



Avaya Aura® System Manager 7.0 LDAP Directory Synchronization Whitepaper

Issue 1.5

February, 2016

Contents

1. Introduction	3
2. LDAP Sync Description	3
3. LDAP Sync Configuration	7
4. LDAP Sync Job Execution	17
5. Synchronization History and Job Status.....	19
6. Stop Synchronization Running Job.....	20
7. Delete Synchronization Jobs.....	21

1. INTRODUCTION

This Whitepaper provides comprehensive details on implementing System Manager and Enterprise Lightweight Directory Access Protocol (LDAP) Directory Integration for User Management.

System Manager synchronizes with Lightweight Directory Access Protocol (LDAP) Directory Servers to enable user provisioning by enterprise directory applications. The following LDAP Directory Servers are supported:

- Active Directory 2003, 2008, and 2012
- OpenLDAP 2.4.21
- IBM Domino 7.0
- Novell eDirectory 8.8
- SunOne Directory/Java System Directory 6.3.

System Manager LDAP synchronization can be executed on demand or on a scheduled basis. When using the System Manager scheduler, there is a limit of 90 simultaneous jobs.

System Manager supports a single domain from any LDAP synchronization source. As such, LDAP forests, trees, and multiple domains from a single data source are not supported. System Manager is able to synchronize users from multiple LDAP sources as long as different BaseDNs are used.

System Manager 7.0 introduces the ability to synchronize Active Directory Roles as defined in a customer's LDAP Directory to System Manager Administrator Roles. This new capability includes both pre-defined system roles as well as custom roles on SMGR. The User Interface for provisioning Admin Group – SMGR Role synchronization will be available as an extension to synchronization interface used to define LDAP User Syncs where you map LDAP fields to SMGR User fields. For more detail please see the Optional Attribute 'userRoles'

2. LDAP SYNC DESCRIPTION

System Manager synchronizes with LDAP Directory Server as follows:

- Five mandatory attributes must be synced from the LDAP Directory Server to System Manager. The five mandatory System Manager attributes are:
 1. sourceUserKey (used to uniquely identify a user)
 2. loginName (used as the System Manager login name)
 3. surname
 4. givenname
 5. displayName

- For most of the optional System Manager attribute, the mapping direction can be from LDAP Directory Server or to LDAP Directory Server, but not both directions. Regardless of the mapping direction, LDAP attributes can be edited in System Manager. However, if these attributes are synced from the LDAP Directory Server, then any changes made in System Manager will be overwritten on the next synchronization.
- The order of synchronization will be from LDAP Directory Server to System Manager, followed by from System Manager to LDAP Directory Server.

For attributes that are synced from LDAP Directory Server to System Manager, Table 1 shows a number of scenarios and the results of the synchronization.

Scenario	Condition	Result
New user created in LDAP Directory Server.	User is part of filter criteria.	New user synchronized into System Manager.
Filter criteria modified	User removed from filter criteria and “Allow Deletion” checkbox is checked.	User not part of filter criteria will be permanently deleted in System Manager.
New user created in LDAP Directory Server or user already exists	User is part of filter criteria and User (same login name) already exists in System Manager	The user is merged in System Manager with the attribute values in LDAP Directory Server.
New user created in LDAP Directory Server or user already exists	User is part of filter criteria and User (same login name) already exists in System Manager but is soft deleted.	The user is not merged in System Manager.
Attribute updated in LDAP Directory Server.	Attribute included in datasource mapping.	Attribute updated in System Manager.
Attribute updated in System Manager.		Attribute will not be updated in LDAP Directory Server. On next synchronization, value in LDAP Directory Server will overwrite changes made in System Manager.
User deleted in LDAP Directory Server.	The “Allow Deletion” checkbox is checked for that datasource and no change has been made in filter criteria.	User permanently deleted in System Manager.
User deleted in LDAP Directory Server.	The “Allow Deletion” checkbox is not checked for that datasource.	User is not deleted in System Manager ¹ .

¹ To delete this user, administrator will need to check the “Allow Deletion” checkbox and perform synchronization.

User soft deleted in System Manager.		User will not be deleted in LDAP Directory Server. The user will fail with “user already exists” error.
User permanently deleted in System Manager.		User will not be deleted in LDAP Directory Server. Instead, user will be created in System Manager at next synchronization.

Table 1: Attributes Synced from LDAP Directory Server to System Manager

For attributes that are synced from System Manager to LDAP Directory Server, Table 2 shows a number of scenarios and the results of the synchronization.

Scenario	Condition	Result
New user created in System Manager.	Datasource mapping does not support synchronization of new user from System Manager to LDAP Directory Server.	New user is not created in LDAP Directory Server.
Attribute updated in LDAP Directory Server.	Attribute included in datasource mapping but sync is in the other direction.	Attribute will not be updated in System Manager. On next synchronization, value in System Manager will overwrite changes made in LDAP Directory Server.
Attribute updated in System Manager.	Attribute included in datasource mapping.	Attributes updated in LDAP Directory Server.

Table 2: Attributes Synced from System Manager to LDAP Directory Server

3. LDAP SYNC CONFIGURATION

Perform the following steps to configure a connection between System Manager and an LDAP Directory Server:

1. Log on to System Manager with administrator privileges.
2. On the Common Console page, click on “Directory Synchronization” (Figure 1).



Figure 1: System Manager Common Console

3. On the “User Synchronization” page, click **New** to create a datasource for System Manager to synchronize with (Figure 2).

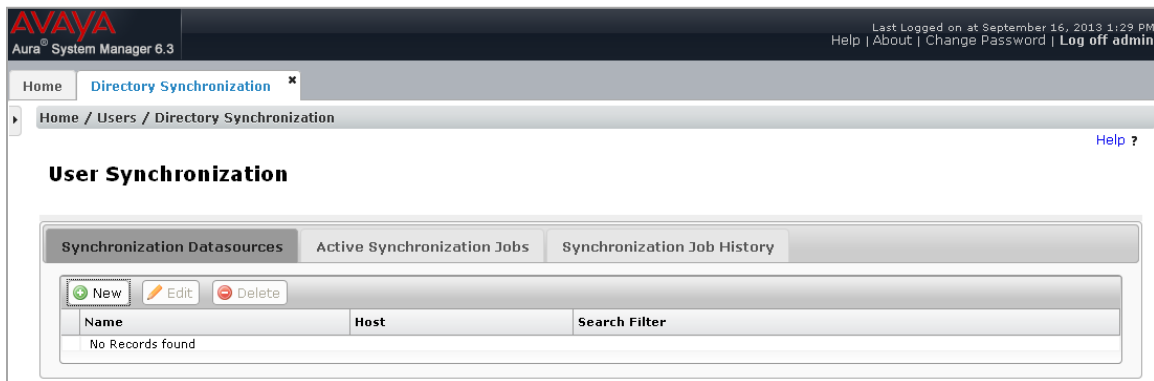


Figure 2: User Synchronization Page

4. On the “New User Synchronization Datasource” page, enter the required Directory Parameters (Figure 3). Table 3 describes the datasource parameters and provides example values.

AVAYA
Aura® System Manager 6.3

Last Logged on at September 16, 2013 1:29 PM
Help | About | Change Password | Log off admin

Home Directory Synchronization x

Home / Users / Directory Synchronization

New User Synchronization Datasource

Help ?

Save Cancel

Directory Parameters

* Datasource Name

* Host

* Principal

* Password

* Port

* Base Distinguished Name

* LDAP User Schema

Search Filter

Use SSL ☐

Allow Deletions ☐

Test Connection

Attribute Parameters

You must verify your LDAP connection before mapping attributes

Save Cancel

Figure 3: New User Synchronization Datasource Page

Connection Parameter	Example Values	Comment
Datasource Name	Win2K8AD	Create a name to identify the LDAP Directory Server. This name will be required to create a sync job.
Host	148.147.163.131	IP Address or host name of the directory server you want to sync users with.
Principal	CN=Administrator,CN=Users,DC=pansv8,DC=platform,DC=avaya,DC=com	LDAP Directory Server user name that has write permissions to create/update users.
Password	<password>	Password of the Principal (user name above) to access LDAP Directory Server.
Port	389	LDAP Directory Server port number to enable System Manager connectivity. Default values are 389 for non-SSL connection and 636 for SSL connection.
Base Distinguished Name	CN=Users,DC=pansv8,DC=platform,DC=avaya,DC=com	Base DN is an element that works in conjunction with the search scope. It's the tree from which users are synced. The sub trees are not considered for syncing the users.
LDAP User Schema	inetOrgPerson	Schema defines the object classes. The object class definitions define the list of attributes that must contain values and the list of attributes that may contain values. Definitions differ depending on your LDAP Directory Server. Default value is inetOrgPerson.
Search Filter	(cn=Alex*) ²	Search filter provides a mechanism for defining the criteria for matching entries in a LDAP search operation. For information about search filter, see http://msdn.microsoft.com/en-us/library/windows/desktop/aa746475(v=vs.85).aspx
Use SSL	False (unchecked)	Checkbox to use SSL. The Appendix A describes the steps to setup SSL connection.
Allow Deletions	False (unchecked)	Checkbox to have System Manager delete previously sync users that have been deleted in the LDAP Directory Server.

Table 3: Datasource Parameters

² To search all users, use (cn=*) as the search criteria.

5. Click **Test Connection**. If the parameters that you enter are incorrect, the test fails and System Manager returns an error message (Figure 4).

AVAYA
Aura System Manager 6.3

Last Logged on at September 16, 2013 1:29 PM
Help | About | Change Password | Log off admin

Home Directory Synchronization x

Home / Users / Directory Synchronization

Status

New User Synchronization Datasource Save Cancel

The following errors have occurred:
Either the principal or password is incorrect for connecting to this data source

Directory Parameters

* Datasource Name Win2K8AD

* Host 148.147.163.131

* Principal m,DC=avaya,DC=com

* Password

* Port 389

* Base Distinguished Name CN=Users,DC=pansv

* LDAP User Schema inetOrgPerson

Search Filter (cn=Alex*)

Use SSL ☐

Allow Deletions ☐

Test Connection

Attribute Parameters

Add Mapping

Figure 4: Test Connection Failure Error Message

6. Once the connection test is successfully completed, the “New User Synchronization Datasource” page will expand to enable the administration of Attribute Parameters (Figure 5).

Figure 5: New User Synchronization Datasource Page after Success of Test Connection

7. Configure the five mandatory attribute mappings. These attributes are grayed out and can only be synced from the LDAP Directory Server to System Manager (Table 4).

LDAP Attribute ³	System Manager Attribute	Detail	Mandatory or Optional
objectGUID	sourceUserKey	Attribute that uniquely defines a user.	Mandatory
userPrincipalName	loginName	System Manager login name. Note: If Microsoft Active Directory is used for external authentication with System Manager, the attribute userPrincipalName of the user in the external server must contain a valid value.	Mandatory
sn	surname	User last name.	Mandatory
givenName	givenName	User first name.	Mandatory
displayName	displayName	User display name.	Mandatory

Table 4: Mandatory Attributes

³ The LDAP attributes shown are examples. Customers can use different LDAP attributes to map against the System Manager attributes. The only requirement is the LDAP attributes contain valid values.

8. Click Add Mapping to configure optional attribute mappings (Table 5 and Figure 6). Configuration is done by choosing the LDAP attribute, the sync direction, the System Manager attribute.

LDAP Attribute	System Manager Attribute	Detail	Mandatory or Optional
middleName	middleName	User middle name.	Optional
msDS-PhoneticLastName	surnameascii	User last name in ascii format	Optional
msDS-PhoneticFirstName	givennameascii	User first name in ascii format	Optional
msDS-PhoneticDisplayName	endPointDisplayName	User endpoint display name	Optional
postalCode	postalCode	Postal or zip code.	Optional
streetAddress	streetAddress	Street address.	Optional

LDAP Attribute	System Manager Attribute	Detail	Mandatory or Optional																												
preferredLanguage	preferredLanguage	<div>User preferred language. LDAP preferredLanguage attribute mapping must be in following format: “LanguageCode_CountryCode” The format for the supported languages are:</div> <table><thead><tr><th>Language</th><th>Supported Format</th></tr></thead><tbody><tr><td>English (United States)</td><td>en_US</td></tr><tr><td>Chinese (Simplified)</td><td>zh_CN</td></tr><tr><td>Japanese (Japan)</td><td>ja_JP</td></tr><tr><td>Korean (Korea)</td><td>ko_KR</td></tr><tr><td>French (France)</td><td>fr_FR</td></tr><tr><td>German (Germany)</td><td>de_DE</td></tr><tr><td>Italian (Italy)</td><td>it_IT</td></tr><tr><td>Russian (Russia)</td><td>ru_RU</td></tr><tr><td>English (United Kingdom)</td><td>en_GB</td></tr><tr><td>Spanish (Mexico)</td><td>es_MX</td></tr><tr><td>Portuguese (Brazil)</td><td>pt_BR</td></tr><tr><td>French (Canada)</td><td>fr_CA</td></tr><tr><td>English (Canada)</td><td>en_CA</td></tr></tbody></table>	Language	Supported Format	English (United States)	en_US	Chinese (Simplified)	zh_CN	Japanese (Japan)	ja_JP	Korean (Korea)	ko_KR	French (France)	fr_FR	German (Germany)	de_DE	Italian (Italy)	it_IT	Russian (Russia)	ru_RU	English (United Kingdom)	en_GB	Spanish (Mexico)	es_MX	Portuguese (Brazil)	pt_BR	French (Canada)	fr_CA	English (Canada)	en_CA	Optional
Language	Supported Format																														
English (United States)	en_US																														
Chinese (Simplified)	zh_CN																														
Japanese (Japan)	ja_JP																														
Korean (Korea)	ko_KR																														
French (France)	fr_FR																														
German (Germany)	de_DE																														
Italian (Italy)	it_IT																														
Russian (Russia)	ru_RU																														
English (United Kingdom)	en_GB																														
Spanish (Mexico)	es_MX																														
Portuguese (Brazil)	pt_BR																														
French (Canada)	fr_CA																														
English (Canada)	en_CA																														
roomNumber	room	Room number.	Optional																												
co	country	Country.	Optional																												
telephoneNumber	businessPhone	Business telephone number.	Optional																												
otherTelephone	otherBusinessPhone	Other business telephone number.	Optional																												

LDAP Attribute	System Manager Attribute	Detail	Mandatory or Optional
facsimileTelephoneNumber	fax	Facsimile or fax number.	Optional
homePhone	homePhone	Home telephone number.	Optional
otherHomePhone	otherHomePhone	Other home telephone number.	Optional
mobile	mobilePhone	Mobile or cellular number.	Optional
otherMobile	otherMobilePhone	Other mobile or cellular number.	Optional
pager	pager	Pager number.	Optional
otherPager	otherPager	Other pager number.	Optional
givenName	preferredGivenName	Given or first name.	Optional
o	organization	Organization.	Optional
department	department	Department.	Optional
employeeID	employeeNo	Employee number.	Optional
st	stateOrProvince	State or province.	Optional
l	localityName	Locality or location.	Optional
displayName	localizedName	User name in local language. Make sure that the LDAP attribute mapping to localizedName is in the format of "Locale.Name". For example, if the locale is English and name is Alex, then the value for displayName here should be "en.Alex".	Optional
msExchHouseldentifier	Microsoft Exchange Handle	Microsoft Exchange communication address for the user for communication with Microsoft SMTP Server.	Optional
o	Microsoft OCS SIP Handle	Microsoft OCS SIP communication address for the user to support OCS SIP-based communication.	Optional
manager	IBM Sametime Handle	IBM Sametime communication address for user to support IBM Sametime. The format should be of type DN=IBMHandle	Optional

LDAP Attribute	System Manager Attribute	Detail	Mandatory or Optional
I	User Provisioning Rule	<p>The user provisioning rule that the user uses. You can map the user provisioning rule to more than one LDAP attribute. However, you cannot map the same LDAP attribute more than once.</p> <p>The user provisioning rule data synchronizes from the LDAP directory server to System Manager only. The value of multiple attribute mapping will be joined by “_” (underscore) to map with value in SMGR.</p> <p>The Appendix B describes the steps to setup User Provisioning Rule.</p> <p>Note: If you map the telephone Number (Avaya E164 handle) and UPR in datasource and the LDAP attribute values change in LDAP, during next synchronization, the system updates only the Avaya E164 handle. The system does not update the Communication Manager extension or SIP handle that is configured in UPR.</p>	Optional
telephoneNumber	Phone Number	<p>Phone Number is mapped to Avaya E164 handle.</p> <p>The value for extension is the last “N” digit value of attribute on User Provisioning Rule page “Use Phone Number last ... digits for Extension”.</p>	Optional
otherMailbox	Mailbox Number	The Messaging mailbox number.	Optional
telexNumber	CS1000 Extension	<p>The extension on CS 1000 server.</p> <p>The data synchronizes from System Manager to the LDAP directory server only.</p>	Optional
primaryTelexNumber	Communication Manager Extension	<p>The extension on Communication Manager.</p> <p>The data synchronizes from System Manager to the LDAP directory server only.</p>	Optional
memberOf	userRoles	<p>The userRoles attribute can either mapped to:</p> <ol style="list-style-type: none"> Groups in LDAP. For example in AD the attribute memberOf contains the fully qualified group name, say CN=DnsAdmin,CN=Users,DC=avaya,DC=com. In this case system will search for role name as DnsAdmin. Other LDAP attribute: System will search for exact name with the value in LDAP attribute to match with role in System Manager. 	Optional

Table 5: Optional Attributes

Directory Parameters

* Datasource Name Win2K8AD

* Host 148.147.163.131

* Principal CN=Administrator,CN=

* Password *****

* Port 389

* Base Distinguished Name CN=Users,DC=pansv

* LDAP User Schema inetOrgPerson

Search Filter (cn=Alex*)

Use SSL ☐

Allow Deletions ☐

Test Connection

Attribute Parameters

Add Mapping

objectGUID	->	sourceUserKey	
userPrincipalName	->	loginName	
sn	->	surname	
givenName	->	givenName	
displayName	->	displayName	
Choose LDAP Attribute	->	Choose SMGR Attribute	Remove

Save Cancel

Figure 6: Optional Attribute Mapping

9. Save the configuration. The LDAP Directory Server will appear in the “Synchronization Datasource” table (Figure 7).

AVAYA
Aura System Manager 6.3

Last Logged on at September 16, 2013 1:29 PM
Help | About | Change Password | Log off admin

Home Directory Synchronization

Home / Users / Directory Synchronization

Help ?

User Synchronization

Synchronization Datasources Active Synchronization Jobs Synchronization Job History

New Edit Delete

Name	Host	Search Filter
Win2K8AD	148.147.163.131	(cn=Alex*)

Select : None

Figure 7: Synchronization Datasource Table

4. LDAP SYNC JOB EXECUTION

Perform the following steps to synchronize System Manager with a LDAP Directory Server:

1. Login to System Manager with administrator privileges.
2. On the Common Console page, click on “Directory Synchronization” (Figure 1).
3. On the “User Synchronization” page, click on the “Active Synchronization Jobs” tab and then click on “Create New Job” button (Figure 8).

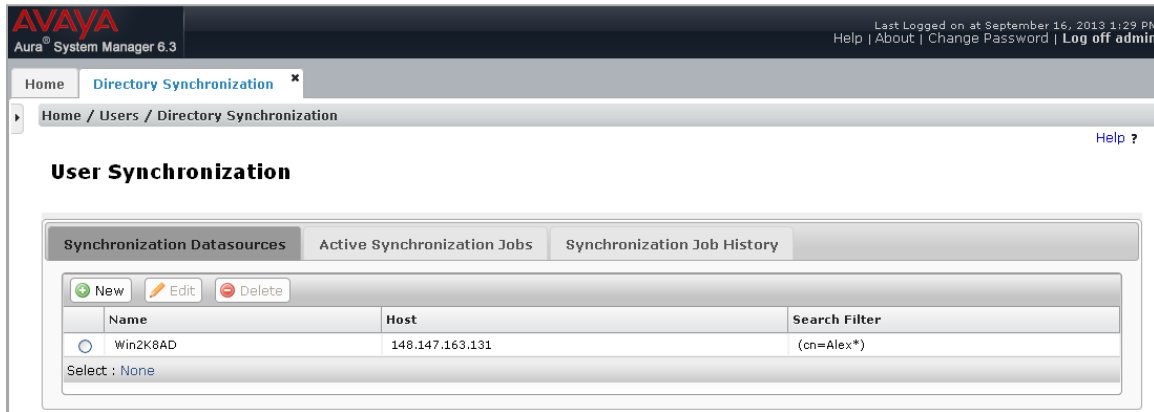


Figure 8: Active Synchronization Jobs Tab

4. To immediately start the synchronization, choose the datasource and click **Run Job** (Figure 9).

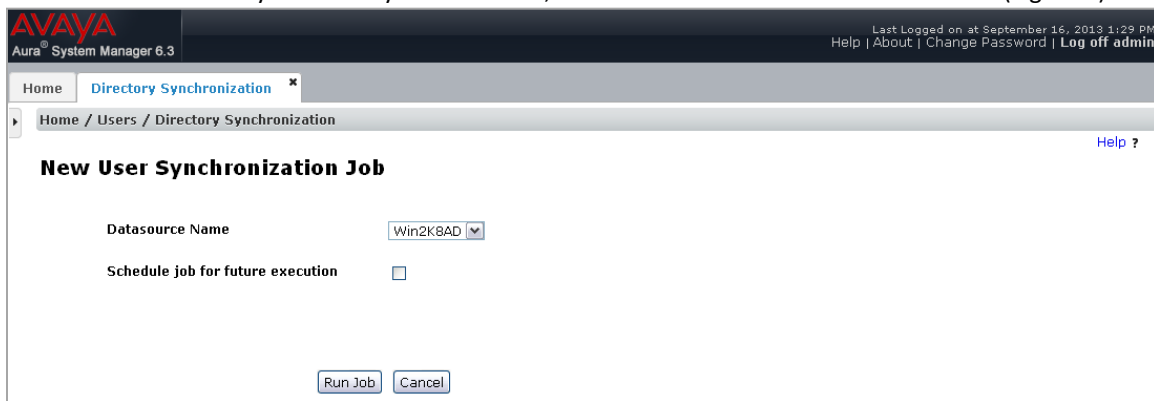


Figure 9: New User Synchronization Job

- To schedule synchronization for a future time, click the **Schedule job for future execution** check box and administer the appropriate information (Figure 10).

AVAYA
Aura System Manager 6.3

Last Logged on at September 16, 2013 1:29 PM
Help | About | Change Password | Log off admin

Home Directory Synchronization x

Home / Users / Directory Synchronization

New User Synchronization Job

Datasource Name Win2K8AD

Schedule job for future execution ☒

Date: September 16 2013

Time: 15 : 17 : 23 24Hr

Time Zone: (+5.30)Chennai, Kolkata, Mumbai, New Delhi, Sri Jayawardenepura

Repeat Job Execution ☐

Schedule job for future execution Cancel

Figure 10: Schedule Synchronization Job

- To repeat the synchronization on a periodic basis, click the “Repeat Job Execution” checkbox and administer the appropriate information (Figure 11). For example, to schedule a synchronization job to run every 2 weeks, in the Recurring Interval box, enter 2 and choose weeks in the drop down list.

AVAYA
Aura System Manager 6.3

Last Logged on at September 16, 2013 1:29 PM
Help | About | Change Password | Log off admin

Home Directory Synchronization x

Home / Users / Directory Synchronization

New User Synchronization Job

Datasource Name Win2K8AD

Schedule job for future execution ☒

Date: September 16 2013

Time: 15 : 17 : 23 24Hr

Time Zone: (+5.30)Chennai, Kolkata, Mumbai, New Delhi, Sri Jayawardenepura

Repeat Job Execution ☒

Recurring Interval

Every 0

minutes
hours
days
weeks
months

Schedule job for future execution Cancel

Figure 11: Schedule Periodic Synchronization

5. SYNCHRONIZATION HISTORY AND JOB STATUS

Perform the following steps to view the synchronization history and job status:

1. Login to System Manager with administrator privileges.
2. On the Common Console page, click on “Directory Synchronization” (Figure 1).
3. On the “User Synchronization” page, click on the “Synchronization Job History” tab (Figure 12).

The screenshot shows the Avaya System Manager 6.3 interface. The top navigation bar includes the Avaya logo, the text "Aura System Manager 6.3", and a user status bar indicating "Last Logged on at September 16, 2013 1:29 PM" with links for "Help", "About", "Change Password", and "Log off admin". The main content area is titled "User Synchronization" and contains three tabs: "Synchronization Datasources", "Active Synchronization Jobs", and "Synchronization Job History". The "Synchronization Job History" tab is selected, showing a table with one item. The table has columns for Name, Start Time, End Time, Status, Job Result, and Action. The single entry is for "Win2K8AD" with a start time of "September 16, 2013 3:23:48 PM +05:30", an end time of "September 16, 2013 3:23:49 PM +05:30", and a status of "COMPLETED". The Job Result column contains a link "View Job Summary", and the Action column contains a "Delete Job" link with a red minus icon.

Name	Start Time	End Time	Status	Job Result	Action
Win2K8AD	September 16, 2013 3:23:48 PM +05:30	September 16, 2013 3:23:49 PM +05:30	COMPLETED	View Job Summary	Delete Job

Figure 12: Synchronization History and Job Status

4. Click on “View Job Summary” to view the details of the synchronization job (Figure 13).

The screenshot shows the "Synchronization Job Summary" page in the Avaya System Manager 6.3 interface. The page title is "Synchronization Job Summary" with a "Back" button. It displays details for the "Win2K8AD" datasource, including the "End Time" of "September 16, 2013 3:23:49 PM +05:30". A "Job Results" section shows a summary of the job: "Added" 1 record, "Modified" 0, "Deleted" 0, "Unchanged" 0, and "Failed" 0. A table lists the added record with columns "Name" and "Description". The "Name" column contains the email address "ahartoch@pansv8.platform.avaya.com". At the bottom, a summary row shows "Total records processed" as 1. A "Back" button is located at the bottom right of the page.

Name	Description
ahartoch@pansv8.platform.avaya.com	

Added	1
Modified	0
Deleted	0
Unchanged	0
Failed	0
Total records processed	1

Figure 13: Synchronization Job Summary

6. STOP SYNCHRONIZATION RUNNING JOB

Perform the following steps to stop running synchronization job:

1. Login to System Manager with administrator privileges.
2. On Common Console page, click on “Directory Synchronization” (Figure 1).
3. On the User Synchronization page, click on the “Active Synchronization Jobs” (Figure 14)



Figure 14: Active Synchronization Jobs

4. When the job is running, “Create New Job” button is hidden and Current Running Job bar is shown. Click on “Stop Job” link to stop the job.

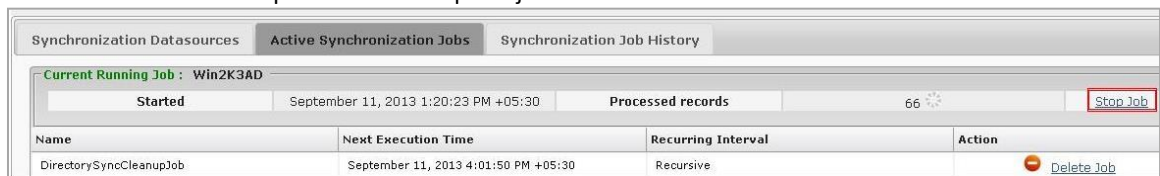


Figure 15: Active Synchronization Job Status

5. When the job is running, the Synchronization Job History Tab will also provide an option to Stop Job under Action column. Once the job is complete the Action changes to Delete Job.

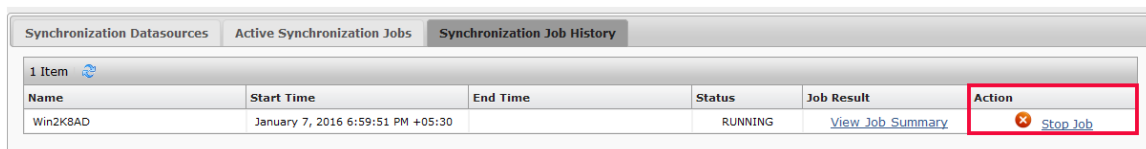


Figure 16: Synchronization Job History

7. DELETE SYNCHRONIZATION JOBS

Perform the following steps to delete synchronization jobs:

1. Login to System Manager with administrator privileges.
2. On the Common Console page, click on “Directory Synchronization” (Figure 1).
3. On the User Synchronization page, click on the Synchronization Job History tab (Figure 12).
4. Click “Delete Job” link for the synchronization jobs to be deleted.
5. A confirmation will be asked to delete the job or not.

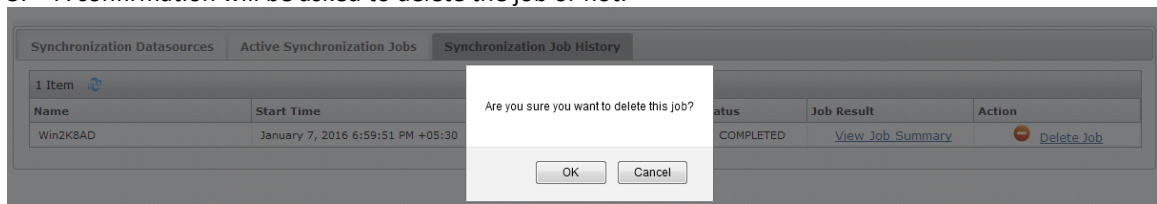


Figure 17: Synchronization Job History Jobs Deletion

SSL Connection Setup for Directory Synchronization

Perform the following steps to set up SSL connection between System Manager and Active Directory LDAP Directory Server:

1. Export certificate from Active Directory in CER format and save it locally.
2. Login to System Manager with administrator privileges.
3. On the Common Console page, click on “Inventory.” On the Inventory page, click on Manage Elements (Figure 18).

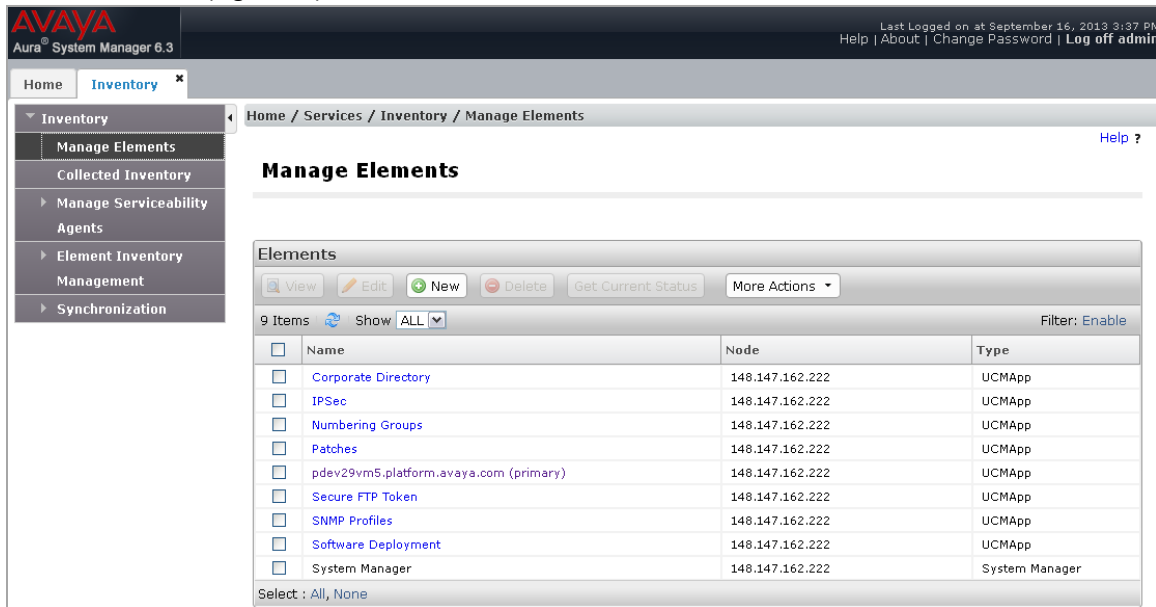


Figure 18: Manage Elements

4. Select the System Manager check box.
5. Click the More Actions button and choose “Configure Trusted Certificates” (Figure 19).

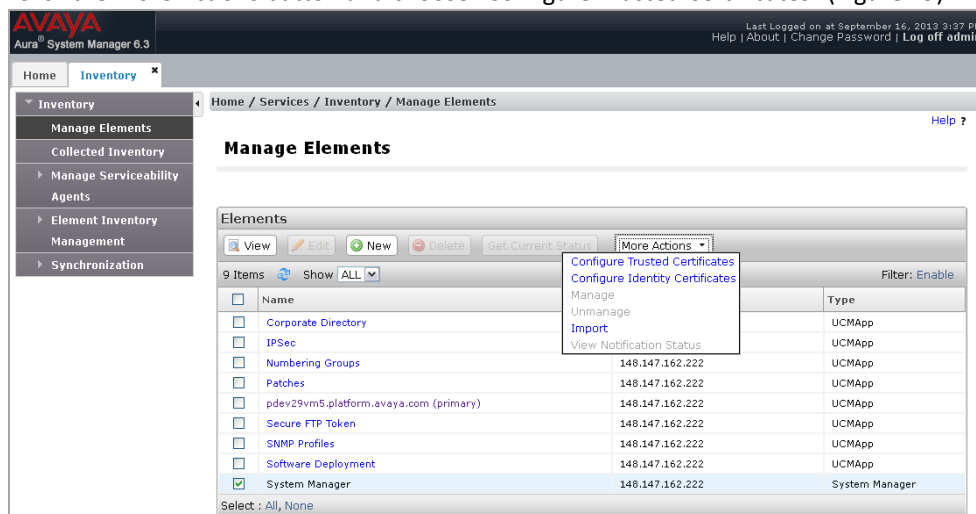


Figure 19: Manage System Manager Trust Certificate

On the Trusted Certificates page, click the Add button (Figure 20: Trusted Certificates)

6.).

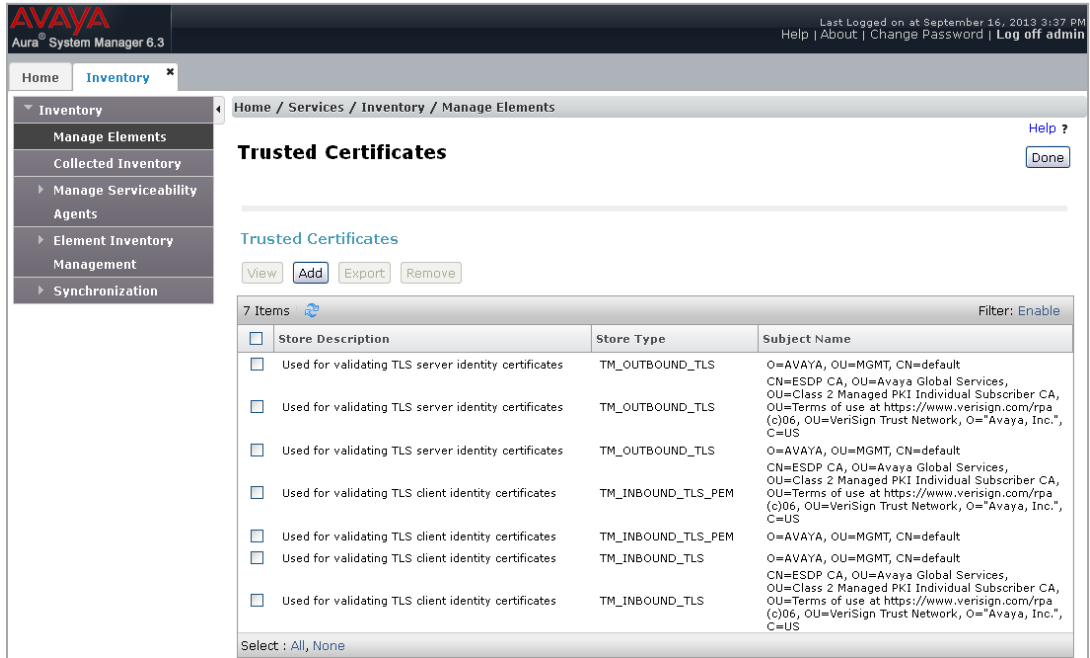


Figure 20: Trusted Certificates

7. On the Add Trusted Certificate page, select “Import from file” (Figure 21). Also, make sure that the “Select Store Type to add trusted certificate” value is set to all.

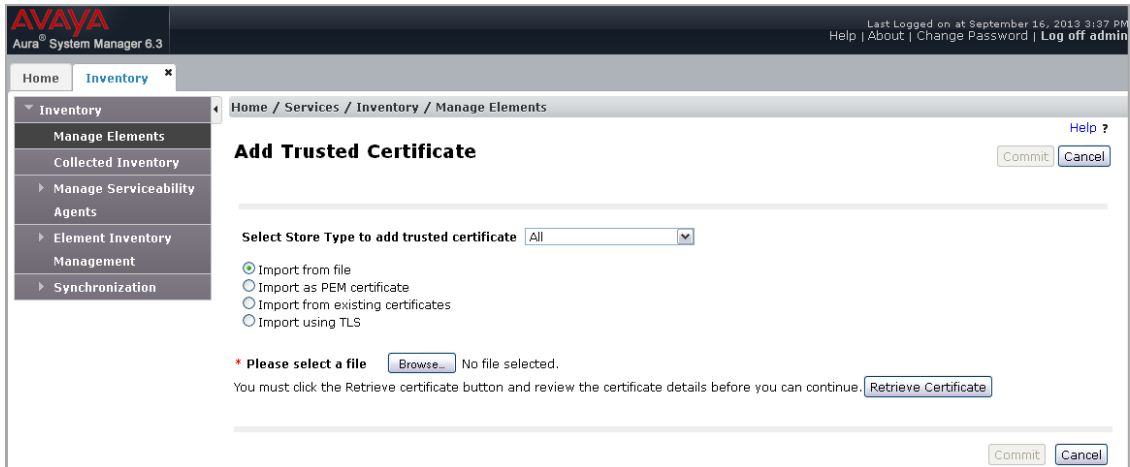


Figure 21: Add Trusted Certificate

8. Click on the browse button and navigate to the location where the LDAP Directory certificate is stored. Select the certificate.

9. Click the “Retrieve Certificate” button.

10. Click the “Commit” button to add the LDAP Directory certificate to System Manager’s trust store (Figure 22).

AVAYA
Aura® System Manager 6.3

Last Logged on at September 16, 2013 3:37 PM
Help | About | Change Password | Log off admin

Home Inventory

Home / Services / Inventory / Manage Elements

Add Trusted Certificate

Commit Cancel

Select Store Type to add trusted certificate All

☒ Import from file
☐ Import as PEM certificate
☐ Import from existing certificates
☐ Import using TLS

* Please select a file Browse... No file selected.

You must click the Retrieve certificate button and review the certificate details before you can continue. Retrieve Certificate

Certificate Details

Subject Details	CN=labesx2vm1, DC=pansy, DC=platform, DC=...	
Valid From	Mon Jul 02 19:00:30 IST 2012	Valid To
Key Size	2048	Sun Jul 02 19:00:35 IST 2017
Issuer Name	CN=labesx2vm1, DC=pansy, DC=platform, DC=...	
Certificate Fingerprint	eaacbbe3edca57513fed20932405db9b6bef6	
CA Certificate	Yes	

Commit Cancel

Figure 22: Committing LDAP Directory Certificate

User Provisioning Rule for Directory Synchronization

System Manager 6.3.4 introduced new workflows that stream line the user provisioning process through the use of User Provisioning Rules (UPR). A UPR enables various predefined templates that consist of user attributes found in a user's communication profiles to be associated with a User as part of the user provisioning workflow. The UPRs are essentially groups of predefined templates that make-up a master communication profile template and provisioning rules that can be associated with users created in System Manager.

User Provisioning Rules can be associated with a User that is being created via the System Manager native User Interface, Web Services API, Bulk Import/Export Utility and LDAP synchronization with an Enterprise Directory Server.

When the User Provisioning Rule is applied with other LDAP Sync Capabilities; fully automated user provisioning can be achieved.

General Guidelines and Capabilities of User Provisioning Rules

- 1) A User Provisioning Rule (UPR) is intended for Day 1 provisioning of the User. Once the UPR is applied during the creation of the User, it is no longer used for user provisioning management.
- 2) A User Provisioning Rule (UPR) is a Template. When the administrator uses a UPR to create user, System Manager populates the default values, the communication addresses, and the communication profiles attributes for the user based on the rules defined in the UPR
- 3) Once a UPR is defined and applied to create a user, the Communication Profile that is part of the UPR cannot not be modified to change, delete or add data in the Communication Profile and be reapplied to the User.
- 4) To add a service that is defined in a Communications Profile to an existing User that was created using a UPR, an administrator can create a new UPR with the new service defined (i.e Presence, Messaging, Collaboration Environment, etc) in the Communications Profile of the new rule and apply it to the User via an LDAP sync. In this case, the new service that is defined in the Communications Profile would be added to the existing user. The following is the general workflow:
 - a. Create a new UPR with the new service defined in the Communication Profile.
 - b. Update The LDAP Enterprise Directory with new UPR for the user or group of users
 - c. Sync the users and all the users will have new profile assigned to them
- 5) Only one Communication Profile Set can be assigned to a UPR
- 6) Once the user is created via a UPR, the System Manager User Provisioning Interfaces such as the System Manager native User Interface, Web Services API, Bulk Import/Export Utility and the Global Endpoint Change Editor can be used to modify a user's attribute as long as that attribute is not part of the Communications Profile. For example, an admin could add CM endpoint features to a user or change buttons.

Perform the following steps to set up User Provisioning Rule to be used for Directory Synchronization:

1. Login to System Manager with administrative privileges.
2. On Common Console page, click on “User Provisioning Rule”

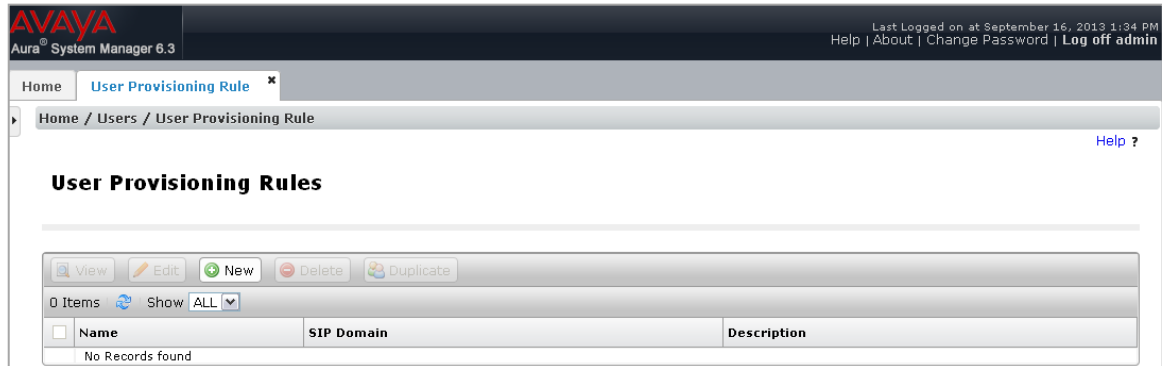


Figure 23: User Provisioning Rules Table

3. Click the “New” button to create a User Provisioning Rule.
4. Provide the required information to be used as default values while creating the user. User Provisioning Rule contains two tabs.
 - a. Basic Tab for the basic information that includes communication profile password, time zone, language preference.

The screenshot shows the 'New User Provisioning Rule' page in the Avaya System Manager 6.3 interface. The page has a breadcrumb trail: Home / Users / User Provisioning Rule. Below the breadcrumb, there's a section titled 'New User Provisioning Rule'. Under this section, there are buttons for Commit and Cancel. Below these buttons, there are two tabs: 'Basic' (selected) and 'Communication Profile'. The 'Basic' tab contains the following fields:

- * User Provisioning Rule Name: Denver_RND
- Description: User Provisioning Rule for Denver city and RND department
- SIP Domain: avaya.com
- Communication Profile Password: [masked]
- Confirm Password: [masked]
- Use Phone Number last: 4 digits for Extension
- Prefix for Avaya E164 Handle: +1303538
- Language Preference: English (United States)
- Time Zone: (-4:0)Eastern Time

 At the bottom left, there's a note '*Required'. At the bottom right, there are buttons for Commit and Cancel.

Figure 24: New User Provisioning Rule Basic Tab

- b. Communication Profile Tab for the communication system that the user must use. For example, Communication Manager and Session Manager. Also includes the rules to assign or create a communication profile for the user. For example, by assigning the next available extension for Communication Manager.

The screenshot displays the Avaya Aura System Manager 6.3 web interface. The top header shows the Avaya logo and 'Aura System Manager 6.3'. On the right, it indicates 'Last Logged on at September 16, 2013 1:34 PM' and provides links for 'Help | About | Change Password | Log off admin'. The breadcrumb trail reads 'Home / Users / User Provisioning Rule'. The main title is 'New User Provisioning Rule', with 'Commit' and 'Cancel' buttons to its right. Below the title, there are two tabs: 'Basic' (marked with a red asterisk) and 'Communication Profile'. The 'Communication Profile' tab is active, showing a list of profiles with checkboxes and expandable arrows:

- ☐ Session Manager Profile
- ☐ CM Endpoint Profile
- ☐ CS 1000 Endpoint Profile
- ☐ Messaging Profile
- ☐ Call Pilot Messaging Profile
- ☐ IP Office Endpoint Profile
- ☐ Conferencing Profile

At the bottom left, there is a red asterisk followed by the text '*Required'. At the bottom right, there are 'Commit' and 'Cancel' buttons.

Figure 25: New User Provisioning Rule Communication Profile Tab

Note: If one need more details on different attributes of User Provisioning Rule, please check Online Help for the same.

5. User Provisioning Rule can be mapped with multiple attributes for LDAP sync, the value of multiple attribute mapping will be joined by "_" (underscore) to map with value in SMGR. Let's take a scenario to better understand the procedure:

Scenario:

A company has two departments at location Denver say RND and Sales.

For RND department, administrator would like to use Communication Manager CM_RND and Session Manager SM_RND.

For Sales department, administrator would like to use Communication Manager CM_Sales and Session Manager SM_Sales.

Administrator can create two "User Provisioning Rule" which can be named as **Denver_RND** and **Denver_Sales**.



Figure26: User Provisioning Rule List Page

During Directory Synchronization mapping, administrator can use following mapping to map location (l) and department attribute to map with User Provisioning Rule.

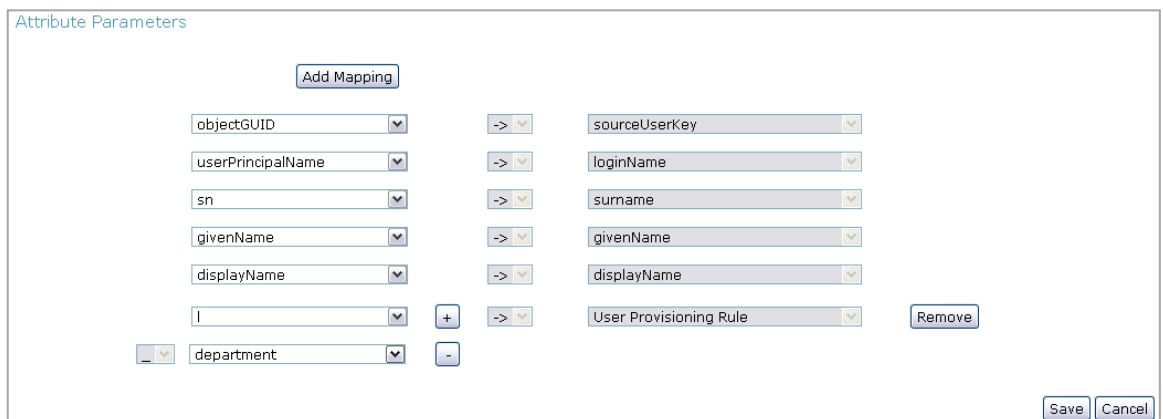


Figure 27: Directory Sync Attribute mapping for User Provisioning Rule

The system will compare the value of "location_{department}" for each user in LDAP with the existing User Provisioning Rule and use it accordingly to create the user.