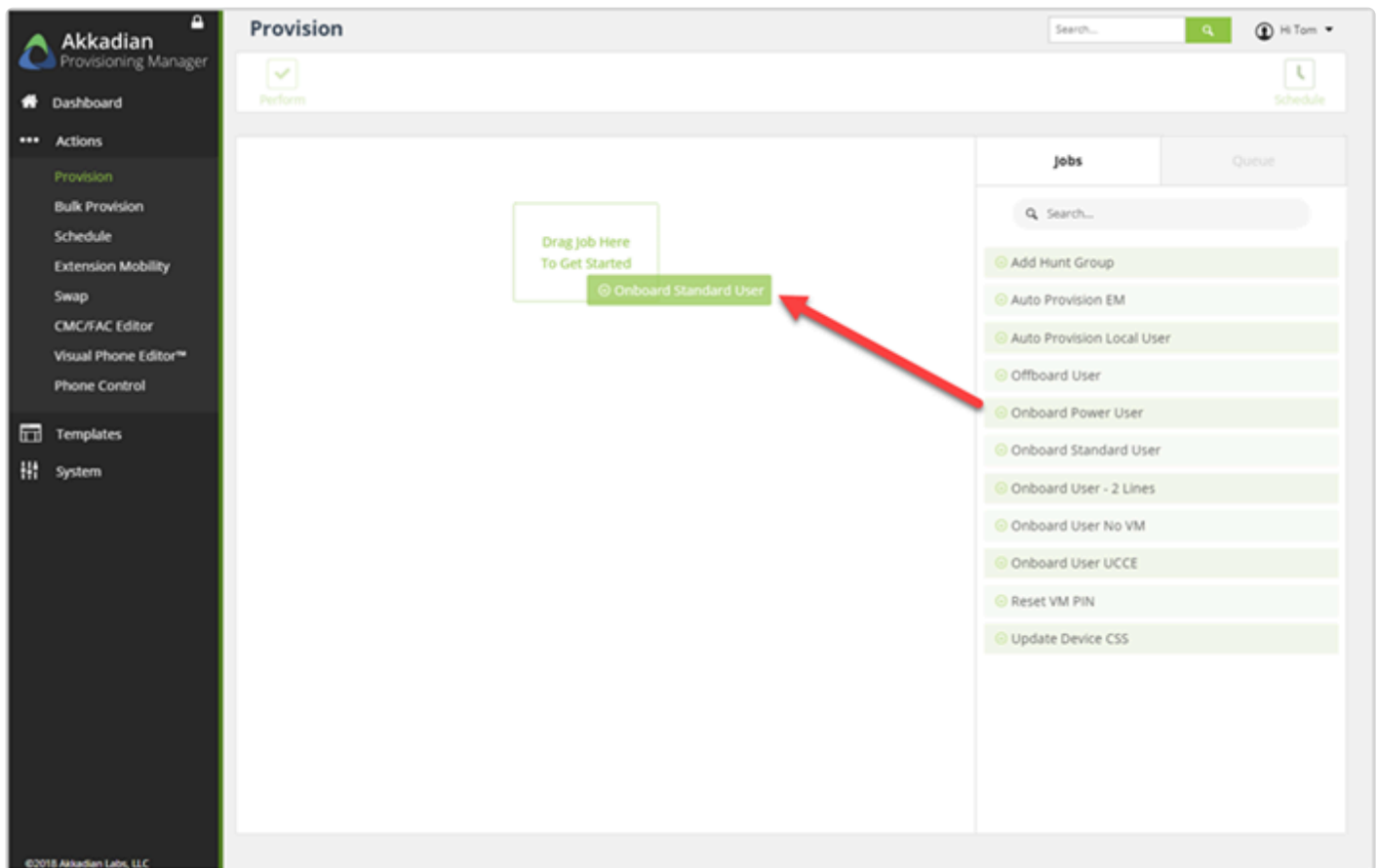12. Click **Save**

Video – Creating Jobs
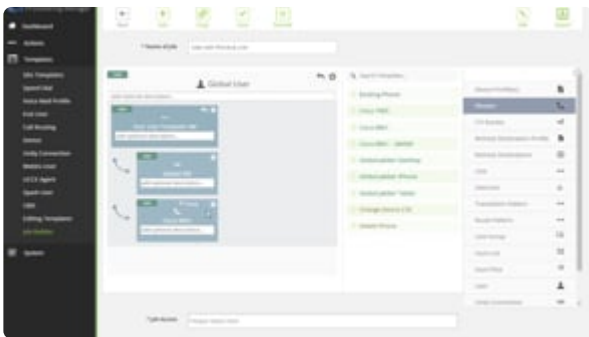
9. Actions

The Actions menu in Provisioning Manager provides access to provisioning as well as many other powerful tools. This section will cover how to use those functions.

9.1 Provisioning

After configuring the Jobs in Provisioning Manager, you are ready to start provisioning! The provisioning experience will vary depending on your Job configurations, so this section will provide general instructions for provisioning.

To begin provisioning:

1. Log into Provisioning Manager
2. From the **Actions** menu, select **Provision**
3. Select the **Job** from the list and drag it into the Provisioning window

4. Complete the provisioning form and click **Provision**

5. When the provision completes, the status will display in the queue
6. Click on **View Details** to see the Job details

7. In the view details pane, you can:
   - Email the Job details or summary
   - Drill-down on any of the Job steps
   - Rollback the Job, depending on the Job configuration

Provision Detail
Completed

- Action Name: Onboard Standard User
- Performed by: tbamert
- Date Performed: 04-05-2018 03:06:26 pm

Rollback

Action Results Detail:

- addLine   DIRECTORY NUMBER: \+16175457503
- updateUser   USERID: GBailey
- addPhone   PHONE NAME: SEPD1A423BF50F3
- addImportVoicemailUser   VM ALIAS: GBailey
- updateVoicemailUser   VM ALIAS: GBailey
- updateNotificationDevice   VM ALIAS: GBailey
- updateNotificationDevice   VM ALIAS: GBailey
- updateUser   USERID: GBailey
- updateUser   USERID: GBailey
- updateUser   USERID: GBailey

OK   **Email All Details**   **Email Summary**

Video – Provisioning
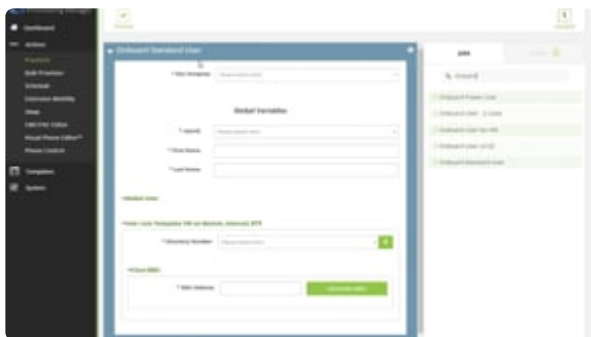
9.2 Bulk Provisioning

Provisioning Manager Jobs can also be used for bulk provisioning. Bulk provisioning can be run in real-time or scheduled.

> ✳ Currently Provisioning Manager only support bulk provisioning for Add and Delete Jobs.

To begin provisioning:

1. Log into Provisioning Manager
2. From the **Actions** menu, select **Bulk Provision**
3. Select the **Job** from the list and drag it into the Bulk Provisioning window
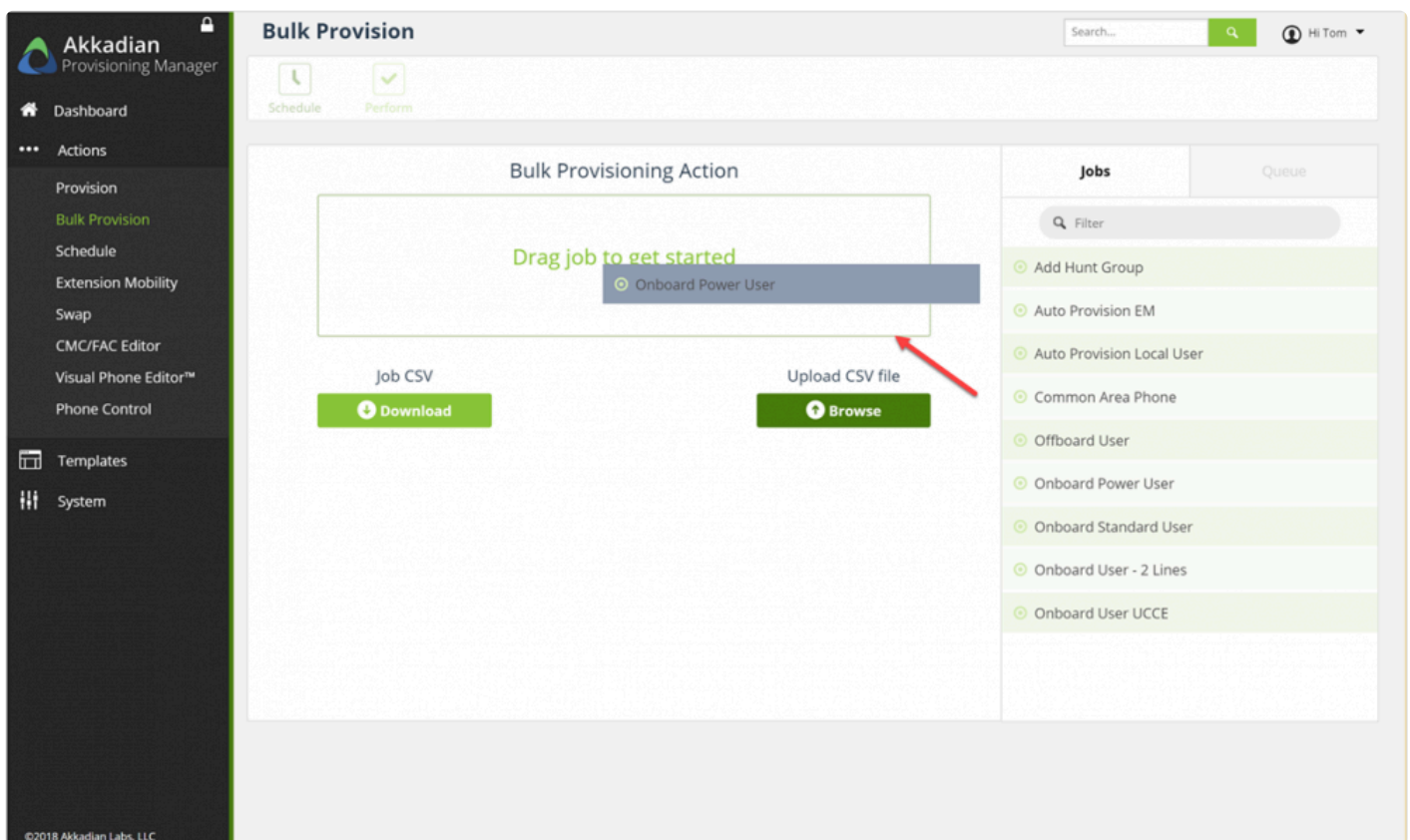
4. Click **Download** the Job CSV
5. Add entries to the CSV

✳ Several fields can be automatically populated using the "auto" parameter. See the examples below.

	A	B	C	D	E	F	G	H	I	J	K
1	=====DO NOT EDIT OR DELETE THIS SECTION=====										
2	eyJhY3Rpb25faWQiOiI1IiwidXNlcI9pZCI6IjIifQ==										
3	===========END METADATA==============										
4	Site Template		UserID	First Name	Last Name	Primary Extension	DN Pool Name	Directory Number	VM Extension	User ID	Overwrite Device 1	Assign Owner Id 1
5	Boston		Aphipps	Adam	Phipps	<auto_1>	Boston	<auto>	<auto_1>	APhipps		APhipps

Bulk Add Example

	A	B	C
1	=====DO NOT EDIT OR DELETE THIS SECTION=====		
2	eyJhY3Rpb25faWQiOiI3IiwidXNlcI9pZCI6IjIifQ==		
3	===========END METADATA==============		
4	CUCM User	Remove All Associated Elements	Remove Associated Shared Lines
5	aphipps	1	1
6			

Bulk Delete Example

1. Upload the CSV file
2. Click **Perform** to process the bulk provision or **Schedule** to process the Jobs at a specified date and time

Video – Provisioning
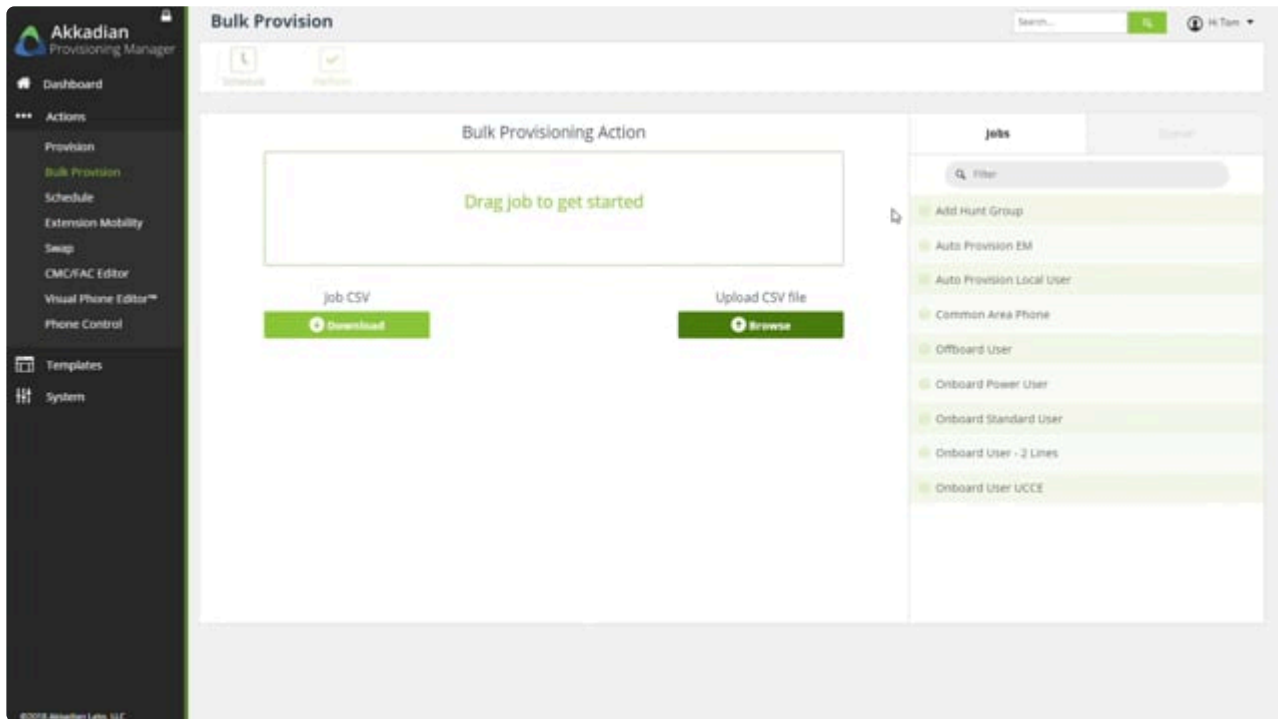
9.3 Schedule

Scheduling provides the ability to view, edit, add and delete scheduled provisioning actions directly from the scheduling window.

To use scheduling:

1. Select **Schedule** from the **Actions** menu
2. On the menu, click **Add** to schedule a job
3. Select the job type
4. For bulk provision select a CSV file from your local computer
5. Set the Date and Time to perform the job
6. Click **Add** to create the job in the queue

The schedule for any Job can be edited by clicking on the **Source Name** or the job can be deleted by checking the box next to the scheduled job you wish to delete and clicking the **Delete** button.

9.4 Extension Mobility

The Extension Mobility tool provides the ability to log users in or out of devices using the Cisco CUCM Extension Mobility service.

Extension Mobility Tool Requirements:

- The Provisioning Manager Application user must have "Authentication by Proxy" rights
- The CUCM Extension Mobility service must be activated and running
- The user and phone must be properly configured to support Extension Mobility

To use the Extension Mobility Tool:

1. Select **Extension Mobility** from the **Actions** menu
2. If prompted select the appropriate **Service Group**
3. If you wish to **"Search by End User"** select the check box
4. If you chose to **"Search by End User"**, locate the end user you wish to log in or out of a device
5. If the user is already logged into a device, the device will appear in the device list. The user can be logged out of the current device by selecting the **Log Out** button
6. If the user is not logged into a device, you can search for a device and log the user in by selecting the **Login** button

9.5 Swap

The Swap feature provides the ability copy configurations between various user components in CUCM. This Swap Tool can swap or copy configuration between:

- Devices – swap phones or device profiles of the same or different model
- Users – migrate device associations and ownership to a new user

The Swap feature can help perform common tasks without building a job.

Using the Device Swap Feature

The Device Swap tool provides the ability swap configurations between most phone and device profile models. This tool is very useful when you need to replace a user's phone or profile with the same or different model. Device swap will provision the new device, copy all applicable settings, apply device ownership and associated the new device with the user. The tool also provides the option to delete the old device upon successful completion of the swap. This feature can be equally as useful when adding a new device to a user as it will copy over pertinent settings and perform all proper associations.

> ✳ Swapping some newer phone models to older phone models may result in errors due to model incompatibility between the Max Call & Busy Trigger.

> ✳ Phone Swap supports Intercom lines, but the Intercom Line will always be removed from the source phone prior to the swap due to CUCM inability to support hared Intercom Lines.

> ✳ If the target device does not support the same number of lines or speed dials, they will show up as unassociated.

Using Device Swap:

1. Select **Swap** from the **Actions** menu
2. If required, select the appropriate **Service Group**
3. Select the Source Device Type: Phone or Device Profile
4. Locate the Source Device. This is the device you want to copy.

5. If you wish to delete the source device upon successful completion of the swap, select the "Delete source device after swap" checkbox
6. Select the Target Device Type. This is the model of the target device.
7. Select the Target Device Protocol. This may vary depending on the model.
8. Select the Target Device Template. The Template is used to configure required settings which are not available to be copied from the source device. For example, if you are going from a SCCP phone to SIP phone, the SIP profile will be configured using the Template.
9. Click **Perform** to complete the swap

> ✱ Templates used for Swap should not contain GVs.

> ✱ If the device is the same model and protocol, a template is not required.

10. Enter the device name or MAC address
11. Click **Perform** to complete the process

The End User Swap tool provides the ability to migrate all line and device associations from one user to another.

Using User Swap:

1. Select **Swap** from the **Actions** menu.
2. Select the End-User Swap Form Tab.
3. Select the appropriate Service Group.
4. Select the Source End User.
5. If you wish to delete the source user upon successful completion of the swap, select the "Delete source end-user after swap" checkbox.
6. Select "New User Account" to create and new user during the process or selecting and existing user as the target. Note – all existing associations will be removed from target user.
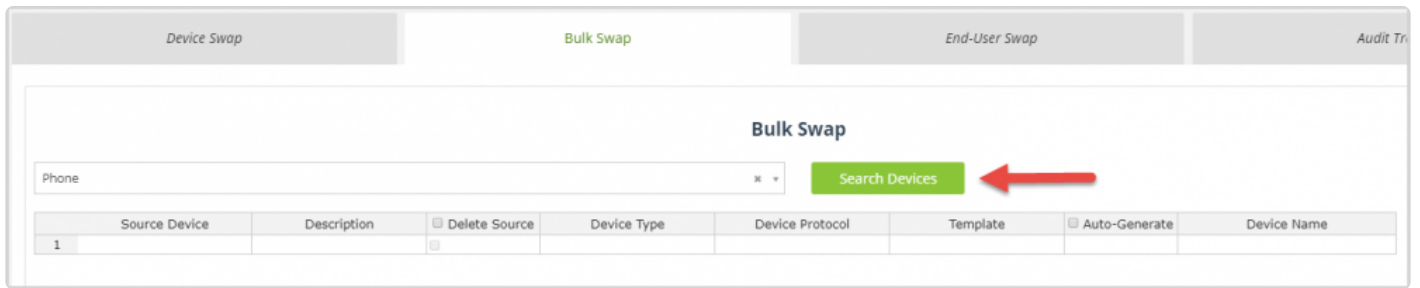7. Click **Perform** to complete the swap.

The Swap feature can also be used in bulk to migrate phones or device profiles. There are two methods to perform device swaps in bulk.

Method 1 – Bulk Swap using CSV Template:

1. Select **Swap** from the **Actions** menu
2. If required, select the appropriate **Service Group**
3. Select the Device Swap or End-User Swap tab
4. At this point, you can download the CSV template by clicking Export located at the top right corner of the page. Optionally you can proceed to populate the remaining fields and Export the template with all the settings prepopulated.
5. Populate the Exported CSV Template and when complete, click the Import button to upload the template.
6. Upon uploading the Template, the system will process the swaps. Do no close your browser or navigate away from the page
7. The process will complete and provide a summary of the processed items

Method 2 – Bulk Swap using Advanced Search:

1. Select **Swap** from the **Actions** menu
2. If required, select the appropriate **Service Group**
3. Select the **Bulk Swap** Tab
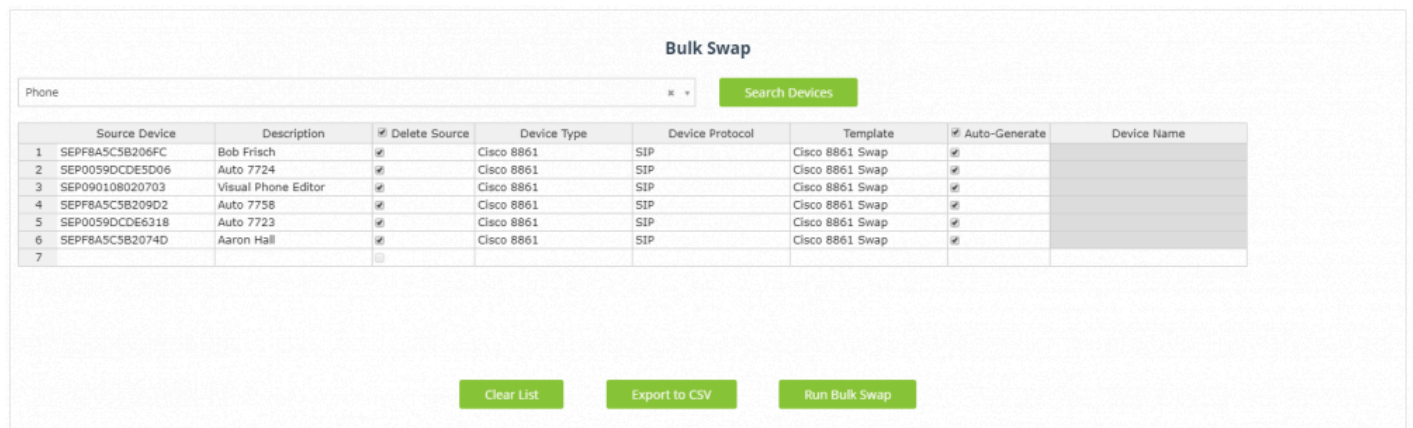4. Click the **Search Devices** button

5. Search for the phones to be swapped using the Search Phones section.

6. As devices are located, you may click **"Add to List"** and repeat the search for more devices to be added to the list. Alternatively, click the **"Add to List and Close"** button to complete adding to the list and return to the Bulk Swap page.

7. On the Bulk Swap page, click "Run Bulk Swap" to process the swap for all devices in the list. Alternatively, you can select "Export to CSV" to process the job later.

Search Phone

Find Phone where:

Device Pool ▾	Contains ▾	Boston	➕
Device Type ▾	Contains ▾	8861	➖
	Please Select Item ▾		

[Search] [Clear Search]

Show [▾] entries

☑	Phone Name	Phone Model	Phone Protocol	Device Pool ▾	Phone Description
☑	SEPF8A5C5B206FC	Cisco 8861	SIP	Boston_DP	Bob Frisch
☑	SEP0059DCDE5D06	Cisco 8861	SIP	Boston_DP	Auto 7724
☑	SEP090108020703	Cisco 8861	SIP	Boston_DP	Visual Phone Editor
☑	SEPF8A5C5B209D2	Cisco 8861	SIP	Boston_DP	Auto 7758
☑	SEP0059DCDE6318	Cisco 8861	SIP	Boston_DP	Auto 7723
☑	SEPF8A5C5B2074D	Cisco 8861	SIP	Boston_DP	Aaron Hall

Showing 1 to 6 of 6 entries

First   Previous   **1**   Next   Last

[Add to List] [Add to List and Close] [Close]

9.6 CMC/FAC Editor

The Provisioning Manager CMC/FAC Editor can be used to edit existing Client Matter and Forced Authorization Codes.

Using the CMC/FAC Editor:

1. Select **CMC/FAC Editor** from the **Actions** menu
2. If required, select the appropriate **Service Group**
3. Select the Code Type
4. Edit the appropriate fields
5. When finished, click **Save**

✳ If CMC or FAC Rules are enabled, please remember that editing the Description field for CMCs and the Name field for FACs may break the link between the user and the code.

9.7 Visual Phone Editor

Visual Phone Editor provides the ability to visually edit a phone or device profile. Visual Phone Editor support the following functions:

- Change phone button template for device
- Associating existing lines to the device
- Edit Line on Device settings for lines on the device
- Rearrange lines using drag and drop
- Rearrange speed dials using drag and drop

Using Visual Phone Editor:

1. Select **Visual Phone Editor** from the **Actions** menu
2. If required, select the appropriate **Service Group**
3. Search for and select the device to edit
4. Perform the desired edit actions using Visual Phone Editor
5. When finished, click **Perform** to apply the changes

Visual Phone Editor™

✔
Perform

Phone: [SEPAD79CA4A48DD] [Cisco 8861] George Bailey   ✕ ▾

Phone Button Templates: 8861 3LN   ✕ ▾

1   ◠ \+16175457506

2   ◠ <LINE>

3   ◉ <SPEED DIAL>

4   ◉ <SPEED DIAL>

5   ◠ <LINE>

9.8 Phone Control

Provisioning Manager Phone Control provides the ability to remotely validate Cisco phone functionality, view remote Cisco phone displays, navigate softkeys or place test calls, without the need for physical presence.

Requirements

- IP connectivity on TCP port 80 to target Cisco IP Phone
- CUCM Application user who is a member of the Standard Server Monitoring and Standard TabSync User groups.
- Web access enabled on the Cisco IP Phone (Provisioning Manager will automatically enable web access if currently disabled)
- Assign Phone Control role to appropriate Provisioning Manager Security Groups
- One of the following phone models:

6921, 6941, 6945, 6961, 7821, 7841, 7861, 7905, 7906, 7911, 7912, 7925, 7926, 7937, 7940, 7941, 7942, 7945, 7960, 7961, 7962, 7965, 7970, 7971, 7975, 8811, 8831, 8841, 8845, 8851, 8861, 8865, 8941, 8945, 8961, 9951, 9971

Configuring Phone Control:

1. Select **Application Servers** from the **System** menu.
2. Select the **Communications Manager** Tab.
3. Select the CUCM application server on which to configure Phone Control.
4. Add the Phone Control username and password in the Phone Control Information section
5. When finished, click **Save**

Using Phone Control:

1. Select **Phone Control** from the **Actions** menu
2. Select the appropriate **Service Group** from the list
3. Locate the Phone using search

Provisioning Manager will check if the phone meets the following requirements:

- The phone has Web Access
- The phone is associated to the Phone Control application user

> ✳ If either of these requirements are not met, Provisioning Manager will prompt to automatically enable on or both options.

4. Once the phone is prepared for connection, Phone Control will automatically connect to the device.
5. When connected, use the Phone Control buttons to control the device. Please note the screen refresh is not real-time and by default refreshes every 5 seconds.

10. Automation

Provisioning Manager offers several out of the box automation solutions which can help fully automate your provisioning process.

Auto-Provisioning with Active Directory – Provisioning Manager can integrate with Active Directory, monitor for new users and automatically provision these users in your UC environment.

Auto-delete Phones – Provisioning Manager can monitor the registration status of devices and based on configurable triggers, can automatically delete devices that have not been registered, reducing license consumption and keeping your system clean.

Auto-deprovisioning – Provisioning Manager can work in conjunction with LDAP integrated users in CUCM and automatically deprovision users and their services.

This section will cover the process of configuring these options in Provisioning Manager.

10.1 Auto-provision

Provisioning Manager provides the ability to integrate with Active Directory and provision accounts based on Active Directory groups. Configuring auto-provisioning with Active Directory requires four steps:

1. **Configure LDAP agreements** – the LDAP agreement is used to access Active Directory. Multiple LDAP agreements may be used with auto provisioning.
2. **Enable Active Directory Auto-provision** – enable the Auto-provisioning service in the Service Group(s) and set the default LDAP agreement.
3. **Configure Auto Provisioning tasks** – Auto Provisioning tasks are used to map Active Directory attributes to Provisioning Manager data. Multiple Auto Provisioning tasks may be configured to provide flexibility.
4. **Schedule Auto Provisioning tasks** – Auto Provisioning tasks must be scheduled to process provisioning tasks.

Step 1 – Configure LDAP Agreements:

Configure an LDAP agreement(s) that will provide Provisioning Manager access to the new users accounts to be auto-provisioned. Reference the LDAP topic in the Initial Configuration section.

Step 2 – Enable Active Directory Auto-provision

1. Select **Service Groups** from the **System** menu
2. In the list, click Service Group Name to edit the item
3. Navigate to the **Active Directory Auto-provision** section
4. Check the **Enable AD Auto-provision** box
5. Choose the Default LDAP server
6. Configure Default Username Bind Attribute
7. When finished, click **Save**

Step 3 – Configure Auto-provisioning Job:

1. Log into Provisioning Manager with an Administrator account
2. Select **Automation** from the **System** menu
3. Click on *Add *to configure a new Auto-provision Job
4. If required, choose a Service Group
5. Provide a name for the Job
6. Check enable (This will enable the task to run once scheduled)

7. Choose the LDAP agreement for this Job
8. Set the **Username Bind Attribute** (This is the attribute used to locate the user to be provisioned)
9. Select a Job for Auto-provisioning by dragging it into the **Attribute Mapping** section
10. Map the Job fields to an AD Attribute. Check to enter custom local values

11. Optionally, configure AD filters to narrow down the search

Step 4 – Scheduling the Auto-provision Jobs:

1. Select **Schedule** from the **Actions** menu
2. On the menu, click **Add** to schedule a job
3. Select the Auto-provision type
4. Select the Auto-provision task
5. Choose the frequency to run the task
6. Choose the starting date of the task
7. Set the task run time
8. Set the notification email
9. Set the **Process all accounts within the last** value. (The task will only process accounts with a create date included in this period)
10. Click **Add** to schedule the task

The schedule for any Job can be edited by clicking on the **Source Name** or the job can be deleted by checking the box next to the scheduled job you wish to delete and clicking the **Delete** button.

Schedule

	Source Name	Service Group	Template	User	Type	Frequency	Run Time	Status
☐	Auto-provision EM Local	CSR11	Auto Provision Local User	tbamert	Auto-provision	DAILY	**Processed** (Details)	✓
☐	Remove Test Phones	CSR11	Onboard Standard User	tbamert	Auto-delete	DAILY	**Processed** (Details)	✓
☐	Auto EM Users	CSR11	Auto Provision EM	tbamert	Auto-provision	DAILY	**Processed** (Details)	✓
☐	Auto EM Users NYC	CSR11	Auto Provision EM	tbamert	Auto-provision	DAILY	**Processed** (Details)	✓

Showing 1 to 4 of 4 entries

First   Previous   1   Next   Last

Dashboard

Actions

Provision
Bulk Provision
Schedule
Extension Mobility
Swap
CMC/FAC Editor
Visual Phone Editor™
Phone Control

Templates

System

Show 15 entries

Delete   Refresh   Add   Manual Run

Hi Tom

10.2 Auto-delete Phone

The Provisioning Manager Auto-delete phone feature can monitor the registration status of phones over a period of time and delete phones that exceed a configured unregistered term.

To Configure Auto-provisioning Job:

1. Log into Provisioning Manager with an Administrator account
2. Select **Automation** from the **System** menu
3. Click on the **Auto-delete Phone** tab
4. Click *Add *to configure a new Auto-delete phone task
5. Configure the Name
6. Check enable (This will enable the task to run once scheduled)
7. Set the **"Not registered in the last"** period
8. Choose the **Action**
9. Choose the **"Update frequency (Hours)"** (This is how often the system will check the device registration status)
10. Configure the **Phone Filters** sections

> ❗ It is important to configure proper filters so no phones are unintentionally deleted. We recommend setting the Action method to report only for new tasks to verify the outcome.

11. Click **Save** to complete the configuration
12. Repeat the process to create additional tasks

Scheduling the Auto-delete phone Jobs:

1. Select **Schedule** from the **Actions** menu

2. On the menu, click **Add** to schedule a job

3. Select the Auto-delete type

4. Select the Auto-delete task

5. Choose the frequency to run the task

6. Choose the starting date of the task

7. Set the task run time

8. Set the notification email

9. Click **Add** to schedule the task

The schedule for any Job can be edited by clicking on the **Source Name** or the job can be deleted by checking the box next to the scheduled job you wish to delete and clicking the **Delete** button.

Schedule

Akkadian
Provisioning Manager

- Dashboard
- **...** Actions
  - Provision
  - Bulk Provision
  - Schedule
  - Extension Mobility
  - Swap
  - CMC/FAC Editor
  - Visual Phone Editor™
  - Phone Control
- Templates
- System

[Delete] [Refresh] [Add]   [Manual Run]

Search... [🔍]   Hi Tom ▼

Show 15 entries

	Source Name	Service Group	Template	User	Type	Frequency	Run Time	Status
☐	Auto-provision EM Local	CSR11	Auto Provision Local User	tbamert	Auto-provision	DAILY	Processed (Details)	✔
☐	Remove Test Phones	CSR11	Onboard Standard User	tbamert	Auto-delete	DAILY	Processed (Details)	✔
☐	Auto EM Users	CSR11	Auto Provision EM	tbamert	Auto-provision	DAILY	Processed (Details)	✔
☐	Auto EM Users NYC	CSR11	Auto Provision EM	tbamert	Auto-provision	DAILY	Processed (Details)	✔

Showing 1 to 4 of 4 entries

First   Previous   **1**   Next   Last

Search Source Name · Search Service Group · Search Template · Search User · Search · Search Freq · Search R

11. Report Builder

Report Builder is a powerful custom reporting tool which allow Administrators to use SQL database queries to generate reports from Cisco Communications Manager.

Browsing the Communications Manager Database:

1. Log into Provisioning Manager as an Administrator
2. Select **Report Builder** from the **System** menu
3. Select a **Service Group**
4. Search for a database table or select on from the list
5. Click on the table name to view the table schema
6. Click on either Custom Query or Visual Query to build a report (Visual Query will provide visual guidance constructing an SQL query)

7. User Visual Query to build the desired query and click **Run Query**

8. Provide a report name and title
9. Select the Enable checkbox to enable the report for scheduling
10. Click **Save** to save the report in the Report List
11. Optionally click on **Export CSV** to export the result

Scheduling a Report

Any Report that has been enabled can be scheduled. To schedule a report:

1. In the Reporting Manager menu select Schedule
2. Click **Add**
3. Select the **Report**
4. Select the **Frequency**
5. Set the **Starting Date**
6. Set the run **Time**
7. Set the **Notification Email** where the report will be delivered
8. (Optional) Add an **Email List**

⏰ Schedule Report   ✕

* **Report**   End User Report ▾

* **Frequency**   Daily ▾

* **Starting Date**   04/06/2018

* **Time**   1 ▾   00 ▾   AM ▾

* **Notification Email**   email@company.com

Email List   Choose

▶ Save   ✖ Close