



Avaya Aura® System Manager 7.0 Solution Deployment Manager Job-Aid

Issue 1.0

February, 2016

Contents

1.	INTRODUCTION	3
1.1	Documentation map	3
1.2	How to Videos	3
1.3	Overview and Document Scope	3
1.4	Automated Avaya Aura Upgrade-Migration and Update Description	4
1.5	Big Picture Workflow View	5
1.6	Definitions and Acronyms	8
2.	SETTING ENVIRONMENT FOR SYSTEM MANAGER SOLUTION DEPLOYMENT MANAGER.....	9
2.1	Solution Deployment Manager Configuration settings	9
2.1.1	User Settings.....	10
2.1.2	Sync Settings.....	12
2.1.3	Software Library Management	14
2.2	Things to know for configuring your elements in System Manager Manage Elements	16
2.3	Upgrade Release Selection	18
3.	STAGING	19
3.1	Element Selection	21
3.2	Supported Elements	21
3.3	Capacity	22
3.4	Refresh element(s)	22
3.5	Analyze	23
3.6	Download	25
3.7	Pre-Upgrade Check	30
3.7.1	Running Pre-upgrade Checks	31
4.	UPGRADE/UPDATE	34
4.1	Utility Services on Appliance Virtualization Platform	34
4.2	Upgrade Configuration	35
4.2.1	Different Box Migration	43
4.2.2	Same Box Migration	46
4.2.3	Failed Migration	51
4.3	Update Configuration	53
4.3.1	Staging for Elements for Patching.....	53
4.3.2	Update	54
4.4	Duplex Migration	59
4.4.1	Preparing duplex Communication Manager for migration	59
4.4.2	Duplex Same Box Migration	60
4.4.3	Duplex Different Box Migration	61
4.5	Upgrade Job Status.....	62

1. INTRODUCTION

This work aid is intended as a quick reference to assist in the setup and accelerated learning of the Solution Deployment Manager (SDM) feature that is part of System Manager Release 7.0.

Always refer to support.avaya.com for the latest official documentation.

1.1 Documentation map

Sl. no	Purpose	Document	Section in the document
1	To set up inventory and discovery	Administering Avaya Aura® System Manager for Release 7.0	Managing inventory
2	To use Solution Deployment Manager	Administering Avaya Aura® System Manager for Release 7.0	Solution deployment and upgrade
3	To deploy Aura 7.0 applications using SDM	Deploying Avaya Aura® applications	-
4	To use SDM to Upgrade or Migrate Aura 7.0 applications	Upgrading and Migrating Avaya Aura® applications to Release 7.0	-
5	To upgrade System Manager on Avaya Appliance and Customer-Provided VE	Upgrading Avaya Aura® System Manager to Release 7.0	-
6	Avaya Aura 7.0 Offering	Avaya Aura 7 Offer Definition	https://sales.avaya.com/documents/1399584208566

Table 1: Documentation map

1.2 How to Videos

1) Installing Avaya Aura Solution Deployment Manager (SDM) Client

- Avaya Knowledge Base link: <https://kb.avaya.com/kb/index?page=content&id=VIDEO101131>
- YouTube link: <https://youtu.be/2-pHPcftTCs>

2) Install Avaya Appliance Virtualization Platform (AVP)

- Avaya Knowledge Base link: <https://kb.avaya.com/kb/index?page=content&id=VIDEO101120>
- YouTube link: <https://youtu.be/7y83M7iXJqs>

3) Installing Utility Services

- Avaya Knowledge Base link: <https://kb.avaya.com/kb/index?page=content&id=VIDEO101129>
- YouTube link: <https://youtu.be/lA9CO5dWKzs>

1.3 Overview and Document Scope

In the Avaya Aura® 7.0, System Manager continues to enhance the Avaya Aura® management experience and reduce the customers total cost of ownership with the introduction of a new software management solution.

Solution Deployment Manager (SDM) is a centralized software management solution in System Manager that enables deployment, upgrades, migrations, and updates to the suite of Avaya Aura® 7.0 applications. Solution Deployment Manager supports these operations on

customer Virtualized Environment and Avaya Provided Appliances that is based on the Appliance Virtualization Platform (AVP). This document focuses on Upgrade Management which consists of migrating/upgrading and updates for Avaya Aura elements.

In System Manager Release 7.0, SDM supports Automated upgrades/updates for following elements:

- Linux based Communication Manager release 5.2.1 and its associated devices, such as Gateways, TN boards, and Media Modules.
- System Platform based Communication Manager release 6.x, Branch Session Manager 6.x and Utility Services 6.x that are included in the CM Templates.
- Communication Manager Messaging running as a service with the various Communication Manager templates.
- Linux-based Session Manager 6.x.

The primary benefits in using the Avaya Aura® 7 automated upgrade-migration capabilities are:

- To move from a manual step-by-step procedure local to the application server to an automated migration procedure.
- To drive application upgrades and migrations remotely from a centralized System Manager.
- To eliminate time lost waiting for each next step in the upgrade-migration process, by using an automated sequencing of tasks with the application upgrade-migration events running in the background without manual intervention.
- To move from multiple manual tasks that require human intervention that can be error prone, to reliable integrated checks that assess and confirm upgrade-migration readiness

1.4 Automated Avaya Aura Upgrade-Migration and Update Description

In System Manager 7.0, several Avaya Aura® applications will support an automated migration path orchestrated by the centralized System Manager - Solution Deployment Manager service. The term “migration” is intended to cover upgrade situations where there is a hardware server change, OS change or Hypervisor change. In these types of scenarios, there can be requirements to perform manual tasks such as backup and restore configuration data; load or unload patches; and deploy new application versions. The automated upgrade-migration process via System Manager was first introduced for Communication Manager 6.x to 6.3.6 upgrades in the Feature Pack 4 timeframe and is enhanced to support simplified upgrade and migration procedures in Avaya Aura® 7.

The automated functionality provided by the Solution Deployment Manager will be phased in throughout the Avaya Aura® 7 releases and feature packs. The initial development in System Manager 7 is focused on automating the migrations of System Platform based Communication Manager (CM) and Branch Session Manager (BSM) release 6.x; as well as the Red Hat Linux based Session Manager (SM) release 6.x and Communication Manager (CM) release 5.2.1 applications. The auto-migration functionality is applicable to the Avaya Provided Appliance Offer introduced as part of Avaya Aura® 7, and to the Avaya Aura® Customer Provided Virtualized Environment. Migrations of Communication Manager include any software or firmware upgrades to Media Modules, TN Boards and Media Gateways.

Automated upgrade-migration tasks include: applying pre-migration Patch, perform a backup of the existing translations and configuration; deploy the Avaya Aura® 7 applications into the VMware environment; and restoring the data from backup.

Solution Deployment Manager also includes a Pre-Upgrade/Migration check that must be run prior to scheduling or executing an application upgrade-migration. The Pre-Upgrade/Migration checks will reduce failures and errors in the field. Pre-upgrade/migration checks include items such as, hardware compatibility (supported server types – Appliance Offer only); validate required software files are downloaded and available in the Software Library; and if there is sufficient CPU, Memory and Hard disk to deploy the Avaya Aura® 7 applications.

For Avaya Aura® 7 migrations, there will be a manual step to install the Appliance Virtualization Platform (AVP). Future releases of Solution Deployment Manager will include the Appliance Virtualization Platform deployment as part of the end-to-end automated migration process. Future releases of System Manager will also extend the automated steps to other Avaya Aura® Applications.

The Solution Deployment Manager also has the ability to perform automated updates such as applying Patches, Service Packs and Feature Packs to applications running on a customer's Aura solution. Applications supporting automated updates include: Communication Manager, Communication Manager Messaging, Branch Session Manager, Session Manager and Utility Services. There is also the ability to patch the Appliance Virtualization Platform (AVP). Future releases of System Manager will also extend the automated update steps to other Avaya Aura® Applications

The Solution Deployment Manager is capable of performing up to 100 simultaneous application/TN Boards/Media Modules upgrade-migration and update jobs at one time. Check [Capacity Section 3.3](#) for more details. When the System Manager's Scheduler is used in conjunction with the Solution Deployment Manager's ability to run upgrades-migrations and updates in parallel, a significant reduction in the time to upgrade-migrate Avaya Aura® elements can be achieved.

Avaya Aura applications that does not support the automated upgrade-migration and update in System Manager 7.0, will be supported in future releases. Currently, some manual procedures are used that require a manual backup, Avaya Aura OVA deployment, and manual restore.

1.5 Big Picture Workflow View

In this section, we provide a high-level overview of using Solution Deployment Manager (SDM) to perform Automated Avaya Aura Application upgrades-migrations and updates. Subsequent sections of this document are intended to provide the detailed steps required to successfully use SDM for Application upgrades-migrations and updates.

Once System Manager 7.0 is operational, the first step in enabling the automated capabilities is to set ensure the supported applications; Communication Manager (CM) Release 5.2.1 and 6.x, Branch Session manager (BSM) Release 6.x and Session Manager (SM) 6.x are defined in the System Manager Elements page. This can be done by using the automated discovery capability (using SNMP) for CM or by manually adding the element to the System Manager Elements Page for SM and BSM. The configuration associated with these elements enable the SDM service to

probe the applications for detailed information related to the current software versions running on the application and hardware in the case of TN Boards, Media Modules and Media Gateways.

The next step is to configure SDM. There are two key pieces of configuration that need to be completed once the elements are defined in the Elements Page in System Manager.

1) **Define User Settings:**

Within this configuration area, SDM is provided all the details to login into PLDS so that software versions discovered on the applications running in the customer network can be compared to what the customer is entitled to. Once this Analysis is complete SDM will provide the option to the customer to download all the required software and files needed to perform the upgrade or update.

Customers who do not allow external connections from System Manager - SDM to PLDS can login to PLDS from a customer's web browser and manually download all required software and files. The downloaded software is stored on a customer supplied server which SDM defines as an Alternate Source. The Alternate Source is used as the reference point when performing the Analysis function that compares what applications versions the customer is running and what they are entitled to.

Only one setting is required, a customer would use either the PLDS interface or the Alternate Source. The Alternate Source would have more manual intervention because the customer is manually selecting all entitled software and files; and downloading the files to the customer network. When using the PLDS option, SDM will automatically analyze the software, gather the entitlements and download the required software and files (if elected to buy customer) to the defined software library. Customer Entitlements are tied to a customer's SOLD-To identification.

2) **Define the Software Library:**

The Software Library can be on System Manager or on a Customer-Provided Server. The library contains all the software that will be used when doing an upgrade-migration of update. When System Manager is utilized as the Software Library, 25GB (profile 1 and 2) or 50GB (Profile 3) of space is allocated depending on the Profile used during the System Manager deployment. If more space is needed and external Library can be deployed by the customer and defined in SDM.

Once the Elements are listed in the Elements Page and the SDM configuration is complete, the customer can open the SDM User Interface and run a **Refresh Element** which will initiate a connection from SMGR-SDM to the supported elements (CM, BSM, SM) to perform a second level inventory. The second level inventory is a service in SDM that probes the applications for detailed software version information.

When the second level inventory is complete, the customer can then run the ANALYSIS function from the SDM User Interface. The ANALYSIS function is what compares what is running on the customer's Aura solution to what the customer is entitled to. Depending on the User Settings, the ANALYSIS function will use PLDS or the Alternate Source to do the comparison. SDM uses a configuration file called 'versions.xml' to perform the comparison.

Once the ANALYSIS function is complete, the customer is presented in SDM, a view of what applications have software running that can be upgraded or updated based on the customer's entitlements.

At this point, the customer can select anyone of the Elements that have a software upgrade or update pending. Once the Element is selected, the customer is required to run a pre-upgrade check that will ensure everything is in place to perform a successful upgrade or update. Once the pre-upgrade check is complete and successful the customer can run the upgrade or update immediately or schedule the job. Information on simultaneous jobs is provided in the Capacity section.

1.6 Definitions and Acronyms

Following are some acronyms used throughout this document:

Term	Meaning
AES	Application Enablement Services
AVP	Appliance Virtualization Platform
BSM	Branch Session Manager
CM	Communication Manager
CMM	Communication Manager Messaging
DNS	Domain Name Service
FQDN	Fully Qualified Domain Name
GUI	Graphical User Interface
GW	Avaya H.248 Media Gateway
HA	High Availability
H.248	Media Gateway Control protocol
LDAP	Lightweight Directory Access Protocol
PLDS	Product Licensing and Delivery System
SDM	Solution Deployment Manager
SIP	Session Initiation Protocol
SM	Session Manager
SMGR	System Manager
SP	System Platform
SSH	Secure Shell
SMI	System Management Interface (Communication Manager)
US	Utility Services
Same Box	Same Box

Table 2: Definitions and Acronyms

2. SETTING ENVIRONMENT FOR SYSTEM MANAGER SOLUTION DEPLOYMENT MANAGER

This section identifies the different configuration areas for setting up the SMGR Solution Deployment Manager.

There are 3 main tasks of System Manager SDM process:

1. SDM Configuration Settings (One Time Configurations):
 - User Settings (Setup System Manager for PLDS access or Alternate Source)
 - Sync Settings
 - Software Library

Note: You can use User Settings or Sync Settings to upgrade or update the elements.

2. Managing Elements Inventory (Automatic Inventory collection or manual adding Managed Elements into the Inventory).
3. Upgrade process execution.
 - Staging
 - Upgrade

2.1 Solution Deployment Manager Configuration settings

The configuration settings are required so SDM has information about the following:

- 1) What software versions customers are entitled to
- 2) Where SDM can download the software that is required for upgrade or update
- 3) Where software will be downloaded to (Library)

One Time Configurations

There are few settings which are required before we start to upgrade/update any element. These configurations are required for SDM to know what state the system is in and what the customers are entitled to.

Settings	Description
User Settings	1. Navigate to Home/Services/Solution Deployment Manager/User Settings
	2. There are two options either to use Alternate Source or provide PLDS Configuration.
	3. User Settings are required for SDM to read version xml files to know the software entitlements for the user.
	4. User Settings are also required to download the files available in PLDS or Alternate Source.
Sync Settings	1. Sync settings consists uploading latest version xml files to \$SUM_HOME/resources/versionsxml
	2. Sync settings also consist of uploading downloaded software to software library.
Software Library	1. Navigate to Home/Services/Solution Deployment Manager/Software Library Management.
	2. Software Library comes with a default local library SMGR_DEFAULT_LOCAL (Storage capacity: 25GB for Profile 1 & 2 and 50GB for Profile 3) which stores downloaded software on System Manager.
	3. If admin wants to configure remote library, it can be done by clicking New, and providing necessary information.
	4. Local library SMGR_DEFAULT_LIBRARY cannot be used for updating Media Gateway, Media Module and TN Boards in System Manager release 7.0, but it is in planning for the first System Manager 7.0.1 Feature Pack.
	5. If the same file server is used for alternate source and software library, make sure to use separate directory for s/w library and

	alternate source.
--	-------------------

Table 3: One Time Configuration Details

2.1.1 User Settings

User Settings consists of two types of configuration. Depending on the need, one of the options can be used.

- PLDS Credentials
- Alternate Source

Setup PLDS access

Using your PLDS account log into the PLDS (<http://plds.avaya.com>) and get your Company ID

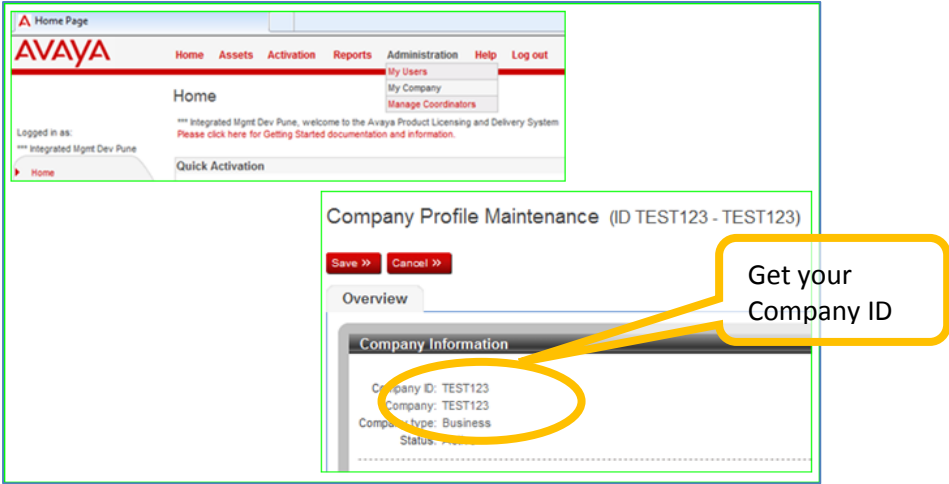


Figure 1: PLDS Account Details

Access the System Manager link **Home/Services/Solution Deployment Manager/ User Settings**. Select the checkbox **Use Avaya Support Site**. Provide **SSO User name, SSO password, Company ID**. This will be used for getting entitlements for Analyze and artifacts (software and files) for download.

Home / Services / Solution Deployment Manager / User Settings

User Settings

Source Configuration

Use Avaya Support Site

☒

Alternate Source

http://148.147.214.158/alternate_

PLDS Configuration (to Use Avaya Support Site)

* SSO User Name

sumdevplds

* SSO Password

••••••••

* Confirm SSO Password

••••••••

* Company ID

AVAYA

Proxy Settings (to Use Avaya Support Site)

Use Proxy

☐

Host

Port

User

Password

Confirm Password

Figure 2: User Settings Page

Setting up Alternate Source

If a customer doesn't have or allow internet connectivity from System Manager to Avaya PLDS, an alternate source can be configured. The Alternate Source is a local server defined in the customer's network that will be used store versions xml files for the different elements that can be upgraded from SDM and the software that will be used as part of the upgrade or update. The versions xml files contains information about the software versions a customer is entitled to upgrade or update

Versions XML Files

The latest versions XML file can be found at

<ftp://ftp.avaya.com/incoming/Up1cku9/tsoweb/SUM/>, there are 8 versions xml file listed below:

- versions_bsm.xml
- versions_compatibility.xml
- versions_sp.xml
- versions_us.xml
- versions.xml
- versions_systemplatform.xml
- versions_cmm.xml
- versions_others.xml

Software Files

Customer will have to download the required software files (ISO, OVAs, bin, etc.) from PLDS and upload to alternate source.

Configuring Alternate Source

An Alternate Source can be used for copying latest versions xml files and downloaded software from PLDS.

To configure alternate source access the System Manager link **Home/Services/Solution Deployment Manager/ User Settings**. Uncheck the checkbox **Use Avaya Support Site** and provide **Alternate Source**, this would require an http URL.

Copy the above mentioned version xml files and downloaded software files from PLDS in the alternate source.

For example: <http://<IP>/SDMDATA/> where **SDMDATA** is an example of the directory name where Software artifacts can be stored. Copy above mentioned version xml files at location **SDMDATA** directory.

Note: An example of Apache http server is provided for reference to configure alternate source. Refer to [Appendix A - Installing a HTTP server on Windows Environment](#)


















Index of /SDMDATA			
Name	Last modified	Size	Description
 Parent Directory		-	
 00.0.440.0-1003.tar	25-Jun-2015 07:09	3.7M	
 BSM-7.0.0.0.124002-e55-01.ova	23-Jun-2015 11:50	1.9G	
 CM-Simplex-07.0.0.0.440-e55-0.o.a	15-Jun-2015 18:08	753M	
 SM-7.0.0.0.124002-e55-01.o.a	17-Jun-2015 08:36	2.0G	
 US-7.0.0.0.10-e55-01 OVF10.o.a	21-Jun-2015 17:15	1.0G	
 dmutility-7.0.0.0.124002.bin	16-Jun-2015 18:48	1.1M	
 versions.html	16-Jul-2015 13:11	491	
 versions.xml	16-Jul-2015 13:12	1.7M	
 versions.xsl	16-Jul-2015 13:12	1.8K	
 versions ASCA.html	16-Jul-2015 13:12	496	
 versions_bsm.xml	16-Jul-2015 13:13	11K	
 versions_cmm.xml	16-Jul-2015 13:13	11K	
 versions_compatibility.xml	16-Jul-2015 13:13	7.9K	
 versions_others.xml	16-Jul-2015 13:13	1.9K	
 versions_sp.xml	16-Jul-2015 13:13	6.5K	
 versions_systemplatform.xml	16-Jul-2015 13:14	15K	
versions_us.xml	16-Jul-2015 13:14	5.7K	
Apache/2.2.3 (Red Hat) Server at 135.9.48.179 Port 80			

Figure 3: Alternate Source Link

2.1.2 Sync Settings

If a customer doesn't have internet connectivity from System Manager to PLDS and doesn't want to configure alternate source, there is also an option to sync version xml files and downloaded software to software library using System Manager.

System Manager comes with pre-configured version xml files for GA Versions of the Avaya Aura applications which will automatically be parsed and the versions will be available on **Home/Services/Solution Deployment Manager/Download Management**.

Version XML Files

The latest versions XML file can be found at

<ftp://ftp.avaya.com/incoming/Up1cku9/tsoweb/SUM/>, there are 8 versions xml file listed below:

- versions_bsm.xml
- versions_compatibility.xml
- versions_sp.xml
- versions_us.xml
- versions.xml
- versions_systemplatform.xml
- versions_cmm.xml
- versions_others.xml

To get updated data about the latest software versions available, the latest versions xml files can be copied from in System Manager at **\$SUM_HOME/resources/versionxml** directory. 7.0.1 Feature Pack will have the capability to upload version xml files from System Manager web interface.

After the files are copied in System Manager navigate to **Home/Services/Solution Deployment Manager/Download Management**, click on Refresh Families to refresh the data available in versions XML files.

Software Files

Navigate to "**Home/Services/Solution Deployment Manager/Software Library Management**" and click "Manage Files" to reach following screen.

Home / Services / Solution Deployment Manager / Software Library Management

Status

Software Library Files

Manage the files screen lists all the files from all the configured software libraries that are configured. Use this screen to view and delete files from software libraries. Click "Done" to go back to the Software Library screen.

View Delete

File Name	Device Type	Software Type	Version	Hardware Compatibility	File Length	Software Library
CM-Simplex-07.0.0.0.440-e55-0.ova	CM_Simplex	OVA Template	7.0.0.0.440	N/A	789241856	SMGR_DEFAULT_LOCAL

Select : All, None

Sync Files from directory

The files which needs to be added to the software library should be placed manually in the path "/swlibrary/staging/sync/" on the System Manager. Once files are placed, refreshing the below table will display those files. Populate data in the table below and click "Sync". Files will be added to the Software Library.

Sync

File Name	MD5 Checksum	Software Library	Product Family	Device Type	Software Type
No data found.					

Figure 4: Software Library Management - Manage Files Page

Copy the required file manually to path “/swlibrary/staging/sync/” on the System Manager. Once done, that file will be listed in the bottom table on UI.

Figure 5: Sync Files from directory section

In case the file is already in versions xml, the fields like ‘Product Family’, ‘Device Type’, ‘Software Type’ and ‘MD5 Checksum’ will be auto populated. If entry of the file is not in versions xml, the value of fields will not be pre-populated. In such cases, the file cannot be used in Upgrade Management for upgrade. Only fresh deployment through VM management and custom patching can be done for such files. Fill in the required data and select the row.

Figure 6: Sync Files from directory section

On click of ‘Sync’, you will see a message pop-up which mentions if the job is scheduled or not.

Figure 7: File Sync started pop-up message

To check the status of job, navigate to “[Home/Services/Scheduler/Pending Jobs](#)”.

Once job is successful, the file should appear in Software Library and get removed from sync table.

Note: If the version xml file doesn’t have the patch which needs to be updated, it needs to be uploaded as Custom Patch.

If the patch is available in version xml file the fields like MD5 Checksum, Product Family, Device Type will be pre-populated.

Here is the list of what values should be selected for which element for **custom patch**

Element	Product Family	Device Type	Software Type
Communication Manager	Media Servers	Avaya Aura (R) Communication Manager VE	CM Custom Patch
Utility Services	Utility Server	Custom Patch	Custom Patch
Session Manager	Session Manager	Custom Patch	Custom Patch
Branch Session Manager	Branch Session Manager	Custom Patch	Custom Patch
Communication Manager Messaging	Communication Manager Messaging	Avaya Aura(R) Communication Manager Messaging VE	CMM Custom Patch

Table 4: Values for Sync Files for different elements

2.1.3 Software Library Management

Software Library is typically a file server which supports SCP, SFTP or FTP protocol.

Software Library is required for storing software files download from PLDS or Alternate Source or synced using Sync option. These software files are later used for migration and patching of the elements.

Navigate to [Home/Services/Solution Deployment Manager/Software Library Management](#) for configuring Software Library.

There is option to configure multiple software libraries. There is a default software library which is pre-configured in System Manager. The partition of [/swlibrary](#) on System Manager is dedicated for local software library which has 25 GB of storage capacity on System Manager Profile 1 & Profile 2 and 50 GB storage capacity on System Manager Profile 3.

A large enterprise that may have many different deployments could require more space than allocated to local software library, in this case a remote software library can be configured. All the software files will be downloaded to that remote library (if selected during download and sync).

Note: An example of Filezilla FTP server is provided for reference to configure software library. Refer to [Appendix A - Installing a FTP server Windows Environment](#)

Add the software library on System Manager as follows:

- 1) Library Server Details – Basic details of the library and the path where you want to copy the downloaded software. Once can choose Local Survivable Processor which means that the LSP can be used as software library. The IP address field will become a drop-down and the LSPs which are configured in [/Home/Services/Inventory/Manage Elements](#) will show up in the drop-down.
Only SCP and FTP Configuration Tab will be available.
- 2) SCP Configurations – Provide username and password if the library server supports SCP protocol.
- 3) SFTP Configurations – Provide username and password if the library server supports sftp protocol.
- 4) FTP Configurations – Provide username and password if the library server supports ftp protocol.
- 5) HTTP/HTTPS Configurations – The http/https protocol here is not used to upload software to software library. Instead the System Platform based CM uses the HTTP/HTTPS configuration to retrieve the software/firmware files from the software library during the upgrade (6.x to 6.x) process.

Add Software Library

A software library contains files that can be used to upgrade the software and firmware of elements.

Use this screen to create a software library and to provide its protocol configurations like FTP, SCP, SFTP and HTTP/HTTPS. System Manager uses the FTP/SCP/SFTP configuration to transfer files to a remote software library during the software/firmware download process. The IP Office use the HTTP/HTTPS configuration to retrieve the software/firmware files from the software library during the upgrade process.

The System Platform based CM uses the the HTTP/HTTPS configuration to retrieve the software/firmware files from the software library during the upgrade (6.x to 6.x) process.

Commit Clear Configuration Cancel

Library Server Details (L) * SCP Configuration (S) SFTP Configuration (T) FTP Configuration (F) HTTP/HTTPS Configuration (H)

Remote Library ☒

Local Survivable Processor(LSP) ☐

* **Name** RemoteLibrary1

* **IP Address** 148.147.216.200

Description

* **Server Path** /library

Default Library ☐

* **Default Protocol** FTP (Enter the values for the mandatory fields in the protocol configuration tab you selected.)

Commit Clear Configuration Cancel

Figure 8: Adding Software Library – Server Details

Library Server Details (L) * **SCP Configuration (S)** SFTP Configuration (T) FTP Configuration (F) HTTP/HTTPS Configuration (H)

Enable SCP ☒

* **User Name** scpuser

* **Password**

* **Confirm Password**

Figure 9: Adding Software Library – SCP Configuration

Library Server Details (L) * SCP Configuration (S) **SFTP Configuration (T)** FTP Configuration (F) HTTP/HTTPS Configuration (H)

Enable SFTP ☒

* **User Name** sftpuser

* **Password**

* **Confirm Password**

Figure 10: Adding Software Library – SFTP Configuration

Library Server Details (L) * SCP Configuration (S) SFTP Configuration (T) **FTP Configuration (F)** HTTP/HTTPS Configuration (H)

Enable FTP ☒

* **User Name** ftpuser

* **Password**

* **Confirm Password**

Figure 11: Adding Software Library – FTP Configuration

2.2 Things to know for configuring your elements in System Manager

Manage Elements

Upgrades and Updates are dependent on elements which are added in Manage Elements under Home/Services/Inventory/Manage Elements. Elements can be discovered using Subnet Discovery ([see Appendix C for more details](#)) or manually adding in Manage Elements.

Communication Manager	
1.	Enable SNMP Configuration in Communication Manager. See Appendix B for details.
2.	It is required to provide SNMP Configuration in Manage Elements configured on a specific CM. See Appendix B for details. This access information is required for fetching the release and configuration data from CM.
3.	If the CM is System Platform based, make sure to add System Platform in the Manage Elements manually or using discovery.
4.	If the CM is discovered using subnet discovery, edit the CM entry in Manage Elements to add SNMP access attributes configured on your CM.
5.	For CM Duplex case - make sure both the CMs are added in Manage Elements.
6.	For CM Duplex case - while manually adding Primary CM, provide Standby IP in Alternate IP field on the SMGR Manage Elements UI.
7.	For CM Duplex case - while manually adding Standby CM, provide Active IP in Alternate IP field on the System Manager Manage Elements UI.
8.	For CM Duplex case - while manually adding Standby CM, make sure to “ Add to Communication Manager ” checkbox is unchecked on the System Manager Manage Elements UI.
9.	Create a prof18 user on CM which would be required for migration to 7.0.

Table 5: Configuring Communication Manager in Manage Elements

System Platform	
1.	Manually adding System Platform, make sure to add admin and root user credentials, this is required to discover VMs running on System Platform. If System Platform is discovered using Subnet Discovery, ensure that you edit and add admin and root user credentials.
2.	The discovery of the System Platform automatically adds Template (The System Platform template which consists of the Virtual Machines deployed is added as an element in Manage Elements) and Utility Services (if available) in to <u>/Home/Services/Inventory/Manage Elements</u> .
3.	The other VMs running under System Platform needs to be either manually added in Manage Elements or to be discovered using Subnet Discovery .
4.	If System Platform is added as the first element, you must run Refresh Element again on System Platform once all the System Platform VMs are added.

Table 6: Configuring System Platform in Manage Elements

Session Manager & Branch Session Manager	
1.	SM and BSM must be added manually in Manage Elements, the subnet discovery is not supported for SM and BSM.
2.	Before adding SM and BSM, SIP Entity is required to be created from <u>Home/Elements/Routing/SIP Entities</u> .
3.	Ensure that you add System Platform associated with BSM.
4.	To get the current version of SM or BSM, ensure that SM or BSM is managed by System Manager.

Table 7: Configuring Session Manager & Branch Session Manager in Manage Elements

Media Gateway	
1.	Ensure SNMP is enabled for your Media Gateway. See Appendix B for details.
2.	Configure SNMP Attributes in System Manager Manage Elements. See Appendix B for details.
3.	Media Gateway cannot be updated using local software library. Only remote software library can be used for updating Media Gateways.
4.	FTP is the only supported protocol to be configured in Remote Software Library to update Media Gateways.

Table 8: Configuring Media Gateway in Manage Elements

Media Module & TN Board	
1.	Media Modules and TN Boards are automatically added to Manage Elements on discovery of Media Gateways and CM respectively.
2.	Media Modules and TN Boards cannot be updated using local System Manager software library. Only remote software library can be used for updating Media Modules and TN Boards.
3.	SCP is the only supported protocol to be configured in Remote Software Library to update TN Boards.
4.	The TN Boards firmware will always be uploaded to the home directory of the SCP user configured in Software Library irrespective of whatever path is provided in Software Library “Library Server Details”.

Table 9: Configuring Media Module & TN Boards in Manage Elements

Communication Manager Messaging (CMM)	
1.	Only CMM running as a service is supported for migration to Release 7.0.
2.	CMM will automatically be added in Manage Elements on discovery of CM.
3.	CM will be the parent of CMM added.
4.	CMM will be upgraded to a new VM.
5.	There is no automatic backup and restore of CMM running as a service. It is recommended to take manual backup of CMM files (follow element specific guide for the steps) and do manual restore if required.
6.	SDM doesn't support backup/restore of CMM as the size of the backup may be very large which could occupy all the space on System Manager.
7.	Make sure to install CMM RFUs (A9021rf+i.rpm and C1317rf+i.rpm from support site) before taking backup on 5.2.1.

Table 10: Configuring Communication Manager Messaging in Manage Elements

2.3 Upgrade Release Selection

System Manager SDM supports backward compatibility for features provided in System Manager Release 6.3.8. This can be achieved by using Upgrade Release Selection. For changing SDM release settings navigate to [Home/Services/Solution Deployment Manager/Upgrade Release Selection](#).

- For upgrade to Release 6.3.8, choose [SMGR 6.3.8](#) from Upgrade to release drop-down and Commit.
- For upgrade to Release 7.0 and above, choose [SMGR 7.0](#) from Upgrade to release drop-down and Commit.

Based on the Upgrade Release Selection, the page [Home/Services/Solution Deployment Manager/Upgrade Management](#) would display 6.3.8 or 7.0 User Interface.

The 6.3.8 user interface provides the flow for Communication Manager upgrades till CM 6.x release.

The 7.0 user interface provides the flow to upgrade Communication Manager, Communication Manager Messaging, Session Manager, Branch Session Manager and Utility Services to 7.0 release.

Figure 12: Upgrade Release Selection Page

3. STAGING

Before we can start upgrading, stage the upgrade so that that we know that upgrade will be successful. Navigate to [Home/Services/Solution Deployment Manager/Upgrade Management](#) for staging the elements to be upgraded.

The staging steps are divided into 4 steps:

Staging Step	Description
Refresh Element(s)	1. Refresh Element fetches the current state of the element for which the operation is triggered.
	2. It is recommended that before start of any upgrade/update operation the element is refreshed.
	3. Refresh element fetches the current version of the element and updates <u>Current Version</u> column.
Analyze	1. Analyze operation parses the versions xml files available either on PLDS or alternate source or local source
	2. It checks the current version populated by Refresh Element and checks entitlements based on Current Version.
	3. Entitlements are based on the Customer's Sold To Identification configured in User Settings for PLDS connections .
	4. If an alternate or local source is used then all the entitled versions defined in the version xml files will be used
	5. The available version for the elements will be populated in <u>Entitled Upgrade Version</u> and <u>Entitled Update Version</u> column.
	6. Analyze always shows the latest load in Entitled Upgrade and Update Version.
	7. Make sure the Current Version is populated for the elements before using the? Analyze operation.
Download	1. If Sync Settings are used, then use Refresh Families to get the latest version xml files data.
	2. The latest version of the element can be downloaded using Download option.
	3. Download will give option to select local software library or remote software library if configured.
	4. If software is downloaded for Media Gateway, Media Module or TN Boards use remote software library.
	5. Make sure to run Analyze again after download of the file is complete.
	6. The download button is enabled if any of the selected element status is Upgrade or Update Required (✖).
	7. Media Server on Download Page is for downloading CM artifacts.
Pre-upgrade Check	1. Make sure elements Release Status or Update status are in Ready For Upgrade or Update state (🔒).
	2. If the target host is selected as Same Box , then Data Store column will not be populated and can be left unselected.
	3. The Data Store column is populated on selection of the target host selected.
	4. The Upgrade/Update To column is populated on selection of Upgrade Source column.
	5. The Flexi Footprint column is populated on selection of Upgrade/Update To column.
	6. In case of patching, the target host will only be populated with the ESXi/AVP host on which the VM resides.
	7. If Upgrade/Update To column are not populated with any data, it means that no software have been downloaded for that element.
	8. If Upgrade/Update To column are not populated with .ova file then the

	Flexi footprint will not be populated and can be left unselected.
	9. For updating an element make sure that trust is established between System Manager and element and ESXi/AVP IP/Name is shown as parent for the element.
	10. If any of the recommended check fails during pre-upgrade check, admin can still continue with upgrade.
	11. If any of the mandatory check fails during pre-upgrade check, the upgrade will not be allowed to continue.
	12. Pre-upgrade check is only available for CM, SM, BSM, CMM and US.

Table 11: Staging Steps for Upgrade

3.1 Element Selection

As part of element selection here are few things to note:

Element Selection for Upgrade	
1.	Once System Platform or any of its elements is selected, all the SP elements will be automatically selected.
2.	The System Platform and associated Template for Release 7.0 and above will be in Non-upgradable state.
3.	If CMM is running as a service in CM, selecting CM or CMM will select both the elements.
4.	Upgrade Management provides element selection in child hierarchy view. Refer to Appendix H - Element Selection for more details.
5.	The Show Selected Elements can be used to filter selected elements, once the link is clicked all the elements will be filtered to show only selected elements.
6.	The Upgrade Management page can refresh automatically once the link Enable Auto Refresh (10 sec) is clicked. This will refresh the page every 10 seconds.
7.	The auto refresh can be disabled by clicking on Disable Auto Refresh link which shows up once enable link is clicked.

Table 12: Element Selection on Upgrade Management Page

3.2 Supported Elements

Here is a list of elements supported for migration and patching from SDM Upgrade Management from Release 7.0 perspective.

Supported Element	Migration	Patching	Description
SP based CM	✓	✗	Patching not supported for SP based CM. Choose SMGR 6.3.8 from Upgrade to release drop-down on Upgrade Release Selection page for patching SP based.
SP based BSM	✓	✗	Patching not supported for SP based BSM.
SP based Utility Services	✓	✗	Patching not supported for SP based Utility Services.
Linux-based SM	✓	✗	Patching not supported for Linux-based SM.
Linux-based CM	✓	✗	Patching not supported for Linux-based CM. Choose SMGR 6.3.8 from Upgrade to release drop-down on Upgrade Release Selection page for patching Linux-based CM.
CMM running as service inside CM	✓	✗	CMM running as service inside CM is only supported. No other flavors of CMM are supported for migration. CMM will automatically be added as element in Manage Elements and will be migrated to a new VM.
Media Gateway, Media Module and TN Boards	N/A	✓	MG, MM and TN Boards patching is supported.
6.x VMware based CM	✗	✗	VE to VE migration support is not available in 7.0. Choose SMGR 6.3.8 from Upgrade to release drop-down on Upgrade Release Selection page for patching Linux-based CM.
6.x VMware based CMM	✗	✗	VE to VE migration/patching support is not available in 7.0.
6.x VMware based SM	✗	✗	VE to VE migration/patching support is not available in 7.0.
7.0 VMware based CM	N/A	✓	Patching support is available for 7.0 VMware-based CM
7.0 VMware based CMM	N/A	✓	Patching support is available for 7.0 VMware-based CMM
7.0 VMware based SM	N/A	✓	Patching support is available for 7.0 VMware-based SM
7.0 VMware based BSM	N/A	✓	Patching support is available for 7.0 VMware-based BSM.
7.0 VMware based Utility Services	N/A	✓	Patching support is available for 7.0 VMware-based US.
7.0 VMware to 7.0 VMware elements	✗	N/A	This is from Beta perspective wherein 7.0 VE elements are already installed. No upgrade is supported. Follow element-specific document for manual backup and restore.

Table 13: Supported elements for migration and patching

3.3 Capacity

System Manager SDM supports simultaneous upgrades/updates for Aura elements making it a very beneficial feature in Avaya Aura 7. The following are the simultaneous job capacities for the elements:

- **5 Upgrade/Update Job Groups:** Multiple elements combined together in an upgrade/update job are considered as a group.
- **20 elements in each job group:** Maximum elements that can be combined in an upgrade/update group is 20. Any supported element type can be combined for upgrade in a group.

Elements in 'Paused State' are also considered in above capacity. If there are 5 job groups in running or in paused state, any further upgrades will not be allowed. The 'Paused State' is the part of the CM, SM, BSM or US upgrade-migration process when the upgrade will pause when the System Platform or Linux-based server has the Appliance Virtualization Platform (AVP) loaded to an existing Server in the customer's solution.

Note: There is a restriction of 90 simultaneous jobs in System Manager Scheduler. The jobs will be sequenced in that case.

3.4 Refresh element(s)

Navigate to Home/Services/Solution Deployment Manager/Upgrade Management, select element(s) to refresh elements, click on Pre-Upgrade Actions→Refresh Element(s). Click on Schedule to start the refresh job.

Name	Parent	Type	Sub-Type	IP Address	Release Status	Update Status	Last Action	Last Action Status	Pre-upgr Check Status
BSM_97	CM_SurvRemoteEmbed	Session Manager	Branch Session Manager	148.147.178.97	?	?			⚠
CM_65		Communication Manager	Avaya Aura(R) Communication Manager	148.147.162.65	?	?			⚠
CM_80	CM_SurvRemoteEmbed	Communication Manager	Avaya Aura(R) Communication Manager	148.147.178.80	?	?			⚠
CM_SurvRemoteEmbed	SP128	Templates		148.147.178.128	?	?			N/A
SP128		System Platform	System Platform	148.147.178.128	?	?			N/A
utility_server_148.147.178.185	CM_SurvRemoteEmbed	Utility Server		148.147.178.185	?	?			⚠

Figure 13: Upgrade Management Page Pre-upgrade Actions – Refresh Element

After completion of the process the Current Version column would be updated with latest information.

Name	Parent	Type	Sub-Type	IP Address	Release Status	Update Status	Last Action	Last Action Status	Pre-upgrade Check Status	Current Version	Ent Up Ver
BSM_97	CM_SurvRemoteEmbed	Session Manager	Branch Session Manager	148.147.178.97	?	?	Refresh Element	✓	⚠	6.0.0.0.600019	
CM_65		Communication Manager	Avaya Aura(R) Communication Manager	148.147.162.65	?	?			⚠	R016x.03.0.124.0	
CM_80	CM_SurvRemoteEmbed	Communication Manager	Avaya Aura(R) Communication Manager	148.147.178.80	?	?	Refresh Element	✓	⚠	R016x.00.0.345.0	
CM_SurvRemoteEmbed	SP128	Templates		148.147.178.128	?	?	Refresh Element	✓	N/A	6.0.0.0.1803	
SP128		System Platform	System Platform	148.147.178.128	?	?	Refresh Element	✓	N/A	6.0.0.0.1803	
utility_server_148.147.178.185	CM_SurvRemoteEmbed	Utility Server		148.147.178.185	?	?	Refresh Element	✓	⚠	6.0.0.0.9	

Figure 14: Refresh Element Action Complete

3.5 Analyze

Analyze is a critical operation in the staging of an upgrade. The basic purpose of analyze is:

1. To get and recommend the latest and greatest available release/update version for selected device.
2. To get the all the entitled versions (major release/update) for selected element and recommend the latest entitled version among them.
3. To get and recommend the different upgrade/update state based on available version, entitled version for selected element(s).

Following are the different release status and update status presently supported.









State	Symbolic Representation	Description
Upgrade Required		New upgrade/release version is available for upgrade but the software file is not downloaded yet in software library.
Ready for Upgrade		Entitled version is downloaded in software library and available for upgrade.
Upgraded		Element is on latest upgrade/release version.
Non Upgradable		Element is non upgradable.
Unknown		The status is not known yet as Analyze is not executed.
Update Required		New update/patch version is available for update but the software file is not downloaded yet in software library.
Ready for Update		Entitled update/patch version is downloaded in software library and available for update.
Updated		Element is on latest update/patch version.
N/A	N/A	There is no further update applicable to this Element and its release version.

Table 14: Symbolic Representation for Analyze Operation

Elements before running Analyze Operation in the screenshots below.

Release Status and Update Status are in Unknown state highlighted below.

Upgrade Management

Enable Auto Refresh(10 sec) | Show Selected Elements










Pre-upgrade Actions

Refresh Element(s)
Analyze
Pre-upgrade Check

Upgrade Actions

Download

Filter: Enable

<input type="checkbox"/>	Name	Parent	Type	Sub-Type	IP Address	Release Status	Update Status	Last Action	Last Action Status	Pre-up Check Status
<input checked="" type="checkbox"/>	BSM_97	CM_SurvRemoteEmbed	Session Manager	Branch Session Manager	148.147.178.97	?	?	Refresh Element		
<input type="checkbox"/>	CM_65		Communication Manager	Avaya Aura(R) Communication Manager	148.147.162.65	?	?			
<input checked="" type="checkbox"/>	CM_80	CM_SurvRemoteEmbed	Communication Manager	Avaya Aura(R) Communication Manager	148.147.178.80	?	?	Refresh Element		
<input checked="" type="checkbox"/>	CM_SurvRemoteEmbed	SP128	Templates		148.147.178.128	?	?	Refresh Element		N/A
<input checked="" type="checkbox"/>	SP128		System Platform	System Platform	148.147.178.128	?	?	Refresh Element		N/A
<input checked="" type="checkbox"/>	utility_server_148.147.178.185	CM_SurvRemoteEmbed	Utility Server		148.147.178.185	?	?	Refresh Element		

Select : All, None

Figure 15: Upgrade Management Page Pre-upgrade Actions - Analyze

Entitled Upgrade Version and Entitled Update Versions are not populated highlighted in blue rectangle below.

Pre-upgrade Actions

Upgrade Actions

Download

6 Items

Show All

Filter: Enable

Type	Sub-Type	IP Address	Release Status	Update Status	Last Action	Last Action Status	Pre-upgrade Check Status	Current Version	Entitled Upgrade Version	Entitled Update Version
Session Manager	Branch Session Manager	148.147.178.97	?	?	Refresh Element	✓	⚠	6.0.0.0.600019		
Communication Manager	Avaya Aura(R) Communication Manager	148.147.162.65	?	?			⚠	R016x.03.0.124.0		
Communication Manager	Avaya Aura(R) Communication Manager	148.147.178.80	?	?	Refresh Element	✓	⚠	R016x.00.0.345.0		
Templates		148.147.178.128	?	?	Refresh Element	✓	N/A	6.0.0.0.1803		
System Platform	System Platform	148.147.178.128	?	?	Refresh Element	✓	N/A	6.0.0.0.1803		
Utility Server		148.147.178.185	?	?	Refresh Element	✓	⚠	6.0.0.0.9		

◀

|||

▶

Select : All, None

Figure 16: Upgrade Management Page Status and Entitled Versions

Click on Pre-upgrade Actions → Analyze, click on Schedule button to start the analyze job. After completion of the analyze job the entitled versions are populated and Release & Update status are showing as Upgrade Required. The Entitled Upgrade Version is also populated with the latest entitled version.

Pre-upgrade Actions

Upgrade Actions

Download

6 Items

Show All

Filter: Enable

Type	Sub-Type	IP Address	Release Status	Update Status	Last Action	Last Action Status	Pre-upgrade Check Status	Current Version	Entitled Upgrade Version	Entitled Update Version
Session Manager	Branch Session Manager	148.147.178.97	✗	N/A	Analyze	✓	⚠	6.0.0.0.600019	7.0.0.0.700007	N/A
Communication Manager	Avaya Aura(R) Communication Manager	148.147.162.65	?	?			⚠	R016x.03.0.124.0		
Communication Manager	Avaya Aura(R) Communication Manager	148.147.178.80	✗	N/A	Analyze	✓	⚠	R016x.00.0.345.0	7.0.0.0.441	N/A
Templates		148.147.178.128	✗	✗	Analyze	✓	N/A	6.0.0.0.1803	N/A	N/A
System Platform	System Platform	148.147.178.128	✗	✗	Analyze	✓	N/A	6.3.0.0.18002	N/A	N/A
Utility Server		148.147.178.185	✗	N/A	Analyze	✓	⚠	6.0.0.0.9	7.0.0.0.0.11	N/A

Select : All, None

Figure 17: Upgrade Management Page Status and Entitled Versions Updated

Note: In the above example if the software files are already downloaded, the Release and Update Status will show as Ready For Upgrade (⚠).

3.6 Download

Download option is available on Upgrade Management Page to download the entitled version from PLDS or alternate source. The download button will be enabled once the selected element Release or Update status is ready for upgrade or update.

If PLDS or Alternate source is not configured, [Sync Settings](#) can be used for already downloaded files to upload to [Software Library](#).

Upgrade Management Enable Auto Refresh(10 sec) | Show Selected Elements

Pre-upgrade Actions ▾ Upgrade Actions ▾ **Download**

6 Items Show All ▾ Filter: Enable

<input type="checkbox"/>	Name	Parent	Type	Sub-Type	IP Address	Release Status	Update Status	Last Action	Last Action Status	Pre-up Check Status
<input checked="" type="checkbox"/>	BSM_97	CM_SurvRemoteEmbed	Session Manager	Branch Session Manager	148.147.178.97	✗	N/A	Analyze	✓	⚠
<input type="checkbox"/>	CM_65		Communication Manager	Avaya Aura(R) Communication Manager	148.147.162.65	?	?			⚠
<input checked="" type="checkbox"/>	CM_80	CM_SurvRemoteEmbed	Communication Manager	Avaya Aura(R) Communication Manager	148.147.178.80	✗	N/A	Analyze	✓	⚠
<input checked="" type="checkbox"/>	CM_SurvRemoteEmbed	SP128	Templates		148.147.178.128	✗	✗	Analyze	✓	N/A
<input checked="" type="checkbox"/>	SP128		System Platform	System Platform	148.147.178.128	✗	✗	Analyze	✓	N/A
<input checked="" type="checkbox"/>	utility_server_148.147.178.185	CM_SurvRemoteEmbed	Utility Server		148.147.178.185	✗	N/A	Analyze	✓	⚠

Select : All, None

Figure 18: Upgrade Management Page Download Action

Clicking on Download button on Upgrade Management Page will navigate to Download Management page ([Home/Services/Solution Deployment Manager/Download Management](#)).

Select Family options to download the software from PLDS or alternate source.

Home

Solution Deployment Manager

Home / Services / Solution Deployment Manager / Upgrade Management

Help ?

Solution Deployment Manager

Upgrade Release Selection

Manage Software

Upgrade Management

Upgrade Jobs Status

VM Management

User Settings

Download Management

Software Library Management

File Download Manager

File Download Manager gets the software/firmware files from the Avaya Product Delivery and Licensing System (PLDS) or directly from your computer (if you have already downloaded from PLDS) on to System Manager. Use these files later to upgrade the software/firmware of devices.

Select Software/Hardware Types.

Refresh Families

The Refresh Families synch/fetch latest artifact(firmware/software) information for supported product families from Alternate Source/Avaya Support Site(with entitlements) and update the same on Download Manager. It might take more time to complete this operation depends on the Source Configuration that selected in User Settings.

[List View]

63 Items

Select	Family Name	Hardware/ Software
<input checked="" type="checkbox"/>	Media Servers	
<input type="checkbox"/>		CM Service Pack
<input type="checkbox"/>		CM Custom Patch
<input type="checkbox"/>		Kernel Update
<input type="checkbox"/>		MPC firmware
<input type="checkbox"/>		SAMP firmware
<input type="checkbox"/>		SES Service Pack
<input type="checkbox"/>		Pre-Installation Patch
<input type="checkbox"/>		CM VMware Tools Service Pack
<input type="checkbox"/>		Platform/Security Update
<input checked="" type="checkbox"/>		OVA Template
<input type="checkbox"/>	System Platform	
<input type="checkbox"/>	TN Boards	
<input checked="" type="checkbox"/>	Branch Session Manager	
<input type="checkbox"/>		Custom Patch
<input checked="" type="checkbox"/>		OVA BSM Template
<input type="checkbox"/>		Update
<input type="checkbox"/>	Utility Server	
<input type="checkbox"/>		Custom Patch
<input checked="" type="checkbox"/>		OVA US Template
<input type="checkbox"/>		Update
<input type="checkbox"/>	Session Manager	
<input type="checkbox"/>	Communication Manager Messaging	
<input type="checkbox"/>	Others	

Select: All None

Show Files

Select Files Download Details.

File Download Status

Delete

0 Items

Show All

Filter: Enable

File Name	Job Name	Current Step	Percentage Completed	Status	Scheduled By
-----------	----------	--------------	----------------------	--------	--------------

Figure 19: Download Management Page

Click on Show Files button after selecting appropriate option. The show files will show available entitled files for the family options selected.
Select the required files from the list of entitled versions.

Select Files Download Details.

* Source Avaya PLDS/Alternate Source

Download

16 Items Show 15 Filter: Enable

<input type="checkbox"/>	File Name	Version	Entitled	File Size (in bytes)	Hardware/ Software	Family Name	Content Type	Software Library	File Description
<input checked="" type="checkbox"/>	BSM-7.0.0.0.700007-e55-01.ova	7.0.0.0.700007	Yes	2066114150	OVA BSM Template	Branch Session Manager	OVA BSM Template	Not Downloaded	Branch Session Manag ... More
<input type="checkbox"/>	CM-Duplex-07.0.0.0.437-e55-0.ova	7.0.0.0.437	Yes	786721792	CM_Duplex	Media Servers	OVA Template	Not Downloaded	CM Duplex OVA for Av ... More
<input type="checkbox"/>	CM-Duplex-07.0.0.0.438-e55-0.ova	7.0.0.0.438	Yes	796050432	CM_Duplex	Media Servers	OVA Template	Not Downloaded	CM Duplex OVA for Av ... More
<input type="checkbox"/>	CM-Duplex-07.0.0.0.439-e55-0.ova	7.0.0.0.439	Yes	784606208	CM_Duplex	Media Servers	OVA Template	Not Downloaded	CM Duplex OVA for Av ... More
<input type="checkbox"/>	CM-Duplex-07.0.0.0.440-e55-0.ova	7.0.0.0.440	Yes	790276096	CM_Duplex	Media Servers	OVA Template	Not Downloaded	Communication Manage ... More
<input type="checkbox"/>	CM-Duplex-07.0.0.0.441-e55-0.ova	7.0.0.0.441	Yes	782730752	CM_Duplex	Media Servers	OVA Template	Not Downloaded	CM Duplex OVA for Av ... More
<input type="checkbox"/>	CM-Simplex-07.0.0.0.437-e55-0.ova	7.0.0.0.437	Yes	788647936	CM_Simplex	Media Servers	OVA Template	Not Downloaded	CM Simplex OVA for A ... More
<input type="checkbox"/>	CM-Simplex-07.0.0.0.438-e55-0.ova	7.0.0.0.438	Yes	797893120	CM_Simplex	Media Servers	OVA Template	Not Downloaded	CM Simplex OVA for A ... More
<input type="checkbox"/>	CM-Simplex-07.0.0.0.439-e55-0.ova	7.0.0.0.439	Yes	782234112	CM_Simplex	Media Servers	OVA Template	Not Downloaded	CM Simplex OVA for A ... More
<input type="checkbox"/>	CM-Simplex-07.0.0.0.440-e55-0.ova	7.0.0.0.440	Yes	789238272	CM_Simplex	Media Servers	OVA Template	Not Downloaded	Communication Manage ... More
<input checked="" type="checkbox"/>	CM-Simplex-07.0.0.0.441-e55-0.ova	7.0.0.0.441	Yes	781126144	CM_Simplex	Media Servers	OVA Template	Not Downloaded	CM Simplex OVA for A ... More
<input type="checkbox"/>	US-7.0.0.0.0.10-e55-01_OVF10.ova	7.0.0.0.0.10	Yes	1076887552	OVA US Template	Utility Server	OVA US Template	Not Downloaded	Utility Services V7. ... More
<input checked="" type="checkbox"/>	US-7.0.0.0.0.11-e55-01_OVF10.ova	7.0.0.0.0.11	Yes	1213202432	OVA US Template	Utility Server	OVA US Template	Not Downloaded	Utility Services GA ... More
<input type="checkbox"/>	US-7.0.0.0.0.7-e55-01_OVF10.ova	7.0.0.0.0.7	Yes	991670272	OVA US Template	Utility Server	OVA US Template	Not Downloaded	Utility Server 7.0 O ... More
<input type="checkbox"/>	US-7.0.0.0.0.8-e55-01_OVF10.ova	7.0.0.0.0.8	Yes	1025384448	OVA US Template	Utility Server	OVA US Template	Not Downloaded	Utility Server 7.0 O ... More

Select : All, None Page 1 of 2

Figure 20: Download Management Files selection section

Click on Download button, the page will be redirected to Library and Protocol Selection Page.

Home / Services / Solution Deployment Manager / Upgrade Management

Files Download Manager - Library and Protocol Selection

Download Reset Cancel

3 Items

File Name	Version	File Size (in bytes)	Hardware/ Software	Family Name	Library	Protocol
BSM-7.0.0.0.700007-e55-01.ova	7.0.0.0.700007	2066114150	OVA BSM Template	Branch Session Manager	SMGR_DEFAULT_LOCAL - 1	
CM-Simplex-07.0.0.0.441-e55-0.ova	7.0.0.0.441	781126144	CM_Simplex	Media Servers	SMGR_DEFAULT_LOCAL - 1	
US-7.0.0.0.0.11-e55-01_OVF10.ova	7.0.0.0.0.11	1213202432	OVA US Template	Utility Server	SMGR_DEFAULT_LOCAL - 1	

Download Reset Cancel

Figure 21: Download Management Library and Protocol Selection Page

- Select the library and protocol. Using the specified protocol and the credentials provided for that protocol the file will be uploaded to the specified software library.
- If the Library selected is local library, the protocol is not required as it will be just copy to the local directory after downloading the file from PLDS or Alternate Source
- Click on Download button to continue the download.
- Download button will redirect to End User Licensing Agreement (EULA). Agree to the license agreement and click Now to start the download.
- Schedule option is also available if software needs to be downloaded at a later time.

END USER LICENSING AGREEMENT

Important-Read Carefully:

AVAYA GLOBAL SOFTWARE LICENSE TERMS
REVISED: March 2015

THIS END USER LICENSE AGREEMENT ("SOFTWARE LICENSE TERMS") GOVERNS THE USE OF PROPRIETARY SOFTWARE AND THIRD-PARTY PROPRIETARY SOFTWARE LICENSED THROUGH AVAYA. READ THESE SOFTWARE LICENSE TERMS CAREFULLY, IN THEIR ENTIRETY, BEFORE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (AS DEFINED IN SECTION A BELOW), BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU," "YOUR," AND "END USER"), AGREE TO THESE SOFTWARE LICENSE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA"). IF YOU ARE ACCEPTING THESE SOFTWARE LICENSE TERMS ON BEHALF OF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE SOFTWARE LICENSE TERMS. IF YOU DO NOT HAVE SUCH AUTHORITY OR DO NOT WISH TO BE BOUND BY THESE SOFTWARE LICENSE TERMS, YOU MUST RETURN OR DELETE THE SOFTWARE WITHIN TEN (10) DAYS OF DELIVERY FOR A REFUND OF THE FEE, IF ANY, YOU PAID FOR THE LICENSE OR IF SOFTWARE IS ACCESSED ELECTRONICALLY, SELECT THE "DECLINE" BUTTON AT THE END OF THESE SOFTWARE LICENSE TERMS OR THE EQUIVALENT OPTION.

A. Definitions

(i) "Affiliate" means any entity that is directly or indirectly controlling, controlled by, or under common control with Avaya Inc. or End User. For purposes of this definition, "control" means the power to direct the management and policies of such party, directly or indirectly, whether through ownership of voting securities, by contract or otherwise; and the terms "controlling" and "controlled" have meanings correlative to the foregoing.

(ii) "Documentation" means information published in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials.

(iii) "Software" means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products and accessories, under either a buy, lease, or modified license, or other arrangement.

☒ I Agree to the above end user license agreement.

[Now](#) [Schedule](#) [Cancel](#)

Figure 22: Download Management End User License Agreement Page.

Clicking on Now button will start the download and will be redirected to File Download Manager where the status of the download can be monitored.

File Download Manager

File Download Manager gets the software/firmware files from the Avaya Product Delivery and Licensing System (PLDS) or directly from your computer (if you have already downloaded from PLDS) on to System Manager. Use these files later to upgrade the software/firmware of devices.

[Delete](#)

File Download Status

3 Items [Show All](#) [Filter: Enable](#)

File Name	Job Name	Current Step	Percentage Completed	Status	Scheduled By
US-7.0.0.0.11-e55-01_OVF10.ova	IUM_file_download_1439816910571	Scheduled for download	0	Download pending	admin
CM-Simplex-07.0.0.0.441-e55-0.ova	IUM_file_download_1439816910571	Scheduled for download	0	Download pending	admin
BSM-7.0.0.0.700007-e55-01.ova	IUM_file_download_1439816910571	Scheduled for download	0	Download pending	admin

Select : All, None

Figure 23: Download Management File Download Status Section

The software will be downloaded from PLDS or alternate source and the time taken for download and uploading the software to software library may vary on size of the file and the download speed. Wait for Current Step to change to File created and Status column to Download completed.

File Download Manager

File Download Manager gets the software/firmware files from the Avaya Product Delivery and Licensing System (PLDS) or directly from your computer (if you have already downloaded from PLDS) on to System Manager. Use these files later to upgrade the software/firmware of devices.

Select Software/Hardware Types. ▶

Select Files Download Details. ▶

File Download Status ▼

Delete

3 Items Show All Filter: Enable

	File Name	Job Name	Current Step	Percentage Completed	Status	Scheduled By
<input type="checkbox"/>	US-7.0.0.0.0.11-e55-01_OVF10.ova	IUM_file_download_1439816910571	File created	100	Download completed	admin
<input type="checkbox"/>	CM-Simplex-07.0.0.0.441-e55-0.ova	IUM_file_download_1439816910571	File created	100	Download completed	admin
<input type="checkbox"/>	BSM-7.0.0.0.700007-e55-01.ova	IUM_file_download_1439816910571	File created	100	Download completed	admin

Select : All, None

Figure 24: Download Management File Download updated status

Once the file is download it is required to run Analyze on the elements again. Navigate to Home/Services/Solution Deployment Manager/Upgrade Management. Select the elements and from Pre-upgrade Actions choose Analyze to schedule the job. After the completion of Analyze job the selected elements are now in **Ready For Upgrade** state (⚠).

Home Solution Deployment Manager Scheduler

Home / Services / Solution Deployment Manager / Upgrade Management

Upgrade Management

Enable Auto Refresh(10 sec) | Show Selected Elements

Pre-upgrade Actions Upgrade Actions Download

6 Items Show All Filter: Enable

	Name	Parent	Type	Sub-Type	IP Address	Release Status	Update Status	Last Action	Last Action Status	Pre-upg Check Status
<input checked="" type="checkbox"/>	BSM_97	CM_SurvRemoteEmbed	Session Manager	Branch Session Manager	148.147.178.97	⚠	N/A	Analyze	✓	⚠
<input type="checkbox"/>	CM_65		Communication Manager	Avaya Aura(R) Communication Manager	148.147.162.65	?	?			⚠
<input checked="" type="checkbox"/>	CM_80	CM_SurvRemoteEmbed	Communication Manager	Avaya Aura(R) Communication Manager	148.147.178.80	⚠	N/A	Analyze	✓	⚠
<input checked="" type="checkbox"/>	CM_SurvRemoteEmbed	SP128	Templates		148.147.178.128	⊗	⊗	Analyze	✓	N/A
<input checked="" type="checkbox"/>	SP128		System Platform	System Platform	148.147.178.128	⊗	⊗	Analyze	✓	N/A
<input checked="" type="checkbox"/>	utility_server_148.147.178.185	CM_SurvRemoteEmbed	Utility Server		148.147.178.185	⚠	N/A	Analyze	✓	⚠

Select : All, None

Figure 25: Upgrade Management Status after Download & Analyze

3.7 Pre-Upgrade Check

Pre-upgrade Check is one of the important steps which help to assess if the upgrade will be successful or fail. Pre-upgrade Check has different Mandatory and Recommended Checks.

- Mandatory are the checks which have to be successful in order for migration to be successful. These checks must be successful to proceed with the upgrade operation.
- Recommended checks are checks which are good to have, but migration can continue even if these checks fail.
- It is mandatory to execute pre-upgrade check before the actual upgrade. If the Pre-upgrade check is not executed Upgrade Actions will be disabled.

Navigate to Home/Services/Solution Deployment Manager/Upgrade management.

Note: To migrate on a different host, ensure to [add ESXi/AVP host from VM Management](#).

During Pre-upgrade check, the ESXi/AVP host needs to be selected so that SDM can assess the host.

Once the pre-upgrade check is executed using Same Box or an ESXi/AVP host, the different result shows up as symbols. Below are some status symbols of Pre-upgrade checks.






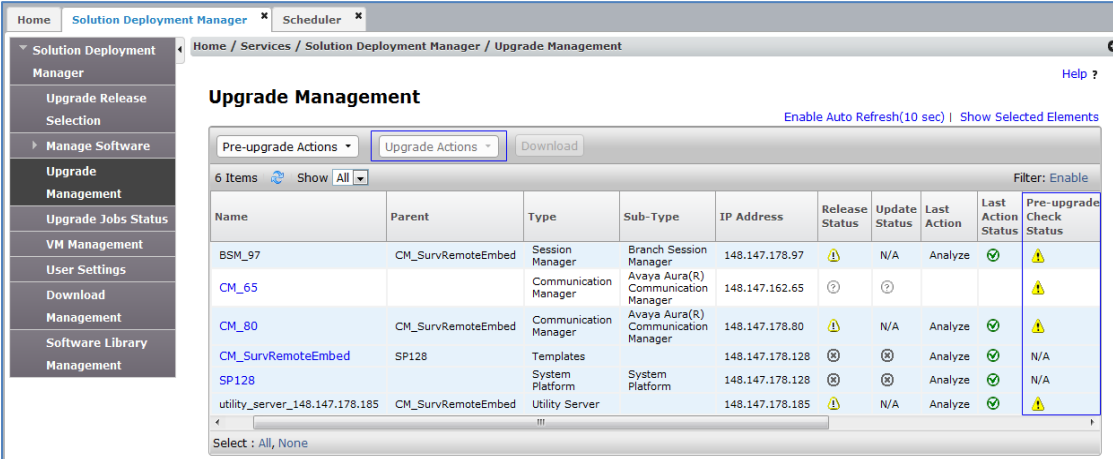
State	Symbolic Representation	Description
Not Executed		Pre-upgrade check has not been executed for the element yet.
Failed		Pre-upgrade check has failed.
Passed		Pre-upgrade check has passed.
Successful with Recommended Failure		All mandatory checks have passed but one or more recommended checks have failed.
Unknown		The check has not started yet.
N/A	N/A	Pre upgrade check is not applicable for the element.

Table 15: Symbolic Representation for Pre-upgrade check Operation



The screenshot displays the 'Upgrade Management' section of the Solution Deployment Manager. It features a sidebar with navigation options like 'Solution Deployment Manager', 'Upgrade Release Selection', 'Manage Software', 'Upgrade Management', 'Upgrade Jobs Status', 'VM Management', 'User Settings', 'Download Management', and 'Software Library Management'. The main area shows a table of upgrade items. The 'Pre-upgrade Actions' dropdown is set to 'Upgrade Actions'. The table has 10 columns: Name, Parent, Type, Sub-Type, IP Address, Release Status, Update Status, Last Action, Last Action Status, and Pre-upgrade Check Status. The items listed are BSM_97, CM_65, CM_80, CM_SurvRemoteEmbed, SP128, and utility_server_148.147.178.185. The Pre-upgrade Check Status column shows symbols: yellow warning triangle for BSM_97, CM_65, and CM_80; red X for CM_SurvRemoteEmbed; green checkmark for SP128; and green checkmark with exclamation mark for utility_server_148.147.178.185.

Figure 25: Upgrade Management Status after Download & Analyze

3.7.1 Running Pre-upgrade Checks

1. Select the elements and go to Pre-upgrade Actions → Pre-upgrade Check. The screenshot below depicts the Pre-upgrade Check configuration:

Home / Services / Solution Deployment Manager / Upgrade Management

Pre-upgrade Configuration

Note: While updating an element, one need to add or manage associated Host from Solution Deployment Manager --> VM Management to get it's parent in Parent Name Column and in the Target Host drop-down.

5 Items Show All

Element Name	Parent Name	IP Address	Current Version	Target Host	Data Store	Upgrade Source	Upgrade/Update To	Flexi Footprint
BSM_97	CM_SurvRemoteEmbed	148.147.178.97	6.0.0.0.600019					
CM_80	CM_SurvRemoteEmbed	148.147.178.80	R016x.00.0.345.0					
CM_SurvRemoteEmbed	SP128	148.147.178.128	6.0.0.0.1803	N/A	N/A	N/A	N/A	N/A
SP128		148.147.178.128	6.3.0.0.18002	N/A	N/A	N/A	N/A	N/A
utility_server_148.147.178.185	CM_SurvRemoteEmbed	148.147.178.185	6.0.0.0.9					

Job Schedule

Run Immediately (selected) / Schedule later

Schedule Job:

Date: August 17 2015

Time: 18:53:25 24Hr

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

Schedule Cancel

Figure 26: Pre-upgrade Configuration page

Select following configurations for Pre-upgrade check:

- **Target Host:** The target host is the ESXi server/AVP or Same Box on which selected element will be migrated. The ESXi list comes from the host added in [Home/Services/Solution Deployment Manager/VM Management](#). Refer to [Appendix E for details on how to add host from VM Management](#).
- **Data Store:** Data Store is the storage location of where the VM will be created. It is populated after selection of Target Host. The list is fetched from the host selected. In case Same Box is selected in Target Host, data store will not be populated and can be left blank.
- **Upgrade Source:** The upgrade source is the software library where the software has been uploaded using [Download option](#) or [Sync option](#). The drop-down will have all the configured libraries.
- **Upgrade/Update To:** Provide option to select the files which are downloaded in the software library. The drop-down is populated after selection of Upgrade Source. For migration it is downloaded ova file for that element type.
- **Flexi Footprint:** Footprint allow configuring element in different flavors, it is based on customer requirement as to which footprint is required based on the hardware. In case of Avaya Virtualization Platform (AVP) footprint will be shown based on the hardware type. The drop-down is populated on selection of OVA.

Home / Services / Solution Deployment Manager / Upgrade Management Help ?

Pre-upgrade Configuration

Note: While updating an element, one need to add or manage associated Host from Solution Deployment Manager --> VM Management to get it's parent in Parent Name Column and in the Target Host drop-down.

5 Items Show All

IP Address	Current Version	Target Host	Data Store	Upgrade Source	Upgrade/Update To	Flexi Footprint
148.147.178.97	6.0.0.0.600019	148.147.178.64	datastore1 (23)	SMGR_DEFAULT_LOCAL	BSM-7.0.0.0.700007-e55-01.ova	BSM 7.0 Profile 2 Max Devices 5,000
148.147.178.80	R016x.00.0.345.0	148.147.178.64	datastore1 (23)	SMGR_DEFAULT_LOCAL	CM-Simplex-07.0.0.0.441-e55-0.ova	CM Survivable Max users 1000
148.147.178.128	6.0.0.0.1803	N/A	N/A	N/A	N/A	N/A
148.147.178.128	6.3.0.0.18002	N/A	N/A	N/A	N/A	N/A
148.147.178.185	6.0.0.0.9	148.147.178.64	datastore1 (23)	SMGR_DEFAULT_LOCAL	US-7.0.0.0.0.11-e55-01_OVF10.ova	Default Resources

Job Schedule

☒ Run Immediately
☐ Schedule later

Schedule Job:

Date: August 17 2015

Time: 20 : 44 : 08 [24Hr]

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

Schedule Cancel

Figure 27: Pre-upgrade Check Configuration populated

Select Run Immediately or Schedule Later and click on Schedule button. The page will be redirected to Upgrade Management Page. The Last Action and Last Action Status will show Pre-upgrade check as last action and status as Pending.

Home / Services / Solution Deployment Manager / Upgrade Management Help ?

Upgrade Management

Enable Auto Refresh(10 sec) | [Show Selected Elements](#)

Pre-upgrade Actions | Upgrade Actions | Download

6 Items Show All Filter: Enable

Name	Parent	Type	Sub-Type	IP Address	Release Status	Update Status	Last Action	Last Action Status	Pre-upgrade Check Status	Current Version
<input checked="" type="checkbox"/> BSM_97	CM_SurvRemoteEmbed	Session Manager	Branch Session Manager	148.147.178.97		N/A	Pre-upgrade Check			6.0.0.0.600019
<input type="checkbox"/> CM_65		Communication Manager	Avaya Aura(R) Communication Manager	148.147.162.65						R016x.03.0.124.0
<input checked="" type="checkbox"/> CM_80	CM_SurvRemoteEmbed	Communication Manager	Avaya Aura(R) Communication Manager	148.147.178.80		N/A	Pre-upgrade Check			R016x.00.0.345.0
<input checked="" type="checkbox"/> CM_SurvRemoteEmbed	SP128	Templates		148.147.178.128			Pre-upgrade Check		N/A	6.0.0.0.1803
<input checked="" type="checkbox"/> SP128		System Platform	System Platform	148.147.178.128			Pre-upgrade Check		N/A	6.3.0.0.18002
<input checked="" type="checkbox"/> utility_server_148.147.178.185	CM_SurvRemoteEmbed	Utility Server		148.147.178.185		N/A	Pre-upgrade Check			6.0.0.0.9

Select : All, None

Figure 28: Pre-upgrade Check Scheduled

Click on Last Action Status icon of each element to check the status of Pre-upgrade check. There are different mandatory and recommended checks which executes as part of Pre-upgrade check. These checks are different for different element types. Click on Done button to close the status window.

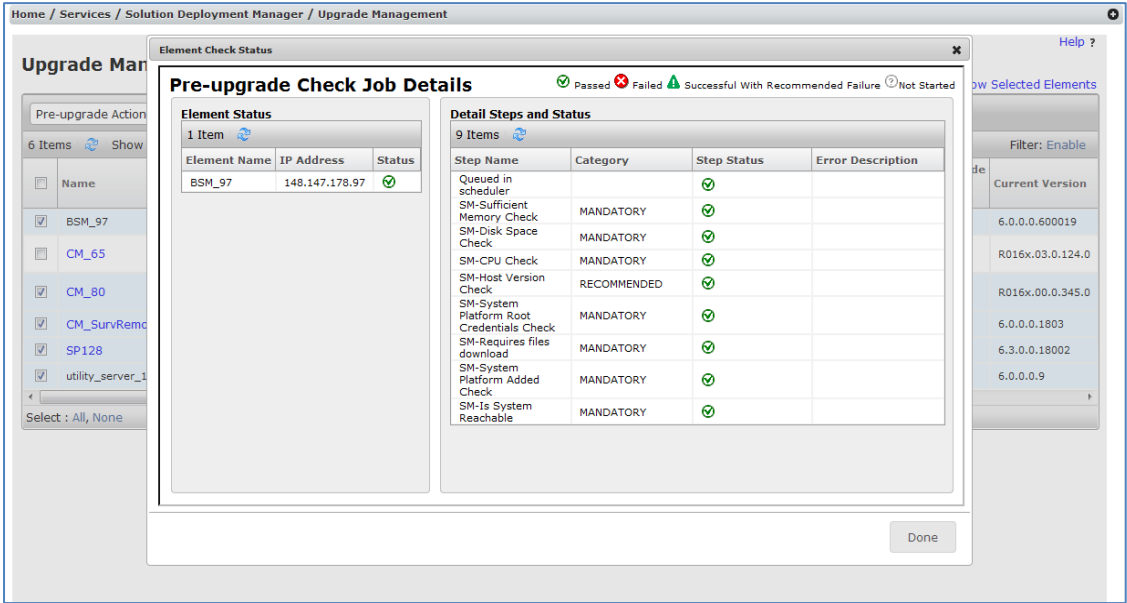


Figure 29: Pre-upgrade Check Status pop-up

Once the Pre-upgrade check job completes the status for Last Action Status will be green and Pre-upgrade Check Status will also show Green (✓).

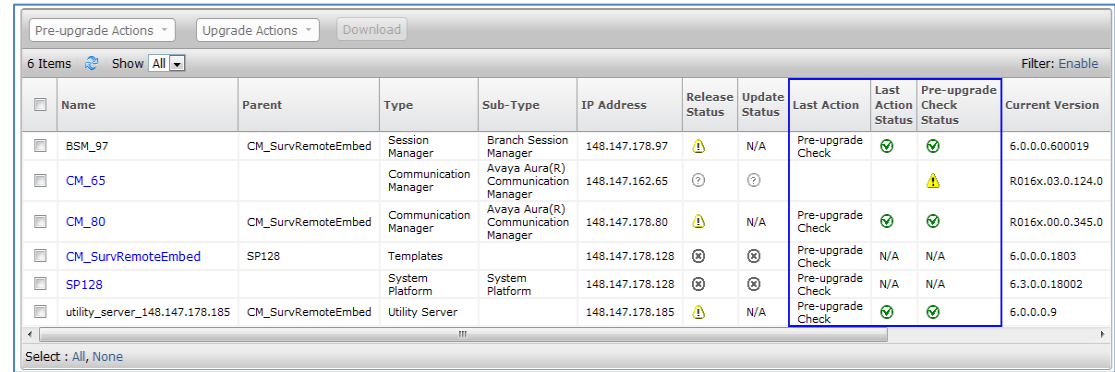


Figure 30: Pre-upgrade Check updated status

4. UPGRADE/UPDATE

Once the staging process completes, the elements are Ready for Upgrade or Update (⚠). The Upgrade Actions > Upgrade/Update will be enabled to start the upgrade or update.

Here is a quick reference on completing staging process to enable Upgrade/Update link:

Enabling Upgrade/Update Link	
1.	Refresh Element operation is complete and Current Version column is populated with current version of the element.
2.	Analyze operation is complete and Entitled Upgrade or Update Version populated with entitled versions.
3.	Download of the entitled upgrade or update version is complete.
4.	Release Status is in “Ready For Upgrade” (⚠) or Update Status is in “Ready For Update” (⚠) State.
5.	Pre-upgrade check is completed for all the selected elements. The status is either in Successful (✅) or Successful with Recommended Failure (⚠) state.

Table 16: Enabling Upgrade/Update Link

4.1 Utility Services on Appliance Virtualization Platform

For Appliance Virtualization Platform (AVP) there is a requirement for Utility Services to be available for the services static route.

There are two use cases for Utility Services.

Use Case 1: Linux-based CM or SM migration. The Utility Services is mandatory when performing a migration of Linux-based systems. For Linux-based CM or SM upgrade/migration, the Utility Services application must be deployed on the target AVP host before the upgrade/migration of the Linux-based CM or SM. VM Management on SMGR-SDM or the SDM-Client is used to deploy the Utility Services OVA to the target AVP Host. Refer to [Appendix F on how to deploy Utility Services from VM Management](#).

Use Case 2: System Platform migration wherein the template already contains Utility Services. In this use case the migration will include Utility Services so it is not required to deploy Utility Services separately to the AVP Host.

Note: If Utility Services is already part of System Platform migration and Utility Services is already deployed on the AVP Host then delete the US which is already deployed on the AVP Host. The automated upgrade/migration process will deploy Utility Services as part of the CM and SM upgrade/migration.

4.2 Upgrade Configuration

This section highlights the important release upgrade configuration requirements.

The example below shows migration of System Platform based release 6.0 applications (CM, SM and BSM) to release 7.0 applications (CM, SM and BSM) running on the Appliance Virtualization Platform (AVP) or a Customer Provided VE solution.

The Upgrade configuration webpage is used to collect all the data which is required to be used during upgrade.

1. Navigate to [Home/Services/Solution Deployment Manager/Upgrade Management](#).
Select the elements to be upgrade.

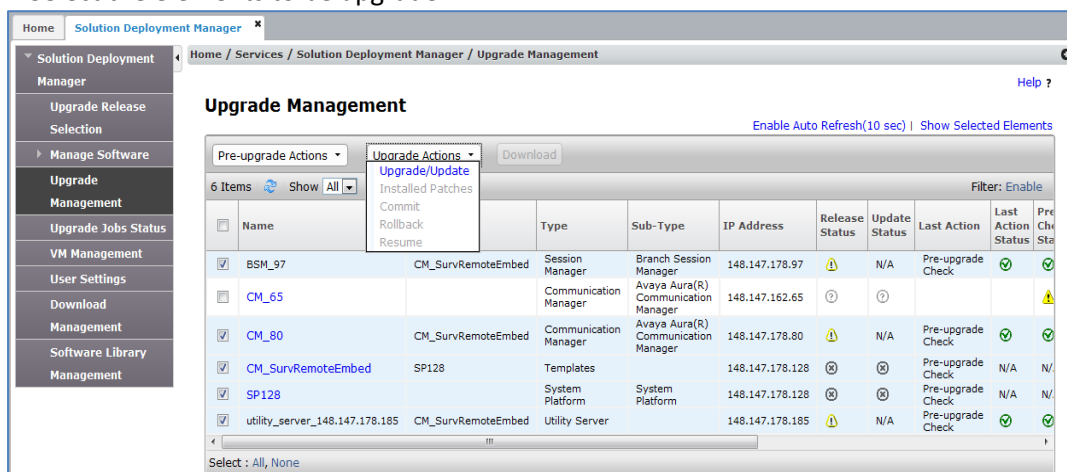


Figure 31: Upgrade Management Page Upgrade Actions - Upgrade/Update

2. From [Upgrade Actions](#) button, select [Upgrade/Update](#) link. The page will be redirected to Upgrade Configuration Page.

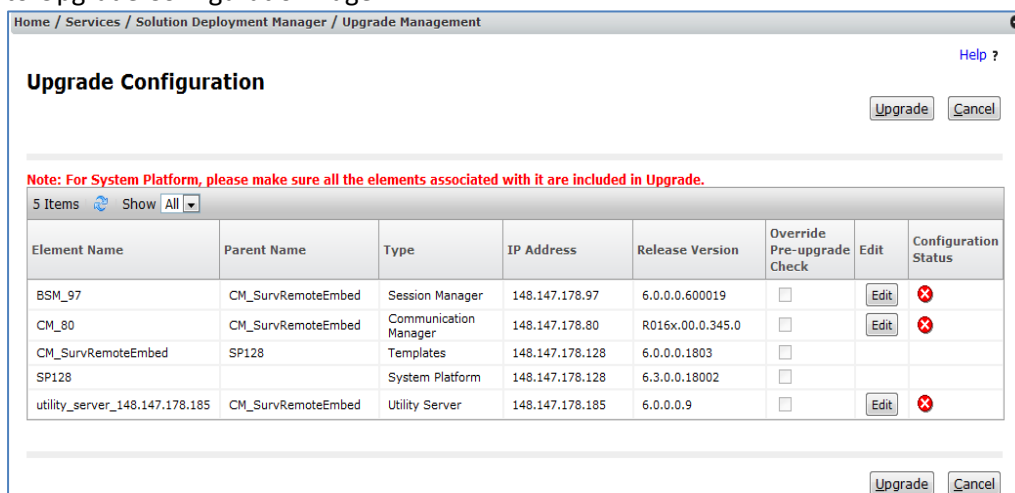


Figure 32: Upgrade Configuration Page

3. Upgrade Configuration page collects upgrade information about the upgradable elements.
 - [Override Pre-upgrade Check](#) is enabled if any of the recommended pre-upgrade check fails for that element. Admin is only allowed to edit configuration if the override pre-upgrade check checkbox is checked.
 - To provide configuration click on [Edit](#) button under [Edit](#) column for each upgradable element. It is required that the configurations of all the elements are provided to proceed for Upgrade.

Here is the description of the fields in the configuration pages:

Configuration	Description
Operation	There may be a case wherein the upgrade and update both are available for a given element. The <u>Operation</u> drop-down provides an option to either choose <u>Upgrade</u> for major release upgrade or <u>Update</u> for applying patches, Service Packs and Feature Packs.
ESXI host	The ESXI host is required so that SDM can deploy the new VMware on that ESXI Host.
	The ESXI host drop-down provides the facility to choose <u>Same Box</u> as one of the option.
	If <u>Same Box</u> is selected, this notifies SDM that the AVP or the VMware ESXi is not yet installed and would require to be installed as part of upgrade.
	Auto installation of AVP or VMware is not supported from SDM. It is a manual process. The migration process will be halted and all the elements will be marked as Paused for the AVP or VMware installation on the Same Box during migration process.
Upgrade Source	<u>Upgrade Source</u> is the configured software library. Select the library on which the software for that element type is downloaded.
Upgrade To	<u>Upgrade To</u> drop-down is populated after selection of Upgrade Source.
	The drop-down contains the software downloaded for that element type.
	Once the OVA file is selected, the <u>Upgrade Configuration Details</u> section is populated with all the information required for the specific OVA.
Existing Administrative User / Existing Administrative Password	These are the username and password on the existing system.
	For CM we require prof18 type of existing user.
	Make sure the ASG users are not used to fill this data.
	For Session Manager and Branch Session Manager, make sure the user is part of <u>susers</u> group.
Pre-populate Data	SDM provided the ability to pre-populate required values for OVA attributes in Upgrade Configuration Details.
	Pre-populate data uses information in Existing Administrative User and Password to fetch and pre-populate the data.
	Some elements have the rule for user locking after multiple login failures. Verify the username and password before click on Pre-populate Data button.
	Verify the pre-populated data for the OVA attributes.
	The pre-populate data button is not available for CMM element as it requires new network configuration data because CMM will be migrated to a new VM from the service running inside the CM template.
	The pre-populate data operation can timeout in case the element is under load and is very slow. In that case the upgrade configuration needs to be provided manually.

Configuration	Description
Upgrade Configuration Details OVA attributes	The mandatory attributes will be marked with red asterisk.
	Pre-populates auto fill some of data fetched from the element. Do not change certain network configuration settings, such as IP address, Hostname/FQDN, Netmask, and Gateway during the upgrade or migration.
	SDM is for upgrade/migration cannot be leveraged to allow IP/FQDN change during migration. The migration fails if the existing network configurations are changed.
	Specifically for Utility Services migration, the network configurations are not marked as mandatory as Utility Services support DHCP configuration. Make sure that information is provided for Public IP Address, Public Netmask and Default Gateway same as of the existing system.
Flexible Footprint	The Flexible Footprint feature allows configuring Aura applications in different sizes (number of Users or Elements for example). The sizes defined by the customer will drive the virtual server resource requirements required for the application to run in the hardware.
	Footprints are populated on selection of Upgrade To drop-down menu.
	In case of Appliance Virtualization Platform (AVP) footprint will be shown based on the hardware type. The drop-down is populated on selection of OVA.
Network Interface	The Network Interfaces are interfaces on which the communication will take place. They are usually Public, Out Of Band Management, Services and Duplication Link.
	In case of AVP they will automatically be populated and are read only.
	There would be a case where the drop down will be populated with physical NIC available on the AVP host. This will be in case of CM Duplex migration where there is a need to create a network interface on selected NIC.
	If the ESXI host is selected as <u>Same Box</u> , the network interfaces will not be shown.
Datastore	Data Store is the storage location on host where the VM will be created. The drop-down is populated after selection of ESXI host.
	If the ESXI host is selected as <u>Same Box</u> , the data store is not shown.
End User License Agreement (EULA)	The EULA is populated when the OVA is selected under <u>Upgrade To</u> column.
	It is mandatory to accept EULA. If the EULA is not accepted the configuration will not be allowed to be saved.

Table 17: Upgrade Configuration Field Description

Clicking on Edit button will open the configuration window. The following screen shots provide an example of the configuration parameters

BSM Upgrade Configuration:

The screenshot shows the 'Edit Upgrade Configuration' window with the following details:

- General Configuration Details:**
 - System: BSM_97
 - IP Address: 148.147.178.97
 - Operation: Upgrade
 - ESXI host: 148.147.178.64
 - Upgrade Source: SMGR_DEFAULT_LOCAL
 - Upgrade To: BSM-7.0.0.0.700007-e55-01.ova
- Upgrade Configuration Details:** (Section header visible, details not fully shown)
- End User License Agreement:**
 - AVAYA GLOBAL SOFTWARE LICENSE TERMS
 - REVISED: March 2015
 - THIS END USER LICENSE AGREEMENT ("SOFTWARE LICENSE TERMS") GOVERNS THE USE OF PROPRIETARY SOFTWARE AND THIRD-PARTY PROPRIETARY SOFTWARE LICENSED THROUGH AVAYA. READ THESE SOFTWARE LICENSE TERMS CAREFULLY, IN THEIR
 - ☒ I Agree to the above end user license agreement.

Buttons: Cancel, Save

Figure 33: Example of Branch Session Manager Upgrade Configuration - 1

The screenshot shows the 'Edit Upgrade Configuration' window with the following details:

- Upgrade Configuration Details:**
 - Upgrade Source: SMGR_DEFAULT_LOCAL
 - Upgrade To: BSM-7.0.0.0.700007-e55-01.ova
- Upgrade Configuration Details:**
 - Existing Administrative User: cust
 - Existing Administrative Password: [Masked]
 - Pre-populate Data: [Button]
 - IP Address: 148.147.178.97
 - Short Hostname: bsm-97
 - Network Domain: smgrdev.avaya.com
 - Netmask: 255.255.255.0
 - Default gateway: 148.147.178.1
 - DNS server(s): 135.27.168.74
 - Timezone: Asia/Kolkata
 - NTP server(s): 0.rhel.pool.ntp.org,1.rhel.pool.ntp.org
 - Login Name: cust
 - Enter Customer Account Password: [Masked]
 - Primary System Manager IP: 148.147.162.185
 - Enrollment Password: [Masked]
 - LSP IP: 148.147.178.80
 - Flexi Footprint: BSM 7.0 Profile 2 Max Devices 5,000
 - Public: VM Network
 - Out of Band Management: VM Network
 - Datastore: datastore1 (23)

Buttons: Cancel, Save

Figure 34: Example of Branch Session Manager Upgrade Configuration - 2

Communication Manager Upgrade Configuration:

Home / Services / Solution Deployment Manager / Upgrade Management

Edit Upgrade Configuration

General Configuration Details | Upgrade Configuration Details | End User License Agreement | Expand All | Collapse All

General Configuration Details

- System: CM_80
- IP Address: 148.147.178.80
- * Operation: Upgrade
- * ESXI host: 148.147.178.64
- * Upgrade Source: SMGR_DEFAULT_LOCAL
- * Upgrade To: CM-Simplex-07.0.0.0.441-e55-0.ova

Upgrade Configuration Details

End User License Agreement

AVAYA GLOBAL SOFTWARE LICENSE TERMS
REVISED: March 2015

THIS END USER LICENSE AGREEMENT ("SOFTWARE LICENSE TERMS") GOVERNS THE USE OF PROPRIETARY SOFTWARE AND THIRD-PARTY PROPRIETARY SOFTWARE LICENSED THROUGH AVAYA. READ THESE SOFTWARE LICENSE TERMS CAREFULLY, IN THEIR

* ☒ I Agree to the above end user license agreement.

* Required

Cancel Save

Figure 35: Example of Communication Manager Upgrade Configuration - 1

Home / Services / Solution Deployment Manager / Upgrade Management

Edit Upgrade Configuration

* Upgrade To: CM-Simplex-07.0.0.0.441-e55-0.ova

Upgrade Configuration Details

- Auto Commit: ☐
- * Existing Administrative User: cmuser
- * Existing Administrative Password: *****
- Pre-populate Data:
- * CM IPv4 Address: 148.147.178.80
- * CM IPv4 Netmask: 255.255.255.0
- * CM IPv4 Gateway: 148.147.178.1
- Out of Band Management IPv4 Address: 0.0.0.0
- Out of Band Management IPv4 Netmask: 0.0.0.0
- * CM Hostname: cm-80
- NTP Server(s):
- DNS Server(s): 135.27.168.74
- Search Domain List:
- * WebLM Server IPv4 Address: 148.147.178.128
- * CM Privileged Administrator User Login: cmuser
- * CM Privileged Administrator User Password: *****
- * Flexi Footprint: CM Survivable Max users 1000
- * Public: VM Network
- * Out of Band Management: VM Network
- * Datastore: datastore1 (23)

Cancel Save

Figure 36: Example of Communication Manager Upgrade Configuration - 2

Utility Services Upgrade Configuration:

Home / Services / Solution Deployment Manager / Upgrade Management

Edit Upgrade Configuration

General Configuration Details | Upgrade Configuration Details | End User License Agreement | Expand All | Collapse All

General Configuration Details

- System: utility_server_148.147.178.185
- IP Address: 148.147.178.185
- * Operation: Upgrade
- * ESXI host: 148.147.178.64
- * Upgrade Source: SMGR_DEFAULT_LOCAL
- * Upgrade To: US-7.0.0.0.11-e55-01_OVF10.ova

Upgrade Configuration Details

End User License Agreement

AVAYA GLOBAL SOFTWARE LICENSE TERMS
REVISED: March 2015

THIS END USER LICENSE AGREEMENT ("SOFTWARE LICENSE TERMS") GOVERNS THE USE OF PROPRIETARY SOFTWARE AND THIRD-PARTY PROPRIETARY SOFTWARE LICENSED THROUGH AVAYA. READ THESE SOFTWARE LICENSE TERMS CAREFULLY, IN THEIR

☒ I Agree to the above end user license agreement.

Cancel Save

Figure 37: Example of Utility Services Upgrade Configuration – 1

Home / Services / Solution Deployment Manager / Upgrade Management

Edit Upgrade Configuration

* Upgrade To: US-7.0.0.0.11-e55-01_OVF10.ova

Upgrade Configuration Details

- * Existing Administrative User: admin
- * Existing Administrative Password: *****
- Pre-populate Data
- * Communication Manager IP: 148.147.178.80
- * Network Time Protocol IP: 0.centos.pool.ntp.org
- * Hostname: us-195
- Timezone setting: Pacific/Samoa
- Utility Services Mode: full_functionality
- * Primary System Manager IP address for application registration: 148.147.162.185
- * Enrollment Password: *****
- Default Gateway: 148.147.178.1
- DNS: 135.27.168.74
- Public IP Address: 148.147.178.185
- Public Netmask: 255.255.255.0
- Out of Band Management IP Address:
- Out of Band Management Netmask:
- * Flexi Footprint: Minimal Resources
- * Public: VM Network
- * Services: VM Network
- * Out of Band Management: VM Network
- * Datastore: datastore1 (23)

Cancel Save

Figure 38: Example of Utility Services Upgrade Configuration - 2

- Click on Save button on Edit Configuration window. The Configuration Status would be turned from red to green. Continue to Edit configuration for other elements.

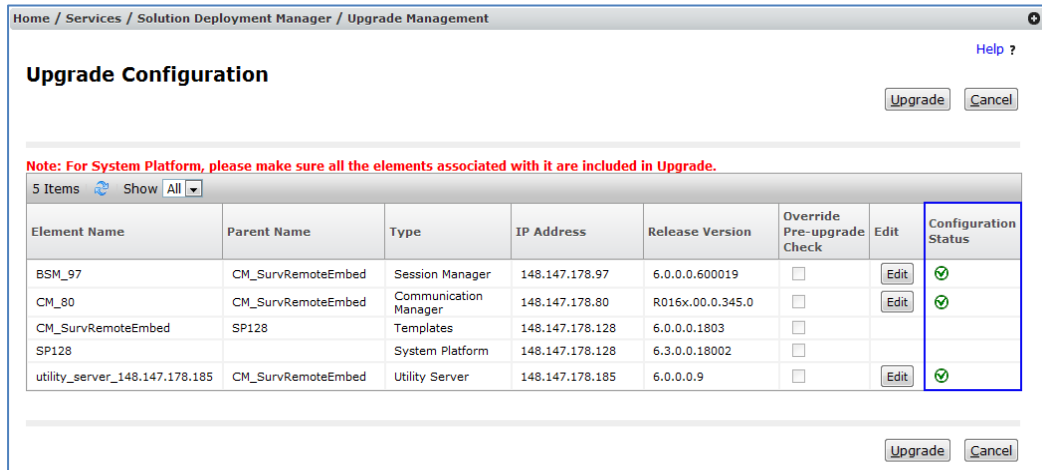


Figure 39: Upgrade Configuration Completed

- Click on Upgrade button. Select Run Immediately or Schedule Later and click on Schedule.

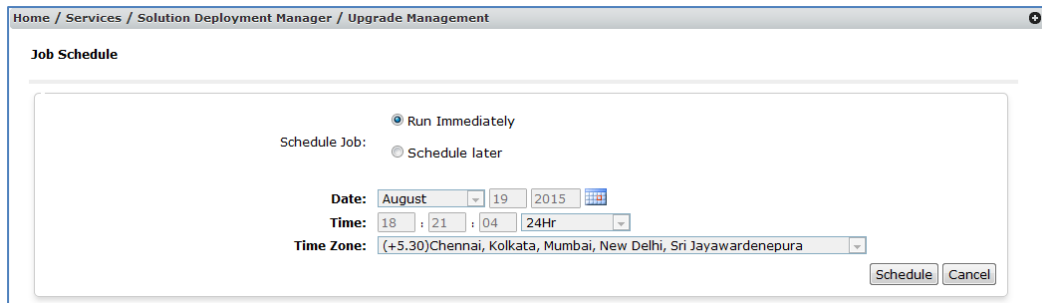


Figure 40: Job Schedule page for Upgrade

- The page will be redirected to Upgrade Management page where Release Status will be in Running State and Last Action and Last Action Status will show Upgrade in pending state.

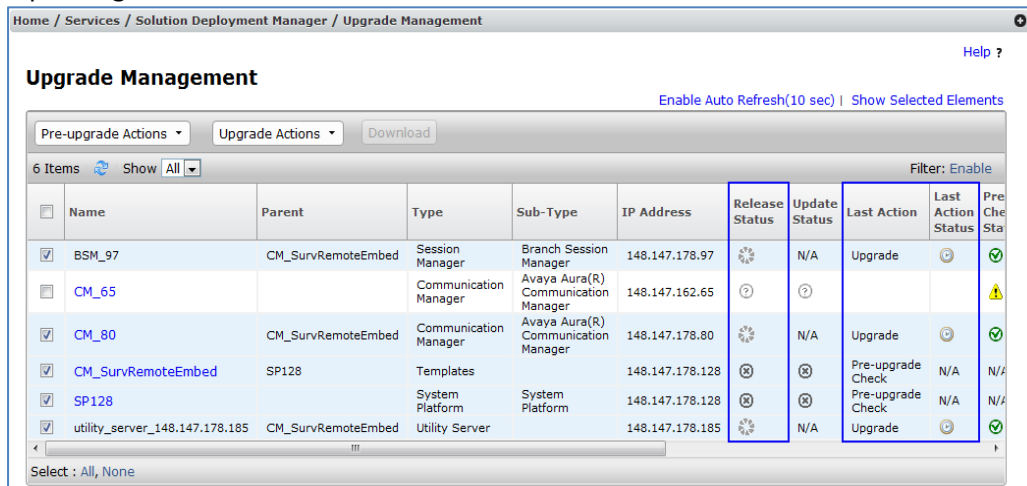


Figure 41: Upgrade Scheduled

- Refresh the page to check the progress or click **Enable Auto Refresh** link to automatically refresh every 10 seconds.

Home / Services / Solution Deployment Manager / Upgrade Management

Upgrade Management

Enable Auto Refresh(10 sec) | Show Selected Elements

Pre-upgrade Actions: Upgrade Actions | Download

6 Items | Show All | Filter: Enable

Name	Parent	Type	Sub-Type	IP Address	Release Status	Update Status	Last Action	Last Action Status	Pre-upgrade Check Status	Current Version
BSM_97	CM_SurvRemoteEmbed	Session Manager	Branch Session Manager	148.147.178.97	⚙️	N/A	Upgrade	⚙️	✅	6.0.0.0.600019
CM_65		Communication Manager	Avaya Aura(R) Communication Manager	148.147.162.65	⚙️	⚙️			⚠️	R016x.03.0.124.0
CM_80	CM_SurvRemoteEmbed	Communication Manager	Avaya Aura(R) Communication Manager	148.147.178.80	⚙️	N/A	Upgrade	⚙️	✅	R016x.00.0.345.0
CM_SurvRemoteEmbed	SP128	Templates		148.147.178.128	⚙️	⚙️	Pre-upgrade Check	N/A	N/A	6.0.0.0.1803
SP128		System Platform	System Platform	148.147.178.128	⚙️	⚙️	Pre-upgrade Check	N/A	N/A	6.3.0.0.18002
utility_server_148.147.178.185	CM_SurvRemoteEmbed	Utility Server		148.147.178.185	⚙️	N/A	Upgrade	⚙️	⚙️	6.0.0.0.9

Select : All, None

Figure 41: Enable Auto or manual Refresh for updated status

- Pre-upgrade check gets executed as part of upgrade as well. When the upgrade or update is in progress, all operations are disabled until the update or upgrade operation is complete.

Home / Services / Solution Deployment Manager / Upgrade Management

Upgrade Management

Enable Auto Refresh(10 sec) | Show Selected Elements

Pre-upgrade Actions: Pre-upgrade Check | Download

6 Items | Show All | Filter: Enable

Name	Parent	Type	Sub-Type	IP Address	Release Status	Update Status	Last Action	Last Action Status	Pre-upgrade Check Status	Current Version
BSM_97	CM_SurvRemoteEmbed	Session Manager	Branch Session Manager	148.147.178.97	⚙️	N/A	Upgrade	⚙️	✅	6.0.0.0.600019
CM_65		Communication Manager	Avaya Aura(R) Communication Manager	148.147.162.65	⚙️	⚙️			⚠️	R016x.03.0.124.0
CM_80	CM_SurvRemoteEmbed	Communication Manager	Avaya Aura(R) Communication Manager	148.147.178.80	⚙️	N/A	Upgrade	⚙️	✅	R016x.00.0.345.0
CM_SurvRemoteEmbed	SP128	Templates		148.147.178.128	⚙️	⚙️	Pre-upgrade Check	N/A	N/A	6.0.0.0.1803
SP128		System Platform	System Platform	148.147.178.128	⚙️	⚙️	Pre-upgrade Check	N/A	N/A	6.3.0.0.18002
utility_server_148.147.178.185	CM_SurvRemoteEmbed	Utility Server		148.147.178.185	⚙️	N/A	Upgrade	⚙️	⚙️	6.0.0.0.9

Select : All, None

Figure 42: Pre-upgrade check runs as part of upgrade

The migration use case will be divided into two parts from this point, depending on what is selected in ESXi host.

- Different Box Migration:** If AVP or ESXi host is selected, it is considered as Different Box Migration which is an automated process. Go to [Different Box Migration](#) for checking the status.
- Same Box Migration:** If **Same Box** value is selected, it is considered as Same Box Migration. Follow [Same Box Migration steps](#) from this point onwards.

4.2.1 Different Box Migration

If the selected value in **ESXi host** in the Edit configuration is an ESXi host or an AVP host, it is considered as a different box migration. This means that the System Platform or Linux-based element will be in stopped state and the elements will be migrated to AVP or ESXi host. This section covers Different Box Migration.

1. Click on Last Action Status to see the upgrade steps for individual elements. The steps will include
 - Taking Backup
 - Downloading the backup on System Manager
 - Stopping the VM.
 - Deploying the new VM.
 - Restoring the backed up data on the newly created VM

Branch Session Manager Status:

Home / Services / Solution Deployment Manager / Upgrade Management

Element Check Status

Upgrade Job Details

Passed Failed Successful With Recommended Failure Not Started

Element Status

1 Item

Element Name	IP Address	Status
BSM_97	148.147.178.97	Not Started

Detail Steps and Status

10 Items

Step Name	Step Status	Error Description
Queued in scheduler	Passed	
Creating Environment Files	Passed	
PreUpgradeCheck	Passed	
SM-Sufficient Memory Check	Passed	
SM-Disk Space Check	Passed	
SM-CPU Check	Passed	
SM-System Platform Root Credentials Check	Passed	
SM-Requires files download	Passed	
SM-System Platform Added Check	Passed	
SM-Is System Reachable	Passed	

Done

Figure 43: Example of Branch Session Manager Upgrade Status

Communication Manager Status:

Home / Services / Solution Deployment Manager / Upgrade Management

Element Check Status

Upgrade Job Details

Passed Failed Successful With Recommended Failure Not Started

Element Status

1 Item

Element Name	IP Address	Status
CM_80	148.147.178.80	Not Started

Detail Steps and Status

16 Items

Step Name	Step Status	Error Description
Queued in scheduler	Passed	
Creating Environment Files	Passed	
PreUpgradeCheck	Passed	
CM-Sufficient Memory Check	Passed	
CM-Disk Space Check	Passed	
CM-CPU Check	Passed	
CM-System Platform Root Credentials Check	Passed	
CM-Requires files download	Passed	
CM-System Platform Added Check	Passed	
CM-Is System Reachable	Passed	
CM-Is Host Name Valid	Passed	
PreUpgradePatch	Passed	
PreMigrationChecks	Passed	
Backup	Passed	
DOWNLOAD_BACKUP	Passed	
Stop	Not Started	

Done

Figure 44: Example of Communication Manager Upgrade Status

Utility Services Status:

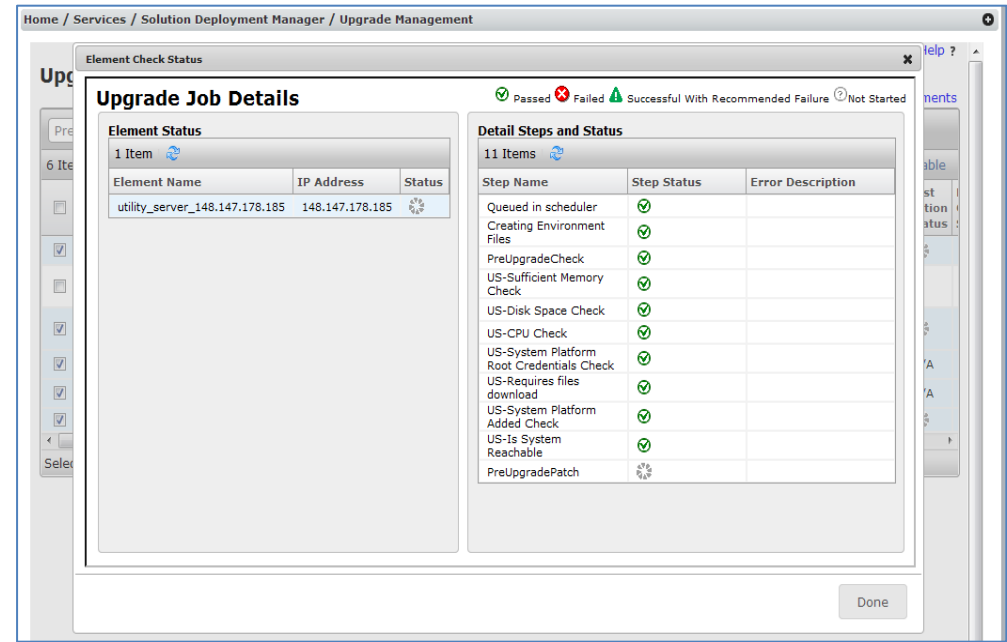


Figure 45: Example of Utility Services Upgrade Status

- The upgrade process will take few minutes to complete the migration. All the System Platform-based elements will be migrated to VMware-based elements. Status can be monitored by clicking on icon in the Last Action Status column.

BSM Upgraded Successfully:

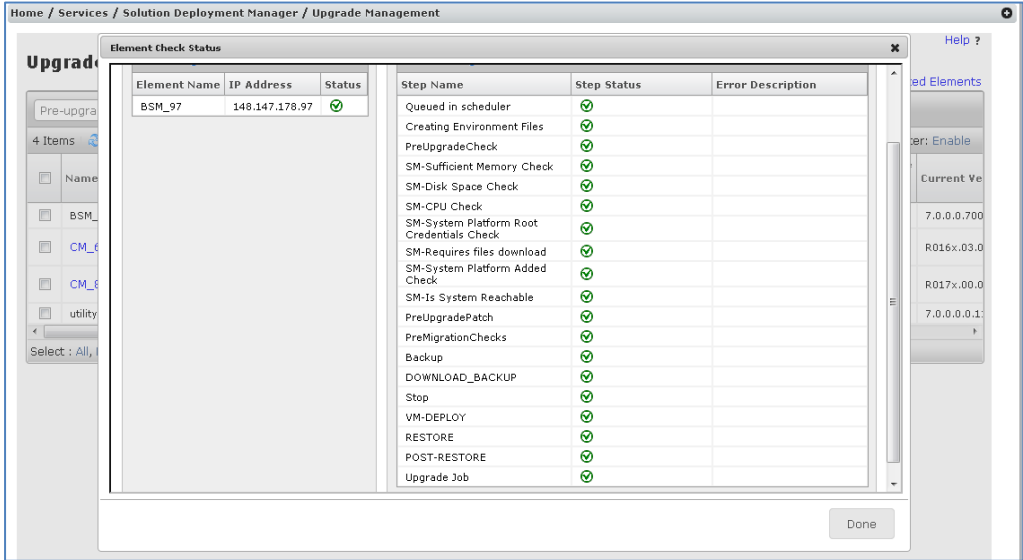


Figure 46: Example of Branch Session Manager Upgrade successfully completed

Communication Manager Upgraded Successfully:

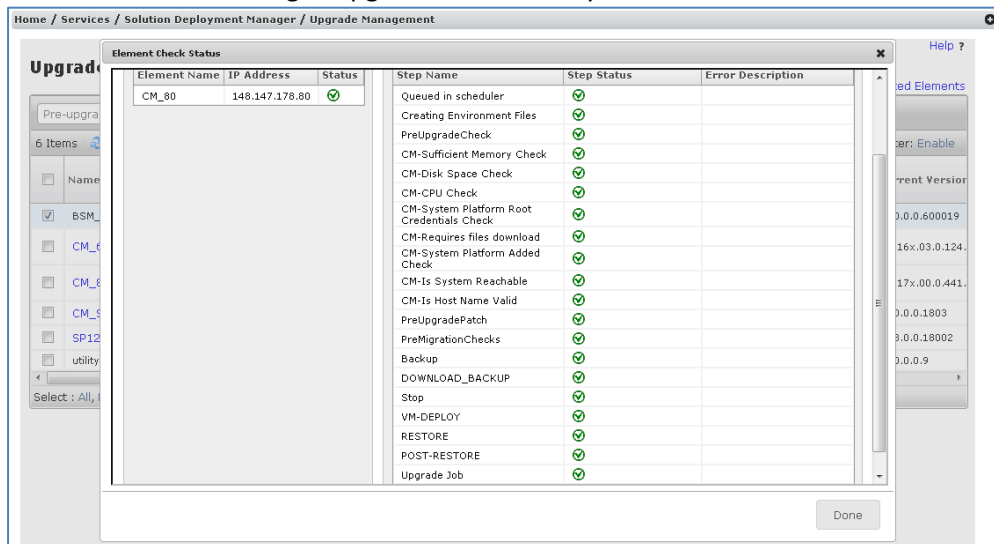


Figure 47: Example of Communication Manager Upgrade successfully completed

Utility Services upgraded successfully:

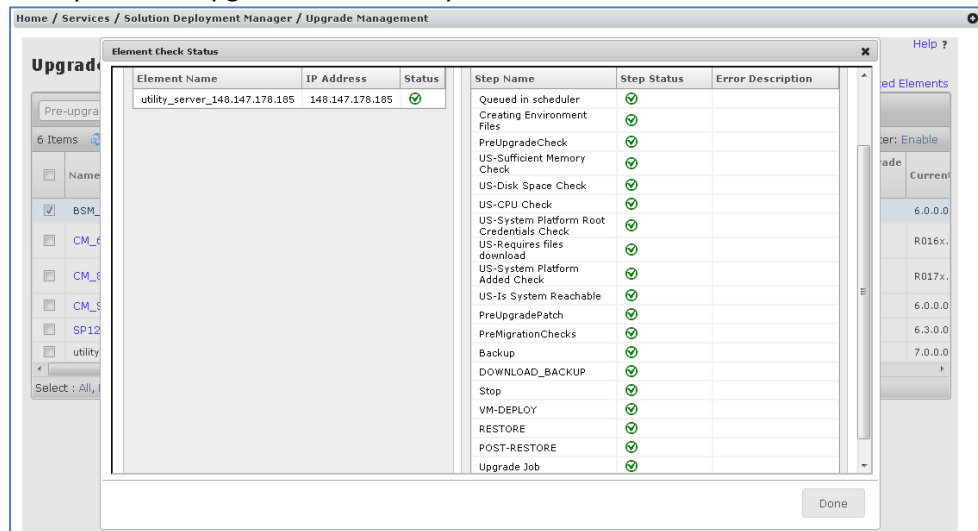


Figure 48: Example of Utility Services Upgrade successfully completed

3. Once the migration for all the elements is complete.
 - The Release Status for all the elements on Upgrade Management will be Upgraded state (✓).
 - The current version is updated to latest version.
 - The parent has changed from System Platform Template to ESXi or AVP Host.
 - **In case of System Platform migration, the System Platform and Templates are removed from Home/Services/Inventory/Manage Elements once the migration is complete for all the elements.**

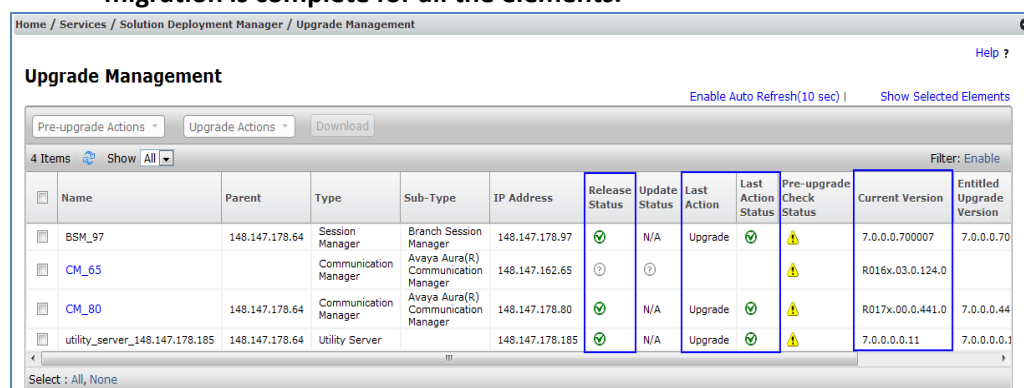


Figure 49: Upgrade Management updated status for upgraded elements

4.2.2 Same Box Migration

If the selected value in **ESXi host** in the Edit configuration is **Same Box**, the process is called as the same box migration. This means that the AVP host or the ESXi VMware will be installed on the same box on which System Platform or Linux-based element is residing. This section covers Same Box Migration.

1. Click on Last Action Status to see the upgrade steps for individual elements. The steps will include:
 - Taking Backup
 - Downloading the backup on System Manager
 - Pause the migration and change element state to Paused.

Branch Session Manager Status:

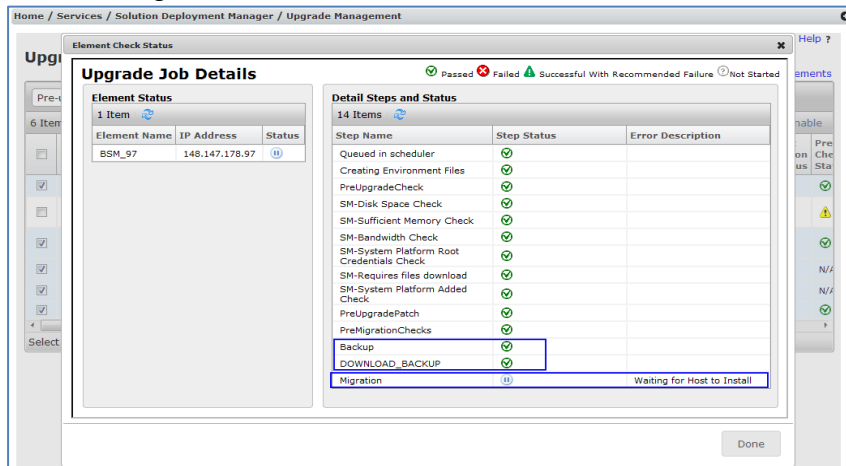


Figure 50: Same Box Migration - Paused State for BSM

Communication Manager Status:

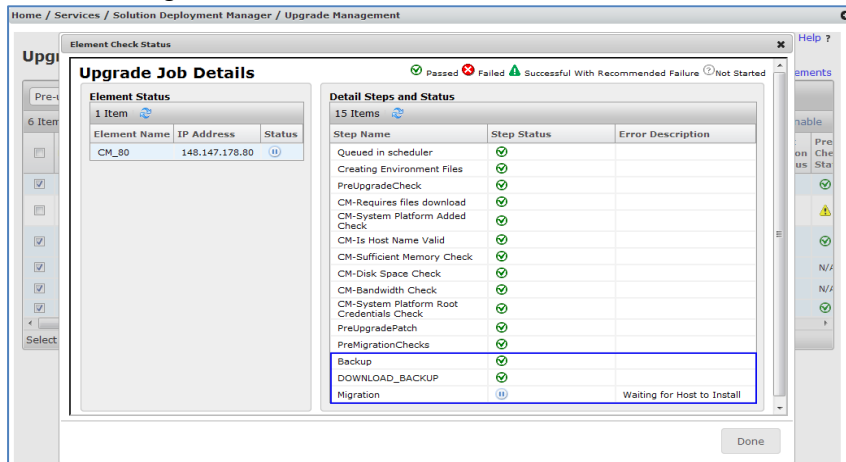


Figure 51: Same Box Migration - Paused State for CM

Utility Services Status:

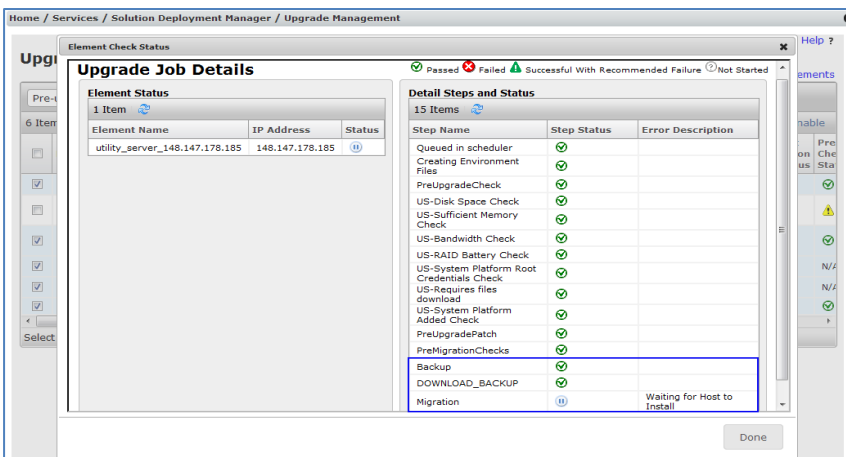


Figure 52: Same Box Migration - Paused State for US

- The migration is halted and all the elements are in Paused state.

Upgrade Management Enable Auto Refresh(10 sec) | Show Selected Elements

Pre-upgrade Actions Upgrade Actions Download

6 Items Show All Filter: Enable

Name	Parent	Type	Sub-Type	IP Address	Release Status	Update Status	Last Action	Last Action Status	Pre Check Status
BSM_97	CM_SurvRemoteEmbed	Session Manager	Branch Session Manager	148.147.178.97	Paused	N/A	Upgrade	Paused	Green
CM_65		Communication Manager	Avaya Aura(R) Communication Manager	148.147.162.65	Paused	Paused			Yellow
CM_80	CM_SurvRemoteEmbed	Communication Manager	Avaya Aura(R) Communication Manager	148.147.178.80	Paused	N/A	Upgrade	Paused	Green
CM_SurvRemoteEmbed	SP128	Templates		148.147.178.128	Failed	Failed	Pre-upgrade Check	N/A	N/A
SP128		System Platform	System Platform	148.147.178.128	Failed	Failed	Pre-upgrade Check	N/A	N/A
utility_server_148.147.178.185	CM_SurvRemoteEmbed	Utility Server		148.147.178.185	Paused	N/A	Upgrade	Paused	Green

Select : All, None

Figure 53: Elements release status in Paused State

- The migration is halted so that admin can install AVP or VMware ESXi host on the same server. Follow the AVP:
 - For Linux-based element, we require one additional IP address for AVP/ESXi Host and one IP address for Utility Services.
 - For System Platform where the utility services VM is already part of the template, the SP C-Dom or Dom-0 IP can be used for installing AVP or VMware ESXi host. If using a different IP ensures that the IP address is in the same subnet as the VM IP addresses.

Once the AVP or VMware ESXi host is installed on the same box, add the host to VM Management. Refer to [Appendix-D for adding host to VM Management](#).

Refer to section [Utility Services](#) for details whether to deploy Utility Services or not.

- Once the host is added to VM Management, we are ready to resume the migration. Select the elements which are in Paused state and click Upgrade Actions > Resume.

Upgrade Management Enable Auto Refresh(10 sec) | Show Selected Elements

Pre-upgrade Actions Upgrade Actions Download

6 Items Show All Filter: Enable

Name	Parent	Type	Sub-Type	IP Address	Release Status	Update Status	Last Action	Last Action Status	Pre Check Status
BSM_97	CM_SurvRemoteEmbed	Session Manager	Branch Session Manager	148.147.178.97	Paused	N/A	Upgrade	Paused	Green
CM_65		Communication Manager	Avaya Aura(R) Communication Manager	148.147.162.65	Paused	Paused			Yellow
CM_80	CM_SurvRemoteEmbed	Communication Manager	Avaya Aura(R) Communication Manager	148.147.178.80	Paused	N/A	Upgrade	Paused	Green
CM_SurvRemoteEmbed	SP128	Templates		148.147.178.128	Failed	Failed	Pre-upgrade Check	N/A	N/A
SP128		System Platform	System Platform	148.147.178.128	Failed	Failed	Pre-upgrade Check	N/A	N/A
utility_server_148.147.178.185	CM_SurvRemoteEmbed	Utility Server		148.147.178.185	Paused	N/A	Upgrade	Paused	Green

Select : All, None

Figure 54: Resume the upgrade from Paused State

- The page will be redirected to Resume configuration.

Home / Services / Solution Deployment Manager / Upgrade Management

Resume Configuration

3 Items Show All

Element Name	Parent Name	IP Address	Current Version	Target Host	Data Store	Flexi Footprint	Network Configuration
BSM_97	CM_SurvRemoteEmbed	148.147.178.97	6.0.0.0.600019			BSM 7.0 Profile 2 Max Devices 5,000	Edit
CM_80	CM_SurvRemoteEmbed	148.147.178.80	R016x.00.0.345.0			CM Survivable Max users 1000	Edit
utility_server_148.147.178.185	CM_SurvRemoteEmbed	148.147.178.185	6.0.0.0.9			Minimal Resources	Edit

Job Schedule

Run Immediately (selected) Schedule later

Schedule Job:

Date: August 20 2015

Time: 20 : 42 : 45 24Hr

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

Schedule Cancel

Figure 55: Resume Configuration Page

- Fill in the required data for all the upgradable elements.

Target Host: Choose the host which was installed on the same hardware and added to VM Management.

Data Store: Choose the Data store where VM will be created.

Flexi footprint: Footprint which will be used in deployment of the OVA.

Home / Services / Solution Deployment Manager / Upgrade Management

Resume Configuration

3 Items Show All

Element Name	Parent Name	IP Address	Current Version	Target Host	Data Store	Flexi Footprint	Network Configuration
BSM_97	CM_SurvRemoteEmbed	148.147.178.97	6.0.0.0.600019	148.147.178.64	datastore1 (23)	BSM 7.0 Profile 1 Max Devices 1,000	Edit
CM_80	CM_SurvRemoteEmbed	148.147.178.80	R016x.00.0.345.0	148.147.178.64	datastore1 (23)	CM Survivable Max users 1000	Edit
utility_server_148.147.178.185	CM_SurvRemoteEmbed	148.147.178.185	6.0.0.0.9	148.147.178.64	datastore1 (23)	Minimal Resources	Edit

Job Schedule

Run Immediately (selected) Schedule later

Schedule Job:

Date: August 20 2015

Time: 20 : 42 : 45 24Hr

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

Schedule Cancel

Figure 56: Resume Configuration populated

- Click on Edit button for each element in Network Configuration Column to provide network interfaces for that VM. Select the value from the available network interfaces and click on Done button. In case of CM-Duplex migration on AVP, Duplication Link network parameter will show physical NICs for creation of a new network interface.

Home / Services / Solution Deployment Manager / Upgrade Management

Resume Configuration

3 Items Show All

Element Name	Parent Name	IP Address	Current Version	Target Host	Data Store	Flexi Footprint	Network Configuration
BSM_97	CM_SurvRemoteEmbed	148.147.178.97	6.0.0.0.600019	148.147.178.64	datastore1 (23)	BSM 7.0 Profile 1 Max Devices 1,000	Edit
CM_80	CM_SurvRemoteEmbed	148.147.178.80	R016x.00.0.345.0	148.147.178.64	datastore1 (23)	CM Survivable Max users 1000	Edit
utility_server_148.147.178.185	CM_SurvRemoteEmbed	148.147.178.185	6.0.0.0.9	148.147.178.64	datastore1 (23)	Minimal Resources	Edit

Job Schedule

Run Immediately (selected) Schedule later

Schedule Job:

Date: August 20 2015

Time: 20 : 42 : 45 24Hr

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

Schedule Cancel

Network Configuration

Network Parameters

* Public VM Network

* Out of Band Management VM Network

Done

Figure 57: Resume Configuration – Network Parameters

8. Select Run Immediately (default) or Schedule later and click on Schedule button for resuming the migration.

The page will be redirected to Upgrade Management Page. The release status will show running and Upgrade Job in Pending state. Refresh the page to check the status of Last Action Status.

Name	Parent	Type	Sub-Type	IP Address	Release Status	Update Status	Last Action	Last Action Status	Pre-upgrade Check Status	Current Version
BSM_97	CM_SurvRemoteEmbed	Session Manager	Branch Session Manager	148.147.178.97	100%	N/A	Upgrade	100%	100%	6.0.0.0.600019
CM_65		Communication Manager	Avaya Aura(R) Communication Manager	148.147.162.65	0%	0%		0%	0%	R016x.03.0.124.0
CM_80	CM_SurvRemoteEmbed	Communication Manager	Avaya Aura(R) Communication Manager	148.147.178.80	100%	N/A	Upgrade	100%	100%	R016x.00.0.345.0
CM_SurvRemoteEmbed	SP128	Templates		148.147.178.128	0%	0%	Pre-upgrade Check	N/A	N/A	6.0.0.0.1803
SP128		System Platform	System Platform	148.147.178.128	0%	0%	Pre-upgrade Check	N/A	N/A	6.3.0.0.18002
utility_server_148.147.178.185	CM_SurvRemoteEmbed	Utility Server		148.147.178.185	100%	N/A	Upgrade	100%	100%	6.0.0.0.9

Figure 58: Resume scheduled

9. The migration will be resumed. Click on Last Action Status for the element to see the status:

BSM Status:

Check Name	Status
Queued in scheduler	100%
Creating Environment Files	100%
PreUpgradeCheck	100%
SM-Disk Space Check	100%
SM-Sufficient Memory Check	100%
SM-Bandwidth Check	100%
SM-System Platform Root Credentials Check	100%
SM-Requires files download	100%
SM-System Platform Added Check	100%
PreUpgradePatch	100%
PreMigrationChecks	100%
Backup	100%
DOWNLOAD_BACKUP	100%
Migration	0%
(Pre-Deployment)	0%
SM-Sufficient Memory Check	100%
(Pre-Deployment) SM-Disk Space Check	100%
(Pre-Deployment) SM-CPU Check	100%
(Pre-Deployment) SM-Host Version Check	100%
(Pre-Deployment) SM-Requires files download	100%
VM-DEPLOY	0%

Figure 59: Example of Branch Session Manager job status

CM Status:

Check Name	Status
PreUpgradeCheck	100%
CM-Requires files download	100%
CM-System Platform Added Check	100%
CM-Is Host Name Valid	100%
CM-Sufficient Memory Check	100%
CM-Disk Space Check	100%
CM-Bandwidth Check	100%
CM-System Platform Root Credentials Check	100%
PreUpgradePatch	100%
PreMigrationChecks	100%
Backup	100%
DOWNLOAD_BACKUP	100%
Migration	0%
(Pre-Deployment)	0%
CM-Sufficient Memory Check	100%
(Pre-Deployment) CM-Disk Space Check	100%
(Pre-Deployment) CM-CPU Check	100%
(Pre-Deployment) CM-Host Version Check	100%
(Pre-Deployment) CM-Requires files download	100%
VM-DEPLOY	0%

Figure 60: Example of Communication Manager job status

US Status:

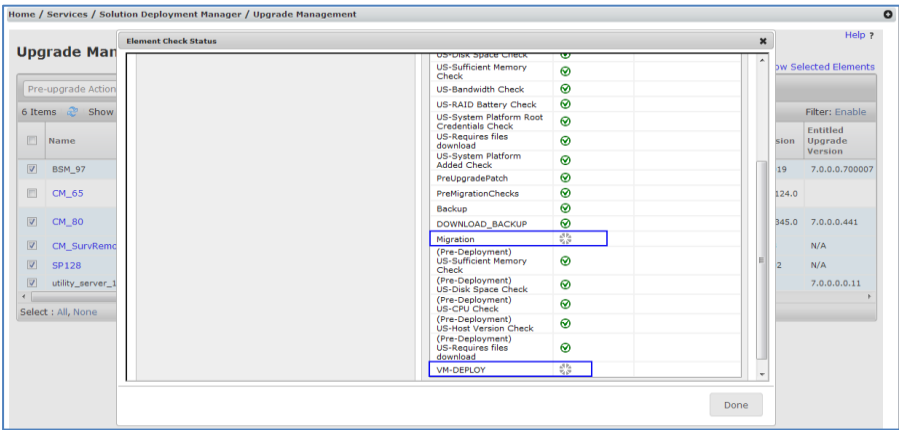


Figure 61: Example of Branch Session Manager job status

10. Once the migration for all the elements is complete.
- The Release Status for all the elements on Upgrade Management will be in Upgraded state (✓).
 - The current version is also updated to latest version.
 - The parent has changed from System Platform Template to ESXi or AVP Host.

In case of System Platform migration, the System Platform and Templates are removed from Home/Services/Inventory/Manage Elements once the migration is complete for all the elements.

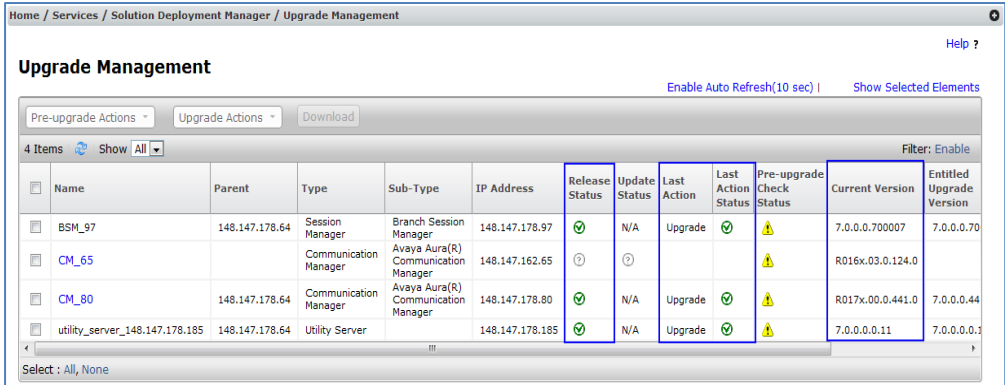


Figure 62: Successful status updated for Resume operation

4.2.3 Failed Migration

There would be cases when the migration would fail for reasons like

- Backup failure.
- Network not reachable.
- Network glitch.
- Element sanity failure.
- Restore failure.
- Others.

SDM handles failure of migration in following two ways:

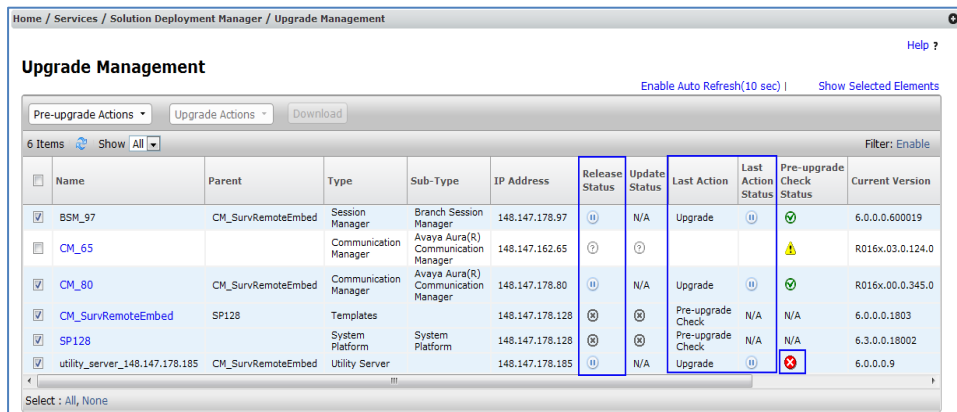
1. Before Backup

- For Linux-based elements: If the migration failure is observed prior taking backup of the element is complete and downloaded to System Manager, the migration is marked as Failed and element Release Status is marked as Ready For Upgrade.
- For System Platform-based elements: If any of the SP based elements migration fails before completing the backup and downloaded to System Manager, all the elements are put in failed state as all the elements needs to migrate together.

2. After Backup

- For Linux-based Metal elements: If the migration has failed on any step after taking the backup and downloaded to System Manager, the element is put in Paused State. This means that the process is halted and can be resumed again by the administrator.
- For System Platform-based elements:
During migration, there is a VM deploy step which deploys the VM on AVP or ESXi Host. Prior to VM deploy step the parent child relation with the SP and SP Template are removed which means the elements are now individual elements and only that element will be marked Paused which has actually failed.
If the VM deploy step is not performed yet then all SP element will be marked as Paused.

Below is an example with screenshots where Utility Services pre-upgrade check has failed but SP backup has been taken and that's why the elements are marked in Paused State.



Name	Parent	Type	Sub-Type	IP Address	Release Status	Update Status	Last Action	Last Action Status	Pre-upgrade Check Status	Current Version
BSM_97	CM_SurvRemoteEmbed	Session Manager	Branch Session Manager	148.147.178.97	Ready For Upgrade	N/A	Upgrade	Success	Success	6.0.0.0.600019
CM_65		Communication Manager	Avaya Aura(R) Communication Manager	148.147.162.65	Paused	Paused			Warning	R016x.03.0.124.0
CM_80	CM_SurvRemoteEmbed	Communication Manager	Avaya Aura(R) Communication Manager	148.147.178.80	Ready For Upgrade	N/A	Upgrade	Success	Success	R016x.00.0.345.0
CM_SurvRemoteEmbed	SP128	Templates		148.147.178.128	Ready For Upgrade	Paused	Pre-upgrade Check	N/A	N/A	6.0.0.0.1803
SP128		System Platform	System Platform	148.147.178.128	Ready For Upgrade	Paused	Pre-upgrade Check	N/A	N/A	6.3.0.0.18002
utility_server_148.147.178.185	CM_SurvRemoteEmbed	Utility Server		148.147.178.185	Ready For Upgrade	N/A	Upgrade	Success	Failed	6.0.0.0.9

Figure 63: Upgrade Job failed for an element

Clicking on Upgrade Last Action Status for Utility Services shows that US pre-upgrade check has failed on Raid Battery

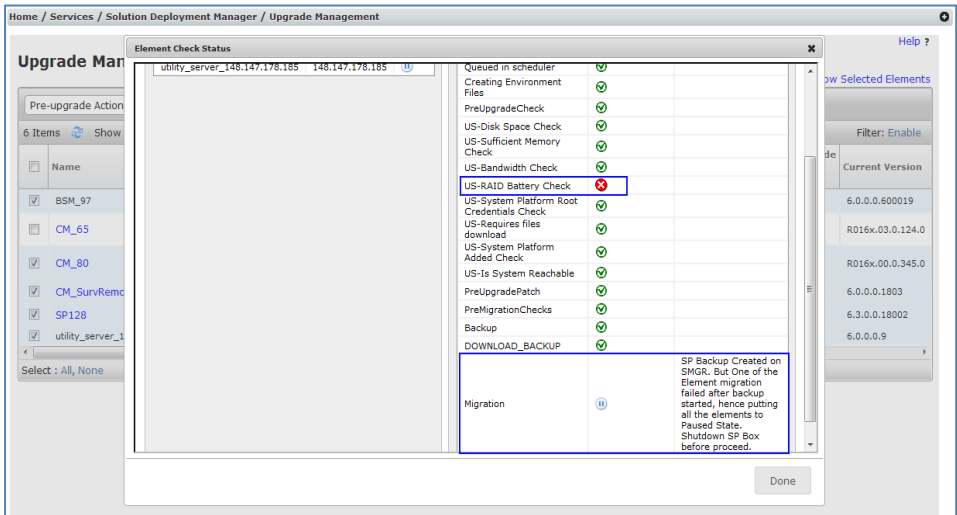


Figure 64: Job failure details - US migration put in Paused state

Clicking on Upgrade Last Action Status for CM will show that CM backup was completed and that's why all the elements are put in Paused State.

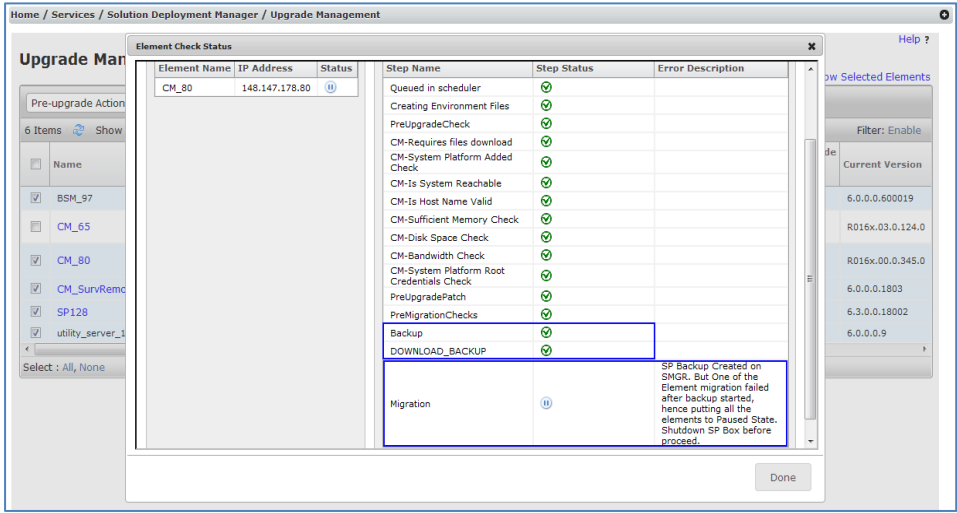


Figure 65: CM migration put in Paused state as US job failed

Clicking on Upgrade Last Action Status for BSM will also show that element is in Paused State

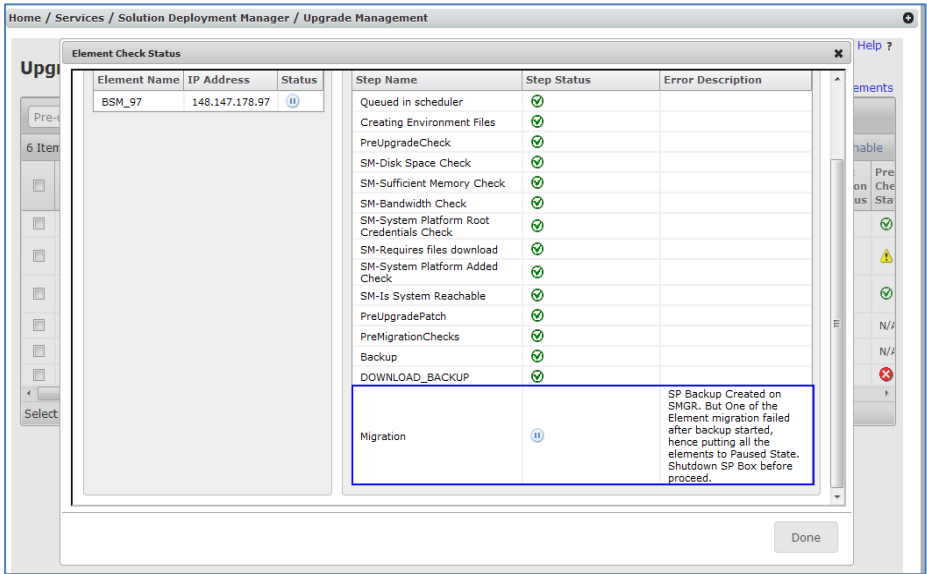


Figure 66: BSM migration put in Paused state as US job failed

4.3 Update Configuration

System Manager SDM supports patching of 7.0 elements from Upgrade Management.

Patching is supported for following 7.0 elements only:

	Elements supported for Patching
1.	Communication Manager
2.	Communication Manager Messaging
3.	Session Manager
4.	Branch Session Manager
5.	Utility Services

Table 18: Supported elements for patching

4.3.1 Staging for Elements for Patching

Here are the steps which are required for patching:

- Add elements in [Home/Services/Inventory/Manage Elements](#) for the patching. Refer to Section [Things to know for configuring your elements in System Manager Manage Elements](#).
- Add Customer VMware ESXi or Avaya Virtualization Platform in VM Management. Refer to [Appendix-D for adding the host in VM Management](#).
- Trust establishment: For 7.0 patching, establish trust between System Manager and the element that needs to be patched. This is required for password less connection to the element and do patch operations. There are two use cases here:
 - a. Element OVA deployed through SDM Client or vSphere client:
If the element is deployed using SDM Client or directly through vSphere client, the trust is not established between System Manager and the element. The trust can be established from VM Management for that element. Refer to [Appendix F – Establishing trust between System Manager and the elements](#).
 - b. Element OVA migration or deployment using System Manager SDM:
If the element is deployed or migrated using System Manager SDM, then trust is automatically be established.
If the host is removed and added again, follow [Appendix F – Establishing trust between System Manager and the elements](#).

4.3.2 Update

Navigate to Home/Services/Solution Deployment Manager/Upgrade Management. In the example below we will be updating:

- Communication Manager Official patch in version xml file.
- Utility Services Custom patch.

Follow below steps for Update:

1. [Refresh Element](#) to get the latest data from element.
2. [Analyze](#) to check if there is any entitled patch available to apply. In the example below, the patch is available for Communication manager but is now downloaded. The update status would be in Update Required state.

Home / Services / Solution Deployment Manager / Upgrade Management

Upgrade Management

Enable Auto Refresh(10 sec) | Show Selected Elements

Pre-upgrade Actions | Upgrade Actions | Download

4 Items | Show | All | Filter: Enable

Name	Parent	Type	Sub-Type	IP Address	Release Status	Update Status	Last Action	Last Action Status	Pre-upgrade Check Status
BSM_97	148.147.178.64	Session Manager	Branch Session Manager	148.147.178.97	✓	N/A	Analyze	✓	⚠
CM_65		Communication Manager	Avaya Aura(R) Communication Manager	148.147.162.65	?	?			⚠
CM_80	148.147.178.64	Communication Manager	Avaya Aura(R) Communication Manager	148.147.178.80	✓	⚠	Analyze	✓	⚠
utility_server_148.147.178.185	148.147.178.64	Utility Server		148.147.178.185	✓	✓	Analyze	✓	⚠

Select : All, None

Figure 67: Patching from Upgrade Management Page

3. [Download](#) or [Sync](#) the entitled patch for Communication Manager.
4. If there is a custom patch which needs to be applied. Upload the custom patch using [Sync settings](#). In this example the custom patch will be applied on Utility Services. Analyze Communication Manager and Utility Services element. The Update Status will change to Ready For Update.

Upgrade Management

Enable Auto Refresh(10 sec) | Show Selected Elements

Pre-upgrade Actions | Upgrade Actions | Download

4 Items | Show | All | Filter: Enable

Name	Parent	Type	Sub-Type	IP Address	Release Status	Update Status	Last Action	Last Action Status	Pre-upgrade Check Status	Current Version	Entitled Upgrade Version
BSM_97	148.147.178.64	Session Manager	Branch Session Manager	148.147.178.97	✓	N/A	Analyze	✓	⚠	7.0.0.0.700007	7.0.0.0.700
CM_65		Communication Manager	Avaya Aura(R) Communication Manager	148.147.162.65	?	?			⚠	R016x.03.0.124.0	
CM_80	148.147.178.64	Communication Manager	Avaya Aura(R) Communication Manager	148.147.178.80	✓	⚠	Analyze	✓	⚠	R017x.00.0.441.0	N/A
utility_server_148.147.178.185	148.147.178.64	Utility Server		148.147.178.185	✓	⚠	Analyze	✓	⚠	7.0.0.0.0.11	7.0.0.0.0.1

Select : All, None

Figure 68: Update Status after Download and Analyze operation

For custom patch, the Entitled Update Version is not applicable (N/A) but Update Status is still Ready For Update. SDM looks for entitled software in version xml files, if no patches are available in version xml SDM looks for uploaded custom patches and mark element as Ready For Update.

Upgrade Management

Enable Auto Refresh(10 sec) | Show Selected Elements

Pre-upgrade Actions | Upgrade Actions | Download

4 Items | Show | All | Filter: Enable

Parent	Type	Sub-Type	IP Address	Release Status	Update Status	Last Action	Last Action Status	Pre-upgrade Check Status	Current Version	Entitled Upgrade Version	Entitled Update Version	Location
148.147.178.64	Session Manager	Branch Session Manager	148.147.178.97	✓	N/A	Analyze	✓	⚠	7.0.0.0.700007	7.0.0.0.700007	N/A	Pune
	Communication Manager	Avaya Aura(R) Communication Manager	148.147.162.65	?	?			⚠	R016x.03.0.124.0			
148.147.178.64	Communication Manager	Avaya Aura(R) Communication Manager	148.147.178.80	✓	⚠	Analyze	✓	⚠	R017x.00.0.441.0	N/A	00.0.441.0-22438	Pune
148.147.178.64	Utility Server		148.147.178.185	✓	⚠	Analyze	✓	⚠	7.0.0.0.0.11	7.0.0.0.0.11	N/A	Pune

Select : All, None

Figure 69: Entitled versions updated after Analyze

5. Run the pre-upgrade check, click **Pre-upgrade Actions >Pre-upgrade Check**. Fill in the details and Schedule the pre-upgrade check to run immediately or later.
 - **Target Host:** The target host is the ESXi server or AVP host on which VM is deployed. For patching the drop-down will only contain one host. Refer to [Appendix E for details on how to add host from VM Management](#).
 - **Data Store:** Data Store is the storage location where the VM will be created. It is populated after you select **Target Host**.
 - **Upgrade Source:** The upgrade source is the software library where the patch has been uploaded using [Download option](#) or [Sync option](#). The drop-down will have local library and all remote library configured.
 - **Upgrade/Update To:** Select from the patch files which are downloaded in the software library. The drop-down is populated after you select **Upgrade Source**. For patching, only the downloaded patches for that element will be listed.
 - **Flexi Footprint:** For patching, the flexi footprint is not required and can be blank.

Pre-upgrade Configuration

Note: While updating an element, one need to add or manage associated Host from Solution Deployment Manager --> VM Management to get it's parent in Parent Name Column and in the Target Host drop-down.

Element Name	Parent Name	IP Address	Current Version	Target Host	Data Store	Upgrade Source	Upgrade/Update To
CM_80	148.147.178.64	148.147.178.80	R017x.00.0.441.0	148.147.178.64	datastore1 (23)	SMGR_DEFAULT_LOCAL	00.0.441.0-22498.tar
utility_server_148.147.178.185	148.147.178.64	148.147.178.185	7.0.0.0.0.11	148.147.178.64	datastore1 (23)	SMGR_DEFAULT_LOCAL	util_patch_test.zip

Job Schedule

☒ Run Immediately
☐ Schedule later

Date: August 21, 2015
 Time: 18:28:17 24Hr
 Time Zone: (+5.30)Chennai, Kolkata, Mumbai, New Delhi, Sri Jayawardenepura

Schedule Cancel

Figure 70: Pre-upgrade check configuration for patching

6. Once the pre-upgrade check is complete, the pre-upgrade check status will be green and Upgrade/Update link will be enabled in Upgrade Actions.

Upgrade Management

Enable Auto Refresh(10 sec) | Show Selected Elements

Pre-upgrade Actions | **Upgrade Actions** | Download

4 Items | Show All | Filter: Enable

Name	Type	Sub-Type	IP Address	Release Status	Update Status	Last Action	Last Action Status	Pre-upgrade Check Status	Current Version	Entitled Upgrade Version
BSM_97	Session Manager	Branch Session Manager	148.147.178.97	✓	N/A	Analyze	✓	⚠	7.0.0.0.700007	7.0.0.0.700007
CM_65	Communication Manager	Avaya Aura(R) Communication Manager	148.147.162.65	⚠	⚠			⚠	R016x.03.0.124.0	
CM_80	Communication Manager	Avaya Aura(R) Communication Manager	148.147.178.80	✓	⚠	Pre-upgrade Check	✓	✓	R017x.00.0.441.0	N/A
utility_server_148.147.178.185	Utility Server		148.147.178.185	✓	⚠	Pre-upgrade Check	✓	✓	7.0.0.0.0.11	7.0.0.0.0.11

Select : All, None

Figure 71: Pre-upgrade check updated status

7. Click on Upgrade/Update option from Upgrade Actions. The page will be redirected to configuration page.

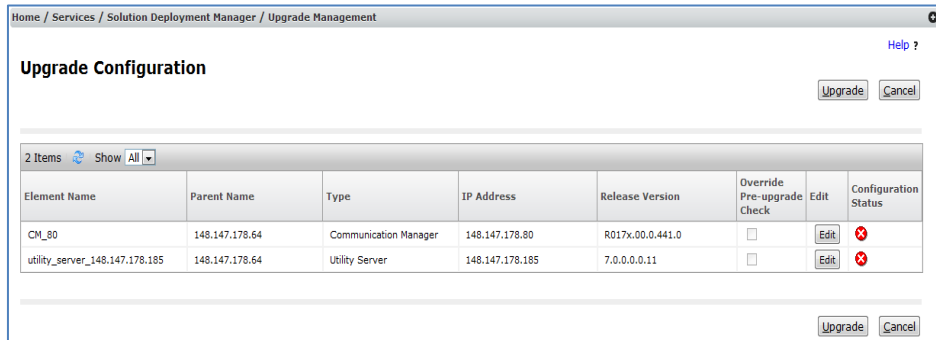


Figure 72: Patch configuration page for patching

8. Click on Edit button for each element to provide update configuration.
 - **Operation:** The operation will be Update.
 - **Upgrade Source:** The upgrade source is the software library.
 - **Select Patch:** The table will be populated with all the patches downloaded for that element under Update Configuration Details. Select one of the patches to apply that patch.
 - **Auto Commit:** Before applying the patch SDM takes snapshot of the VM for some patches. If the patch fails the snapshot is reverted to previous state. If the auto commit checkbox is checked the snapshot is deleted once the patch is successful. If the checkbox is left unchecked, the patch can be committed later from Installed Patches under Upgrade Actions. By default the patch will be auto committed in 24 hours.
 - **End User License Agreement:** Accept the EULA to Save the configuration.

Click on **Save** to save the configuration.

Communication Manager Configuration:

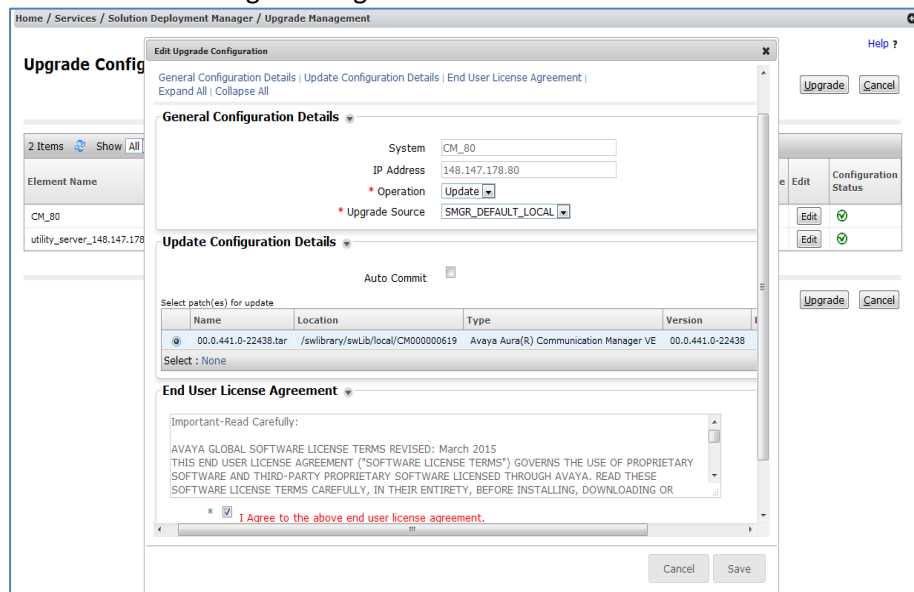


Figure 73: Example of Communication Manager patch configuration

Utility Services Configuration:

Upgrade Config

2 Items Show All

Element Name

CM_80

utility_server_148.147.178

Edit Upgrade Configuration

General Configuration Details | Update Configuration Details | End User License Agreement |

Expand All | Collapse All

General Configuration Details

System: utility_server_148.147.178.185

IP Address: 148.147.178.185

* Operation: Update

* Upgrade Source: SMGR_DEFAULT_LOCAL

Update Configuration Details

Auto Commit

Name	Location	Type	Version	Restart Required?
util_patch_test.zip	/swlibary/swLib/local/FU_US1440161832700	Custom Patch		false

Select: None

End User License Agreement

Important-Read Carefully:

AVAYA GLOBAL SOFTWARE LICENSE TERMS REVISED: March 2015
THIS END USER LICENSE AGREEMENT ("SOFTWARE LICENSE TERMS") GOVERNS THE USE OF PROPRIETARY SOFTWARE AND THIRD-PARTY PROPRIETARY SOFTWARE LICENSED THROUGH AVAYA. READ THESE SOFTWARE LICENSE TERMS CAREFULLY, IN THEIR ENTIRETY, BEFORE INSTALLING, DOWNLOADING OR

☒ I Agree to the above end user license agreement.

Cancel Save

Upgrade Cancel

Upgrade Cancel

Figure 74: Example of Utility Services patch configuration

- The configuration status will be green for the elements. Click on Upgrade and Schedule to schedule it immediately or later.

Home / Services / Solution Deployment Manager / Upgrade Management

Help ?

Upgrade Configuration

Upgrade Cancel

2 Items Show All

Element Name	Parent Name	Type	IP Address	Release Version	Override Pre-upgrade Check	Edit	Configuration Status
CM_80	148.147.178.64	Communication Manager	148.147.178.80	R017x.00.0.441.0	<input type="checkbox"/>	Edit	✓
utility_server_148.147.178.185	148.147.178.64	Utility Server	148.147.178.185	7.0.0.0.0.11	<input type="checkbox"/>	Edit	✓

Upgrade Cancel

Figure 75: Patch configuration completed

- Schedule of the job will redirect the page to Upgrade Management page where the status of the elements can be monitored.

Home / Services / Solution Deployment Manager / Upgrade Management

Help ?

Upgrade Management

Enable Auto Refresh(10 sec) | Show Selected Elements

Pre-upgrade Actions Upgrade Actions Download

4 Items Show All

Filter: Enable

Name	Parent	Type	Sub-Type	IP Address	Release Status	Update Status	Last Action	Last Action Status	Pre-upgrade Check Status	Current Version	Entitled Upgrade Version
BSM_97	148.147.178.64	Session Manager	Branch Session Manager	148.147.178.97	✓	N/A	Analyze	✓	⚠	7.0.0.0.700007	7.0.0.0.70
CM_65		Communication Manager	Avaya Aura(R) Communication Manager	148.147.162.65	ⓘ	ⓘ			⚠	R016x.03.0.124.0	
CM_80	148.147.178.64	Communication Manager	Avaya Aura(R) Communication Manager	148.147.178.80	✓	⚙	Upgrade	⚙	✓	R017x.00.0.441.0	N/A
utility_server_148.147.178.185	148.147.178.64	Utility Server		148.147.178.185	✓	⚙	Upgrade	⚙	✓	7.0.0.0.0.11	7.0.0.0.0.11

Select: All, None

Figure 76: Patch scheduled

- Click on Last Action Status for each element to check the status of the update.
- Communication Manager Status:

Upgrade Job Details

Element Status: 1 Item

Element Name	IP Address	Status
CM_80	148.147.178.80	✓

Detail Steps and Status: 8 Items

Step Name	Step Status	Error Description
Queued in scheduler	✓	
Patch-Install	✓	
PreUpdateCheck	✓	
CM-Requires files download	✓	
CM-Disk Space Check	✓	
CM-Host Version Check	✓	
CM-Is System Reachable	✓	
CM-Is Trust Established between SMGR and VM	✓	

Figure 77: Communication Manager patch job details

Utility Services Status:

Pre-upgrade Check Job Details

Element Status: 1 Item

Element Name	IP Address	Status
utility_server_148.147.178.185	148.147.178.185	✓

Detail Steps and Status: 6 Items

Step Name	Category	Step Status	Error Description
Queued in scheduler		✓	
US-Requires files download	MANDATORY	✓	
US-Disk Space Check	MANDATORY	✓	
US-Host Version Check	RECOMMENDED	✓	
US-Is System Reachable	MANDATORY	✓	
US-Is Trust Established between SMGR and VM	MANDATORY	✓	

Figure 78: Utility Services patch job details

- Communication Manager and Utility Services patches have been successfully installed on respective elements.

Upgrade Management

4 Items | Show: All | Filter: Enable

Name	Parent	Type	Sub-Type	IP Address	Release Status	Update Status	Last Action	Last Action Status	Pre-upgrade Check Status
BSM_97	148.147.178.64	Session Manager	Branch Session Manager	148.147.178.97	✓	N/A	Analyze	✓	⚠
CM_65		Communication Manager	Avaya Aura(R) Communication Manager	148.147.162.65	?	?			⚠
CM_80	148.147.178.64	Communication Manager	Avaya Aura(R) Communication Manager	148.147.178.80	✓	✓	Upgrade	✓	✓
utility_server_148.147.178.185	148.147.178.64	Utility Server		148.147.178.185	✓	✓	Upgrade	✓	✓

Figure 79: Upgrade Management updated status after patching

4.4 Duplex Migration

There is a process to migrate CM Duplex as it involves migrating two CMs. It is required as one of the CM must always be available to serve the endpoints and there is no down time for calls.

4.4.1 Preparing duplex Communication Manager for migration

The CM duplex system contains two CMs which are linked together. Here are steps to migrate the CM Duplex systems:

1. Add both CM systems in Home/Services/Inventory/Manage Elements. Refer to section [Things to know for configuring your elements in System Manager Manage Elements](#).
2. If it is System Platform based add System Platform associated with CMs Manage Elements. Refer to section [Things to know for configuring your elements in System Manager Manage Elements](#).
3. Adding System Platform will trigger second level discovery which will bring Template in the system and the parent association will be created with SP and CM. Below is an example of two CMs added along with SP.

<div> <div>Pre-upgrade Actions</div> <div>Upgrade Actions</div> <div>Download</div> </div>											
<div> <div>6 Items</div> <div>Show All</div> <div>Filter: Enable</div> </div>											
<input checked="" type="checkbox"/>	Name	Parent	Type	Sub-Type	IP Address	Release Status	Update Status	Last Action	Last Action Status	Pre-upgrade Check Status	Current Version
<input checked="" type="checkbox"/>	cm03-emat1-sp		System Platform	System Platform	135.64.105.173	?	?	Refresh Element	✓	N/A	6.3.0.0.1105
<input checked="" type="checkbox"/>	cm03-emat2-sp		System Platform	System Platform	135.64.105.175	?	?			N/A	6.3.0.0.1105
<input checked="" type="checkbox"/>	CM03-ES-EMAT	CM_Duplex	Communication Manager		135.64.105.181	!	N/A	Analyze	✓	!	R016x.03.0.12
<input checked="" type="checkbox"/>	CM03-ES-EMAT1	CM_Duplex	Communication Manager	Avaya Aura(R) Communication Manager	135.64.105.180	?	?			!	R016x.03.0.12
<input checked="" type="checkbox"/>	CM_Duplex	cm03-emat2-sp	Templates		135.64.105.175	?	?			N/A	6.3.0.0.1105
<input checked="" type="checkbox"/>	CM_Duplex	cm03-emat1-sp	Templates		135.64.105.173	?	?			N/A	6.3.0.0.1105

Figure 80: Upgrade Management - Communication Manager Duplex systems upgrade

4. Login to **Activated CM** and run following commands on **SAT terminal**:
 - a. save translation
5. From **Activated CM** and run following command from CLI
 - b. server -u (This will lock the translation to be sent to Standby server).

4.4.2 Duplex Same Box Migration

1. Perform steps [Refresh](#), [Analyze](#), [Download](#) and [Pre-upgrade check](#) for Standby CM only to bring it to “**Ready For Upgrade**” state.
2. Start upgrade of first CM which is in Standby state.
 - a. Select CM or SP of the standby CM and click on Upgrade.
 - b. Fill upgrade configuration of CM by click on Edit button.
 - c. Schedule the upgrade of Standby CM.
 - a. Ensure that you install the Appliance Virtualization Platform host, and add the Appliance Virtualization Platform host from VM Management.
 - b. Resume the configuration once the upgrade is in Paused State.
 - c. Check the job status for upgrade job which will take some time to complete
3. Standby CM will be upgraded after last step.
4. Duplication Parameter on Standby system needs to be configured again.

This can be done from CM UI click Administration → Server (Maintenance) → Server Configuration and configure following parameters

 - a. Network Configuration.
 - b. Duplication Parameters.
 - c. Server Role
5. From the command line interface of the standby Communication Manager, perform the following:
 - a. To release the server from the busy out state, type server –r
 - b. Type server, and ensure that the duplication link is active and the standby server refreshes.
6. Interchange the upgraded standby CM and the activated CM using following CLI command on Activated CM.
 - a. server -if
7. Repeat the step#1 and #2 for the other CM.
8. Both the CMs will now be upgraded.
9. Repeat Step#4 and #5 after the second CM Upgrade/Migrate.
10. Make final interchange on activated CM using following CLI command
 - a. server -if

4.4.3 Duplex Different Box Migration

1. Perform steps [Refresh](#), [Analyze](#), [Download](#) and [Pre-upgrade check](#) for now Standby only CM to bring it to “**Ready For Upgrade**” state.
2. Start upgrade of the CM which is in Standby state.
 - a. Select CM or SP of the standby CM and click on Upgrade.
 - b. Fill upgrade configuration of CM by click on Edit button.
 - c. Schedule the upgrade of Standby CM.
 - d. Check the job status for upgrade job which will take some time to complete.
3. The Standby CM will be upgraded wherein data is also restored back in 7.0 CM.
4. Configure Duplication Parameter on Standby system.

This can be done from CM UI:

- a. From Administration → Server (Maintenance) → Server Configuration → Network Configuration.
 - b. From Administration → Server (Maintenance) → Server Configuration → Duplication Parameters.
5. From **Standby CM CLI** run following command below to release the **BUSY OUT** state.
 - a. **server -r**
 6. From **Active CM CLI** run following command below to busy-out the server. This will bring Active Server in **BUSY OUT**.
 - a. **server -if**

This will bring Standby Server in Active Mode since there is no duplication link between Active CM and the new Standby CM.
 7. Verify that all the CM elements (like TN Boards, MG, MM, IPSI, etc.) got registered with new Active server and the calls are getting processed with new Active Server.
 8. Follow steps Refresh, Analyze and Pre-upgrade check for other CM now to bring it to “**Ready For Upgrade**” state.
 9. Start upgrade of the CM which was in Active state.
 - a. Select CM or SP of the standby CM and click on Upgrade.
 - b. Fill upgrade configuration of CM by click on Edit button.
 - c. Schedule the upgrade of Standby CM.
 - d. Check the job status for upgrade job which will take some time to complete.
 10. The CM will be upgraded wherein data is restored back in 7.0 CM.
 11. Configure Duplication Parameter on the upgraded system.

This can be done from CM UI click Administration → Server (Maintenance) → Server Configuration and configure following parameters

 - a. Network Configuration.
 - b. Duplication Parameters.
 - c. Server Role
 12. From **Upgraded CM CLI** run following command below to release the busied-out state.
 - a. **server -r**
 13. Make final interchange on **activated CM** using following CLI command
 - a. **server -i**

4.5 Upgrade Job Status

All the upgrade actions which are performed can be monitored using Upgrade Job Status. There are two ways the status can be checked.

- **Per Element Basis**

Any job executed for any element can be monitored from Upgrade Management Page under Last Action and Last Action Status. The two columns show what last operation was executed on that particular element and the status of it. If admin clicks on Last Action Status value, a pop-up will show the details of the action.

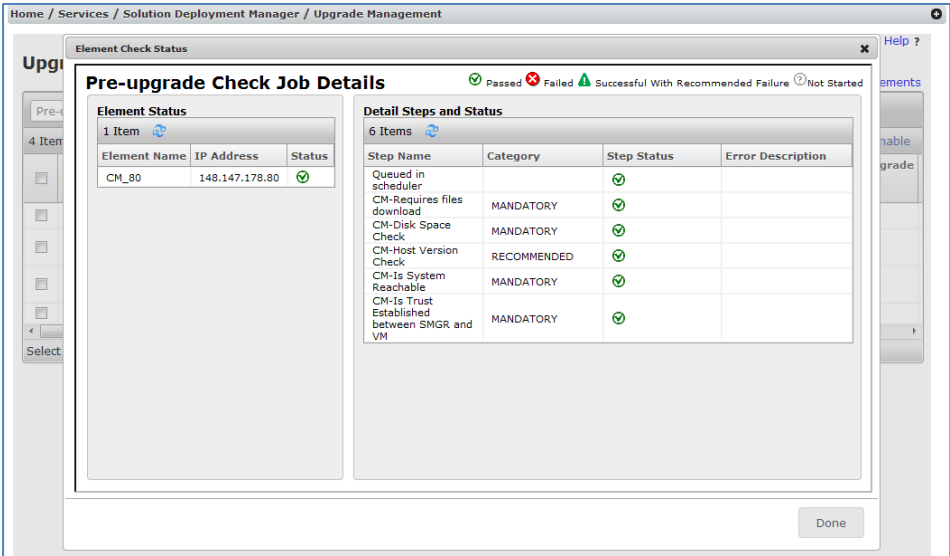


Figure 81: Per-element job details

- **Per Job Basis**

Admin can monitor the upgrade jobs from **Upgrade Job Status** under Solution Deployment Manager. To monitor the upgrade jobs, admin needs to select which type of job he/she would like to monitor.

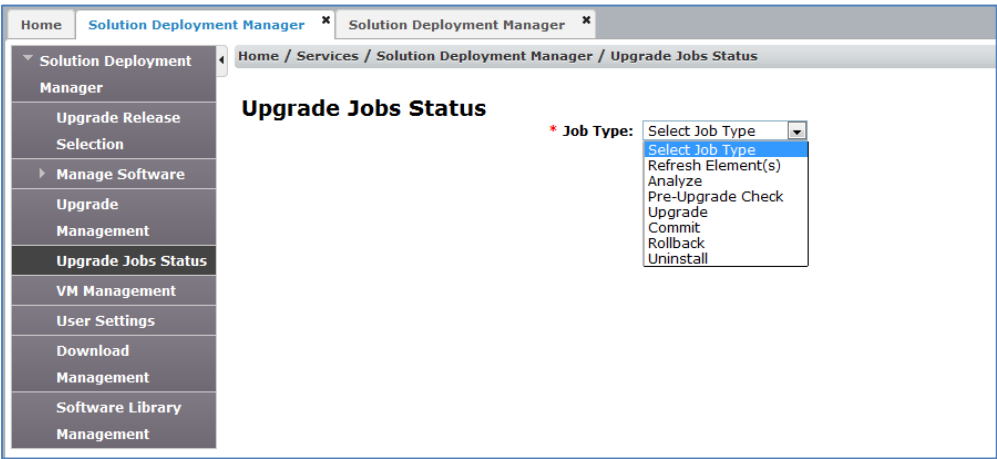


Figure 82: Upgrade Job Status Page

Once the job type is selected, the table with all the jobs will be shown:

Home / Services / Solution Deployment Manager / Upgrade Jobs Status

Upgrade Jobs Status

* Job Type: Upgrade

3 Items Show All

Job Name	Start Time	End Time	Status	% Complete	Element Records	Success Records
Upgrade_JobGroup_56e06eeb-6b8e-4ac2-9eb4-6a956965a74b	Aug 21, 2015 7:37 PM	Aug 21, 2015 7:51 PM	SUCCESSFUL	100	2	2
Upgrade_JobGroup_0b01a32c-f2af-4eba-aaa5-4c6d3937f494	Aug 20, 2015 7:48 PM	Aug 20, 2015 10:04 PM	SUCCESSFUL	100	3	3
Upgrade_JobGroup_b41e40e4-874b-4335-a892-085e5d4bcd67	Jun 11, 2015 9:56 PM		PAUSED	0	2	0

Select : All, None

Figure 83: Job List for selected Upgrade Job Type

Click on the job name to see the status of the job

Home / Services / Solution Deployment Manager / Upgrade Jobs Status

Upgrade Job Details

Element Job Status Details

Passed Failed Successful With Recommended Failure Not Started

Element Status

2 Items

Element Name	IP Address	Status
utility_server_148.147.178.185	148.147.178.185	✓
CM_80	148.147.178.80	✓

Detail Steps and Status

8 Items

Step Name	Step Status	Error Description
Queued in scheduler	✓	
Patch-Install	✓	
PreUpdateCheck	✓	
US-Requires files download	✓	
US-Disk Space Check	✓	
US-Host Version Check	✓	
US-Is System Reachable	✓	
US-Is Trust Established between SMGR and VM	✓	

Figure 84: Upgrade Job Details of an upgrade job

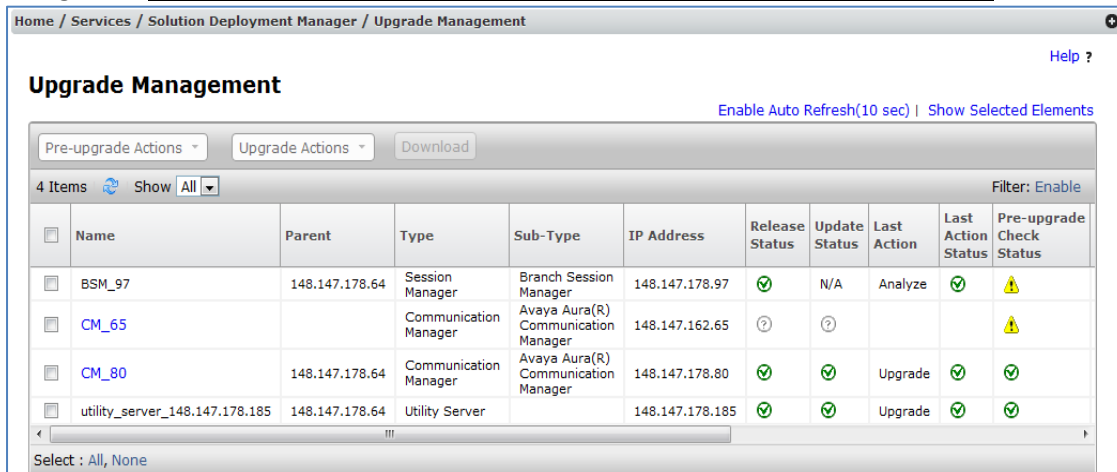
Click on each element from Element Status table to see its status on Details Steps and Status table. By default the first element is selected.

4.6 Installed Patches

SDM provided a view to the installed patches for the elements. There are various operations that can be performed on the installed patches depending on the patches support.

The patches operations are only for elements on Release 7.0.

Navigate to Home/Services/Solution Deployment Manager/Upgrade Management.



Home / Services / Solution Deployment Manager / Upgrade Management

Help ?

Upgrade Management

Enable Auto Refresh(10 sec) | Show Selected Elements

Pre-upgrade Actions | Upgrade Actions | Download

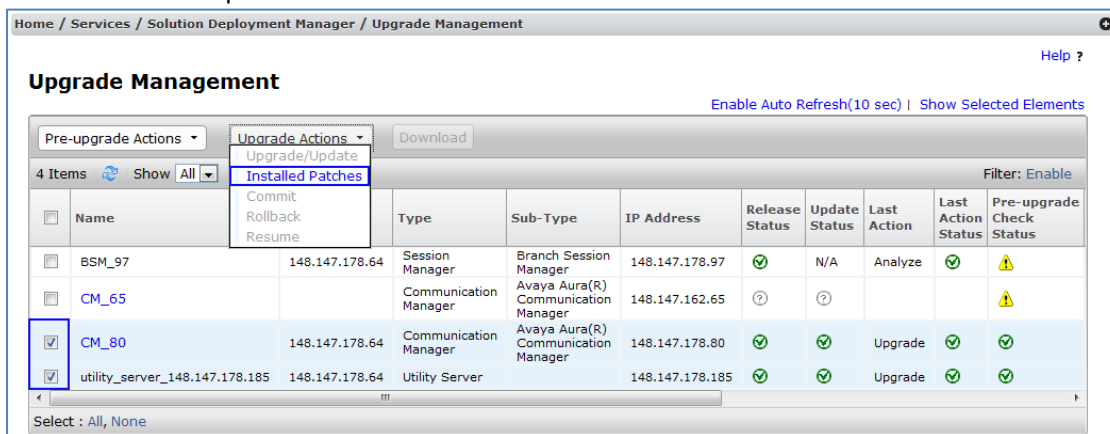
4 Items | Show | All | Filter: Enable

Name	Parent	Type	Sub-Type	IP Address	Release Status	Update Status	Last Action	Last Action Status	Pre-upgrade Check Status
BSM_97	148.147.178.64	Session Manager	Branch Session Manager	148.147.178.97	✓	N/A	Analyze	✓	⚠
CM_65		Communication Manager	Avaya Aura(R) Communication Manager	148.147.162.65	?	?			⚠
CM_80	148.147.178.64	Communication Manager	Avaya Aura(R) Communication Manager	148.147.178.80	✓	✓	Upgrade	✓	✓
utility_server_148.147.178.185	148.147.178.64	Utility Server		148.147.178.185	✓	✓	Upgrade	✓	✓

Select : All, None

Figure 85: Upgrade Management Page

1. Select the element(s) on the Upgrade Management page, from Upgrade Actions go to Installed patches.



Home / Services / Solution Deployment Manager / Upgrade Management

Help ?

Upgrade Management

Enable Auto Refresh(10 sec) | Show Selected Elements

Pre-upgrade Actions | Upgrade Actions | Download

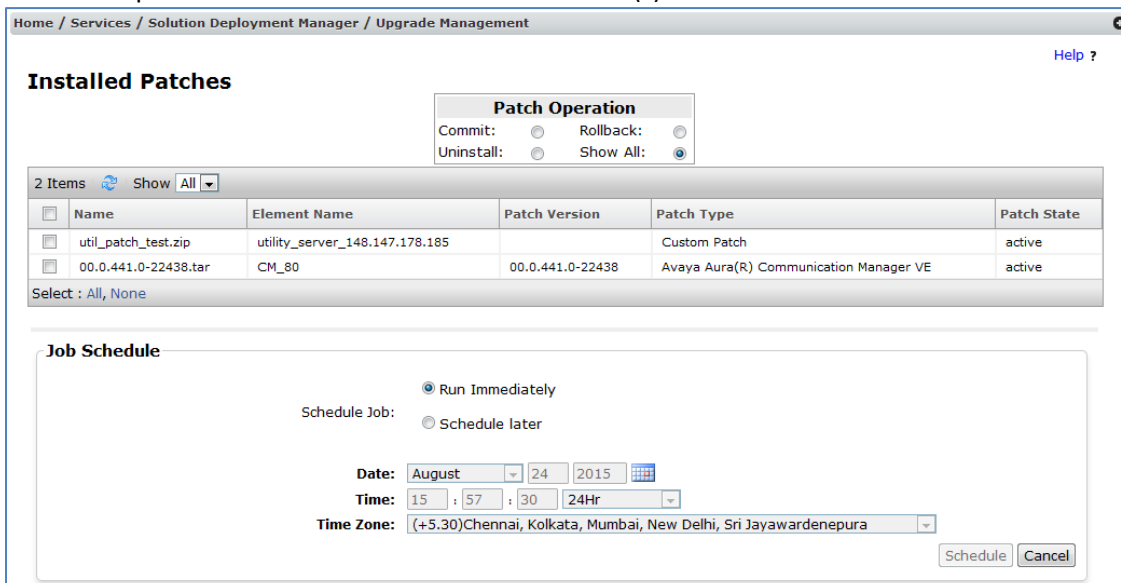
4 Items | Show | All | Filter: Enable

Name	Parent	Type	Sub-Type	IP Address	Release Status	Update Status	Last Action	Last Action Status	Pre-upgrade Check Status
BSM_97	148.147.178.64	Session Manager	Branch Session Manager	148.147.178.97	✓	N/A	Analyze	✓	⚠
CM_65		Communication Manager	Avaya Aura(R) Communication Manager	148.147.162.65	?	?			⚠
<input checked="" type="checkbox"/> CM_80	148.147.178.64	Communication Manager	Avaya Aura(R) Communication Manager	148.147.178.80	✓	✓	Upgrade	✓	✓
<input checked="" type="checkbox"/> utility_server_148.147.178.185	148.147.178.64	Utility Server		148.147.178.185	✓	✓	Upgrade	✓	✓

Select : All, None

Figure 86: Upgrade Management Page Upgrade Actions – Installed Patches

2. The page will be redirected to Installed Patches Page. The table will show all the patches installed on the selected element(s).



Home / Services / Solution Deployment Manager / Upgrade Management

Help ?

Installed Patches

Patch Operation

Commit: ☐ Rollback: ☐
Uninstall: ☐ Show All: ☒

2 Items | Show | All

Name	Element Name	Patch Version	Patch Type	Patch State
util_patch_test.zip	utility_server_148.147.178.185		Custom Patch	active
00.0.441.0-22438.tar	CM_80	00.0.441.0-22438	Avaya Aura(R) Communication Manager VE	active

Select : All, None

Job Schedule

Run Immediately ☒ Schedule Job: ☐ Schedule later

Date: August 24 2015

Time: 15 : 57 : 30 24Hr

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

Schedule Cancel

Figure 87: Installed Patches page

- The operations provided for patches are available in Patch Operations. The default is Show All option which shows all the patches.
- To perform any operation on patches click on any of the Patch Operation. There are different operations which are supported by different patches provided by elements.
Commit: SDM takes a VM snapshot of the element before applying some patches. The patch table will only show patches that can be committed. If the patch is committed the snapshot will be removed and element will contain the patch.

The screenshot shows the 'Installed Patches' window. At the top, the 'Patch Operation' menu has 'Commit' selected. Below the menu, there is a table with 0 items. The table headers are: Name, Element Name, Patch Version, Patch Type, and Patch State. The table content shows 'No Patches'.

Figure 88: Patch list based on selected patch operations - Commit

Rollback: SDM takes a VM snapshot of the element before applying some patches. The patch table will only show patches that can be rolled back and has not been committed yet. If the patch is rolled back then the snapshot is reverted to the previous state.

The screenshot shows the 'Installed Patches' window. At the top, the 'Patch Operation' menu has 'Rollback' selected. Below the menu, there is a table with 0 items. The table headers are: Name, Element Name, Patch Version, Patch Type, and Patch State. The table content shows 'No Patches'.

Figure 89: Patch list based on selected patch operations - Rollback

Uninstall: The patches which support uninstallation will only be listed in the patch table.

The screenshot shows the 'Installed Patches' window. At the top, the 'Patch Operation' menu has 'Uninstall' selected. Below the menu, there is a table with 2 items. The table headers are: Name, Element Name, Patch Version, Patch Type, and Patch State. The table content shows two patches: 'util_patch_test.zip' and '00.0.441.0-22438.tar'. Below the table, there is a 'Job Schedule' section with options to 'Run Immediately' or 'Schedule later'. The 'Run Immediately' option is selected. The 'Schedule Job' section includes fields for Date (August 24, 2015), Time (15:57:30), and Time Zone ((+5.30)Chennai, Kolkata, Mumbai, New Delhi, Sri Jayawardenepura). There are 'Schedule' and 'Cancel' buttons at the bottom right.

Figure 90: Patch list based on selected patch operations - Uninstall

- Select the patches from the tables to uninstall. Click on Schedule to run immediately or scheduler later. The page will be redirected to Upgrade Management Page where the progress of the patch can be monitored.

Upgrade Management Enable Auto Refresh(10 sec) | Show Selected Elements

Pre-upgrade Actions Upgrade Actions Download

4 Items Show All Filter: Enable

	Name	Parent	Type	Sub-Type	IP Address	Release Status	Update Status	Last Action	Last Action Status	Pre-upgrade Check Status
<input type="checkbox"/>	BSM_97	148.147.178.64	Session Manager	Branch Session Manager	148.147.178.97	✓	N/A	Analyze	✓	⚠
<input type="checkbox"/>	CM_65		Communication Manager	Avaya Aura(R) Communication Manager	148.147.162.65	?	?			⚠
<input checked="" type="checkbox"/>	CM_80	148.147.178.64	Communication Manager	Avaya Aura(R) Communication Manager	148.147.178.80	✓	⚠	Uninstall	✓	✓
<input checked="" type="checkbox"/>	utility_server_148.147.178.185	148.147.178.64	Utility Server		148.147.178.185	✓	⚠	Uninstall	✓	✓

Select : All, None

Figure 91: Uninstallation of patches scheduled

- Click on Last Action Status of each element to check the status of Uninstallation of the patch.

Home / Services / Solution Deployment Manager / Upgrade Management

Element Check Status

Uninstall Job Details Passed Failed Successful With Recommended Failure Not Started

Element Status

1 Item

Element Name	IP Address	Status
CM_80	148.147.178.80	✓

Detail Steps and Status

2 Items

Step Name	Step Status	Error Description
Queued in scheduler	✓	
Patch-Uninstall	✓	

Done

Figure 92: Uninstallation Job details

- Patch uninstallation is complete and both the elements patch have been uninstalled, the update status has changed to Ready For Update.

Home / Services / Solution Deployment Manager / Upgrade Management

Upgrade Management Enable Auto Refresh(10 sec) | Show Selected Elements

Pre-upgrade Actions Upgrade Actions Download

4 Items Show All Filter: Enable

	Name	Parent	Type	Sub-Type	IP Address	Release Status	Update Status	Last Action	Last Action Status	Pre-upgrade Check Status
<input type="checkbox"/>	BSM_97	148.147.178.64	Session Manager	Branch Session Manager	148.147.178.97	✓	N/A	Analyze	✓	⚠
<input type="checkbox"/>	CM_65		Communication Manager	Avaya Aura(R) Communication Manager	148.147.162.65	?	?			⚠
<input type="checkbox"/>	CM_80	148.147.178.64	Communication Manager	Avaya Aura(R) Communication Manager	148.147.178.80	✓	⚠	Uninstall	✓	✓
<input type="checkbox"/>	utility_server_148.147.178.185	148.147.178.64	Utility Server		148.147.178.185	✓	⚠	Uninstall	✓	✓

Select : All, None

Figure 93: Updated status on Upgrade Management page

Setting up Alternate Source and Software Library

For SDM fresh deployment/upgrade/migration software library with following protocols are supported

1. FTP
2. SFTP
3. SCP

Also, if multiple protocols are used then make sure you have same user home/landing folder configured for all the protocols.

To set the Software Library you need to enable FTP and SCP/SFTP services. For this purpose we suggest to use:

- Apache HTTP server (httpd-2.0.64-win32-x86-openssl-0.9.8o.msi);
- FileZilla FTP server (FileZilla_Server-0_9_43.exe);

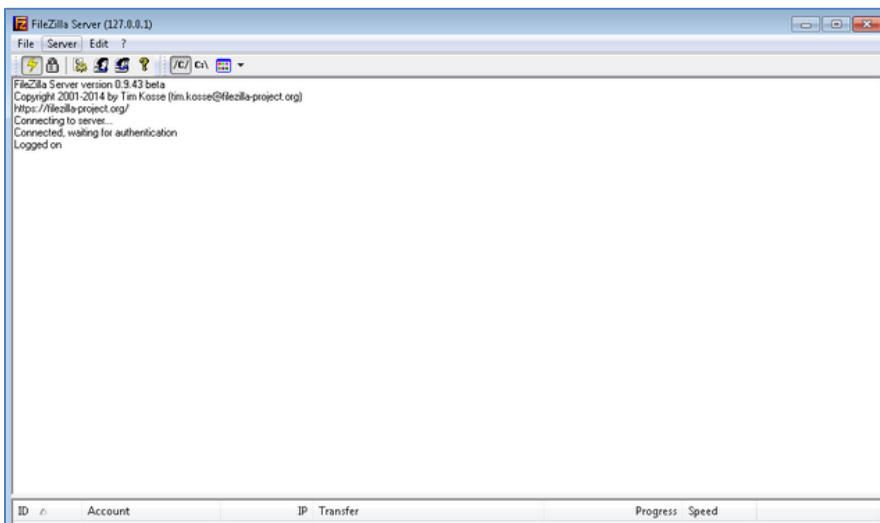
Installing a HTTP server on Windows Environment:

Run the httpd-2.0.64-win32-x86-openssl-0.9.8o.msi installer as administrator, provide domain name, server name and email id. Complete the installation. Start the Apache server.

Create a folder name downloads at location C:\Program Files (x86)\Apache Group\Apache2\htdocs\ and provide all the privileges to it. E.g. C:\Program Files (x86)\Apache Group\Apache2\htdocs\downloads\ Test by creating a file under this folder and access it from browser.

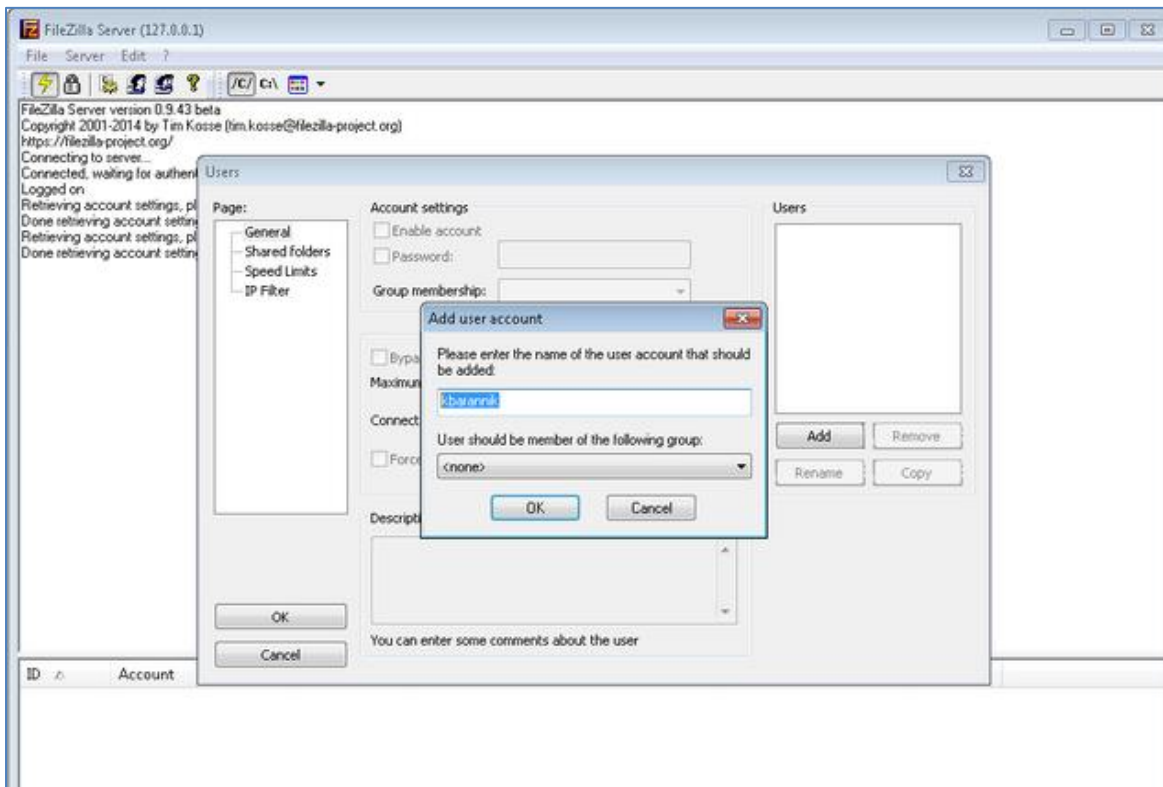
Installing a FTP server Windows Environment:

Install FileZilla_Server-0_9_43.exe as administrator, and after complete installation open the filezilla server interface.

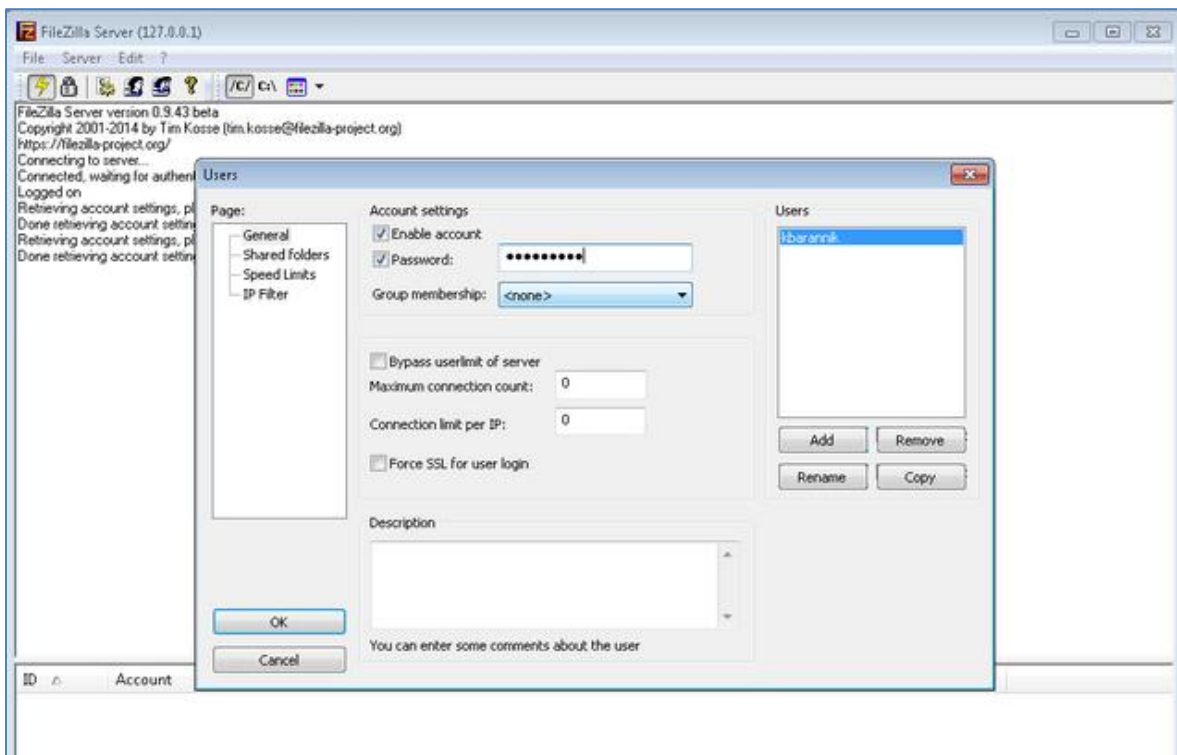


Click on Edit Menu → Users.

Under General Page, click Add under Users.



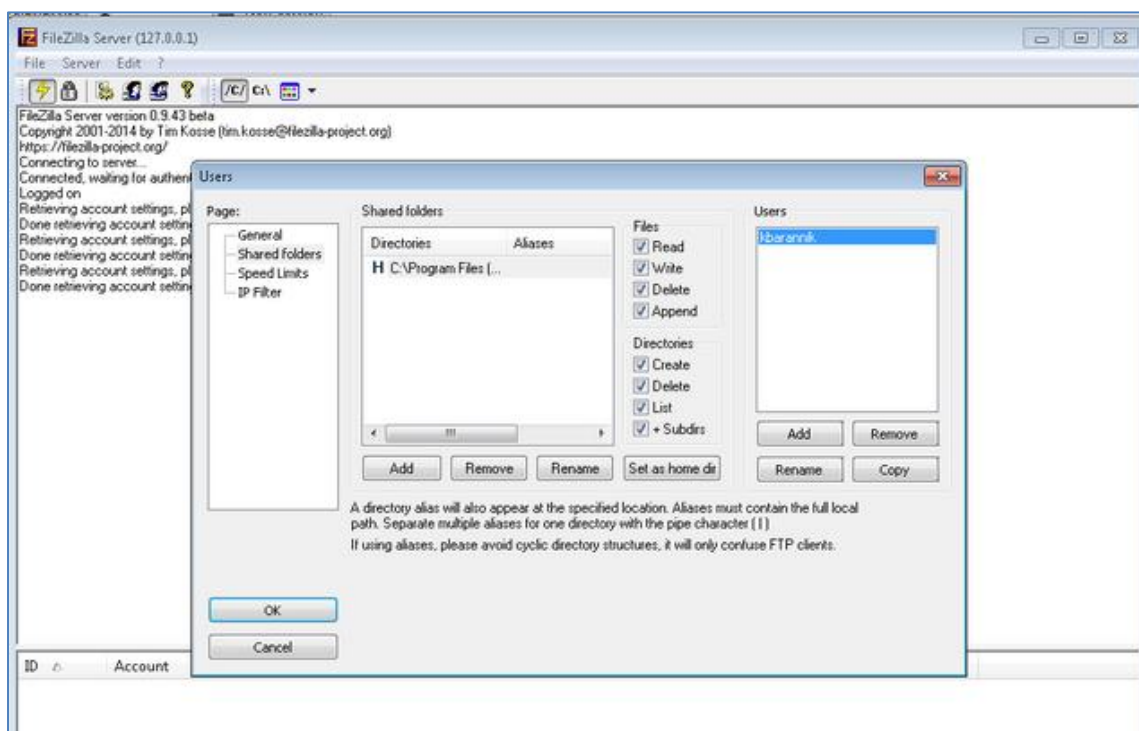
Provide a user name.
 Then click Ok.
 Check checkbox Password.
 Enter the password
 Click Ok.



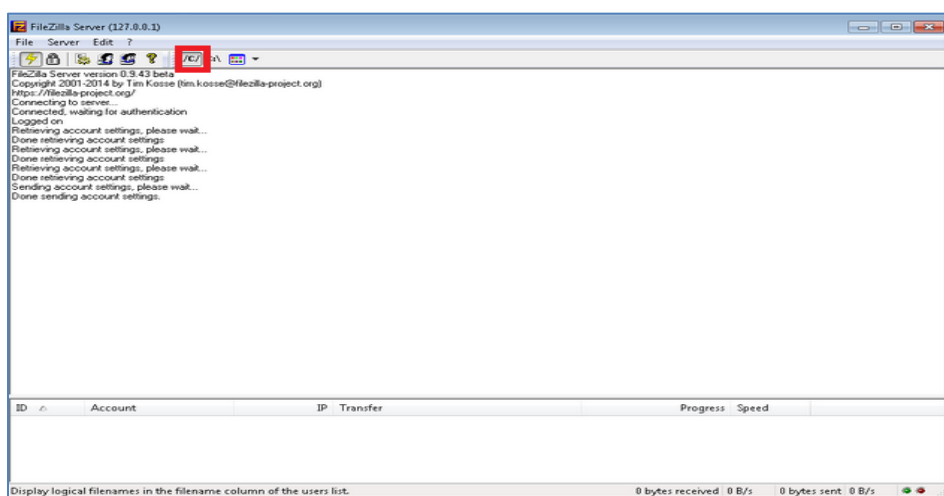
It will now ask for a folder, so now go to Shared Folders page
 Click on Add and provide the folder location till downloads.
 Click ok

Provide all the privileges under files and directories section i.e. read, write, delete etc.

Click on Set as Home Directory to "C:\Program Files (x86)\Apache Group\Apache2\htdocs\downloads\" and then ok.



Also make sure Logical file name option is selected. By default this option is selected.



Test from ftp client.

Appendix B

Setting up CM and Media Gateway SNMP Access

Configuring Communication Manager for administration and SNMP access

Access CM SMI web interface (CM 5.2.1 example)

Configure prof18 suser account

Configure SNMPv1 communities

The left screenshot shows the 'Administrator Accounts -- Change Login' page. The 'Additional groups (profile)' field is set to 'prof18', which is highlighted with a yellow circle. The right screenshot shows the 'SNMPv1 Communities' configuration page. The 'Community Name (read-only)' is set to 'public' and the 'Community Name (read-write)' is set to 'publiccrw', both highlighted with a yellow circle.

Access System Manager UI and manually add CM in the Manage Elements

Home / Services / Inventory / Manage Elements

The top screenshot shows the 'Add Communication Manager' form. The 'Name' field is set to 'S8300DSUMFP4LSP'. The bottom screenshot shows the 'Add Communication Manager' form. The 'Read Community' field is set to 'public' and the 'Write Community' field is set to 'publiccrw', both highlighted with a yellow circle.

At this step need to make sure that CM Administrator account and SNMPv1 access credentials are identical in CM SMI and System Manager Manage Elements administration.

Configuring H.248 Gateway access

Using SSH access H.248 GW CLI interface

```
ima-003(super)# snmp-server community read-only public read-write publicrw  
Done!
```

Access System Manager UI and manually add H.248 GW in the Manage Elements

Home / Services / Inventory / Manage Elements. Make sure GW root access password and SNMPv1 credentials in System Manager are identical to what is administered in GW

The image displays three screenshots from the Access System Manager (ASM) UI, illustrating the steps to configure H.248 Gateway access.

Top Screenshot: Manage Elements - General
This screenshot shows the 'General' tab for a new element. The 'Name' field is set to 'G350'. The 'Type' is 'Communication Manager and G350 Media Gateway'. The 'Description' is 'Avaya Inc., G350 Media Gateway, SW Version 30.21.0'. The 'Node' is '30.134.1.24'. The 'Device Type' is 'Avaya G350'.

Bottom Left Screenshot: Access Profile - Details
This screenshot shows the 'Access Profile Details' for the 'H248GWAccess' profile. The 'Name' is 'H248GWAccess'. The 'Login Name' is 'root'. The 'Port' is '22'. The 'Use ASG Key' checkbox is unchecked. The 'Password' and 'Confirm Password' fields are filled with masked characters. The 'Save' and 'Cancel' buttons are at the bottom.

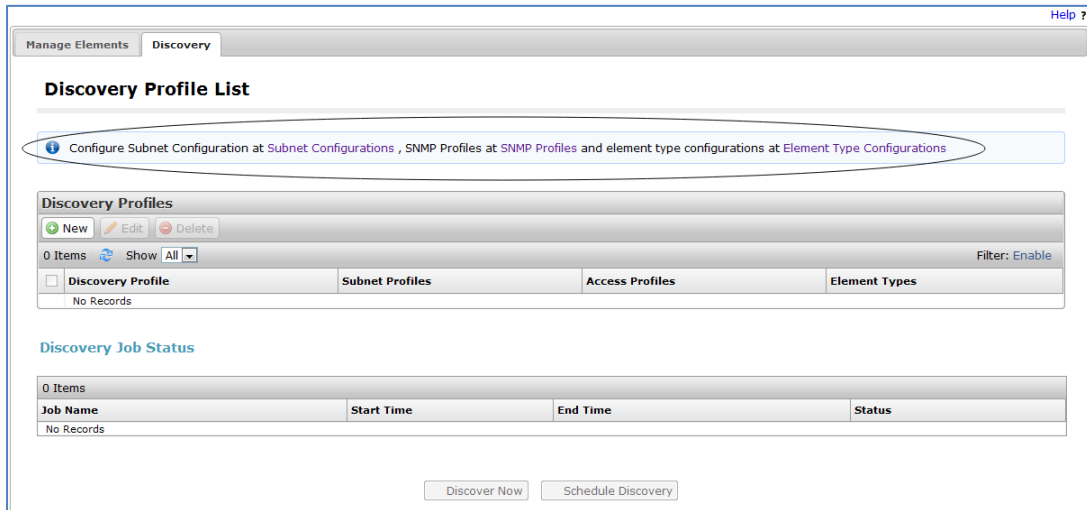
Bottom Right Screenshot: Access Profile - Details
This screenshot shows the 'Access Profile Details' for the 'G350-V1' profile. The 'Profile Name' is 'G350-V1'. The 'Description' is empty. The 'Type' is 'V1'. The 'Read Community' is 'public'. The 'Write Community' is 'publicrw'. The 'Timeout' is '5000'. The 'Retries' is '3'. The 'Type', 'Read Community', 'Write Community', 'Timeout', and 'Retries' fields are circled in yellow.

Red arrows indicate the flow of configuration: from the 'G350-V1' profile in the top screenshot to the 'G350-V1' profile in the bottom right screenshot, and from the 'H248GWAccess' profile in the bottom left screenshot to the 'H248GWAccess' profile in the bottom right screenshot.

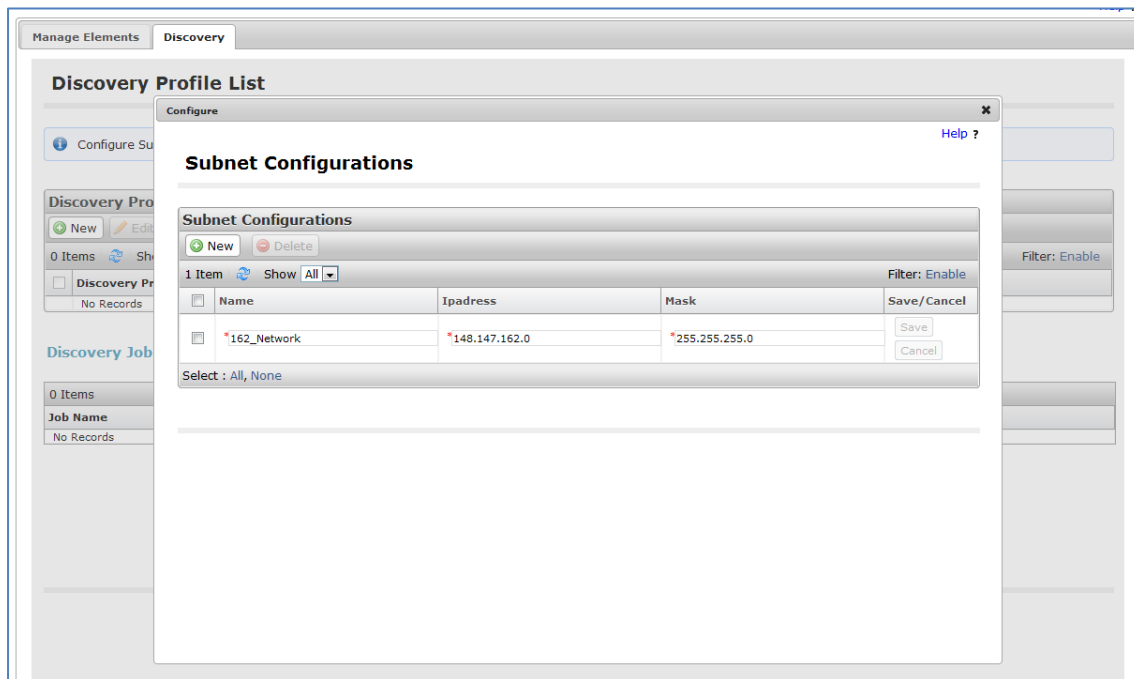
Appendix C

Subnet Discovery Configuration

Elements can be discovered using Subnet Discovery from Home/Services/Inventory/Manage Elements - Discovery Tab. Below is some screenshots which will help in configuring discovery for elements.



1. Configure Subnet Configuration by clicking on the link Subnet Configurations on the Info Note on top of the screen.



2. Configure SNMP Profile by clicking on SNMP Profiles on the Info Note on top of the screen.

The screenshot shows the 'Discovery Profile List' window with the 'Configure' tab selected. The main title is 'SNMP Access Profiles'. Below it, there is a 'Profile List' section with a table containing one item, 'SNMPProf1'. The table has columns for Profile Name, Type, Read Community, Write Community, User, Auth Type, Priv Type, Privileges, Timeout, Retries, and Description. The 'SNMPProf1' entry has Type 1, Read Community 'public', Write Community 'private', Timeout 5000, and Retries 3. There are also 'New', 'Edit', and 'Delete' buttons at the top of the table.

Profile Name	Type	Read Community	Write Community	User	Auth Type	Priv Type	Privileges	Timeout	Retries	Description
SNMPProf1	1	public	private					5000	3	

3. Element Type Configuration can also be configured for a particular element type, this can be done by clicking on Info Note on top of the screen.

The screenshot shows the 'Discovery Profile List' window with the 'Configure' tab selected. The main title is 'Element Type Access Profile Management'. Below it, there is a dropdown menu for 'Element Type' set to 'Communication Manager'. Underneath, there is a table titled 'Element Type Access Profiles' with columns for Name, Protocol, Login User Name, and System Profile. The table contains two items: 'CMGeoWSURL' with Protocol 'URI' and System Profile 'true', and 'CMMTEJBAPP' with Protocol 'URI' and System Profile 'true'. There are also 'New', 'View', 'Edit', and 'Delete' buttons at the top of the table. A note at the bottom states: 'Note: View, Edit and Delete operations are not allowed for System Profile(s)'.

Name	Protocol	Login User Name	System Profile
CMGeoWSURL	URI		true
CMMTEJBAPP	URI		true

- Click on New Discovery Profile for configuring Discovery Profiles for discovery of elements. Select Subnet Configuration, Element Type Access Profiles, SNMP Profile List and Commit.

Create Discovery Profile

*DiscoveryProfile Name: Commit Cancel

Subnet Configurations

1 Item Show All Filter: Enable

Name	Ipadress	Mask
162_Network	148.147.162.0	255.255.255.0

Select : All, None

Element Type Access Profiles

28 Items Show 15 Filter: Enable

Element Types	Discovery ElementType Access Profiles	Choose ElementType Access Profiles
<input type="checkbox"/> Application Enablement Services		Choose Element Access
<input type="checkbox"/> Avaya Aura® Media Server		Choose Element Access
<input checked="" type="checkbox"/> Communication Manager	CMGeoWSURL_CMNTEJBAFP	Choose Element Access
<input type="checkbox"/> Meeting Exchange and Conferencing 6.0		Choose Element Access
<input type="checkbox"/> Engagement Development Platform	Collaboration Environment TM	Choose Element Access
<input type="checkbox"/> ESXi Host		Choose Element Access
<input type="checkbox"/> IP Office		Choose Element Access
<input type="checkbox"/> Media Gateway		Choose Element Access
<input type="checkbox"/> Media Module		Choose Element Access
<input type="checkbox"/> Messaging	MessagingGeoWSURL	Choose Element Access
<input type="checkbox"/> Conferencing		Choose Element Access
<input type="checkbox"/> OneX Portal		Choose Element Access
<input type="checkbox"/> Other Applications		Choose Element Access
<input type="checkbox"/> Presence Services	xcp,stat	Choose Element Access
<input checked="" type="checkbox"/> Session Manager	Session Manager	Choose Element Access

Select : All, None 1 of 2

Profile List

1 Item Show All Filter: Enable

Profile Name	Type	Read Community	Write Community	User	Auth Type	Priv Type	Privileges	Timeout	Retries	Description
SNMPProf1	1	public	private					5000	3	

Select : All, None Commit Cancel

- One can create multiple Discovery Profiles to start discovery. Select from the list of Discovery Profiles and click on Discover Now. It will take some time depending on your Subnet Configuration to discover number of elements.

Discovery Profile List

Configure Subnet Configuration at [Subnet Configurations](#) , SNMP Profiles at [SNMP Profiles](#) and element type configurations at [Element Type Configurations](#)

Discovery Profiles

New Edit Delete

1 Item Show All Filter: Enable

Discovery Profile	Subnet Profiles	Access Profiles	Element Types
DiscoveryProfile1	162_Network		Communication Manager

Select : All, None

Discovery Job Status

0 Items

Job Name

No Records

Discovery Status

Discovery is Running...

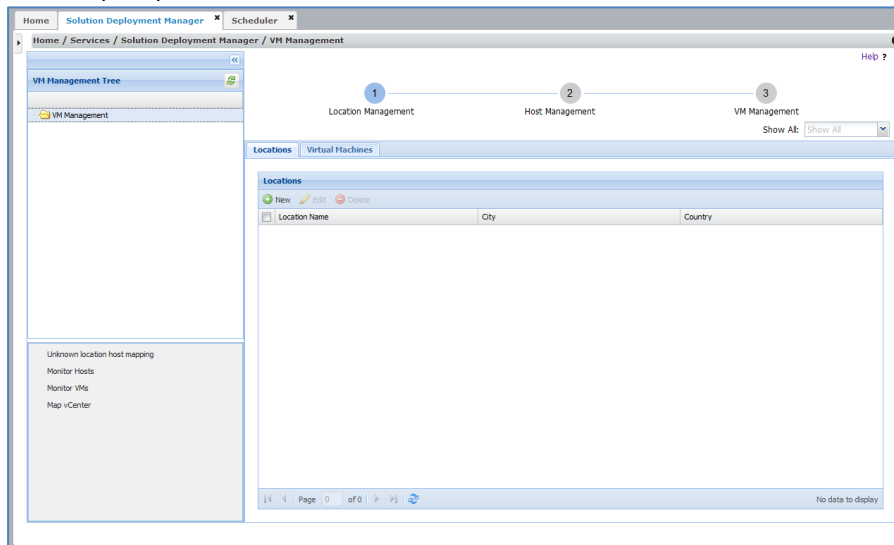
Number of Elements Discovered : 0

Discover Now Schedule Discovery

- After discovery element will show up in **Home/Services/Inventory/Manage Elements – Manage Elements Tab**.

Adding a location on VM Management

Hosts can be added from VM Management. The host can be customer VMware (ESXi) or Appliance Virtualization Platform (AVP).



1. Click on New button to create a location, the page will be directed to New Location. Enter required information and click Save.

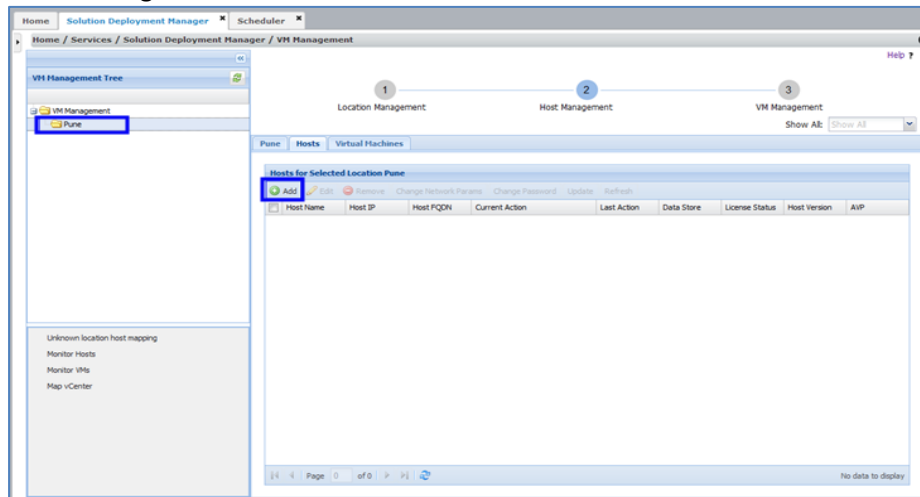
The screenshot shows the 'New Location' form. It contains several input fields for location details: Name (Pune), Address (Avaya India Pvt. Ltd., Tower-11, Cybercity, Magarpatta City), City (Pune), State/Province/Region (Maharashtra), Zip/Postal Code (411013), and Country (India). There is also a section for 'Optional Location Information' with fields for DefaultGateway, DNS Search List, DNS Server1, DNS Server2, NetMask, and NtpServer. The form has 'Save' and 'Cancel' buttons at the bottom right.

2. VM Management Tree will show the location created.

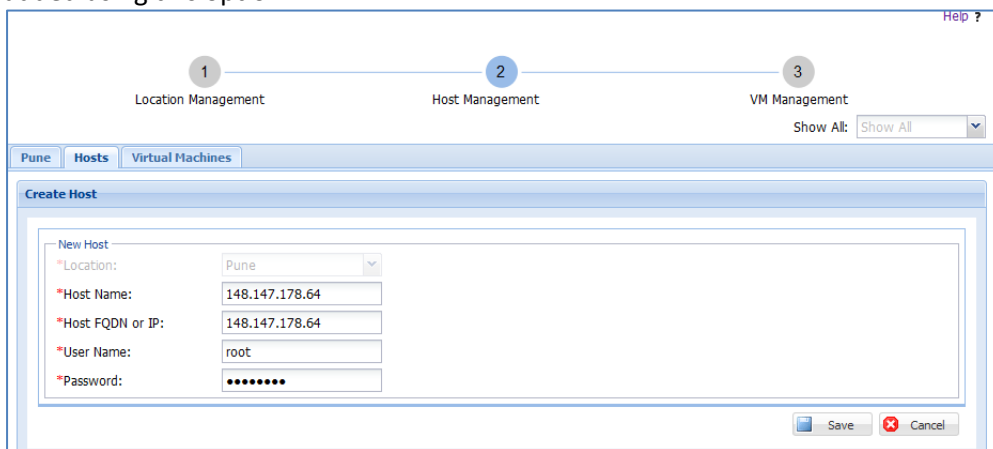
Adding a host on VM Management

To add a host on VM Management, it is required to create a location under which the host will be created. If the location is already created follow the below steps, to create a location refer to [Adding location on VM Management](#)

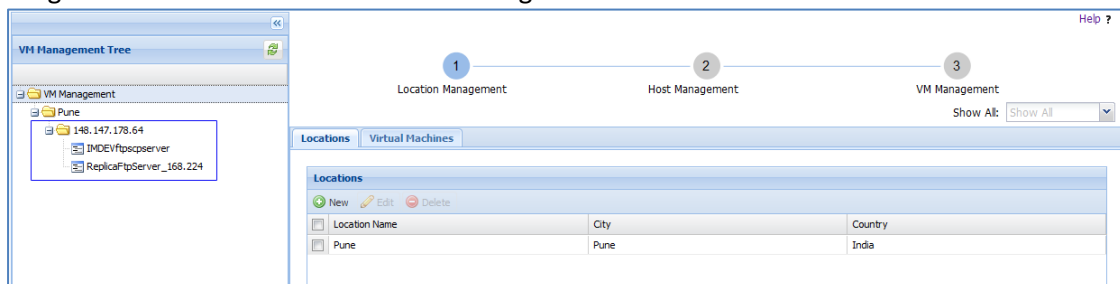
1. Navigate to Home/Services/Solution Deployment Manager/VM Management. Click on the location on VM Management Tree and click on Add button to create a host.



2. Click on Add button on Hosts Tab to add a host. Fill in required information and click on Save to save the host under the location. AVP servers and ESXi Hosts which are not managed from vCenter can be added using this option.



3. Click Ok on the alert shown. The host is added and the page will be directed to Location Management. The host is added to VM Management Tree under the location.



4. If the ESXi host (non AVP Host only) is managed via vCenter, it is required to manage map vCenter in VM Management and add host via Map vCenter UI.
 - Click on [Map vCenter](#) from VM Management Page.
 - Click on [Add](#) to map vCenter.

- Fill in vCenter IP/FQDN, User Name and Password and click on Save. Clicking on Save will trigger discovery of all the hosts on that vCenter. The time taken for discovery will vary based on the hosts on the vCenter.

Note: SSO User Name and Password will not work for authenticating vCenter. Create a local user on vCenter for managing it.

VM Management Tree

- VM Management
 - Pune
 - 148.147.178.64
 - IMDEV/tpscpserver
 - ReplicaFtpServer_168.224

Unknown location host mapping

Monitor Hosts

Monitor VMs

Map vCenter

Map vCenter

New vCenter

vCenter IP/FQDN: smgrvc-smgrdev.avaya

User Name: Administrator@vsphen

Password:

Save Cancel Refresh

If you do not click Commit after you move the host from Managed Hosts to Nonmanaged Hosts or from Nonmanaged Hosts to Managed Hosts, and you refresh the table, the page displays the same host in both tables. Click Commit to get an updated list of managed and nonmanaged hosts. While managing hosts from vCenter, select all edited hosts. By default, the system selects only the latest edited host.

Managed Hosts

Host IP/FQDN	Host Name	Location	Edit
Please wait...			

Nonmanaged Hosts

Host IP/FQDN	ESXi Version
Please wait...	

Page 0 of 0 No data to display

Page 1 of 3 Displaying 1 - 15 of 43

- The hosts (ESXi) will appear in right side table under Nonmanaged Hosts. Select the host you want to add to VM Management and click on left green arrow to manage hosts from VM Management.

The screenshot shows the Host Management interface. On the left is the 'Managed Hosts' table, which is currently empty. On the right is the 'Nonmanaged Hosts' table, which contains a list of hosts. A green arrow button is highlighted between the two tables, indicating the action to move a host from non-managed to managed.

Host IP/FQDN	Host Name	Location	Edit
No data to display			

Host IP/FQDN	ESXi Version
<input checked="" type="checkbox"/> 148.147.162.18	ESXi 5.5
<input checked="" type="checkbox"/> 148.147.162.197	ESXi 5.1
<input checked="" type="checkbox"/> 148.147.162.236	ESXi 5.5
<input type="checkbox"/> 148.147.162.27	ESXi 5.5
<input type="checkbox"/> 148.147.162.42	ESXi 5.5
<input type="checkbox"/> 148.147.162.58	ESXi 5.5
<input type="checkbox"/> 148.147.162.97	ESXi 5.5
<input type="checkbox"/> 148.147.168.206	ESXi 5.0
<input type="checkbox"/> 148.147.168.220	ESXi 5.0
<input type="checkbox"/> 148.147.168.237	ESXi 5.0

- Once the arrow button is clicked the hosts will move to Managed Hosts table. Select the host and from drop-down select a location for the hosts and click Bulk Update.

The screenshot shows the Host Management interface after the hosts have been moved. The 'Managed Hosts' table now contains three hosts, all with the location 'Pune' selected in the drop-down menu. The 'Nonmanaged Hosts' table still contains the remaining hosts.

Host IP/FQDN	Host Name	Location	Edit
<input checked="" type="checkbox"/> 148.147.162.18	148.147.162.18	Pune	
<input checked="" type="checkbox"/> 148.147.162.236	148.147.162.236	Pune	

Host IP/FQDN	ESXi Version
<input type="checkbox"/> 148.147.162.197	ESXi 5.1
<input type="checkbox"/> 148.147.162.27	ESXi 5.5
<input type="checkbox"/> 148.147.162.42	ESXi 5.5
<input type="checkbox"/> 148.147.162.58	ESXi 5.5
<input type="checkbox"/> 148.147.162.97	ESXi 5.5
<input type="checkbox"/> 148.147.168.206	ESXi 5.0
<input type="checkbox"/> 148.147.168.220	ESXi 5.0
<input type="checkbox"/> 148.147.168.237	ESXi 5.0
<input type="checkbox"/> 148.147.168.252	ESXi 5.5
<input type="checkbox"/> 148.147.175.98	ESXi 5.0

- Click on Commit button to save the host in VM Management. Click Ok on the alert. The page will be redirected to Location Management and the hosts managed will start showing up in VM Management Tree.

The screenshot shows the VM Management interface. On the left is the 'VM Management Tree' showing a hierarchy of hosts under the 'Pune' location. On the right is the 'Locations' table, which contains one entry for 'Pune'.

Location Name	City	Country
Pune	Pune	India

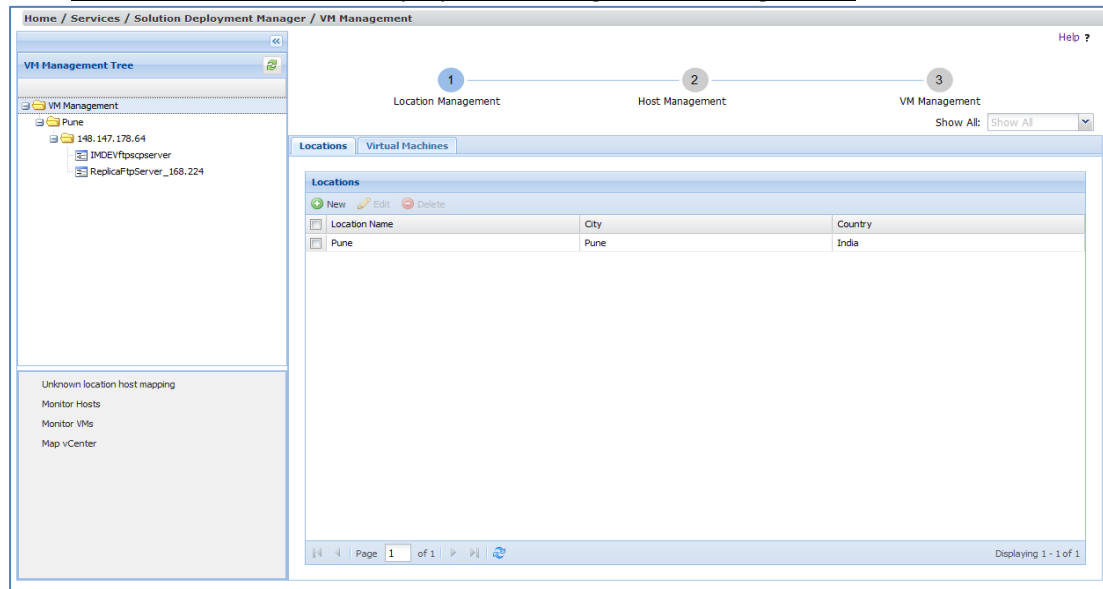
Appendix F

Adding Utility Services using VM Management

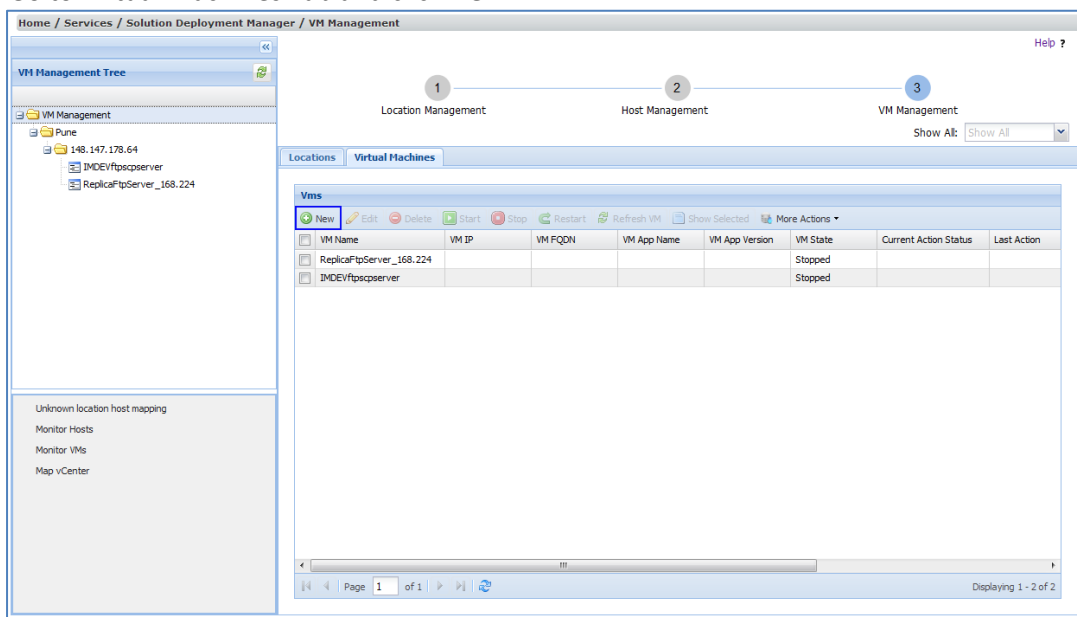
The Utility Services can be added from VM Management on a customer VMware (ESXi) or Avaya Virtualization Platform (AVP).

Follow [Appendix D on how to add a host in VM Management](#) before following below steps:

Navigate to [Home/Services/Solution Deployment Manager/VM Management](#).



1. Go to Virtual Machines Tab and click **New**.



2. Clicking of New button will redirect to the new VM page

Home / Services / Solution Deployment Manager / VM Management

1 Location Management 2 Host Management 3 VM Management

Show All: Show All

Locations Virtual Machines

VM Deployment

Select Location and Host

Select Location: Select Host: Host FQDN:

To deploy the virtual machine with Out of Band Management (OOBM), ensure that OOBM is enabled on AVP or Host.

Select Resource Pool and Data Store

Resource Pool: AVP host: Model: Datacenter / Cluster: Data Store:

Capacity Details

Name	Full Capacity	Free Capacity	Reserved Capacity	Sta...
datastore1 (23)	1112 GB	942 GB		
CPU	17880 MHz	15480 MHz		
CPU Cores	16	16		
Memory	9622 Mb	8538 MB		
PerCPUCapacity	2400 MHz			

Deploy OVA

3. Fill in the required information under following section:

Select Location and Host section:

- Select Location: The location created where the host is added.
- Select Host: All the host will be populated associated with the location selected.
- VM Name: The name of the VM to be deployed.

Home / Services / Solution Deployment Manager / VM Management

1 Location Management 2 Host Management 3 VM Management

Show All: Show All

Locations Virtual Machines

VM Deployment

Select Location and Host

Select Location: Pune Select Host: 148.147.178.64 Host FQDN: 148.147.178.64

To deploy the virtual machine with Out of Band Management (OOBM), ensure that OOBM is enabled on AVP or Host.

VM Name: UtilityServices-1 ☐ ME Deployment

Select Resource Pool and Data Store

Resource Pool: Resources AVP host: No Model: ProLiant DL360 G7 Datacenter / Cluster: ha-datacenter Data Store:

Capacity Details

Name	Full Capacity	Free Capacity	Reserved Capacity	Sta...
datastore1 (23)	1112 GB	942 GB		
CPU	17880 MHz	15480 MHz		
CPU Cores	16	16		
Memory	9622 Mb	8538 MB		
PerCPUCapacity	2400 MHz			

Deploy OVA

4. Selecting the Host will populate the data in Select Resource Pool and Data Store & Capacity Details. The Data Store will be populated available on the Host. Select one of the Data Store from the list.

Home / Services / Solution Deployment Manager / VM Management

1 Location Management 2 Host Management 3 VM Management

Locations Virtual Machines

VM Deployment

Select Resource Pool and Data Store

Resource Pool: Resources

AVP host: No

Model: ProLiant DL360 G7

Datacenter / Cluster: ha-datacenter

Data Store: datastore1 (23)

Capacity Details

Name	Full Capacity	Free Capacity	Reserved Capacity	Status
datastore1 (23)	1112 GB	942 GB		
CPU	17880 MHz	15480 MHz		
CPU Cores	16	16		
Memory	9622 Mb	8538 MB		
PerCPU Capacity	2400 MHz			

Deploy OVA

Select Software Library:

Select OVA:

Select Flexi Footprint:

* Configuration Parameters * Network Parameters

5. Select required values in Deploy OVA section

- Select Software Library: Select one of the [software library](#) configured in System Manager where the utility services OVA is [downloaded](#).
- Select OVA: All the OVAs will be populated available in the software library selected.
- Select Flexi Footprint: Select the footprint available as part of the US OVA.

Selection of the footprint will update the Capacity Details table and will do pre-deployment checks whether the OVA will fit on the host selected. The status will be green or red for different capacity.

Home / Services / Solution Deployment Manager / VM Management

1 Location Management 2 Host Management 3 VM Management

Locations Virtual Machines

VM Deployment

Select Resource Pool and Data Store

Resource Pool: Resources

AVP host: No

Model: ProLiant DL360 G7

Datacenter / Cluster: ha-datacenter

Data Store: datastore1 (23)

Capacity Details

Name	Full Capacity	Free Capacity	Reserved Capacity	Status
Data Store	1112 GB	942 GB	20 GB	✓
CPU	17880 MHz	15480 MHz	NA MHz	✓
CPU Cores	16	16	1	✓
Memory	9622 Mb	8538 Mb	NA Mb	✓
PerCPU Capacity	2400 MHz	NA	0 MHz	✓

Deploy OVA

Select Software Library: SMGR_DEFAULT_LOCAL

Select OVA: US-7.0.0.0.0.11-e55-01_OVF10.ova

Select Flexi Footprint: Minimal Resources

* Configuration Parameters * Network Parameters

Product: Utility Services

6. The selection of the OVA will populate Configuration and Network Parameters tabs. The data is parsed from the OVA and section is dynamically rendered. Fill the required information to deploy the Utility Services OVA.

The screenshot shows the 'VM Deployment' section of the 'Solution Deployment Manager' interface. The 'Configuration Parameters' tab is active. The 'Version' is 7.0.0.0.0.11. The 'Application' section contains the following fields: 'Communication Manager IP' (148.147.162.65), 'Network Time Protocol IP' (0.centos.pool.ntp.org), 'Hostname' (utilityserver1.smgdev.avaya.com), 'Timezone setting' (Etc/UTC), 'Utility Services Mode' (full_functionality), 'Primary System Manager IP address for application registration' (148.147.162.185), 'Enrollment Password' (masked with dots), and 'Confirm Password' (masked with dots). The 'Networking Properties' tab is also visible but not active.

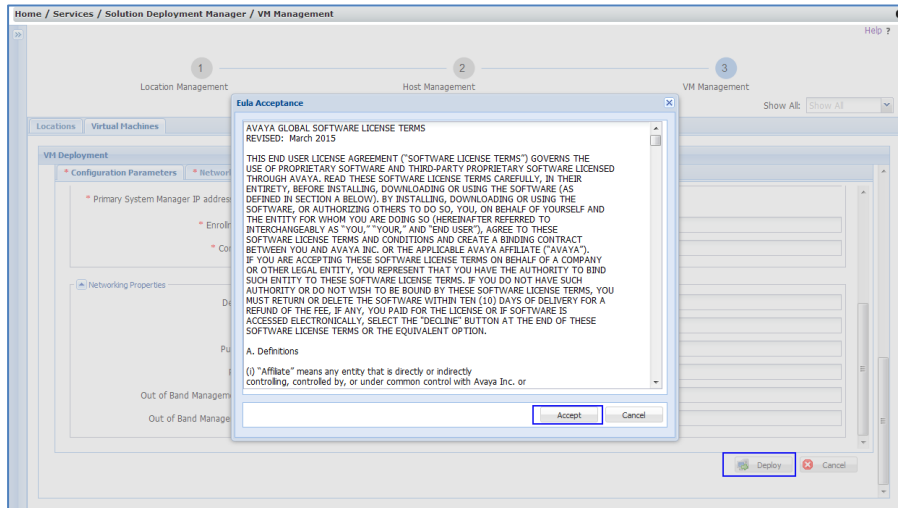
Note: It is required to fill Networking Properties for Utility Services if DHCP is not configured. Utility Services support DHCP for the deployment wherein the network parameters are configured from DHCP. If you are not using DHCP make sure to fill the data. If the OOBM is not used do not fill OOBM IP and Netmask.

The screenshot shows the 'Networking Properties' tab of the 'VM Deployment' section. The 'Default Gateway' is 148.147.162.1, 'DNS' is 148.147.162.5, 'Public IP Address' is 148.147.162.228, and 'Public Netmask' is 255.255.255.0. The 'Out of Band Management IP Address' and 'Out of Band Management Netmask' fields are highlighted with a red box. The 'Out of Band Management IP Address' field has a tooltip that says 'The IP address for this interface. Leave blank if DHCP is desired.' The 'Out of Band Management Netmask' field has a tooltip that says 'The netmask or prefix for this interface. Leave blank if DHCP is desired.'

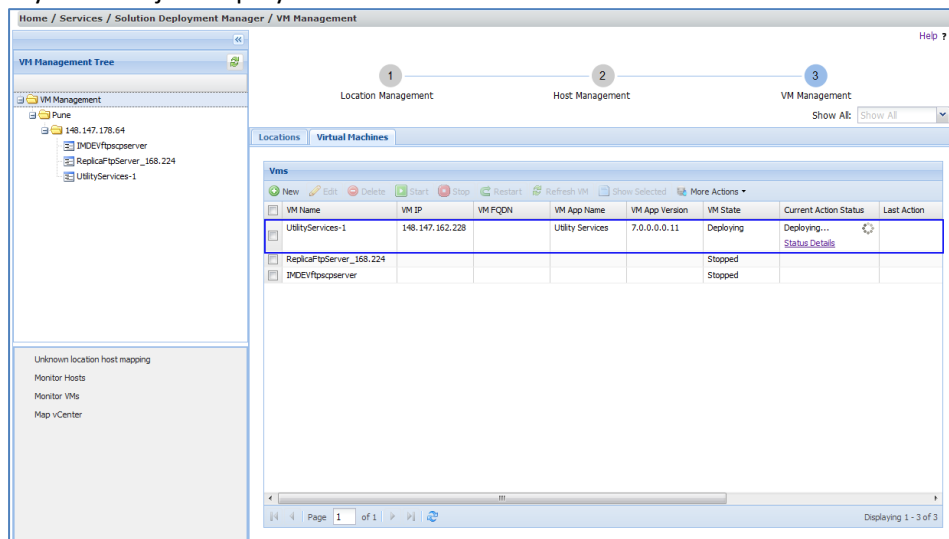
Select the network interfaces from Network Parameters Tab.

The screenshot shows the 'Network Parameters' tab of the 'VM Deployment' section. The 'Public' network is set to 'VM Network', the 'Services' network is set to 'VM Network', and the 'Out of Band Management' network is set to 'VM Network'.

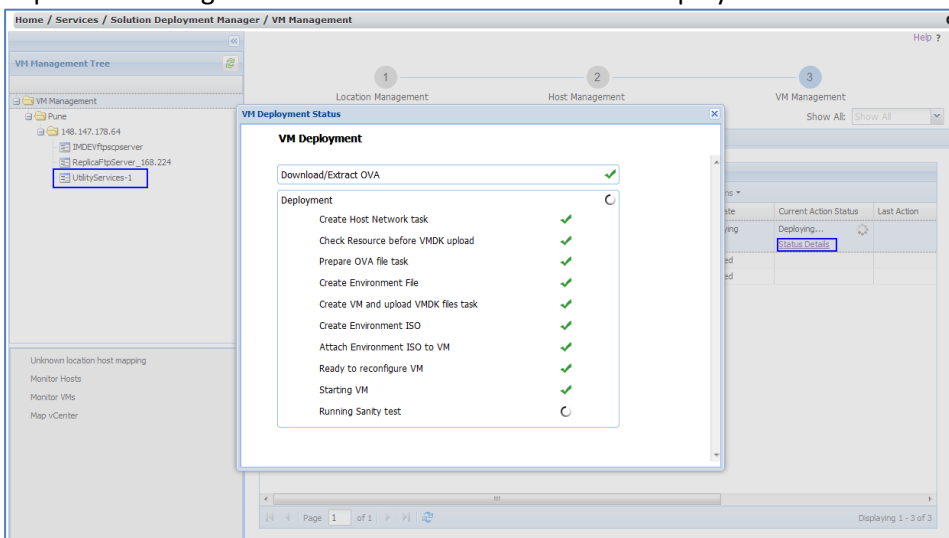
- Click on Deploy button to start the deployment of Utility Services and Accept the EULA to continue the deployment



- The page will be redirected to Location Management. Go to Virtual Machines Tab to see the status of the Utility Services just deployed.



- Click on Status Details link under Current Action Status to check the status of the deployment. The deployment will take few minutes to complete. The newly created Utility Services will be deployed and show up in VM Management Tree under the host used for deployment.

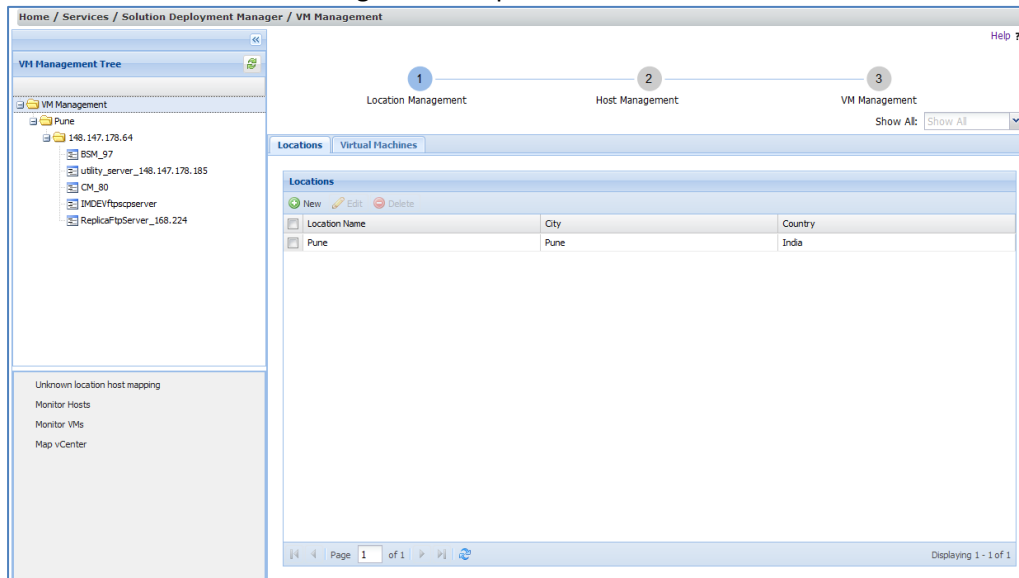


Appendix G

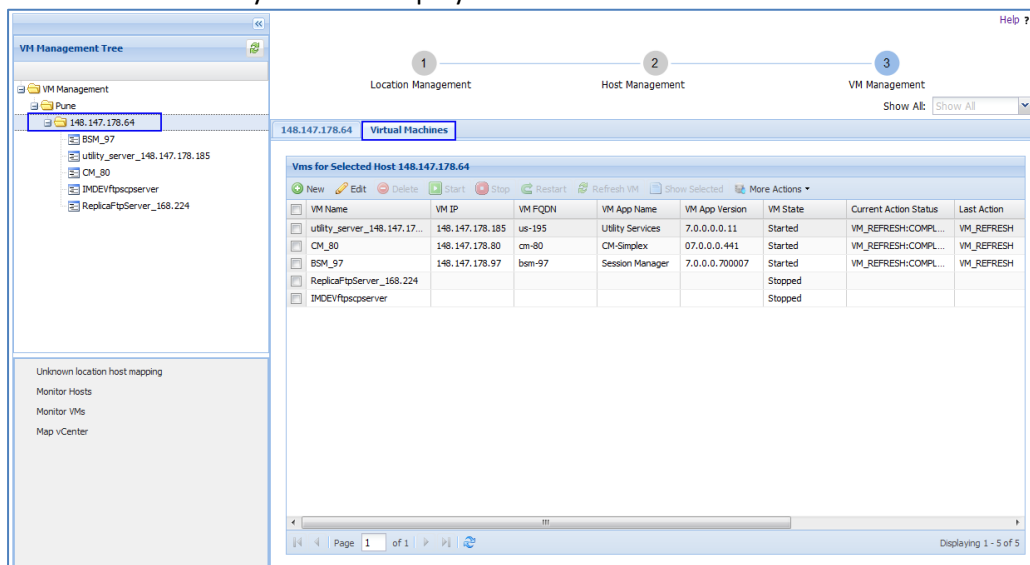
Establishing trust between SMGR and the Elements

The trust is required so that password less patching can be done from System Manager SDM. It is also required to fetch the element details. Refer to [Appendix-D on how to add a host to VM Management](#).

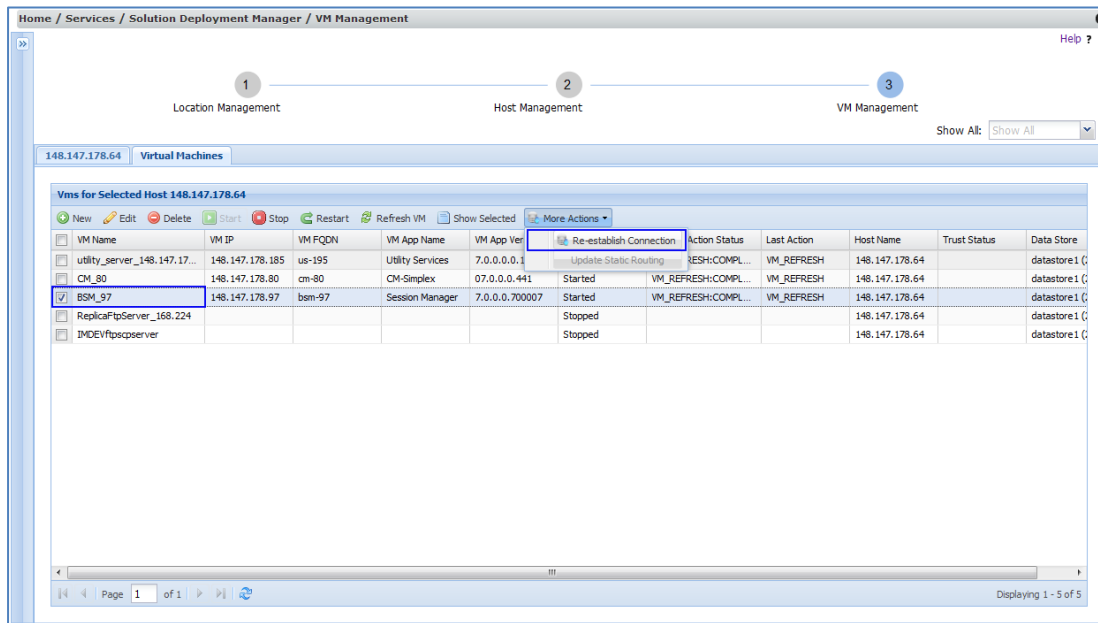
Navigate to Home/Services/Solution Deployment Manager/VM Management. In the example, we will establish trust for Branch Session Manager. The steps are same for other elements.



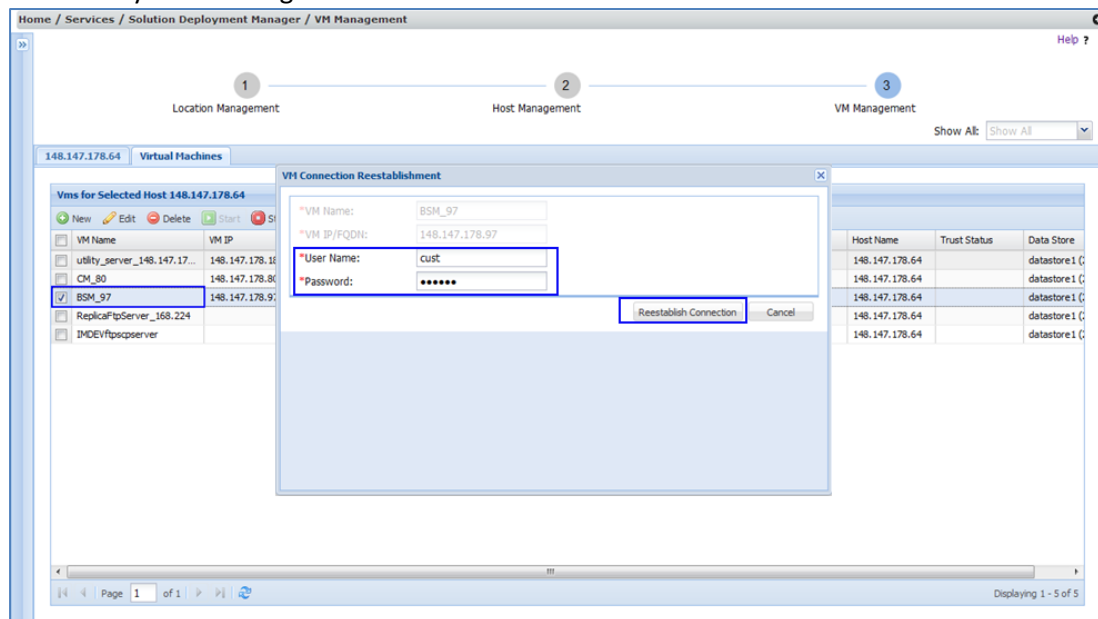
1. Select the host where your VM is deployed and click on the Virtual Machine tab.



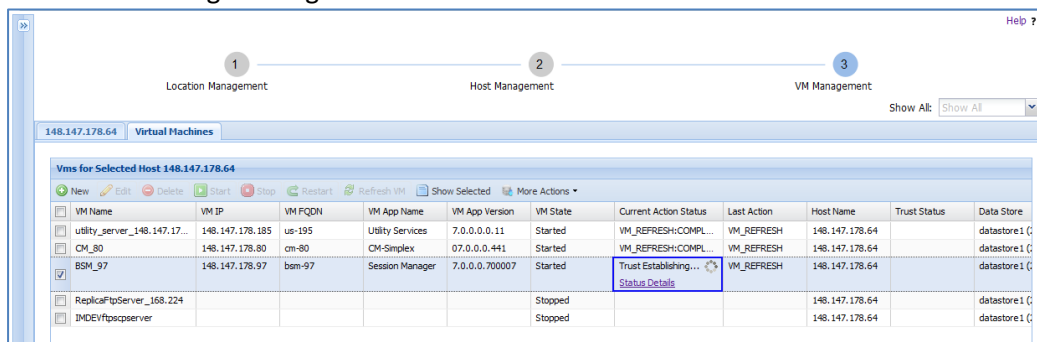
2. Select one of the VMs listed in Virtual Machines tab. Click **More Actions >Re-establish Connection**.



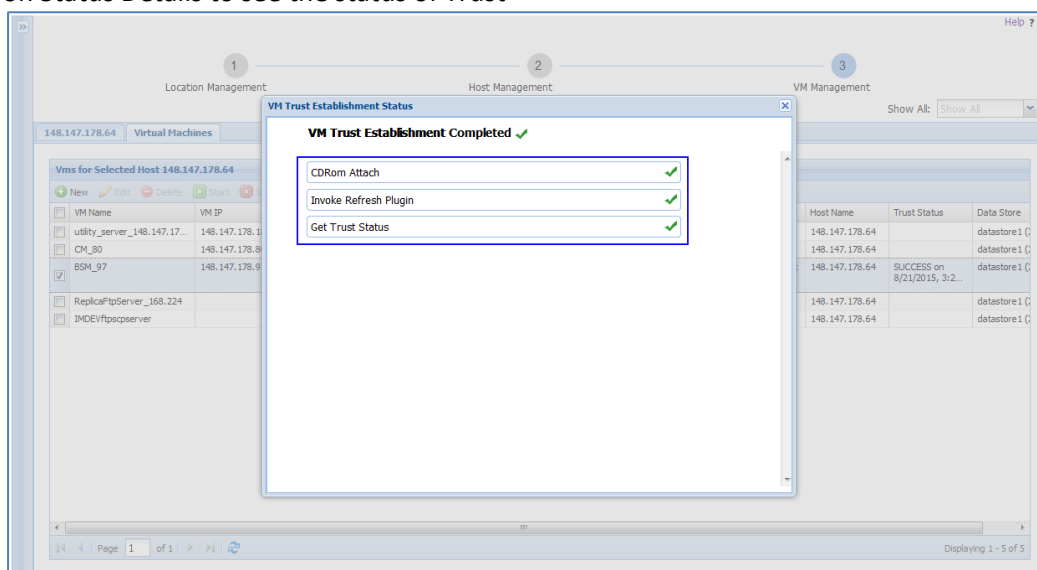
3. Clicking on the link will open VM Connection Reestablishment Window. Provide the User Name and Password for the BSM to establish trust. The password is to be passed only once and will not be stored in System Manager.



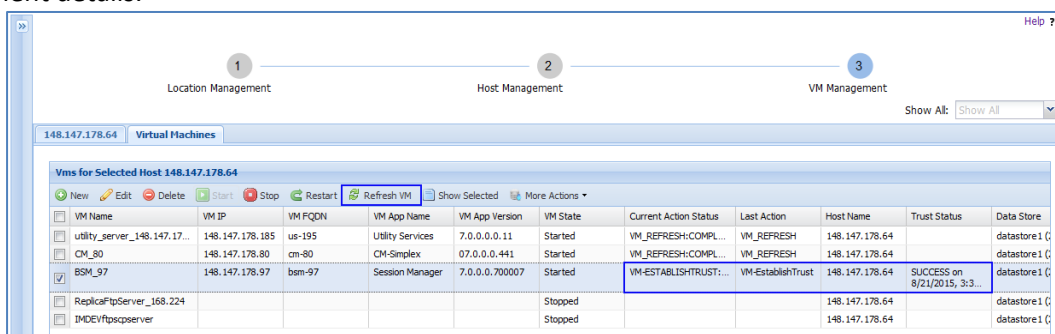
- Click on Reestablish Connection button, the window will close and the Current Action Status will show Trust Establishing running.



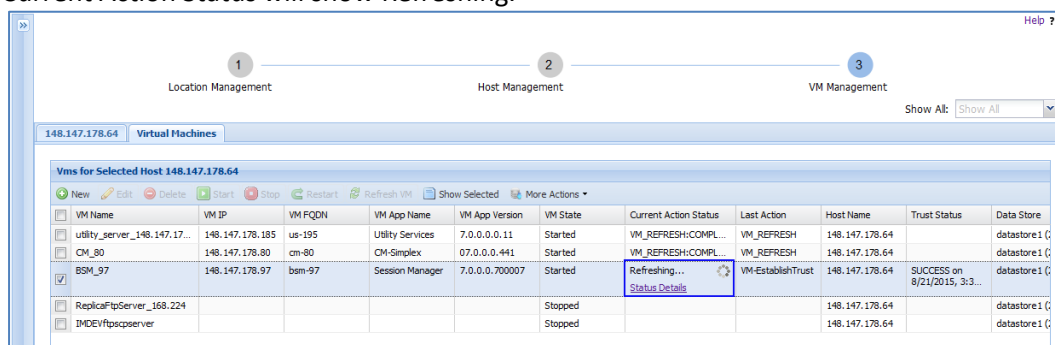
- Click on Status Details to see the status of Trust



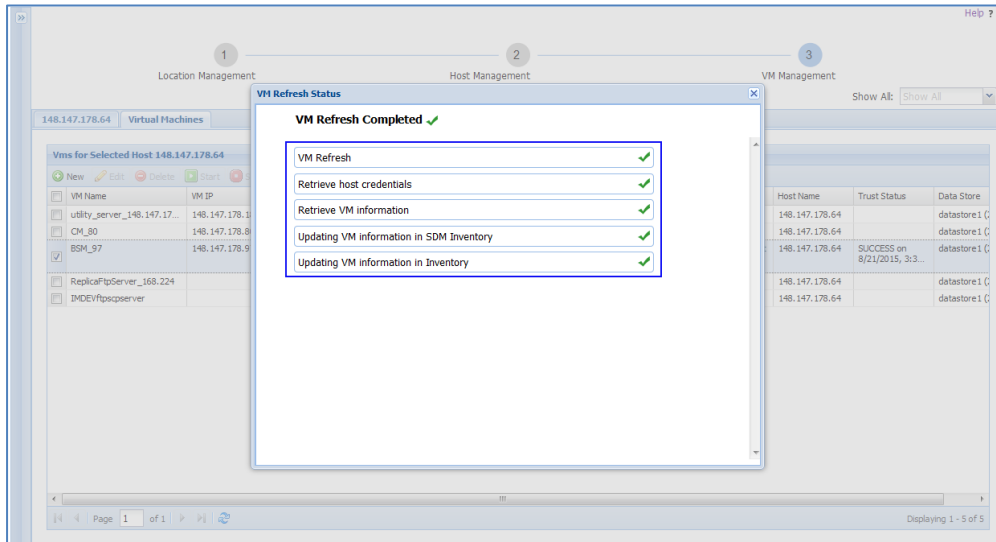
- Once the trust is established with the VM. Select the VM again and Refresh VM to fetch the latest element details.



- The Current Action Status will show Refreshing.



8. Click on Status Details to check the Refresh status.



9. Close the Refresh Status Window.

Appendix H

Element Selection on Upgrade Management Page

Upgrade Management comes with a default selection view in a flat structure wherein all the elements are provided in a table format with all the elements. There is also provision to select elements in child hierarchy view.

Navigate to [Home/Services/Solution Deployment Manager/Upgrade Management](#).

1. The element Type System Platform, Templates, Communication Manager and Media Gateway have clickable Name column.

Home / Services / Solution Deployment Manager / Upgrade Management

Help ?

Upgrade Management

Enable Auto Refresh(10 sec) | Show Selected Elements

Pre-upgrade Actions Upgrade Actions Download

6 Items Show All Filter: Enable

<input type="checkbox"/>	Name	Parent	Type	Sub-Type	IP Address	Release Status	Update Status	Last Action	Last Action Status	Pre Che Sta
<input type="checkbox"/>	BSM_97	CM_SurvRemoteEmbed	Session Manager	Branch Session Manager	148.147.178.97	!	N/A	Pre-upgrade Check	✓	✓
<input type="checkbox"/>	CM_65		Communication Manager	Avaya Aura(R) Communication Manager	148.147.162.65	?	?			!
<input type="checkbox"/>	CM_80	CM_SurvRemoteEmbed	Communication Manager	Avaya Aura(R) Communication Manager	148.147.178.80	!	N/A	Pre-upgrade Check	✓	✓
<input type="checkbox"/>	CM_SurvRemoteEmbed	SP128	Templates		148.147.178.128	⊗	⊗	Pre-upgrade Check	N/A	N/A
<input type="checkbox"/>	SP128		System Platform	System Platform	148.147.178.128	⊗	⊗	Pre-upgrade Check	N/A	N/A
<input type="checkbox"/>	utility_server_148.147.178.185	CM_SurvRemoteEmbed	Utility Server		148.147.178.185	!	N/A	Pre-upgrade Check	✓	✓

Select : All, None

Home / Services / Solution Deployment Manager / Upgrade Management

Help ?

Upgrade Management

Enable Auto Refresh(10 sec) | Show All Elements

Pre-upgrade Actions Upgrade Actions Download

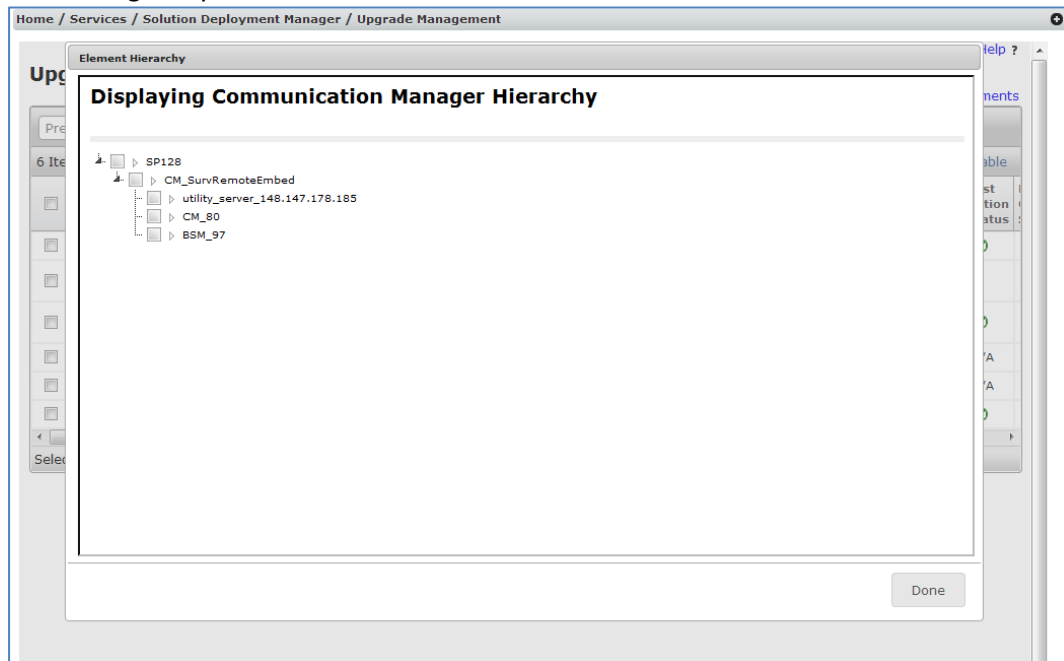
4 Items Show All Filter: Enable

<input checked="" type="checkbox"/>	Name	Parent	Type	Sub-Type	IP Address	Release Status	Update Status	Last Action	Last Action Status
<input checked="" type="checkbox"/>	CM-175.96	CM_Duplex	Communication Manager	Avaya Aura(R) Communication Manager	148.147.175.96	!	N/A	Analyze	✓
<input checked="" type="checkbox"/>	CM_Duplex	SystemPlatform	Templates		148.147.175.95	⊗	⊗	Analyze	✓
<input checked="" type="checkbox"/>	MG_450		Media Gateway	Avaya G450	148.147.182.11	⊗	⊗	Analyze	✓
<input checked="" type="checkbox"/>	SystemPlatform		System Platform	System Platform	148.147.175.95	⊗	⊗	Analyze	✓

Select : All, None

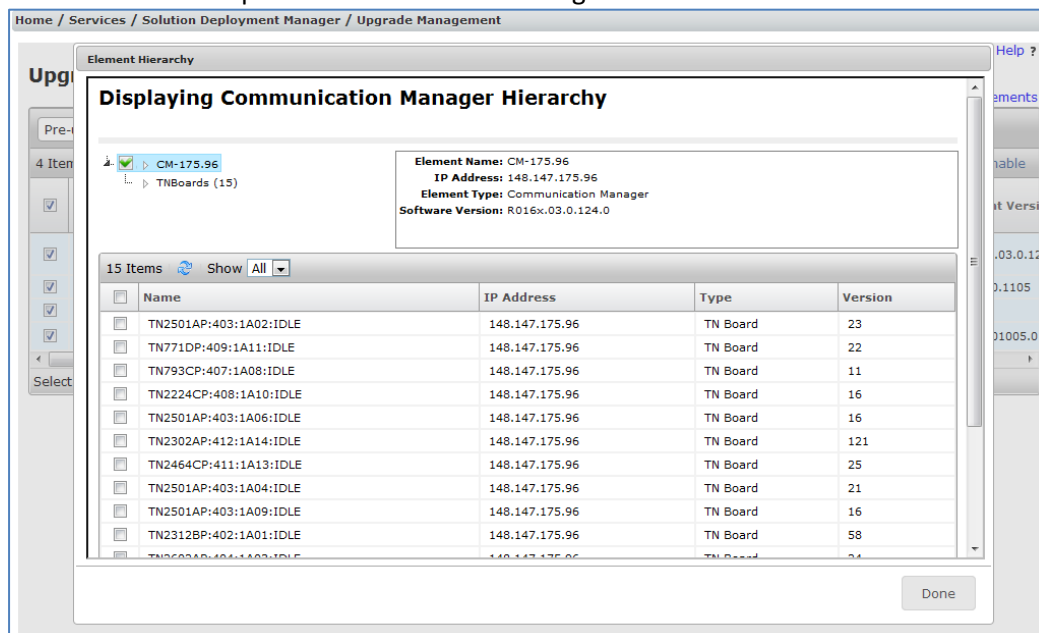
2. Clicking on the Name of the element shows the child hierarchy.

- Clicking on System Platform:



Select the elements in this window and click on Done button will carry the selection on the Upgrade Management page.

- Clicking on CM with TN Boards. The window will show TNBoards as link under CM and the number of TN Boards associated with it. Click on CM to see the CM details, click on TNBoards link will open the table below showing details of TN Boards:



Select the elements in this window and click on Done button will carry the selection on the Upgrade Management page.

- Clicking on Media Gateway with Media Modules. The window will show Media Modules as link under Media Gateway and number of Media Modules associated with it. Click on Media Gateway to see Media Gateway details, click on Media Modules link will open the table showing details of Media Modules:

Displaying Communication Manager Hierarchy

Element Name: MG_450
 IP Address: 148.147.182.11
 Element Type: Media Gateway
 Software Version: 34.5.1

Name	IP Address	Type	Version
Avaya MM717:167::IDLE	148.147.182.11	Media Module	15
Avaya MM716:161::IDLE	148.147.182.11	Media Module	99
Avaya MM714:163::IDLE	148.147.182.11	Media Module	99
Avaya G450:253::IDLE	148.147.182.11	Media Module	4.1.12
Avaya G450:252::IDLE	148.147.182.11	Media Module	30.25.0
Avaya MP80:251::IDLE	148.147.182.11	Media Module	N/A
Avaya MM722:250::IDLE	148.147.182.11	Media Module	8
Avaya G450:157::IDLE	148.147.182.11	Media Module	34.5.1
Avaya MM712:166::IDLE	148.147.182.11	Media Module	15

Select : All, None

Done

Select the elements in this window and click on Done button will carry the selection on the Upgrade Management page.

Appendix I

Same Box

- During migration flow, the Same Box is referred at many places including the drop-down values in Pre-upgrade checks and migration.
- If the same hardware on which the element is installed needs to be used for installing Appliance Virtualization Platform (AVP) or customer's VMware ESXi Host it is referred as "Same Box".
- During migration if the drop-down is populated with "Same Box" it notifies SDM that same hardware needs to be used which changes the flow of pre-upgrade checks and migration.