Upgrading Avaya Session Border Controller

Release 10.2.x
Issue 1
March 2024

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published in varying media which may include product information, subscription or service descriptions, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of Avaya. End user agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End user.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or Documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Please refer to your agreement with Avaya to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link “Warranty & Product Lifecycle” or such successor site as designated by Avaya. Please note that if the product(s) was purchased from an authorized Avaya channel partner outside of the United States and Canada, the warranty is provided by said Avaya Channel Partner and not by Avaya.

Licenses

License types

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Unless otherwise stated, each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE H.264 CODEC OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

You acknowledge and agree that it is Your responsibility to comply with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud

“Toll Fraud” is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, please contact your Avaya Sales Representative.

Security Vulnerabilities

Information about Avaya’s security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security.

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: https://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: https://support.avaya.com for Product or Cloud Service notices and articles, or to report a problem with your Avaya Product or Cloud Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Trademarks

Contents

Chapter 1: Introduction

Purpose

This document provides checklists and procedures to upgrade an older version of Avaya Session Border Controller to Release 10.2 or to migrate data from an older Avaya SBC system to a newly-installed Release 10.2 system. This document also includes procedures to roll back an upgrade or migration.

Chapter 2: Upgrade overview

Upgrade overview

This document provides the procedures for upgrading or migrating to Avaya SBC Release 10.2.

To upgrade to a new release of Avaya SBC, there are two distinct processes you can use:

- Standard upgrade process
- Migration process

The standard upgrade process has limitations for certain deployment types, and if your deployment type does not allow the standard upgrade process, you must use the migration process. The migration process is more universal and can be used for any deployment type, even if the standard upgrade process might work.

⚠ **Caution:**

Doing an upgrade or migration on your system is service affecting. Plan upgrades or migrations for a maintenance period or when there is no traffic or during a low traffic period.

You can upgrade Avaya SBC in two ways:

- You can do an in-place software upgrade reusing the existing hardware or VMware servers.
- You can migrate data from an old Avaya SBC system to a newly-installed Avaya SBC system.

A key advantages of using an upgrade procedure is that:

- You can start the upgrade from the web interface.
- You do not need to install the system with the release to be upgraded which sometimes requires manual intervention.

This document also includes procedures to roll back an upgrade or migration.

Supported upgrade paths

For the latest information about the standard upgrade process and migration process and the required patches to do an upgrade or a migration, see *Avaya Session Border Controller Release Notes* on the Avaya Support site at http://support.avaya.com.

The following table provides information related to the direct upgrade support of all previous releases:

Release	Standard upgrade process to 10.2	Migration process to 10.2
6.2	Not Supported	Not Supported
6.3	Not Supported	Not Supported
7.0	Not Supported	Not Supported
7.1	Not Supported	Not Supported
7.2	Not Supported	Not Supported
8.0	Not Supported	Not Supported
8.0.1	Not Supported	Not Supported
8.1	Not Supported	Not Supported
8.1.1	Not Supported	Not Supported
8.1.2	Not Supported	Not Supported
8.1.3.0	Not Supported	Not Supported
8.1.3.2	Not Supported	Supported
10.1.0.0 (Legacy boot)	Not Supported	Supported
10.1.0.0 (UEFI boot)	Supported	Supported
10.1.2	Supported	Supported
10.1.2.1	Supported	Supported

You must use the migration procedures found in the chapter *Migrating a system to Avaya SBC Release 10.2* for any of the following deployment types or special conditions:

- JTIC deployments on any type of platform or cloud service.
- KVM or Nutanix deployments on a Virtualized Environment Platform
- Any deployments that return the partition size or unsupported hardware error messages when running the pre-upgrade check tool.
- Any deployments on cloud services such as Amazon Web Services, Microsoft® Azure, or Google Cloud Platform.

You cannot use the standard upgrade process on these deployment types.

About Avaya SBC servers

The Avaya SBC servers are fully integrated, user-installable chassis. Avaya SBC supports the following hardware and VMware servers:

Hardware	10.2
CAF 0251	No
CAD 0230	No
Dell R320	No
Dell R330	No
Dell R630	No
Dell R640 - Profile 3	Yes
Dell R640 - Profile 5	Yes
Dell R340	Yes
Dell 3240	Yes
Dell VEP1425N	Yes

For technical specifications of these servers, see “Specifications and requirements”.

Supported device types

Device	Device Type		
	EMS	ASBC	EMS + ASBC
Dell R640 - P3(Hardware)	Supported	Supported	Supported
Dell R640 - P5(Hardware)	Supported	Supported	Supported
Dell R340(Hardware)	Supported	Supported	Supported
Dell 3240(Hardware)	Not Supported	Not Supported	Supported
Dell VEP1425N	Not supported	Not supported	Supported

Supported device configurations

Hardware servers that support upgrades to this release

For the latest information about the standard upgrade process and migration process and the required patches to do an upgrade or a migration, see *Avaya Session Border Controller Release Notes* on the Avaya Support site at http://support.avaya.com.

Note:

A reinstallation might be required if the system has failed after an upgrade and requires a rebuild and reinstallation of the Avaya SBC software. The servers that support upgrades to this release of Avaya SBC can also be reinstalled with this release of Avaya SBC software.

Server	NIC Ports	DVD drive	Upgrade supported for	Supported device configuration		
				EMS	SBC	EMS+SBC
Dell™ PowerEdge™ R640 Avaya Solutions Platform 110 Appliance server - Profile 3	6	Yes	10.2	Supported	Supported	Supported
Dell™ PowerEdge™ R640 Avaya Solutions Platform 110 Appliance server - Profile 5	6	Yes	10.2	Supported	Supported	Supported
Dell™ PowerEdge™ R340 Avaya Solutions Platform 110 Appliance server	6	No	10.2	Supported	Supported	Supported
Dell 3240	5	No	10.2	No	No	Supported
Dell VEP1425N	4	Yes	10.2	Not supported	Not supported	Supported

Virtual platforms that support upgrades to this release

- VMware ESXi 7.0 and 8.0, KVM, or Nutanix on a Virtualized Environment Platform – for more information about the supported hardware, see *Deploying Avaya Session Border Controller on a Virtualized Environment Platform*
- Avaya Aura® Virtualized Appliance Platform – for more information about the supported hardware, see *Deploying Avaya Session Border Controller on an Avaya Aura® Appliance Virtualization Platform*
- Amazon Web Services cloud service
- Microsoft® Azure cloud service

For the latest information about the standard upgrade process and migration process and the required patches to do an upgrade or a migration, see *Avaya Session Border Controller Release Notes* on the Avaya Support site at http://support.avaya.com.

Note:

A reinstallation might be required if the system has failed after an upgrade and requires a rebuild and reinstallation of the Avaya SBC software. The servers that support upgrades to this release of Avaya SBC can also be reinstalled with this release of Avaya SBC software.

Chapter 3: Pre-upgrade tasks

Pre-upgrade checklist

Caution:

Doing an upgrade or migration on your system is service affecting. Plan upgrades or migrations for a maintenance period or when there is no traffic or during a low traffic period.

Tasks	References	✔
Install the latest service packs and patches required for the current Avaya SBC system.	Latest software updates and patch information on page 13	
Ensure that the system does not show any alarms related to disk space.	Checking system alarms on page 14	
Disable all debug logs.	Disabling debug logs on page 14	
Ensure that the SBC servers in the deployment have unique host names.	Checking the status of the deployed servers on page 14	
Ensure that the EMS and SBC are in the commissioned or registered state.	Checking the status of the deployed servers on page 14	
Ensure that the SBC instances are not in sync state.	To verify whether SBC instances have a problem with synchronization, clone a SigMa profile, save the profile, and then check whether any SBC moves to the sync state. If any SBC instance is in the sync state, log a ticket with Avaya Support to get the issue addressed.	
If you revert the VMware snapshot before upgrading, ensure that you restore the VMware snapshots in the following order: 1. EMS 2. SBC		
For an SBC HA pair, ensure that the HA state is showing primary and secondary, respectively.		

Table continues…

Tasks	References	✔
Ensure that you place all manually installed RPMs, which came as a patch, in the following directory: `/archive/SBC-RPM-Repository/RPMs/`		
Download the upgrade-related files from the Avaya Support Site or from the Avaya PLDS website. Copy these files to the server on which you are doing the upgrade. If you upgrade using a USB device, ensure that the USB device has at least 4 GB of free space for the upgrade files.	Download upgrade files on page 15	
View all the downloaded upgrade files that are on your system. You might want to delete any upgrade files that are older than your last two upgrades.	Managing downloaded upgrade packages on page 15	
Copy upgrade package to Avaya SBC HA pair servers or single Avaya SBC servers.	Copying upgrade package to Avaya SBC HA pair servers or single Avaya SBC server on page 15	
If you have rolled back before upgrading, ensure that you have rebooted your device before starting the upgrade again.		
Upgrades from one major release to another major release require license upgrade. If you are adding new features with an upgrade, you must upgrade your license. You must download the new license and install on it on the WebLM server before you start the upgrade.	About licensing requirements on page 38	

Note:

You cannot administer an SBC that is on an earlier version than the EMS until you upgrade the SBC to the same version as EMS.

Latest software updates and patch information

Before you start the deployment or upgrade of an Avaya product or solution, download the latest software updates or patches for the product or solution. For more information, see the latest release notes, Product Support Notices (PSNs), and Product Correction Notices (PCNs) for the product or solution on the Avaya Support website at https://support.avaya.com/.

After deploying or upgrading a product or solution, use the instructions in the release notes, PSNs, or PCNs to install any required software updates or patches.

For third-party products used with an Avaya product or solution, see the latest release notes for the third-party products to determine if you must download and install any updates or patches.

Checking system alarms

About this task

Use the following procedure to check the system alarms for disk space availability.

For more information about system alarms, see *Maintaining and Troubleshooting Avaya Session Border Controller* document.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the toolbar, click **Alarms**.

   The EMS server displays the Alarms Viewer screen.
3. Select the Avaya SBC device for which you want to view the alarms.

   The alarms section displays all the currently active alarms for the selected Avaya SBC security device.

Disabling debug logs

About this task

Use the following procedure to disable the debug logs before starting the upgrade procedure to free memory while upgrading.

Procedure

1. Log in to the EMS server web interface with administrator credentials.
2. Navigate to **Monitoring & Logging** > **Debugging**.
3. Clear the check box for debug logs.
4. Click **Save** to save the changes.

   The EMS server disables all the debug logs.

Checking the status of the deployed servers

About this task

Use the following procedure to ensure that EMS and Avaya SBC are in the commissioned state.

Procedure

1. Log in to the EMS web interface with administrator credentials.

2. Navigate to **Device Management** > **Devices** to check the status of the deployed EMS and Avaya SBC servers.

Download upgrade files

Download the following files from the PLDS website at https://plds.avaya.com/.

- `sbce-10.2.0.0-86-23974-92eaecaf70d0f680f8f9601673555179.tar.gz`
- `sbce-10.2.0.0-86-23974-92eaecaf70d0f680f8f9601673555179.tar.gz.asc`
- `sbce-10.2.0.0-86-23974-signatures.tar.gz`
- `sbce-10.2.0.0-86-23974_uberutility-bb73c1d9c2f12e31b9165b94702f49de.tar.gz`

Managing downloaded upgrade packages

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the **Device** menu, click **EMS** or the SBC name to administer.
3. Navigate to **Software Management**

   The system displays the list of software packages that have been downloaded to the EMS or SBC server. For multiple SBC servers, use **Select Device** to select the SBC for which you want to delete old upgrade packages.
4. Select the old upgrade package you want to delete.
5. Click **Delete**.

   The system deletes the upgrade package and signature file from the server.

Copying upgrade package to Avaya SBC HA pair servers or single Avaya SBC server

About this task

For upgrades starting from Release 8.1.2 to 10.2 and future releases, the upgrade package must be copied from EMS to Avaya SBC using “Software Management” screen.

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. On the **Device** menu, click **EMS**.
3. Click **Software Management**.

   The system displays the list of software packages that have been downloaded to the EMS.
4. Select the package from the list and all the Avaya SBC servers in the **Device** list. Click **Copy Package**.

   For example, for 10.1.2 to 10.2 upgrade, select package **sbce-10.2.xxxx.tar.gz / sbce10.2.xxxx.tar.gz.asc** in the list and the Avaya SBC servers from the **Device** list.

   The GUI displays copy successful message after package copying is successful.

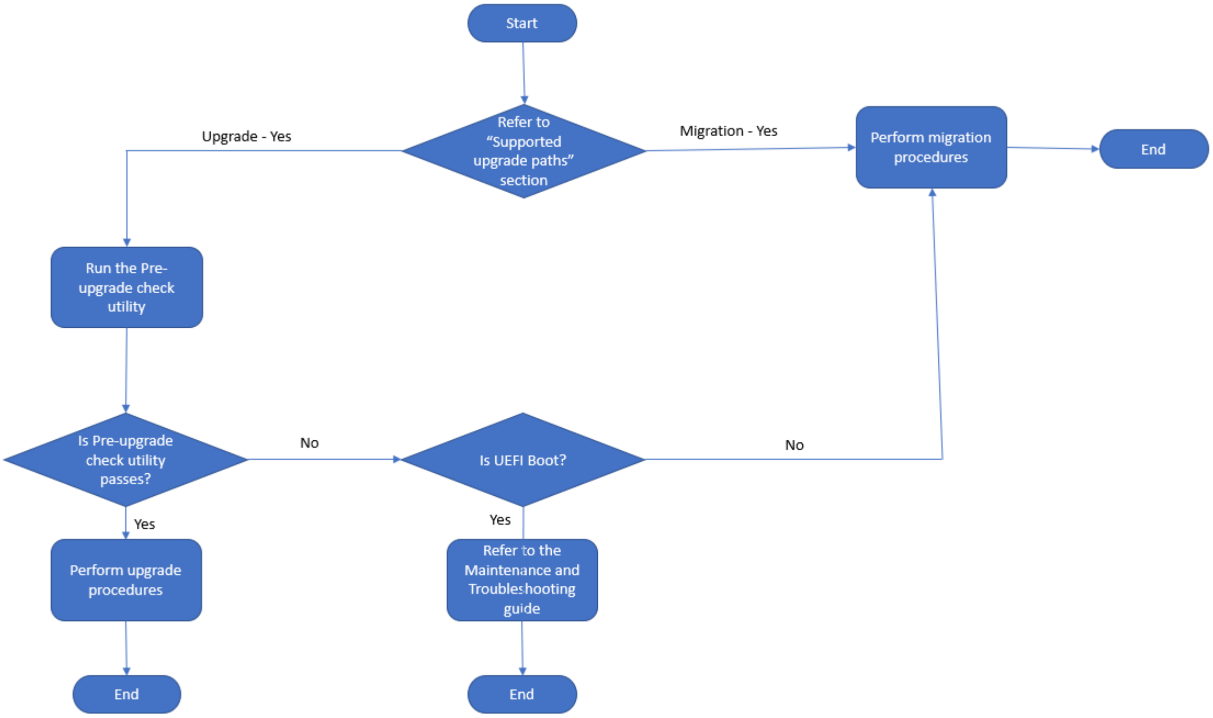
   The software management screen on Avaya SBC now displays the new uploaded upgrade package.
5. If the GUI displays failure message on package copy, contact Avaya support site at http://support.avaya.com.

Chapter 4: Upgrading or migrating a system to Avaya SBC Release 10.2

About upgrading and migrating Avaya SBC

General upgrade information

This section provides the upgrade and migration procedures for Avaya SBC.


Start
Refer to "Supported upgrade paths" section
Upgrade - Yes
Migration - Yes
Perform migration procedures
End
Run the Pre-upgrade check utility
Is Pre-upgrade check utility passes?
No
Is UEFI Boot?
No
Yes
Perform upgrade procedures
Yes
Refer to the Maintenance and Troubleshooting guide
End
End

⚠ **Caution:**

Doing an upgrade or migration on your system is service affecting. Plan upgrades or migrations for a maintenance period or when there is no traffic or during a low traffic period.

For the latest information about the standard upgrade process and migration process and the required patches to do an upgrade or a migration, see *Avaya Session Border Controller Release Notes* on the Avaya Support site at http://support.avaya.com.

Support for both web interface upgrades and command line migrations in the same deployment

The following scenarios describe how both upgrades and migrations can be used within the same deployment.

- If the Primary EMS is corrupted (for example, partition requirements are not met), but the SBC (HA or single) is operational, you can first do a command line migration on the Primary EMS, and then do a web interface upgrade on the SBC.
- If the Primary EMS is operational, but there are operational problems with the SBC (HA or single), you can first do a web interface upgrade on the Primary EMS, then do a command line migration on the SBC.
- If one SBC in an HA pair is operational but the other SBC in the HA pair is corrupted, you can first do a web interface upgrade on the operational SBC, then do a command line migration on the other SBC.

In summary, you can use either the web interface upgrades or command line migrations within the same deployment depending on the condition of each EMS and SBC component.

Important:

When upgrading or migrating a deployment to a new release, you may see “Data Replication is broken” alarms. For more information about this alarm and how to fix it, see *Maintaining and Troubleshooting Avaya Session Border Controller*.

Support for both web interface rollbacks and command line rollbacks in the same deployment

Similar to the using both upgrades and migrations in the same deployment, you can use web interface rollbacks and command line rollbacks in the same deployment. See the following example scenarios.

- If the web interface rollback on the SBCs worked properly, but there was some problem rolling back the EMS using the web interface, you can use the command line rollback procedures.
- If there is a problem rolling back one or more SBCs using the web interface, then you can use the command line rollback procedures as required. You can still roll back the other SBCs and the EMS using the web interface procedure.

Running the pre-upgrade check

About this task

Use the following procedure to run a pre-upgrade tool to check whether you can upgrade from a particular release to the most recent release, or if you will be required to migrate data from the old system onto a newly-install system.

Note:

You can do the pre-upgrade check at any time and it does not require a maintenance window. You do not need to run a pre-upgrade tool if you are upgrading from service pack.

Before you begin

Download the upgrade files as described in Download upgrade files on page 15.

Procedure

1. Log in to the Avaya SBC CLI as a super user.
2. Enter the following command to create a temporary directory:

   ```
   mkdir /usr/local/ipcs/urutmp
   ```

3. Enter the following command to move to the temporary directory:

   ```
   cd /usr/local/ipcs/urutmp
   ```

4. Move the uber utility package tar file to the SBC at the following directory:

   ```
   /usr/local/ipcs/urutmp
   ```

5. Run the following command to untar the downloaded utility package:

   ```
   tar
   -zxvf /usr/local/ipcs/urutmp/sbce-10.2.0.0-86-23974_uberutility-
   bb73c1d9c2f12e31b9165b94702f49de.tar.gz
   ```

6. Run the following command to run the pre-upgrade check:

   ```
   ./pre-upgrade-check
   ```

   - If the pre-upgrade check is successful, the system displays a message similar to the following example:

   ```
   System Verification Done. Pre-Upgrade Verification Test Pass. Upgrade can be
   proceed further.
   ```

   Note:

   If you get this message, you can use the upgrade procedures.

   - If the pre-upgrade check fails, the system displays a message similar to the following example:

   ```
   The required disk size is not available to upgrade from this release. Please
   refer to the upgrade document for the procedure to upgrade using alternative
   method
   ```

   Important:

   If you get this failure message, you must use the migration procedures.

7. Run the following commands to change to the location of the directory, list the contents of the directory to make sure you want to remove all the files, and remove the temporary directory:

   ```
   cd /usr/local/ipcs
   ```

   ```
   ls
   ```

   ```
   rm -rf -i urutmp
   ```

Next steps

Choose one of the following tasks:

- If the pre-upgrade check is successful, follow the upgrade procedures to upgrade from a specific release to the latest release.
- If the pre-upgrade check fails, use the migration procedure to migrate to the latest release on a newly-installed system.

Creating a backup before doing an upgrade

About this task

You must always do a backup of your current system before you start an upgrade or migration procedure.

Before you begin

Download the upgrade files as described in Download upgrade files on page 15.

Confirm that you have enough free space in the directory where the backup file is created. It is recommended to use `/archive` directory.

Procedure

1. Log in to the Avaya SBC CLI as a super user.
2. Enter the following command to create a directory for backup:

   ```
   mkdir /usr/local/ipcs/urutmp
   ```

3. Enter the following command to move to the backup directory:

   ```
   cd /usr/local/ipcs/urutmp
   ```

4. Move the uber utility package tar file to the backup directory:

   `/usr/local/ipcs/urutmp`

5. Run the following command to untar the downloaded utility package:

   ```
   tar -zxvf /home/ipcs/sbce-10.2.0.0-86-23974_uberutility-bb73c1d9c2f12e31b9165b94702f49de.tar.gz
   ```

6. Run the following command to take the backup:

   ```
   /usr/local/ipcs/peon/venv/bin/python ursbce.py --takemigratebackup --filename_with_path="$(hostname)-$(grep -i MGMT_IP /usr/local/ipcs/etc/sysinfo | cut -d = -f2)-backup-$(cat /etc/sbce-version).tar.gz"
   ```

   The backup is created in the current directory.

7. Run the following command to copy the backup `.tar` file to an external server with Linux OS:

```
scp <backup_file_path>/sbce-backup-<version>-<sbce hostname>.tar.gz
<server address>
```

Use a “winscp” tool to copy the backup file to an external server with Windows OS.

8. Run the following commands to change to the location of the directory, list the contents of the directory to make sure you want to remove all of the files, and remove the temporary directory:

```
cd /archive
```

```
ls
```

```
rm -rf -i createbkp
```

Upgrading a system to Avaya SBC Release 10.2

Upgrade checklist

This checklist contains procedures for upgrading the EMS or SBC using either the web interface or the CLI. You might need to do one or several of these upgrade tasks depending on your deployment.

Sr. No.	Tasks/ Actions	Links/ Notes	✔
1	Install the signature file and ASC file that you downloaded from the Avaya Support Site or from the Avaya PLDS website.	Adding the key bundles file and uploading upgrade files to EMS on page 22	
2	Check if the system can be upgraded using the pre-upgrade script. For unsupported servers, the upgrade will fail.	Running the pre-upgrade check on page 18	
3	Back up your data before starting the upgrade.	Creating a backup before doing an upgrade on page 20	
Upgrade Procedures			
4A	Upgrade the standalone EMS and SBC system using the web interface.	Upgrading a standalone EMS and SBC using the web interface on page 23	
	Upgrade the primary EMS using the web interface.	Upgrading EMS using the web interface for active-active EMS on page 24	
	Upgrade the secondary EMS using the web interface, if present. While upgrading secondary EMS, the primary EMS must be upgraded and functional otherwise you will not be able to upgrade SBC using secondary EMS.	Upgrading EMS using the web interface for active-active EMS on page 24	

Table continues…

Sr. No.	Tasks/ Actions	Links/ Notes	✔
	Upgrade the single SBC servers using the web interface.	Upgrading single SBC servers using the web interface on page 27	
	Upgrade the SBC HA pairs using the web interface	Upgrading SBC HA pair servers using the web interface on page 26	
	Upgrade the EMS and SBC using the CLI.	Upgrading EMS or SBC using the CLI on page 29	
4B	If the upgrade fails for any reason, roll back to the previous release.	Rolling back an upgrade using the web interface on page 31 Rolling back an upgrade using the CLI on page 32	
Upgrade and migration verification			
5	Check the upgrade status using the following log file: `/archive/log/icu/ursbce.log`		
6	Use the following command to check the upgrade status: **`grep UPGRADE_STATE /usr/local/ipcs/etc/sysinfo`**	The system displays one of the following messages: • `UPGRADE_STATE=UPGRADE_COMPLETED` for a successful upgrade. • `UPGRADE_STATE=UPGRADE_FAILED` for a failed upgrade.	
7	Update the server interworking, if required.		

Adding the key bundles file and uploading upgrade files to EMS

About this task

You must upload and install the key bundles and PGP keys for the Avaya SBC product.

Important:

To clarify the file naming convention for the key bundles and PGP keys, the file name does include the word “signature” in the file name. For example:

```
sbce-10.2.0-NN-NNNNN-signatures.tar.gz
```

Do not let the file naming confuse as to the purpose of this file. Also, note that the administration UI calls this the **Signature file**. This is really the key bundles file.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the menu bar, select **EMS**.
3. Navigate to the **Device Management** > **Key Bundles** tab.
4. Click **Choose File** on the **Upload Key Bundle** section.

5. Select the key bundles and PGP keys file (signature file) to upload.
6. Click **Upload** to upload the key bundle file.

   System displays **Verify Key Bundle** window.
7. Verify the key and click **Install**.

   System displays **Configuration update successful** notification on screen after successful installation.
8. Click **Updates** tab.
9. Select **Upgrade from uploaded file** in **System Upgrade** section.
10. Click **Choose file** for **Upgrade Package** and select `tar.gz` file.
11. Click **Choose file** for **Signature** and select `.asc` file.
12. Click **Upgrade**.

    The system displays a status bar **Preparing Upgrade**.

    After the preparing upgrade process is complete, the system displays **Upgrade EMS Device** notification box.
13. Click **Start Upgrade**.

    Note:

    Till step 14, the procedure remains same for Single Box or Multi-SBC. Further steps are applicable for Multi-SBC setup where SBC and EMS are separate.
14. Navigate to **EMS** > **Software Management**.

    The system displays a list of packages and devices.
15. Select the updated package and devices to copy the file.
16. Click **Copy Package**.

    After the copy package process is complete, the system displays **Copy task is completed successfully** notification.
17. Navigate to **EMS** > **Device Management** > **Updates** tab.
18. Click **Upgrade**.

    The system upgrades all the SBCs that are in older version.

Upgrading a standalone EMS and SBC using the web interface

Procedure

1. Log on as administrator to the EMS you want to upgrade. You must upgrade the primary EMS first.
2. Navigate to **Device Management** > **Updates**.

3. Do one of the following to select the upgrade file:
    - Select **Upgrade from local file** and select the correct upgrade file from the drop-down list.
    - Select **Upgrade from uploaded file** and browse to the correct upgrade file and signature file.
4. Click **Upgrade**.

    The system displays an upgrade confirmation screen. Read the information to understand what will happen during and after the upgrade.

    Important:

    If you get a message stating that the selected upgrade package has been tampered with or that it has not be signed with a trusted PGP key, the upgrade cannot continue. This could be caused by a number of factors:

    - The upgrade package has been compromised or is corrupt.
    - The upload of the upgrade package was incomplete, which sometimes happens using older versions of Internet Explorer.
    - The ASC file is not in place.

    Click **Finish** to close the error message and correct any possible errors before starting the upgrade again.
5. Click **Start Upgrade**.

    The EMS server displays the Upgrade EMS Device screen followed by a screen that shows the upgrade log messages. The upgrade process takes some time. Do not try to manually reboot the server when an upgrade is in progress. After the upgrade is complete, the EMS server displays the **Return to EMS** button.
6. Click **Return to EMS** to log back in to EMS.
7. To verify whether the upgrade was successful or not, do one of the following tasks:
    - Log on as administrator to the EMS you just upgraded, navigate to **Device Management** > **Devices**, verify that the EMS has been upgraded to the new version with a status of **Commissioned**, and that any connected SBCs are still on the old version with a status of **Commissioned (Upgrade Required)**.
    - From the command line interface, run the `ipcs-version` command to view the current version and status of the EMS and SBC.
8. Repeat this procedure for the secondary EMS, if it is part of the deployment.

Upgrading EMS using the web interface for active-active EMS

About this task

Use this procedure to upgrade the primary EMS, followed by upgrading the secondary EMS. Before upgrading the secondary EMS, the primary EMS must be upgraded first and be in functional operating condition. If the secondary EMS is not upgraded, you will not be able to later upgrade the SBC using the secondary EMS.

Procedure

1. Log on as administrator to the EMS you want to upgrade. You must upgrade the primary EMS first.
2. Navigate to **Device Management** > **Updates**.
3. Do one of the following to select the upgrade file:
   - Select **Upgrade from local file** and select the correct upgrade file from the drop-down list.
   - Select **Upgrade from uploaded file** and browse to the correct upgrade file and signature file.
4. Click **Upgrade**.

   The system displays an upgrade confirmation screen. Read the information to understand what will happen during and after the upgrade.

   Important:

   If you get a message stating that the selected upgrade package has been tampered with or that it has not be signed with a trusted PGP key, the upgrade cannot continue. This could be caused by a number of factors:

   - The upgrade package has been compromised or is corrupt.
   - The upload of the upgrade package was incomplete, which sometimes happens using older versions of Internet Explorer.
   - The ASC file is not in place.

   Click **Finish** to close the error message and correct any possible errors before starting the upgrade again.
5. Click **Start Upgrade**.

   The EMS server displays the Upgrade EMS Device screen followed by a screen that shows the upgrade log messages. The upgrade process takes some time. Do not try to manually reboot the server when an upgrade is in progress. After the upgrade is complete, the EMS server displays the **Return to EMS** button.
6. Click **Return to EMS** to log back in to EMS.
7. To verify whether the upgrade was successful or not, do one of the following tasks:
   - Log on as administrator to the EMS you just upgraded, navigate to **Device Management** > **Devices**, verify that the EMS has been upgraded to the new version with a status of **Commissioned**, and that any connected SBCs are still on the old version with a status of **Commissioned (Upgrade Required)**.
   - From the command line interface, run the `ipcs-version` command to view the current version and status of the EMS and SBC.

8. Repeat this procedure for the secondary EMS.

Upgrading SBC HA pair servers using the web interface

About this task

Use this procedure to upgrade SBC HA pairs. If you have more than one SBC server pair in your HA deployment, repeat this procedure for each HA pair of servers.

Before you begin

Ensure that the primary EMS server is upgraded before upgrading HA pair servers.

Ensure that the status of the HA SBC servers or the separate SBC server is in the Commissioned state.

Ensure the upgrade package is copied to the SBC HA pair. For more information, see “Copying upgrade package to Avaya SBC HA pair servers or single Avaya SBC server”.

Procedure

1. Log in to the primary EMS web interface with administrator credentials.
2. Navigate to **Device Management** > **Updates**.
3. Click **Upgrade**.

   The system displays the Upgrade Devices window. Select the devices you want to upgrade. The system determines whether you must upgrade one device at a time. That is, more than one device might need an upgrade, but only those devices that are active in the window can be selected. For example, if you have an HA pair of SBC devices, you must upgrade the primary SBC before you upgrade the secondary SBC.

   ❗ **Important:**

   If you get a message stating that the selected upgrade package has been tampered with or that it has not be signed with a trusted PGP key, the upgrade cannot continue. This could be caused by a number of factors:

   - The upgrade package has been compromised or is corrupt.
   - The upload of the upgrade package was incomplete, which sometimes happens using older versions of Internet Explorer.
   - The ASC file is not in place.

   Click **Finish** to close the error message and correct any possible errors before starting the upgrade again.
4. Select the check box in the **Device Name** column that you want to upgrade.
5. Click **Next**.

   The system starts the upgrade. You can click **View Log** to view the log file to follow the progress of the upgrade or you can just wait for the status bar to complete. The log file cannot be viewed when the device is rebooting.

The upgrade process takes some time. Do not try to manually reboot the server when an upgrade is in progress. After the upgrade is complete, the system displays a message indicating that the upgrade is complete. You can click **View Log** again to view the upgrade messages.

6. Click **Finish**.

   The system returns to the Device Management with the **Updates** tab selected.

   Note:

   - Until all of the SBC devices managed by this EMS have been upgraded, the EMS displays the following message for SBC HA pairs on the **Updates** tab:

     ```
     One or more devices are in an upgrade required state. If you would like
     to upgrade these devices now, please click the Upgrade button below.
     You may also choose to rollback your EMS at this point.
     ```

     HA system pairs and all other SBC systems must be upgraded before this message is resolved.

   - If the EMS server becomes non-functional during the upgrade, after the upgrade is complete, you must enable the EASG feature manually to allow the EASG logins for the customers.

7. Do one of the following steps:

   - If you have more devices to upgrade, click **Upgrade** to repeat this procedure and upgrade the next SBC device.
   - If you have upgraded all SBC devices that require an upgrade, select the **Devices** tab to confirm that all devices are upgraded to the correct version and that the status shows **Commissioned**. You can also run the `ipcs-version` command from the command line interface to view the current version and status of the EMS and SBC.

Upgrading single SBC servers using the web interface

About this task

Use this procedure to upgrade a single SBC server that is not in an HA pair. When more than one SBC server is in the deployment, repeat this procedure for each SBC server.

Before you begin

Ensure that the primary EMS server is upgraded before upgrading HA pair servers.

Ensure that the status of the HA SBC servers or the separate SBC server is in the Commissioned (Upgrade required) or Registered (Upgrade required) state.

Ensure the upgrade package is copied to the SBC HA pair. For more information, see “Copying upgrade package to Avaya SBC HA pair servers or single Avaya SBC server”.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. Navigate to **Device Management** > **Updates**.

The EMS server displays the Upgrade Devices window.

Important:

If you get a message stating that the selected upgrade package has been tampered with or that it has not be signed with a trusted PGP key, the upgrade cannot continue. This could be caused by a number of factors:

- The upgrade package has been compromised or is corrupt.
- The upload of the upgrade package was incomplete, which sometimes happens using older versions of Internet Explorer.
- The ASC file is not in place.

Click **Finish** to close the error message and correct any possible errors before starting the upgrade again.

3. Select the check box next to the devices that you want to upgrade.

   The devices can be upgraded one at a time or as a group. If you select more than one device, the devices are put in a queue and upgraded one at a time. The system shows any systems that have not been upgraded as in the “Commissioned (Upgrade required)” or “Registered (Upgrade required)” state.

4. Click **Next**.

   The EMS server displays logs. The upgrade process takes some time. Do not reboot when an upgrade is in progress. After the upgrade is complete, the EMS server displays a message box indicating that the Device is upgraded.

5. Click **Finish**.

   Note:

   After the SBC has been upgraded, the following message is displayed for individual SBC servers and HA pairs on the Updates tab:

   ```
   One or more devices are in an upgrade required state. If you would like to
   upgrade these devices now, please click the Upgrade button below. You may
   also choose to rollback your EMS at this point.
   ```

   HA system pairs and all other SBC servers must be upgraded before this message is resolved.

   Note:

   If the EMS server becomes non-functional during the upgrade then after the upgrade is complete you must enable the EASG feature manually to allow the EASG logins for the customers.

6. To verify whether the upgrade was successful or not, do one of the following tasks:

   - Log on as administrator to the EMS you just upgraded, navigate to **Device Management** > **Devices**, verify that the EMS has been upgraded to the new version with a status of **Commissioned**, and that any connected SBCs are still on the old version with a status of **Commissioned (Upgrade Required)**.

- From the command line interface, run the **`ipcs-version`** command to view the current version and status of the EMS and SBC.

Upgrading EMS or SBC using the CLI

About this task

Use this procedure to upgrade either the EMS or SBC using the command line interface (CLI). Use the following order to upgrade multiple systems using the CLI:

1. Upgrade the primary EMS.
2. Upgrade the secondary EMS.
3. Upgrade the SBC systems in any order. For an HA pair, upgrade the secondary SBC first followed by the primary SBC to avoid failover conditions that might interfere with the upgrade.

Procedure

1. Log in to the CLI with administrator credentials.
2. Using root permissions, move the upgrade tar file from the ipcs user home directory to `/archive/urpackages` directory.
3. Ensure that the md5sum of the upgrade tar file matches the checksum given in the name of the file.

   You can use the **`md5sum`** command to verify whether the md5sum and the checksum match.
4. Run the following command to create a temporary directory:

   ```
   mkdir /usr/local/ipcs/temp
   ```

   Where, *temp* is the name of the temporary directory.

   If the temporary directory already exists in the system, use the following commands to change to the location of the directory, list the contents of the directory to make sure you want to remove all of the files, and delete the files in the temporary directory:

   ```
   cd /usr/local/ipcs/temp/
   ```

   ```
   ls
   ```

   ```
   rm -rf -i *
   ```
5. Run the following command to access the temporary directory:

   ```
   cd /usr/local/ipcs/temp
   ```
6. Run the following command to extract the upgrade tar file in the `temp` directory:

   ```
   tar -xvf /archive/urpackages/
   sbce-10.2.0.0-86-23974-92eaecaf70d0f680f8f9601673555179.tar.gz
   ```

7. Run the following command to make the script executable:

   ```
   chmod +x ursbce.py
   ```

8. Run the following command to start the upgrade:

   ```
   ./ursbce.py -U --daemonize
   ```

   Caution:

   Use the --daemonize option while using CLI-based upgrades over SSH. Without the --daemonize option, the upgrade fails if your connection drops because of inactivity.

9. Wait for the system to reboot.

10. Run the following command to verify the version of the system:

    ```
    cat /etc/sbce-version
    ```

    The file `/archive/log/icu/ursbce.log` contains upgrade related logs.

Next steps

To verify whether the upgrade was successful, log in to the EMS server and on the Device Management page, verify the current SBC and EMS versions.

Note:

If the EMS server becomes non-functional before starting the upgrade or during the upgrade, then after the successful upgrade of EMS, use the **`sbceconfigurator.py update-connection-info`** command to update the version information of SBC in the EMS server.

Rolling back an upgrade

Using rollback procedures, you can roll back from a upgraded release to an earlier release. Avaya SBC supports following methods of rolling back an upgrade:

- Rolling back using web interface
- Rolling back using CLI interface

Caution:

When doing a rollback, the rollback can fail if there were operational issues in the previous release to which you are rolling back. To help troubleshoot rollback problems, see *Maintaining and Troubleshooting Avaya Session Border Controller*.

Use the following order to when rolling back multiple systems:

1. Roll back single SBC systems in any order.
2. For an SBC HA pair, you must roll back the primary SBC first followed by the secondary SBC.
3. Roll back the secondary EMS first.
4. Roll back the primary EMS last.

Rolling back an upgrade using the web interface

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. Navigate to **Device Management** > **Updates**.

   The EMS server displays the current EMS version and the available upgrade and rollback options.
3. Click **Rollback**. The **Rollback** button shows the release to which you can roll back.

   The system displays the Rollback Devices window. Select the devices you want to roll back. The system determines the order in which you must roll back devices. For example, if you have an HA pair of SBC devices, you must roll back the secondary SBC before you roll back the primary SBC.
4. Select the check box in the **Device Name** column that you want to roll back.
5. Click **Next**.

   The system starts the rollback. You can click **View Log** to view the log file to follow the progress of the rollback or you can just wait for the status bar to complete. The rollback process for an SBC device should not take very long.
6. Click **Finish**.

   The system returns to the Device Management with the **Updates** tab selected.

   Note:

   - Until all of the SBC devices managed by this EMS have been rolled back, the EMS displays the following message for SBC HA pairs on the **Updates** tab:

     ```
     One or more devices are in an orphan state. If you would like to upgrade
     these devices now, please click the Upgrade button below.
     ```

     HA system pairs and all other SBC systems must be rolled back before this message is resolved.
   - If the EMS server becomes non-functional during the upgrade, after the upgrade is complete, you must enable the EASG feature manually to allow the EASG logins for the customers.
7. Do one of the following steps:
   - If you have more SBC devices to roll back, click **Rollback** to repeat this procedure and roll back the next SBC device.
   - If you have rolled back all SBC devices that require a rollback, select the **Devices** tab to confirm that all SBC devices are rolled back to the correct version and that the status shows **Commissioned**. You can also run the **`ipcs-version`** command from the command line interface to view the current version and status of the EMS and SBC.

- If only the EMS remains to roll back, the system displays the following message:

```
One or more devices are in an orphan state. If you would like to upgrade these
devices now, please click the Upgrade button below. You may also choose to
rollback your EMS at this point.
```

8. Click **Rollback EMS**.

   The system displays a warning message about rolling back the EMS.

9. Click **Start Rollback** to roll back the EMS.

   The EMS server displays the Rollback EMS Device screen followed by a screen that shows the rollback log messages. The rollback process takes some time. Do not try to manually reboot the server when a rollback is in progress. After the rollback is complete, the EMS server displays the **Return to EMS** button.

10. Click **Return to EMS** to log back in to EMS.
11. To verify whether the upgrade was successful or not, do one of the following tasks:
    - Log on as administrator to the EMS you just upgraded, navigate to **Device Management** > **Devices**, verify that the EMS has been rolled back with a status of **Commissioned**, and that any connected SBCs are rolled back on the same version with a status of **Commissioned**.
    - From the command line interface, run the **`ipcs-version`** command to view the current version and status of the EMS and SBC.
12. Repeat Steps 7–11 on the secondary EMS, if it is part of the deployment.
13. If after doing the rollback on all systems you see any of the systems display “DOWN” on the **Device Management** > **Devices** tab, log on as root to the OS and run the following command to restart each system so that the systems synchronize with each other:

    ```
    /etc/init.d/ipcs-init restart
    ```

Rolling back an upgrade using the CLI

Procedure

1. Log in to Avaya SBC CLI using administrative privileges.
2. Run the following command to start the roll back:

   ```
   /usr/local/ipcs/icu3/scripts/ursbce.py -R --daemonize
   ```

   ⚠ **Caution:**

   Use the --daemonize option while using CLI-based upgrades over SSH. Without the --daemonize option, the upgrade fails if your connection drops because of inactivity.

   After the rollback is complete, you can check the rollback logs stored at:

   ```
   /archive/log/icu/ursbce.log
   ```

   Avaya SBC will reboot after the rollback is successfully completed.

3. If after doing the rollback on all systems you see any of the systems display “DOWN” on the **Device Management** > **Devices** tab, run the following command to restart each system so that the systems synchronize with each other:

   `/etc/init.d/ipcs-init restart`

Mount failure during rollback

Condition

During rollback, the system displays messages similar to the following example:

```
         Mounting /tmp
         Mounting /home
. . .
. . .
[FAILED] Failed to mount /home.
See 'systemctl status home.mount' for details
. . .
. . .
Welcome to emergency mode! After logging in, type "journalctl -xb" to view
system logs, "systemctl reboot" ro reboot, "systemctl default" or ^D to
try again to boot into default mode.
Give root password for maintenance
(or type Control-D to continue):
```

Cause

During rollback, the `/etc/fstab` file was not properly updated and the `/home` partition was not able to mount.

Solution

1. At the error message prompt, enter the root password.
2. At the OS prompt, run the following command:

   `cat /archive/backup/upgrade/upgrade.conf | grep home`

3. Record the partition number of the `/home` partition.
4. Run the following command and check to see if the `/home` partition number matches what you found in the `upgrade.conf` file.

   `more /etc/fstab`

5. If the partition numbers do not match, edit the `/etc/fstab` file so that the partition number matches what you found in the `upgrade.conf` file.
6. Save and close the file.
7. Reboot the SBC server.
8. If this does not fix the problem, contact Avaya support.

Migrating a system to Avaya SBC Release 10.2

Migration checklist

This checklist contains procedures for migrating the EMS or SBC using the CLI.

Sr. No.	Tasks/ Actions	Links/ Notes	✔
1	Check if the system can be upgraded using the pre-upgrade script. For unsupported servers, the upgrade will fail.	Running the pre-upgrade check on page 18	
2	Ensure that the following resources are configured correctly on the Avaya SBC instance to be migrated: • CPU • Disk • Network interfaces	-	
3	Back up your data before starting the upgrade.	Creating a backup before doing an upgrade on page 20	
Migration procedures			
4A	Migrate backed up data onto a new system.	Migrating backed up data onto a new system on page 34	
4B	Roll back a restored system to a previous release.	Rolling back a restored system to a previous release on page 35	

Migrating backed up data onto a new system

About this task

Use the following order to migrate multiple systems:

1. Migrate data to the primary EMS first.
2. Migrate data to the SBC systems in any order. For an HA pair, migrate data to the secondary SBC first followed by the primary SBC to avoid failover conditions that might interfere with the migration.
3. Migrate data to the secondary EMS last.

Important:

The migration process works on the same appliance type.

Before you begin

Back up your data on each system. For more information, see Creating a backup before doing an upgrade on page 20.

Procedure

1. Install the Release 10.2 primary EMS or SBC with the same management IP addresses. For more information, see *Deploying Avaya Session Border Controller on a Hardware Platform*.

   Note:

   Do not add or attach the Avaya SBCs to the EMS GUI. Keep them installed separately on the Release 10.2 load and follow the migration steps.

2. Copy the `.tar` backup file from the external server to the following directory on the installed EMS or SBC:

   ```
   /archive/backup/upgrade
   ```

3. Run the following command to restore the backed up data:

   ```
   /usr/local/ipcs/icu3/scripts/ursbce.py --restoremigratebackup
   --filename_with_path=/archive/backup/upgrade/sbce-backup-<sbce
   version>-<sbce hostname>.tar.gz
   ```

4. Reboot the servers in the deployment after the restore is completed.

   Note:

   - If the primary EMS is migrated, the secondary EMS must be installed for changes to take effect on the secondary EMS.
   - If the primary EMS is restore migrated, the secondary EMS has to be freshly installed so that it can connect to the primary EMS. Restore migration is not needed for secondary EMS. After fresh installation, secondary EMS should be able to fetch all details from primary EMS.
   - If the secondary EMS is migrated, it will take around 15 minutes for the changes to take effect in the connected Avaya SBCs.

Rolling back a restored system to a previous release

About this task

Use the following order to when rolling back multiple systems:

1. Roll back the SBC systems in any order. For an HA pair, roll back the secondary SBC first followed by the primary SBC to avoid failover conditions that might interfere with the rollback.
2. Roll back the secondary EMS first.
3. Roll back the primary EMS last.

Caution:

When doing a rollback, the rollback can fail if there were operational issues in the previous release to which you are rolling back. To help troubleshoot rollback problems, see *Maintaining and Troubleshooting Avaya Session Border Controller*.

Before you begin

Download the upgrade files as described in Download upgrade files on page 15.

Back up your data on each system. For more information, see Creating a backup before doing an upgrade on page 20.

Procedure

1. Install primary EMS or SBC with the same management IP address as of the external server IP address where the backup file is saved. For more information, see *Deploying Avaya Session Border Controller on a Hardware Platform*.

   Important:

   The restore process works only on the same appliance type.

2. Copy the `.tar` backup file from the external server to the following directory on the installed EMS or SBC:

   `/archive/backup/upgrade`

3. Enter the following command to create a new restore directory:

   ```
   mkdir /usr/local/ipcs/temp
   ```

4. Enter the following command to move to the new restore directory:

   ```
   cd /usr/local/ipcs/temp
   ```

5. Move the uber utility package tar file to the new restore directory:

   `/archive/restorebkp/`

6. Run the following command to untar the downloaded utility package:

   ```
   tar -zxvf /home/ipcs/sbce-10.2.0.0-86-23974_uberutility-bb73c1d9c2f12e31b9165b94702f49de.tar.gz
   ```

7. Run the following command to restore data:

   ```
   ./rollbackmigratebackup /archive/backup/upgrade/sbc1-10.133.48.65-backup-10.2.0.0-86-23974.tar.gz
   ```

8. Run the following commands to change to the location of the directory, list the contents of the directory to make sure you want to remove all of the files, and remove the temporary directory:

   ```
   cd /archive
   ```

   ```
   ls
   ```

   ```
   rm -rf -i restorebkp
   ```

9. Reboot the system.

Next steps

After you successfully complete rollback on the primary EMS:

1. Delete the secondary EMS from the system.
2. Install secondary EMS and it will automatically execute the restore information from primary EMS.

Chapter 5: Licensing requirements

About licensing requirements

Avaya SBC uses the Avaya Product Licensing and Delivery System (PLDS) to create licenses and download Avaya SBC software. PLDS is not integrated with WebLM. Use PLDS to perform operations such as license activations, license upgrades, license moves and software downloads.

There are two licensed versions of Avaya SBC:

- Standard Services delivers non-encrypted SIP trunking.
- Advanced Services adds Mobile Workspace User, Media Replication, and other features to the Standard Services offer.

Avaya Aura® Mobility Suite and Collaboration Suite licenses include Avaya SBC.

Avaya SBC uses WebLM version 8.0 or later for licensing requirements. You can install the Avaya SBC license file on a primary Element Management System (EMS) using the Device Management page.

Important:

You must not enable the local WebLM option and install an Avaya SBC license file on the secondary EMS if used in an active-active deployment. If you install a license file on a secondary EMS in an active-active deployment, the licensing system will always show that the secondary EMS is in **Grace Period State**.

Ensure that the license file of the WebLM server displays the product code Session Border Controller E AE. Before you configure the license file, you can view the **License State**, **Grace Period State**, and **Grace Period Expiration Date** fields on the Dashboard page. You have a 30-day grace period from the day of installation or upgrade to install the license. Avaya SBC works normally during the grace period.

Important:

Licenses and a WebLM server are required for new installations or upgrades.

The license file contains the following information:

- Product name
- Supported software version
- Expiration date
- Host ID

The primary host ID of WebLM is used for creating the license file.

- Licensed features
- Licensed capacity

All hardware Avaya SBC devices can use a local WebLM server for licenses. However, for mixed deployment environments with EMS on VMware and Avaya SBC on hardware, use a WebLM server installed on VMware or System Manager WebLM.

Avaya SBC supports pooled licensing. As opposed to static license allocation, Avaya SBC dynamically reserves and unreserves pooled licenses when needed. For example, customers with multiple Avaya SBC devices can use a pool of licenses dynamically across the devices as required.

For integration with Microsoft® Teams, Avaya SBC requires the Premium license and Premium HA license permissions in addition to the Standard Services and Advanced Services licenses.

For the use of AMR-WB codec, Avaya SBC requires counting license for AMR-WB codec license and AMR-WB codec HA tracking license. This is applicable to both static and dynamic licenses.

Avaya SBC licensed features

To use a feature, you must ensure that the license file that you upload to WebLM has the appropriate licenses for the feature. You cannot configure or use a feature if the correct license for that feature is not present in the license file.

License feature	Description
VALUE_SBCE_STD_SESSION_1	Specifies the number of standard session licenses.
VALUE_SBCE_STD_HA_SESSION_1	Specifies the number of standard service HA session licenses.
VALUE_SBCE_ADV_SESSION_1	Specifies the number of session licenses for remote worker, media recording, and encryption. **Note:** You must buy and deploy a standard session license with every advanced license feature.
VALUE_SBCE_ADV_HA_SESSION_1	Specifies the number of advanced service HA session licenses.
VALUE_SBCE_PREM_SESSION	Specifies the number of premium session licenses. Premium licenses are required when using Microsoft Teams.

Table continues…

License feature	Description
VALUE_SBCE_PREM_HA_SESSION	Specifies the number of premium service HA session licenses. Premium licenses are required when using Microsoft Teams.
VALUE_SBCE_VIDEO_CONF_SVC_SESSION_1	Specifies the number of Avaya Meetings Server video conferencing session licenses.
VALUE_SBCE_VIDEO_CONF_HA_SVC_SESSION_1	Specifies the number of Avaya Meetings Server video conferencing HA session licenses.
VALUE_SBCE_CES_SVC_SESSION_1	Specifies the number of Client Enablement Services session licenses.
VALUE_SBCE_CES_HA_SVC_SESSION_1	Specifies the number of Client Enablement Services HA session licenses.
VALUE_SBCE_TRANS_SESSION_1	Specifies the number of transcoding session licenses.
VALUE_SBCE_TRANS_HA_SESSION_1	Specifies the number of transcoding HA session licenses.
VALUE_SBCE_ELEMENTS_MANAGED_1	Specifies the maximum number of Avaya SBC elements managed.
VALUE_SBCE_VIRTUALIZATION_1	Specifies that the download of virtual system installation files for VMware, KVM, Amazon Web Services, and Microsoft® Azure is permitted.
VALUE_SBCE_ENCRYPTION_1	Specifies that both media and signaling can be encrypted for Avaya SBC. This license is required when using any advanced licenses.
FEAT_SBCE_HIGHAVAILABILITY_CONFIG_1	Specifies the configuration of HA for the setup.
FEAT_SBCE_DYNAMIC_LICENSING_1	Specifies that dynamic or pooled licensing is permitted for Avaya SBC. The quantity of this license must match the quantity of standard licensing in the system being managed.
VALUE_SBCE_RUSSIAN_ENCRYPTION_1	Specifies Avaya SBC encryption only for signaling.
VALUE_SBCE_NG911	Specifies the number of AMR-WB codec licenses.
VALUE_SBCE_NG911_HA	Specifies the number of AMR-WB codec HA licenses.

License installation

You can install Avaya SBC license on either of the following servers:

- The WebLM server on System Manager
- The local WebLM server

Installing a license on WebLM server on System Manager

Before you begin

Get the license file from the Avaya Product Licensing and Delivery System (PLDS) website at https://plds.avaya.com/.

About this task

If you experience problems while installing the license file, see the License file installation errors section in *Administering standalone Avaya WebLM*.

Procedure

1. Log in to the System Manager web interface.
2. On the home page, in the **Services** section, click **Licenses**.
3. In the left navigation pane, click **Install license**.
4. Browse to the location where you saved the license file, and select the file to upload.
5. Click **Install**.
6. Verify that the license is installed. If the installation is successful, a new menu item named ASBC appears in the left navigation pane. Click **ASBC** to view the licensed features.

Installing a license file on the local WebLM server

Procedure

1. Log in to the WebLM application. If you are logging in for the first time, the system prompts you to change the default password.
2. In the left navigation pane, click **Install License**.

   The system displays the Install License page.
3. In the **Enter license path** field, select the downloaded license from your computer and click **Install**.

   After the license is successfully installed, the system displays a new menu **ASBC**.
4. Click **ASBC** to view the license information.

Configuring the WebLM server IP address using the EMS web interface

Before you begin

Install the Avaya SBC license file on a WebLM Release 8.0 or later server installed on System Manager, a local WebLM, or a standalone WebLM server. For more information about installing license files and WebLM, see *Administering standalone Avaya WebLM*.

Get the URL for the WebLM server.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. Navigate to **Device Management** > **Licensing**.
3. Do one of the following tasks:
   - For a WebLM server or standalone server installed on System Manager , in the **WebLM Server URL** field, type the URL of the WebLM server and click **Save**.

     The URL format of the WebLM server installed on System Manager is:

     `https://<SMGR_server_IP>:52233/WebLM/LicenseServer`

     The URL format of the standalone WebLM server is:

     `https://<WEBLM_server_IP>:52233/WebLM/LicenseServer`.
   - For an external WebLM server, type the link for the external WebLM server in **External WebLM Server URL** and click **Save**.
4. Click **Refresh Existing License** to refresh the existing licenses.
5. Click **Verify Existing License** to verify the existing WebLM license to confirm it is trusted.

   If the WebLM license is trusted, a pop window will display the certificate details. Otherwise, you can select the option to trust the WebLM certificate manually.
6. On the Dashboard screen, check the **License State** field.

   If the configuration is successful, the **License State** field shows `OK`.
7. Click the **Devices** tab.
8. Locate the Avaya SBC device you configured, and click **Edit**.

   The EMS server displays the Edit Device dialog box.
9. In the **Standard Sessions**, **Advanced Sessions**, **Scopia Video Sessions**, and **CES Sessions** fields, type the number of licensed sessions depending on the license you purchased.
10. Click **Finish**.

Configuring the WebLM server IP address using CLI

Before you begin

Install the Avaya SBC license file on a WebLM Release 8.0 or later server installed on System Manager, a local WebLM, or a standalone WebLM server. For more information about installing license files and WebLM, see *Administering standalone Avaya WebLM*.

Get the URL for the WebLM server.

Procedure

1. Log in to the CLI with administrator credentials.
2. Run the following command to configure an external WebLM server URL:

   ```
   sbceconfigurator.py config-weblm-url <WebLM URL>
   ```
3. Reboot Avaya SBC.

About centralized licensing

Using Centralized Licensing feature, the WebLM server can directly distribute the licenses to Avaya SBC connected to different Element Management System (EMS) in different networks.

The Centralized Licensing feature provides the following advantages:

- Eliminates the need to install and configure multiple WebLM servers, one for each Avaya SBC setup.
- Eliminates the need to log in to each WebLM server to manage licenses for each Avaya SBC setup.
- Reduces the VMware licensing cost for installing and configuring multiple WebLM OVAs on VMware.
- Provides a centralized view of license usage for Avaya SBC.

Note:

- The setup does not support the Centralized Licensing feature.
- The Centralized Licensing feature is optional. Use the Centralized Licensing feature when you have more than one Avaya SBC setup.

Chapter 6: Resources

Documentation

The following table lists the documents related to this product. Download the documents from the Avaya Support website at http://support.avaya.com

Title	Description	Audience
Design		
Avaya Session Border Controller Overview and Specification	High-level functional and technical description of characteristics and capabilities of the Avaya SBC.	Sales engineers, solution architects, and implementation engineers
Avaya Session Border Controller Release Notes	Describes any last minute changes to the product, including patches, installation instructions, and upgrade instructions.	Sales and deployment engineers, solution architects, and support personnel
Avaya Solutions Platform Overview and Specification	Describes the key features of Avaya Solutions Platform servers.	IT Management, sales and deployment engineers, solution architects, and support personnel
Implementation		
Deploying Avaya Session Border Controller on a Hardware Platform	Describes how to plan and deploy an Avaya SBC system on the supported set of hardware servers.	Sales and deployment engineers, solution architects, and support personnel
Deploying Avaya Session Border Controller on a Virtualized Environment Platform	Describes how to plan and deploy an Avaya SBC system on customer-provided VMware servers.	Sales and deployment engineers, solution architects, and support personnel
Deploying Avaya Session Border Controller on a Google Cloud Platform	Describes how to plan and deploy an Avaya SBC system on a Google Cloud Platform.	Sales and deployment engineers, solution architects, and support personnel

Table continues…

Title	Description	Audience
Deploying Avaya Session Border Controller on an Amazon Web Services Platform	Describes how to plan and deploy an Avaya SBC system on Amazon Web Services.	Sales and deployment engineers, solution architects, and support personnel
Deploying Avaya Session Border Controller on a Microsoft® Azure Platform	Describes how to plan and deploy an Avaya SBC system on a Microsoft® Azure platform.	Sales and deployment engineers, solution architects, and support personnel
Avaya Session Border Controller Port Matrix	Describes the incoming and outgoing port usage required by the product.	Sales and deployment engineers, solution architects, and support personnel
Upgrading Avaya Session Border Controller	Describes how to upgrade to the latest release of Avaya SBC.	Sales and deployment engineers, solution architects, and support personnel
Installing the Avaya Solutions Platform 110 Appliance	Describes how to install Avaya Solutions Platform 110 Appliance servers.	Sales and deployment engineers, solution architects, and support personnel
Administration		
Administering Avaya Session Border Controller	Describes configuration and administration procedures.	Implementation engineers and administrators
Maintenance and Troubleshooting		
Maintaining and Troubleshooting Avaya Session Border Controller	Describes troubleshooting and maintenance procedures for Avaya SBC.	Implementation engineers
Maintaining and Troubleshooting Avaya Solutions Platform 110 Appliance	Describes procedures to maintain and troubleshoot Avaya Solutions Platform 110 Appliance servers.	Implementation engineers
Using		
Working with Avaya Session Border Controller and Microsoft® Teams	Describes how to set up, maintain, and use Avaya SBC with Microsoft Teams.	Implementation engineers and administrators
Working with Avaya Session Border Controller Multi-Tenancy	Describes how to set up, maintain, and use the Avaya SBC Multi-tenancy feature.	Implementation engineers and administrators
Working with Avaya Session Border Controller Geographic-Redundant Deployments	Describes how to set up, maintain, and use the Avaya SBC Geographic-redundant deployment feature.	Implementation engineers and administrators

For Dell documentation, go to https://www.dell.com/support/.

For HP documentation, go to https://www.hpe.com/support.

Finding documents on the Avaya Support website

Procedure

1. Go to https://support.avaya.com.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support** > **Documents**.
4. In **Search Product**, start typing the product name and then select the appropriate product from the list displayed.
5. In **Select Release**, select the appropriate release number.

   This field is not available if there is only one release for the product.
6. **(Optional)** In **Enter Keyword**, type keywords for your search.
7. From the **Select Content Type** list, select one or more content types.

   For example, if you only want to see user guides, click **User Guides** in the **Select Content Type** list.
8. Click 🔍 to display the search results.

Accessing the port matrix document

Procedure

1. Go to https://support.avaya.com.
2. At the top of the screen, click **Sign In**.
3. Type your **EMAIL ADDRESS** and click **Next**.
4. Enter your **PASSWORD** and click **Sign On**.
5. Click **Product Documents**.
6. Click **Search Product** and type the product name.
7. Select the **Select Content Type** from the drop-down list
8. In **Choose Release**, select the required release number.
9. In the **Content Type** filter, select one or both the following categories:
   - **Application & Technical Notes**
   - **Design, Development & System Mgt**

   The list displays the product-specific Port Matrix document.
10. Press **Enter**.

Avaya Documentation Center navigation

For some programs, the latest customer documentation is now available on the Avaya Documentation Center website at https://documentation.avaya.com.

Important:

For documents that are not available on Avaya Documentation Center, click **More Sites** > **Support** on the top menu to open https://support.avaya.com.

Using the Avaya Documentation Center, you can:

- Search for keywords.

  To filter by product, click **Filters** and select a product.
- Search for documents.

  From **Products & Solutions**, select a solution category and product, and then select the appropriate document from the list.
- Sort documents on the search results page.
- Click **Languages** (🌐) to change the display language and view localized documents.
- Publish a PDF of the current section in a document, the section and its subsections, or the entire document.
- Add content to your collection using **My Docs** (☆).

  Navigate to the **Manage Content** > **My Docs** menu, and do any of the following:

  - Create, rename, and delete a collection.
  - Add topics from various documents to a collection.
  - Save a PDF of the selected content in a collection and download it to your computer.
  - Share content in a collection with others through email.
  - Receive collection that others have shared with you.
- Add yourself as a watcher using the **Watch** icon (👁).

  Navigate to the **Manage Content** > **Watchlist** menu, and do the following:

  - Enable **Include in email notification** to receive email alerts.
  - Unwatch selected content, all content in a document, or all content on the Watch list page.

  As a watcher, you are notified when content is updated or deleted from a document, or the document is removed from the website.
- Share a section on social media platforms, such as Facebook, LinkedIn, and Twitter.
- Send feedback on a section and rate the content.

Note:

Some functionality is only available when you log in to the website. The available functionality depends on your role.

Training

The following courses are available on the Avaya Learning website at www.avaya-learning.com. After logging into the website, enter the course code or the course title in the **Search** field and click **Go** to search for the course.

Note:

Avaya training courses or Avaya learning courses do not provide training on any third-party products.

Course code	Course title
20600W	Avaya Session Border Controller 8.1 Technical Delta
21098W	Session Border Controller 8.0 Technical Delta
20660W	Administering the Avaya Session Border Controller for Enterprise - SIP Trunk
60660W	Administering Avaya SBC Release 8 for Remote Worker
20660T	Administering Avaya SBC Release 8 Test
20800C	Implementing and Supporting Avaya SBC — Platform Independent
20800T	Avaya SBC Platform Independent and Support Test
20800V	Implementing and Supporting Avaya SBC — Platform Independent
26160W	Avaya SBC Fundamentals
7008T	Avaya SBC for Midmarket Solutions Implementation and Support Test
7008W	Avaya SBC for Midmarket Solutions Implementation and Support
2035W	Avaya Unified Communications Roadmap for Avaya Equinox Clients
43000W	Selling Avaya Unified Communications Solutions
71300	Integrating Avaya Communication Applications
72300	Supporting Avaya Communication Applications

Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

- To find videos on the Avaya Support website, go to https://support.avaya.com/ and do one of the following:
  - In **Search**, type `Avaya Mentor Videos`, click **Clear All** and select **Video** in the **Select Content Type**.
  - In **Search**, type the product name. On the Search Results page, click **Clear All** and select **Video** in the **Select Content Type**.

    The **Video** content type is displayed only when videos are available for that product.

  In the right pane, the page displays a list of available videos.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and do one of the following:
  - Enter a keyword or keywords in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click a topic name to see the list of videos available. For example, Contact Centers.

  Note:

  Videos are not available for all products.

Support

Go to the Avaya Support website at https://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Index