Administering Avaya Breeze™

Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

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, and 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. Note that 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

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya's website at: https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

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

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, 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 G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. 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 for complying 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, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: https://support.avaya.com or such successor site as designated by Avaya.

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).

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

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 Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted 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.

Contents

Chapter 1: Overview

This guide describes the procedures for administering Avaya Breeze™ and for installing and administering snap-ins running on Avaya Breeze™.

The Avaya Breeze™ provides a virtualized and secure application platform where Java programmers can develop and dynamically deploy advanced engagement capabilities that extend the power of Avaya Aura®. Avaya Breeze™ is also the platform where you can run Avaya snap-ins like Context Store, Engagement Designer, and Work Assignment.

Snap-in or service is the term used to describe a dynamically deployable component that delivers all or part of this functionality. Some functionality is provided by a group of services. Customers, business partners, and Independent Software Vendors (ISVs) can use the platform as the deployment vehicle for their applications (services).

🛈 **Important:**

This guide assumes that you have installed and configured Avaya Breeze™. For administration tasks required to set up Avaya Breeze™, see *Deploying Avaya Breeze™*.

Document changes since last issue

The following changes have been made to this document since the last issue:

- Updated the "Snap-in deployment checklist" topic to include information about Callable snap-in.
- Added the "Creating a routing policy" topic.
- Added the "Creating a dial pattern" topic.
- Added the "Assigning a service profile to an implicit user pattern" topic.
- Updated the "Administering whitelist for HTTP Security" topic to include information about Trusted Host by Cluster.
- Updated the "Administering client certificate challenge for HTTPS" topic to include information about Trusted Host by Cluster.
- Updated the "Administering HTTP CORS security" topic to include information about Trusted Host by Cluster.
- Updated the "Cluster Editor field descriptions" topic to include description of the **Enable Cluster Database** field.

- Updated the "Cluster administration field descriptions" topic to update description of the **Cluster Database** and **Cluster Database Connection** fields.

Documentation

See the following related documents at http://support.avaya.com.

Title	Description	Audience
Understanding		
Avaya Breeze™ Overview and Specification	Describes the Avaya Breeze™ from a functional view. Includes a high-level description of the platform as well as topology diagrams, customer requirements, and design considerations.	Sales engineers Programmers System administrators Services and support personnel
Avaya Aura® System Manager Overview and Specification	Describes tested product characteristics and capabilities, including product overview and feature descriptions, interoperability, performance specifications, security, and licensing requirements.	Sales engineers Programmers System administrators Services and support personnel
Implementing		
Deploying Avaya Breeze™	Describes the procedures to deploy and administer Avaya Breeze™. Also contains the procedures to deploy, administer, and license an Avaya Media Server for use with Avaya Breeze™.	Services and support personnel
Upgrading Avaya Breeze™	Describes the procedures to upgrade Avaya Breeze™.	Services and support personnel
Implementing and Administering Avaya Aura® Media Server	Provides the procedures to install, configure, use, and troubleshoot Avaya Aura® Media Server.	System administrators Services and support personnel
Deploying and Updating Avaya Aura® Media Server Appliance	Provides installation, configuration and administration information for Avaya Aura® Media Server when it is installed on customer-provided servers.	System administrators Services and support personnel

Table continues…

Title	Description	Audience
Deploying Avaya Aura® System Manager	Describes how to deploy Avaya Aura® System Manager in a virtualized environment using VMware.	System administrators Services and support personnel
Avaya Aura® System Manager Solution Deployment Manager Job-Aid	Quick reference to using Solution Deployment Manager.	System administrators Services and support personnel
Migrating and Installing Avaya Appliance Virtualization Platform	Checklists and procedures for installing, migrating, configuring, administering, and troubleshooting Avaya Appliance Virtualization Platform.	System administrators Services and support personnel
Customizing		
Getting Started with the Avaya Breeze™ SDK	Describes the procedures to install and configure the Eclipse IDE, Apache Maven, and the Avaya Breeze™ SDK.	Programmers
Avaya Breeze™ Snap-in Development Guide	Describes the key concepts needed to develop the different types of Avaya Breeze™ snap-ins.	Programmers
Avaya Breeze™ FAQ and Troubleshooting for Snap-in Developers	Provides snap-in troubleshooting procedures. Answers questions such as "Why did my SDK installation fail?"	Programmers
Avaya Breeze™ API Javadocs	Overview and description of the API classes and uses.	Programmers
Supporting		
Maintaining and Troubleshooting Avaya Breeze™	Contains the list of alarms and errors related to Avaya Breeze™ and the procedures to troubleshoot and fix the problems.	Services and support personnel
Troubleshooting Avaya Aura® Session Manager	Contains information for troubleshooting Avaya Aura® Session Manager, alarm code descriptions, and procedures for resolving alarms.	Services and support personnel
Troubleshooting Avaya Aura® System Manager	Provides procedures for troubleshooting errors for System Manager and the Avaya Aura® applications that System Manager supports.	Services and support personnel
Using		
Quick Start to Deploying Avaya Breeze™ Snap-ins	Walks through the steps to install and administer the different types of snap-ins.	Programmers System administrators

Table continues…

Title	Description	Audience
Administering Avaya Breeze™	Provides the procedures to administer and configure Avaya Breeze™ and snap-ins.	System Administrators Services and Support personnel
Administering Avaya Aura® Session Manager	Describes the routing administration and management of Avaya Aura® Session Manager instances.	System Administrators Services and support personnel
Administering Avaya Aura® System Manager for Release 7.0.1	Describes the administration and management of Avaya Aura® System Manager.	System Administrators Services and support personnel

Finding documents on the Avaya Support website

About this task

Use this procedure to find product documentation on the Avaya Support website.

Procedure

1. Use a browser to navigate to the Avaya Support website at http://support.avaya.com/.

2. At the top of the screen, enter your username and password and click **Login**.

3. Put your cursor over **Support by Product**.

4. Click **Documents**.

5. In the **Enter your Product Here** search box, type the product name and then select the product from the drop-down list.

6. If there is more than one release, select the appropriate release number from the **Choose Release** drop-down list.

7. Use the **Content Type** filter on the left to select the type of document you are looking for, or click **Select All** to see a list of all available documents.

   For example, if you are looking for user guides, select **User Guides** in the **Content Type** filter. Only documents in the selected category will appear in the list of documents.

8. Click **Enter**.

Training

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

Course code	Course title
8U00040E	Knowledge Access: Avaya Avaya Breeze™ Implementation and Support
5105	Avaya Avaya Breeze™ Implementation and Maintenance Test
2014V/W	What is New in Avaya Avaya Breeze™ 3.1

Avaya Breeze™ videos

Avaya Breeze™ provides the following videos to help in the development and deployment of snap-ins. Access these videos at http://www.avaya.com/breezedeveloper.

Title	Audience
Getting Started with the Avaya Breeze™ SDK: Windows	Programmers
Getting Started with the Avaya Breeze™ SDK: Linux	Programmers
Creating Your First Service — Part 1	Programmers
Creating Your First Service — Part 2	Programmers
Server Installation and Configuration with vCenter	System Administrators, Services and Support personnel
Server Installation and Configuration without vCenter	System Administrators, Services and Support personnel
Service Installation, Configuration, and Test	Programmers
Understanding the Dynamic Team Formation Sample Service	Programmers
Understanding the Hello Sample Service	Programmers
Understanding the Multi-Channel Broadcast Sample Service	Programmers
Understanding the Whitelist Sample Service	Programmers

Support

Platform support

Go to the Avaya Support website at www.avaya.com/Support for the most up-to-date product documentation, and product notices. Also search for release notes, service packs, and patches. 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.

Developer support

Go to the Avaya DevConnect website at http://www.avaya.com/breezedeveloper to access the Avaya Breeze™ API, SDK, sample applications, developer-oriented technical documentation, and training materials.

Chapter 2: Cluster Administration

Cluster Administration

Creating a new cluster

Before you begin

Load the required services for your cluster on the Service Management page. For more information on loading a service, see Administering *Avaya Breeze*™.

About this task

Use the Create Cluster page to:

- Select a cluster profile.
- Configure the cluster attributes.
- Add Avaya Breeze™ servers to a cluster.
- Install snap-ins on a cluster.

Procedure

1. On System Manager, in **Elements**, click **Avaya Breeze™**.

2. In the left navigation pane, click **Cluster Administration**.

3. On the Cluster Administration page, click **New**.

4. On the Create Cluster page, select the cluster profile of your choice.

   ✱ **Note:**

   You must select a cluster profile to view the appropriate cluster attributes.

   Either select the general purpose cluster profile or a product specific cluster profile. Use the **Context Store** profile for the Context Store snap-in, **Work Assignment** profile for the Work Assignment snap-ins, **Core Platform** profile for Presence Services, **General Purpose Large** profile for the Engagement Call Control snap-in and the **General Purpose** profile for other snap-ins.

5. Enter the cluster attributes for your cluster. You can edit the default cluster attributes the system displays.

   The name and the IP address of a cluster must be unique.

You cannot edit all the cluster attributes. Some attributes are read-only.

6. If you will be installing snap-ins that use the cluster database, check **Enable Cluster Database**.

7. (Optional) Click the **Servers** tab to assign Avaya Breeze™ servers to the cluster.

   > ❗ **Important:**
   >
   > Do not assign servers with different releases to the same cluster. All servers in the cluster should be running the same Avaya Breeze™ version.
   >
   > For more information on upgrading clusters, see *Upgrading Avaya Breeze*™.

8. (Optional) Click the **Services** tab to install snap-ins to this cluster.

   When you add snap-ins to a cluster, the highest version of the required snap-ins are automatically assigned to the cluster for installation. For the product specific cluster profiles, you must load the required snap-ins from the Service Management page before you install the snap-in.

9. Click **Commit** to create the cluster.

   The **Service Install Status** in the Cluster Administration page displays a green tick symbol after all the assigned services are successfully installed on all the servers in the cluster.

   To view the Avaya Breeze™ servers in the cluster, click **Show** in the **Details** column of the cluster. The system displays the members of the cluster, and the status of each instance in the cluster.

   Click a specific Avaya Breeze™ server to go to the Avaya Breeze™ Instance Editor page. You can view and edit the properties of the Avaya Breeze™ server from this page.

   > ✳ **Note:**
   >
   > When you administer a new Avaya Breeze™ server, you must add the server to a cluster. If you do not add the Avaya Breeze™ server to a cluster, you cannot install snap-ins on that server.

Enabling HTTP load balancing in an Avaya Breeze™ cluster

Before you begin

When you select the load balancing option during **Edit** operation, you must first change the state of the cluster to **Deny New Service**. After enabling the load balancing functionality, you can change the state of the cluster back to **Accept New Service**.

> ✳ **Note:**
>
> You need not enable load balancing if you use an external load balancer or if you are running a single server cluster.

Procedure

1. On System Manager, in **Elements**, click **Avaya Breeze™**.

2. In the left navigation pane, click **Cluster Administration**.

3. If you are enabling load balancing for an existing cluster, on the Cluster Administration page complete the following actions:

   a. Click the checkbox in front of the cluster.

   b. From the **Cluster State** drop-down menu, select **Deny New Service**.

   c. Verify that the **Cluster State** column for the cluster changed to **Denying**.

   d. Click **Edit**.

4. If you are creating a new cluster with load balancing enabled, on the Cluster Administration page complete the following actions:

   a. Click **New**.

   b. Specify the attributes of the cluster.

5. In the Cluster Attributes section select the **Is load balancer enabled** check box to enable load balancing.

6. In the Basic section **Cluster IP** field, assign the IP address for the cluster.

   ✳ **Note:**

   The **Cluster IP** address used for load balancing must be unique. That is, this IP address must not match the Security Module IP address or the management IP address. The Security Module IP address must be on the same subnet as the Avaya Breeze™ **Cluster IP** address.

7. Click **Commit**.

   Two Avaya Breeze™ servers are automatically designated as active and standby to perform the load balancing functionality.

8. On the Cluster Administration page, from the **Cluster State** drop-down menu, select **Accept New Service** to put the cluster in service.

HTTP load balancing in an Avaya Breeze™ cluster

Enable load balancing for a cluster if you want to scale the HTTP services without targeting a particular Avaya Breeze™ server. All the requests are sent to the cluster IP address. When you enable load balancing, two Avaya Breeze™ servers are chosen as the active and standby load balancing servers. The active load balancer distributes the HTTP requests to all the other servers in the cluster in a round robin fashion.

Load balancing validations

The following are the validations when you enable load balancing in a cluster:

- Load balancing is not supported in a single server cluster.
- By default the load balancing check box is not selected.
- For load balancing to function, the cluster must have two Avaya Breeze™ servers that have the SIP Entity IP addresses in the same subnet as the cluster IP address. The active server starts

a network alias using the cluster IP address. If the active server is down, the standby starts a network alias with the cluster IP address. The standby server takes over as the active load balancer.

- With load balancing, you cannot remove the active or the standby Avaya Breeze™ server from the cluster unless another servers meets the subnet validation.

Session affinity

Session affinity ensures that all the requests from the same client are directed to the same back end Avaya Breeze™ server in a cluster. Session affinity is mandatory for snap-ins like the WebRTC Snap-in.

Multi-cluster geo-redundancy

With multi-cluster geo-redundancy, do not use round-robin for load balancing HTTP requests. Rather use *fixed list* (rrset-order fixed), not the default. Each location should have its own DNS server, and each DNS server should have *A record* entries with the name in different orders, putting the more local cluster first.

Editing clusters

About this task

Use the Edit Cluster page to:

- Configure cluster attributes.
- Assign one or more Avaya Breeze™ servers to the cluster.
- Remove one or more Avaya Breeze™ servers from the cluster.
- Assign snap-ins to the cluster.
- Remove snap-ins from the cluster.

😊 **Note:**

If you want to work with Avaya Breeze™ servers that are assigned to a legacy cluster, you must first upgrade the legacy cluster.

Procedure

1. On System Manager, in **Elements**, click **Avaya Breeze™**.
2. In the left navigation pane, click **Cluster Administration**.
3. On the Cluster Administration page, select the cluster that you want to edit.
4. Click **Edit**.

   😊 **Note:**

   To modify the cluster attributes, you must place the cluster in the Deny New Service state.

   You cannot modify the cluster attributes that are greyed out.

5. On the Edit Cluster page, edit the cluster attributes.

6. (Optional) Click the **Servers** tab. Select specific Avaya Breeze™ instances to add the instances to the cluster.

   To remove Avaya Breeze™ servers and to move the servers to the unassigned pool, clear the Avaya Breeze™ servers from the selected list.

7. (Optional) Click the **Services** tab. Select the snap-ins that you want to assign to the cluster.

   To remove an existing snap-in from the cluster, click **U** to uninstall the snap-in or **F** to force uninstall the snap-in. The snap-in moves to the available services pool. However, force uninstall brings down active sessions that access the snap-in.

8. Click **Commit** to save the changes.

   ✱ **Note:**

   If the change you make does not comply with the basic cluster requirements, the edit is not successful. The system displays the appropriate error message.

Assigning an Avaya Breeze™ server to a cluster

Procedure

1. On System Manager, in **Elements**, click **Avaya Breeze™**.

2. In the left navigation pane, click **Cluster Administration**.

3. On the Cluster Administration page, do one of the following:

   • Click **New** and select a cluster profile.

   • Select a cluster, and click **Edit**.

4. Click the **Servers** tab.

5. From the **Unassigned Servers** table, click the **+** sign next to the **Name** column to add the Avaya Breeze™ server to your cluster.

   You can add one server to only one cluster.

   If the cluster already has five servers, you cannot assign any more Avaya Breeze™ servers to that cluster. Core Platform cluster profile alone supports up to 10 servers in a cluster.

   When you add an Avaya Breeze™ server to a cluster, the server must be in the Deny New Service state. Only after the required snap-ins are auto-installed on the server, you must place the server in the Accept New Service state.

   Even when one of the assigned servers is not reachable by System Manager, you cannot edit any of the tabs on the Cluster Administration page.

6. Click **Commit** to assign the server to the cluster.

> **Note:**
>
> If you add a server to a single sever cluster it impacts service as WebSphere restarts to update the GigaSpaces properties. However, if you add a server to a cluster that has two or more servers, it does not impact service.

Deleting an Avaya Breeze™ server from a cluster

Procedure

1. On System Manager, in **Elements**, click **Avaya Breeze™**.

2. In the left navigation pane, click **Cluster Administration**.

3. On the Cluster Administration page, select the cluster from which you want to delete a Avaya Breeze™ server.

4. Click **Edit**.

5. On the Cluster Editor page, click the **Servers** tab.

6. From the **Assigned Servers** table, click the **x** sign next to the **Name** column .

7. Click **Commit** to delete the server from the cluster you selected.

   > **Note:**
   >
   > When you remove either the primary or the secondary Lookup server from a cluster, all the other servers in the cluster restart due to the configuration change. The system
   >
   > displays 🔎 against the Lookup server on the **Server Administration** and **Cluster Administration** pages.

Related links

Validations when removing a server from a cluster

You cannot delete an Avaya Breeze™ server from a cluster if:

- The minimum number of servers are not available in the Accept New Service state.
- The Avaya Breeze™ server is not in the Deny New Service state.
- The server is functioning as a load balancing server or as a lookup server, and you do not have another available server to take over.

Additional validations when Cluster Database is enabled

The following are the validations when you want to remove a server from a cluster database without auto switch over.

> **Note:**
>
> You must use manually switch over the active server to a standby server, or make an idle server a Standby Procedure, or both before removing servers.

- In a cluster with a single server you can remove the server provided the server is in the Deny New Service state.

- In a cluster with two servers, you can remove the standby or both the servers without any validation. If you want to remove the active server, you must manually switch over the active with the standby before you remove the current active server.

- In a cluster with three or more servers, you can remove a server if the server is in the Idle mode. If the server is an active server or a standby server, the delete action is blocked.

  If you want to remove the standby server, perform a manual switch over with the Idle server before you remove the server. If you want to remove the active server, perform a manual switch over with the standby before you remove the server.

Related links

Performing manual switch over from active server to standby server

Before you begin

1. Ensure that the cluster contains two or more servers.
2. Perform this procedure only when the standby server is ready.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze™**
2. Click **Cluster Administration**.
3. Click **show**.
4. On the **Cluster Database** column, click:
   - **Active**: To convert an active server to standby server.
   - **Standby**: To convert a standby server to an active server.
5. Click **Continue**.

Related links

Converting an idle server to the standby server

About this task

Perform this procedure only when the cluster contains three or more servers.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze™**

2. Click **Cluster Administration**.

3. Click **show**.

4. On the **Cluster Database** column, click **Idle**.

   This setting will convert the idle server to a standby server and will convert the existing standby server to an idle server.

5. Click **Continue**.

Related links

[Validations when removing a server from a cluster](#) on page 19

Installing a snap-in on a cluster

Procedure

1. On System Manager, in **Elements**, click **Avaya Breeze™**.

2. In the left navigation pane, click **Cluster Administration**.

3. On the Cluster Administration page, perform one of the following actions:

   • Click **New**. Select the cluster profile type and enter the required cluster attributes.

   • Select a cluster and click **Edit**.

   ⊛ **Note:**

   If the snap-in being installed requires Cluster Database, a warning message is display that you must enable Cluster Database before the snap-in is installed. For more information, see "Enabling Cluster Database".

4. Click the **Services** tab.

5. From the **Available Services** table, click the **+** sign next to the **Name** column to add the snap-in to the cluster.

6. Click **Commit** to install the snap-in to the cluster.

   For every cluster type there is a set of required snap-ins that must be loaded so that they can be automatically installed on the cluster. If one or more of the required snap-ins is not loaded, the system displays a warning message. You cannot create or edit the cluster successfully.

In a closed cluster, you cannot install snap-ins that are not part of the optional or mandatory snap-in list.

Enabling Cluster Database on a cluster

Procedure

1. On System Manager, in **Elements**, click **Avaya Breeze™**.

2. In the left navigation pane, click **Cluster Administration**.

3. Select the cluster that you want to edit, and click **Cluster State** > **Deny New Service**.

4. Click **Continue**.

5. Click **Edit**.

6. In the General tab, select the **Enable Cluster Database** check box.

7. Leave the **Enable Database Auto Switchover** field at the default setting, unless you want to manually control when a failover must occur.

8. Click **Commit**.

9. Select the cluster, and click **Cluster State** > **Accept New Service**.

10. Click **Continue**.

Uninstalling a snap-in from a cluster

Procedure

1. On System Manager, in **Elements**, click **Avaya Breeze™**.

2. In the left navigation pane, click **Cluster Administration**.

3. On the Cluster Administration page, select the cluster or clusters from which you want to uninstall the snap-in.

4. Click **Edit**.

5. On the Cluster Editor page, click the **Services** tab.

6. From the **Installed Services** tab, do one of the following:

   • Click the **U** sign against the snap-ins that you want to uninstall.

   • Click the **F** sign for the snap-ins that you want to force uninstall. When you click **F**, the snap-ins are immediately uninstalled and the system does not wait for the snap-in activities to complete.

7. Click **Commit** to uninstall the snap-in from the cluster.

   You cannot uninstall a required snap-in from a cluster unless another version of the snap-in is installed in the cluster.

You can choose to uninstall a snap-in from specific clusters while retaining the snap-in in other clusters.

Performing a switch over in a cluster database

About this task

You must perform the following procedure when the auto switch over of servers is not enabled in a cluster. Manually perform the switch over of the servers in this scenario. You might also need to perform this procedure when you remove a server from a cluster, or when you perform maintenance actions like upgrading a server within a cluster.

When the switch over is complete, the **Cluster Database** column changes from **Active** to **Standby** or vice versa.

Procedure

1. On System Manager, in **Elements**, click **Avaya Breeze™**.

2. In the left navigation pane, click **Cluster Administration**.

3. Click the **Details** of the cluster in which you want to perform the switch over.

   The system displays the details with the active server and the backup server.

4. Do one of the following:

   • Click **Active** to perform the switch over. In the confirmation dialog box, click **Continue** to switch over the active server.

   • Click **Standby** to perform the switch over. In the confirmation dialog box, click **Continue** to switch over the standby server.

Deleting clusters

Before you begin

Place the cluster in Deny New Service state before you delete the cluster.

Procedure

1. On System Manager, in **Elements**, click **Avaya Breeze™**.

2. In the left navigation pane, click **Cluster Administration**.

3. On the Cluster Administration page, select the cluster or clusters that you want to delete.

4. Click **Delete**.

5. On the Delete Confirmation page, click **Delete**.

   When you delete a cluster, the Avaya Breeze™ instances assigned to the cluster are automatically removed from the cluster. The services installed in the cluster are automatically removed.

> **✱ Note:**
>
> You cannot delete a legacy cluster.

Adding a Trust Certificate to all Avaya Breeze™ servers in a cluster

Before you begin

Certificates that you intend to add as trusted certificates must be accessible to System Manager.

Procedure

1. On System Manager, in **Elements**, click **Avaya Breeze™**.

2. In the left navigation pane, click **Cluster Administration**.

3. Select the cluster to which you want to administer the trusted certificates.

4. Click **Certificate Management** > **Install Trust Certificate (All Avaya Breeze™ Instances)** to download the trusted certificate for all the servers in the cluster.

   > **✱ Note:**
   >
   > The Trust Certificate that you are about to add will apply to all the Avaya Breeze™ servers assigned to the cluster.

5. From the **Select Store Type to install trusted certificate** menu, select the appropriate store type.

6. Click **Browse** to the location of your Trust Certificate, and select the certificate.

7. Click **Retrieve Certificate**, and review the details of the Trusted Certificate.

8. Click **Commit** .

Related links

Store types of the trusted certificates

Store Type/Interface/ Service	Common Name	Connected peer party	Usage/Function
Security Module SIP	securitymodule_sip	Session Manager	SIP link
Management	smmgmt	System Manager	Data replication and other management information. The Avaya Breeze™ management link that communicates with System Manager.

Table continues…

Store Type/Interface/ Service	Common Name	Connected peer party	Usage/Function
SPIRIT	spiritalias	SAL server on System Manager	SAL
Security Module HTTPS	securitymodule_http	HTTPS interface to external HTTPS clients or servers	HTTPS
WebSphere	websphere	SECMOD, WebSphere	—

Chapter 3: Service Administration

Snap-in deployment checklists

The following are the types of Avaya Breeze™ snap-ins:

- Call-intercept snap-ins
- Callable snap-ins
- Other types of snap-ins:
  - Outbound calling snap-ins
  - HTTP-invoked snap-ins
  - Collaboration Bus-invoked snap-ins

Callable snap-ins are called directly by users rather than being called on behalf of the user who makes or receives a call.

Licensed snap-ins that are purchased separately from Avaya Breeze™ might require additional steps to deploy. For more information, see the snap-in documentation.

Call-intercept snap-in deployment checklist

No.	Task	Notes	Link/Reference	✔
1	Install the snap-in license.	This step applies only to Avaya-developed snap-ins that you purchase separately. Skip this step when installing a preloaded snap-in. Preloaded snap-ins are provided with Avaya Breeze™ Element Manager without additional charges.	See *Quick Start to Deploying Avaya Breeze™ Snap-ins*.	
2	Load the snap-in.	Skip this step when installing a preloaded snap-in. Preloaded snap-ins are provided free with Avaya Breeze™ Element Manager .	[Loading the snap-in](#) on page 29	

Table continues…

No.	Task	Notes	Link/Reference	✔
3	Configure snap-in attributes.	—	Configuring snap-in attributes at the service profile level on page 31	
4	Install the snap-in.	—	Installing the snap-in on page 33	
5	Create a service profile.	—	Creating a Service Profile on page 35	
6	Create a new user profile.	This step is required only for users who are not administered in System Manager as explicit users. For implicit users, create the implicit user rule.	Creating a new user profile on page 48	
7	Assign service profile to users.	Skip this step if the service profile that contains your snap-in is already assigned to the users who want to receive the snap-in.	Assigning a Service Profile to an administered user on page 49	
8	Create an application and the application sequence.	Skip this step if you have an application sequence administered for Avaya Breeze™.	Application Sequences and implicit sequencing on page 37	
9	Administer implicit sequencing for a user or group of users.	Skip this step if you have administered implicit sequencing for Avaya Breeze™.	Administering implicit sequencing for Avaya Breeze on page 45	
10	Test the snap-in.	—	Testing a call-intercept snap-in on page 39	

Callable snap-in deployment checklist

No.	Task	Notes	Link	✔
1	Install the snap-in license.	This step applies only to Avaya-developed snap-ins that you purchase separately. Skip this step when installing a preloaded snap-in. Preloaded snap-ins are provided with Avaya Breeze™ Element	See *Quick Start to Deploying Avaya Breeze™ Snap-ins*.	

Table continues…

No.	Task	Notes	Link	✔
		Manager without additional charges.		
2	Load the snap-in.	Skip this step when installing a preloaded snap-in. Preloaded snap-ins are provided with Avaya Breeze™ Element Manager without additional charges.	Loading the snap-in on page 29	
3	Configure the snap-in attributes.	—	Configuring snap-in attributes at the service profile level on page 31	
4	Install the snap-in.	—	Installing the snap-in on page 33	
5	Determine the dial string of the callable snap-in.	—	—	
6	Determine the pattern that includes the dial string and optionally includes other callable snap-in dial strings.	—	—	
7	Create a routing policy using which Session Manager can determine which calls to route to Avaya Breeze™ SIP Entity.	—	Creating a routing policy on page 40	
8	Create the dial pattern that matches with the pattern specified in Step 6.	—	Creating a dial pattern on page 40	
9	Create a service profile with a single callable snap-in.	—	Creating a Service Profile on page 35	
10	Create an implicit user pattern in Avaya Breeze™ that exactly matches the dial string determined in Step 5.	The implicit user pattern: • Must not match with any other callable snap-in or end user dial strings. • Must not be included in a Session Manager implicit user pattern.	Assigning a Service Profile to implicit users on page 47	
11	Select a routing policy with Avaya Breeze™ as the destination and a dial pattern that maps the pattern to the Avaya Breeze™ destination.	—	See Administering Avaya Breeze™.	
12	Assign the service profile created in Step 5 to the implicit user pattern.	—	Assigning a service profile to an implicit user pattern on page 41	

Other types of snap-ins deployment checklist

No.	Task	Notes	Link	✔
1	Install the snap-in license.	This step applies only to Avaya-developed snap-ins that you purchase separately. Skip this step when installing a preloaded snap-in. Preloaded snap-ins are provided with Avaya Breeze™ Element Manager without additional charges.	See *Quick Start to Deploying Avaya Breeze™ Snap-ins.*	
2	Load the snap-in.	Skip this step when installing a preloaded snap-in. Preloaded snap-ins are provided with Avaya Breeze™ Element Manager without additional charges.	Loading the snap-in on page 29	
3	Configure the snap-in attributes.	—	Configuring snap-in attributes at the service profile level on page 31	
4	Install the snap-in.	—	Installing the snap-in on page 33	
5	Create a service profile or add the snap-in to an existing service profile.	Skip this step for snap-ins that do not require a service profile.	Service Profiles on page 34	
6	Assign a service profile to a user.	Skip this step if the service profile that contains the snap-in is already assigned to the users who want to receive the snap-in.	Assigning a Service Profile to an administered user on page 49	
7	Test the snap-in.	—	Testing a non-call-intercept snap-in on page 39	

Loading the snap-in

About this task

This task describes how to load a snap-in to System Manager from your development environment or alternate location. You can skip this step when installing a pre-loaded snap-in. Pre-loaded snap-ins are provided without additional charge with the Avaya Breeze™ Element Manager.

Procedure

1. On System Manager, in **Elements**, click **Avaya Breeze**.

2. In the left navigation pane, click **Service Management**.

3. Click **Load**.

4. On the Load Service page, depending on the browser used, click **Browse** or **Choose File**, and browse to your snap-in file location.

5. Click **Open**.

   Your snap-in file should end with `.svar`. The Service Archive (svar) file is provided by service developers.

6. On the Load Service page, click **Load**.

   For Avaya snap-ins only, you will be prompted to accept the Avaya End User License Agreement (EULA).

7. If you agree to the Avaya EULA, click **Accept**.

   Your snap-in displays on the Service Management page with a **State** of **Loaded**.

   If you clicked **Cancel** to reject the agreement, the load action stops.

Related links

[Service Management field descriptions](#) on page 87

Configure service attributes

There are four levels of service attributes: Service Profile, Service Cluster, Service Global and default. This order specifies the attribute level from the most specific level to the most generic. When an Avaya Breeze™ server is determining the attribute value to a snap-in, the server checks the value specified against the user's service profile. If no value has been specified, the server checks if an attribute value has been specified at the cluster level. Again if a value has not been specified, the server checks for the attribute value at the global level. If no value is found, the server uses the default attribute value.

✱ **Note:**

You cannot configure some service attributes at the user level. In this case, the server first determines the attribute at the cluster level.

Snap-in developers can specify attribute scoping. The possible values are:

- Global: The attribute is visible only in the **Service Globals** tab.
- Global and Cluster: The attribute is visible in the **Service Globals** tab and **Service Cluster** tab.
- Global, Cluster, and Service Profile: This is the default value if the snap-in developer does not specify any value. The attribute is visible in all the three tabs in the **Configuration** > **Attributes** page.

Related links

Configuring snap-in attributes at the service profile level

Customize snap-ins for a specific group of users by assigning attributes to the snap-in in the Service Profile. You can assign attributes either as part of adding a snap-in to a Service Profile or at a later time.

Before you begin

Create or add a service profile. For more information, see the topic *Creating a Service Profile*.

Procedure

1. On System Manager, in **Elements**, click **Avaya Breeze™**.

2. In the left navigation pane, click **Configuration** > **Attributes**.

3. Click the **Service Profile** tab.

4. From the **Profile** field, select the Service Profile that contains the snap-in and the attributes that you want to configure.

5. From the **Service** field, select the snap-in in the Service Profile that contains the attributes you want to configure.

   The system displays all the attribute groups with the attributes that you can configure for the snap-in.

6. For the attribute that you want to change:

   a. Click **Override Default**.

   b. Enter the new value or string in the **Effective Value** field.

7. Click **Commit** to save your changes.

Related links

Configuring snap-in attributes at the cluster level

Perform this procedure only after installing the snap-in.

Procedure

1. On System Manager, in **Elements**, click **Avaya Breeze™**.

2. In the left navigation pane, click **Configuration** > **Attributes**.

3. Click the **Service Clusters** tab.

4. From the **Cluster** field, select the cluster to which you want to configure the snap-in attributes.

5. From the **Service** field, select the service to which you want to configure the snap-in attributes.

   The system displays all the attribute groups with the attributes that you can configure for the snap-in.

6. For the attribute that you want to change:

   a. Click **Override Default**.

   b. Enter a new value or string in the **Effective Value** field.

7. Click **Commit** to save the changes.

Related links

Configuring snap-in attributes at the global level

About this task

Use this task to configure values for attributes that will replace the default values assigned in the snap-in. Perform this task to configure attributes for a snap-in when that snap-in is not included in a Service Profile, or when the snap-in attributes are not configured uniquely for the Service Profile. Perform this task to configure attributes for email, conferencing (Scopia) and text messaging (Clickatell SMS) connector services.

Procedure

1. On System Manager, in **Elements**, click **Avaya Breeze™**.

2. In the left navigation pane, click **Configuration** > **Attributes**.

3. Click the **Service Globals** tab.

4. From the **Service** drop-down menu, select the service that contains the service attributes you want to configure.

   The system displays all the attribute groups with the attributes that you can configure for the snap-in.

5. For the attribute you want to change:

   a. Click **Override Default**.

   b. Enter the new value or string in the **Effective Value** field.

6. Click **Commit** to save your changes.

Related links

[Attribute Configuration field descriptions](#) on page 64

Installing the snap-in

About this task

For .svar files larger than 50 MB, schedule snap-in installation during a maintenance window.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze**.

2. In the left navigation pane, click **Service Management**.

3. Select the snap-in that you want to install.

4. Click **Install**.

5. Select the cluster where you want the snap-in to reside, and click **Commit**.

6. To see the status of the snap-in installation, click the Refresh Table icon located in the upper-left corner of the **All Services** list.

   Installed with a green check mark indicates that the snap-in has completed installation on all the Avaya Breeze™ servers in the cluster. **Installing** with a yellow exclamation mark enclosed in a triangle indicates that the snap-in has not completed installation on all the servers.

7. Designate the Preferred Version.

   If you want to designate this newly installed snap-in as the Preferred Version, complete the following steps. Avaya Breeze™ uses the Preferred Version of a snap-in even if you install a later version of the same snap-in.

   a. From the **All Services** list, select the version of the snap-in that you installed.
   b. Click **Set Preferred Version**.
   c. Select the clusters for which you want this to be the preferred version, and click **Commit**.
   d. Reboot the clusters for which you set the preferred version.

      It can take several minutes for System Manager to propagate the snap-in to your Avaya Breeze™ servers.

8. To track the progress of a snap-in installation, on the Server Administration page, click the **Service Install Status** for an Avaya Breeze™ server.

   The system displays the Service Status page with the installation status of all the snap-ins installed on that server.

Related links

[Service Management field descriptions](#) on page 87

Service Profiles

A Service Profile is an administered group of snap-ins. Some snap-ins are associated with users. That is, these snap-ins are added to a Service Profile. You must associate a snap-in with a user when:

- You use a Call-Intercept snap-in. You must place the Call-Intercept snap-in in a Service Profile. Events published on the Eventing Framework have the user's name in the **User** field.

- Java snap-ins subscribe to events. The snap-ins can optionally specify whether a Service Profile is needed. In this case, the snap-in must be in a user's service profile to be notified when a event is published with that user in the metadata.

- The **Service Profile Needed:** attribute is set to **true** in the Engagement Designer Start dialog box. Here, the workflow must match the one in the user's Service Profile that is started when an event is published with the user in the metadata.

You can use a Service Profile to:

- Assign the same group of snap-ins to a group of users, thereby eliminating the need to administer each snap-in individually for each user. To do this, you assign the same Service Profile to each member of the group.

- Use the Service Profile to link one or many Avaya Breeze™ snap-ins to a user or a group of users.

  Tailor the attributes of any snap-in in the Service Profile to the requirements of a specific group of users. For example, you could create one Service Profile for the entire sales department so they could enjoy the same Avaya Breeze™ snap-ins and attributes of those snap-ins. And then, create a different Service Profile for the finance department, with some of the same snap-ins, but with different attributes for the snap-ins.

  You can thus create a single Service Profile and assign the service profile to multiple users who require the same snap-ins, eliminating the need to administer these snap-ins individually for each user.

You must include a snap-in in a Service Profile to associate it with users; users are associated with a Service Profile and not individual snap-ins.

Related links

Creating a Service Profile

About this task

Use this procedure to create a new Service Profile and add your snap-in to it. You can skip this procedure if you want to add the snap-in to an existing Service Profile or if your snap-in is not user associated and therefore does not go in a Service Profile.

Procedure

1. On System Manager, in **Elements**, click **Avaya Breeze™**.

2. In the left navigation pane, click **Configuration** > **Service Profiles**.

3. Click **New**.

4. Type a name for the Service Profile.

5. Select the **All Services** tab.

6. Select the snap-in and version to add to the profile.

   a. In the list of **Available Service to Add to this Service Profile**, click **Advanced** next to the snap-in name.

   b. From the **Service Version** field, select the version of the snap-in to use in the Service Profile. Select from the following choices:

      • If you designated your snap-in as the Preferred Version at installation, select **Preferred** to use that version of the snap-in. If you later designate a different version of the snap-in as the Preferred Version, the Service Profile automatically uses the new Preferred Version.

      • Select **Latest** to always use the version of the snap-in with the latest version number.

      • Select a specific version number.

   c. Click **Add**.

7. To add your snap-in to the Service Profile without selecting a version, in the **Available Service to Add to this Service Profile** list, click the **+** next to the snap-in.

8. Click **Commit** to save the Service Profile.

   ⊛ **Note:**

   You cannot add Call Control and Eventing Services (CECS), Eventing connector, and other connectors to a Service Profile. These connectors are directly invoked by the Avaya Breeze™. However, the Service Profiles you created before upgrading from Release 2.0 may contain the connectors. Avaya recommends that you remove these connectors from the Service Profile if they were added previously.

Related links

Configuring service invocation for service profiles

About this task

Use the **Service Invocation Details** tab to configure the calling service invocation order and the called service invocation order. You can have up to five call intercept snap-ins assigned to a single service profile. To set the order of the call intercept services, perform the following procedure.

Procedure

1. On System Manager, in **Elements**, click **Avaya Breeze™**.

2. In the left navigation pane, click **Configuration** > **Service Profiles**.

3. Do one of the following:

   • Click **New**.

   • Click **Edit**.

4. On the Service Profile Editor page, complete the details of the service profile.

5. Click the **Service Invocation Details** tab. Based on the service you have added to your service profile, the appropriate call intercept services are listed in the **Calling Service Invocation Order** table and the **Called Service Invocation Order** table.

6. In the **Order: First to Last** column, click the arrows to move the services up or down in the invocation order of the call intercept services.

7. Click **Commit** to save the changes.

Related links

[Service Profiles](#) on page 34

Searching service profiles

About this task

Use the search bar on the Service Profile Configuration page to search service profiles. The search will bring all the results that contain the search string. You can search service profiles by using the search bar on various pages in System Manager.

Procedure

1. On System Manager, in **Elements**, click **Avaya Breeze™**.

2. In the left navigation pane, click **Configuration** > **Service Profiles**.

3. On the Service Profile Configuration page, type your search string in the search bar.

   The system displays all the service profiles that contains your search string.

4. Hover your mouse over a service profile.

   The system displays a pop-up window with **Edit**, **Users**, and **Bulk Edit** options.

5. Click **Users** to view the list of users who have this Service Profile assigned to them.

6. Click **Edit** to edit the details of the service profile.

7. Click **Bulk Edit** to edit the Service Profile of the associated users for this Service Profile.

   The system displays the User Bulk Edit page, where you can edit the Service Profile of the associated users.

Related links

[Service Profiles](#) on page 34

Application Sequences and implicit sequencing

An Application Sequence is required in combination with implicit sequencing for call-intercept snap-ins to route calls for a specific user or group of users to Avaya Breeze™. In this way, calls to or from the user will invoke Avaya Breeze™ snap-ins.

An Application Sequence is required only for call-intercept snap-ins, that is, snap-ins that are invoked when a user receives or makes a call.

To set up the Application Sequence with implicit sequencing you must:

1. Add the target Avaya Breeze™ as an Application.

2. Add the Avaya Breeze™ Application to an Application Sequence.

3. Assign the Application Sequence to the implicit user (number or pattern) you want connected to Avaya Breeze™ snap-ins (administering implicit sequencing).

Implicit sequencing administration for Avaya Breeze™

Avaya Breeze™ uses implicit sequencing for both SIP and non-SIP endpoints. (This is unlike Communication Manager, which uses explicit sequencing for SIP endpoints.) Therefore, you must set up implicit sequencing for all SIP and non-SIP endpoints that receive call-intercept snap-ins.

With an Application Sequence, snap-ins are invoked when a user receives a call, makes a call, or in both cases. Administer this choice on the Session Manager Implicit User Rule Editor page for a user or group of users. On this page:

• The **Origination Application Sequence** tells Session Manager to invoke the Avaya Breeze™ for the user when making calls. Use the Origination Application Sequence for Calling Party snap-ins.

• The **Termination Application Sequence** tells Session Manager to invoke the Avaya Breeze™ for the user when receiving calls. Use the Termination Application Sequence for Called Party snap-ins.

For simplicity, select both sequences, in which case Avaya Breeze™ is invoked when the user either makes a call or receives a call. For maximum efficiency, if you have a Calling Party snap-in, select an **Origination Application Sequence** that includes Avaya Breeze™. If you have a Called Party snap-in, select a **Termination Application Sequence** that includes Avaya Breeze™.

> ✱ **Note:**
>
> See *Deploying Avaya Breeze™* for instructions on how to configure Communication Manager to force calls to Session Manager for sequencing.

Creating an Application and Application Sequence

This procedure:

- Administers a target Avaya Breeze™ instance as an Application.
- Administers the Application as part of an Application Sequence. This only needs to be done once for each Avaya Breeze™ instance.

Procedure

1. Administer the target Avaya Breeze™ instance as an Application:

   a. On the System Manager **Home** page, under **Elements**, select **Session Manager** > **Application Configuration** > **Applications**.

   b. Click **New**.

   c. In the **Name** field, type a descriptive name for the Avaya Breeze™ instance.

   d. For the **SIP Entity**, select the Avaya Breeze™ where the service resides.

      For information about creating the SIP Entity, see *Deploying Avaya Breeze™*.

   e. To save your changes, click **Commit**.

2. Administer the Application as part of an Application Sequence:

   a. On the System Manager **Home** page, under **Elements**, select **Session Manager** > **Application Configuration** > **Application Sequences**.

   b. Click **New**.

   c. In the **Name** field, type a descriptive name for the Application Sequence.

   d. In the list of **Available Applications** click the **+** sign next to the Avaya Breeze™ Application that you created.

   e. If you don't want calls to fail when Avaya Breeze™ is not available, deselect the **Mandatory** check box if it is selected.

      Session Manager stops processing a call if it cannot reach a mandatory application.

   f. To save your Application Sequence, click **Commit**.

Testing a call-intercept snap-in

About this task

Testing a call-intercept snap-in can be as easy as calling from or to a user assigned to the Service Profile, and making sure you get the desired results.

Procedure

1. Make a call to or from the user you assigned to the Service Profile that contains the snap-in.

   • For a calling party snap-in, make the call from the user.

   • For a called party snap-in, make the call to the user.

2. Verify that the test call uses the new snap-in attributes you administered for the Service Profile.

Related links

Call-Intercept call considerations on page 39

Call-Intercept call considerations

In some deployment scenarios you might need to deploy Avaya Breeze™ with Engagement Designer or Work Assignment. In such deployments, Avaya Breeze™ supports Call Preserving fail over with full functionality on existing calls if an Avaya Breeze™ server fails. However, to ensure the Call Preserving functionality, note the following call considerations:

• If Avaya Breeze™ is invoked twice on a single call, you must deploy the Avaya Breeze™ snap-ins on separate clusters. For example, the Real-Time Speech snap-in may be configured to intercept calls after Engagement Designer has routed the call to an agent that was selected by Work Assignment. In this case, you must deploy Real-Time Speech and Engagement Designer on different clusters.

• Call Preservation only works on Call-Intercept calls.

• You must not select the **Use early pre-answer media** check box in the cluster attributes.

• If the call is alerting on the called party at the time of the failure, takeover will not be successful.

Related links

Testing a call-intercept snap-in on page 39

Testing a non-call-intercept snap-in

Procedure

1. Test your snap-in by invoking it by whatever means is appropriate to the snap-in.

   For example, invoke your snap-in from a URL.

2. Verify that the snap-in provides the expected functionality and that it is using the administered snap-in attributes.

   For troubleshooting help, see *Maintaining and Troubleshooting Avaya Breeze™* and *Avaya Breeze™ FAQ and Troubleshooting for Snap-in Developers*.

Creating a routing policy

Procedure

1. On the System Manager web console, in the **Elements** section, click **Routing** > **Routing Policies**.
2. Click **New**.
3. In the **General** section, enter a routing policy name and notes in the relevant fields.
4. In the **Retries** field, enter the number of retries for the destination SIP entity.

   The default value in **Retries** field is 0. The valid values are from 0 to 5.
5. Select the **Disabled** check box to disable the routing policy.
6. In the **SIP Entities as Destination** section, select **Avaya Breeze™**.
7. In the **Time of Day** section, click **Add** to associate the Time of Day routing parameters with this Routing Policy.
8. Select the Time of Day patterns that you want to associate with this routing pattern and click **Select**.
9. Enter the relative Rankings that you want to associate with each Time Range.

   Lower ranking values indicate higher priority.
10. In the **Dial Patterns and Regular Expressions** sections, click **Add** to associate existing Dial Patterns and Regular Expressions with the Routing Policy.
11. Click **Commit**.

Creating a dial pattern

Procedure

1. On the System Manager web console, in the **Elements** section, click **Routing** > **Dial Patterns**.
2. Click **New**.
3. Enter the dial pattern.

   The system auto-populates the **Min** and **Max** fields.

Administering Avaya Breeze™

4. In the **Originating Locations and Routing Policies** section, click **Add**.

5. In the **Originating Locations** section, select the required locations.

6. In the **Routing Policies** section, select the routing policy that we created earlier.

7. Click **Select**.

8. Click **Commit**.

Assigning a service profile to an implicit user pattern

Procedure

1. On System Manager, in **Elements**, click **Avaya Breeze™**.

2. Click **Configuration** > **Implicit User Profiles**.

3. Click **New**.

4. In the **Service Profile** field, select a service profile that has only one callable snap-in added.

5. In the **Pattern** field, specify the pattern defined earlier.

6. Click **Commit**.

Starting a snap-in

About this task

The start snap-in functionality is required when you:

- Upgrade some snap-ins, specifically the Presence snap-in.
- Change some port assignments for snap-ins.
- Change the capacity of clusters.
- Change some configuration parameters of a snap-in. You must restart the snap-in for the configuration change to take effect.

✱ **Note:**

Start snap-in is available only for those snap-ins that have registered for this functionality. For the other snap-ins, installation automatically starts the snap-in.

Procedure

1. On System Manager, in **Elements**, click **Avaya Breeze™**.

2. In the left navigation pane, click **Service Management**.

3. On the Service Management page, select the snap-in that you want to start.

4. Click **Start**.

> ✱ **Note:**
>
> If the snap-in is already installed on all the servers, the **Start** button is disabled.

5. In the Confirm Start Service dialog box, select the cluster or clusters in which you want to start the snap-in.

6. Click **Start**.

   On the Service Management page, the **Service Install Status** changes to **Starting** and then **Installed**.

   > ✱ **Note:**
   >
   > Restarting the Avaya Breeze™ server does not affect the snap-in install status.

Stopping a snap-in

About this task

The stop snap-in functionality is required when you:

- Upgrade some snap-ins, specifically the Presence snap-in.
- Change some port assignments for snap-ins.
- Change the capacity of clusters.
- Change some configuration parameters of a snap-in. You must restart the snap-in for the configuration change to take effect.

> ✱ **Note:**
>
> Stop snap-in is available only for those snap-ins that have registered for this functionality.

Procedure

1. On System Manager, in **Elements**, click **Avaya Breeze™**.

2. In the left navigation pane, click **Service Management**.

3. On the Service Management page, select the snap-in that you want to stop.

4. Click **Stop**.

   > ✱ **Note:**
   >
   > If the snap-in is not in the **Installed** state, the Stop button is disabled.

5. In the Stop Service dialog box, select the cluster or clusters where you want to stop the snap-in.

6. Click **Stop**.

   The **Service Install Status** of the snap-in changes to **Stopping** and then **Stopped**.

> ⊛ **Note:**
>
> If the snap-in is stopped even in one Avaya Breeze™ server, the aggregate status of the snap-in displays **Stopped** only.

Uninstalling a snap-in

Procedure

1. On System Manager, in **Elements**, click **Avaya Breeze™**.

2. In the left navigation pane, click **Service Management**.

3. On the Service Management page, select the snap-in that you want to remove.

4. Click **Uninstall**.

5. From the Confirm Uninstall Service pop-up dialog box, select the cluster or clusters from which you want to remove the snap-in.

   > ⊛ **Note:**
   >
   > You cannot uninstall a required snap-in from a cluster unless another version of the required snap-in is already installed in the cluster.
   >
   > The state of a snap-in as shown on the Service Management page is the aggregated status of the snap-in installation across clusters. If you uninstall a snap-in from a cluster, and if the snap-in is in the installed state in another cluster, the status continues to display as Installed.

6. If you want to forcefully remove the snap-in, select the **Force Uninstall** check box in the same pop-up dialog box.

   For a snap-in the system displays the SIP activity and the Active Link in the Cluster Administration page. If you force uninstall the snap-in, the snap-in will be uninstalled immediately without waiting for the Active Link value to come to zero.

   In a normal scenario the activity drains in about two hours and the Activity Link value comes to zero. This is when the snap-in is uninstalled.

Deleting a snap-in

About this task

You must uninstall a snap-in from all the clusters before you delete the snap-in. When you delete the snap-in, the snap-in is removed from the System Manager database.

Procedure

1. On System Manager, in **Elements**, click **Avaya Breeze™**.

2. In the left navigation pane, click **Service Management**.

3. On the Service Management page, select the service that you want to delete.

4. Click **Delete**.

   > ❶ **Important:**
   >
   > Verify that the service is in the **Loaded** state before you click **Delete**.

5. In the Delete Service Confirmation dialog box, select the **Please Confirm** check box.

6. Click **Delete**.

Chapter 4: User Administration

Administering implicit sequencing for Avaya Breeze™
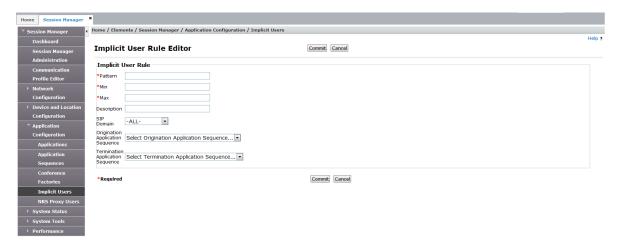
Administer implicit sequencing for a user or group of users for Avaya Breeze™ so that an application sequence can be assigned to those users for call-intercept snap-ins. Avaya Breeze™ uses implicit sequencing for both SIP and non-SIP endpoints. Therefore, you must administer implicit sequencing for all SIP and non-SIP endpoints that receive call-intercept snap-ins.

Before you begin

Create the Application and Application Sequence for the Avaya Breeze™ server before starting this task.

Procedure

1. On the System Manager **Home** page, under **Elements**, select **Session Manager** > **Application Configuration** > **Implicit Users**.

2. Click **New**.

3. In the **Pattern** field, specify the pattern as defined for Session Manager and Communication Manager digit routing.

   For non-SIP users, the dial pattern should be the same pattern format as used in the Routing Policy Dial pattern. For SIP users, as a best practice use E.164 patterns to scope the SIP users either singularly or as a range. If that is not desired, use the Communication Address

defined on **User** > **User Management** > **Manage Users** User Profile **Communication Profile** tab. The pattern range used can include both SIP and non-SIP users.

For example, in the **Pattern** field, do one of the following:

- Enter the user's full E.164 number (or minimally enter the Communication Address defined on **User** > **User Management** > **Manage Users** User Profile **Communication Profile** tab for that user) for a single user.

- Enter "x" patterns as wildcards, to match multiple users.

For example, for a single user using E.164 format, enter +13035551212, alternatively enter +1303555xxxx to match all users with the +1303555 prefix.

4. The **Min** value is auto-populated based on the pattern.

5. The **Max** value is auto-populated based on the pattern.

6. Do not change the **SIP Domain** default of `-ALL-`.

> ⁂ **Note:**
>
> If you use multi-domain routing, see *Administering Avaya Aura® Session Manager* for information about what to enter in this field.

7. Select the Application Sequence for the **Origination Application Sequence** from the drop-down menu.

   The **Origination Application Sequence** tells Session Manager to invoke Avaya Breeze™ for the user when making calls. Use the Origination Application Sequence for Calling Party snap-ins.

8. Select the Application Sequence for the **Termination Application Sequence** from the drop-down menu.

   The **Termination Application Sequence** tells Session Manager to invoke Avaya Breeze™ for the user when receiving calls. Use the Termination Application Sequence for Called Party snap-ins.

9. To save your changes, click **Commit**.

Assign a Service Profile to a user or Implicit User Pattern

Users are associated with a Service Profile and not with individual snap-ins. Assign a Service Profile to a user in the following ways:

- Implicit users – Create an Implicit User Profile Rule that encompasses all users you want to use the Service Profile. Assign the Service Profile to that group. Users do not need to be administered on System Manager.

- Administered users – Assign the Service Profile to an individual user who is administered on System Manager. To use this method, any SIP or H.323 user the Service Profile is assigned to must be administered as an explicit user. In general SIP users are already administered in

System Manager as explicit users, but H.323 users may not be. Therefore, you may need to create a new user profile for a user you want to assign the Service Profile.

If a Service Profile is assigned to a user through both explicit and implicit administration, the explicitly assigned Service Profile takes precedence.

Related links

Assigning a Service Profile to implicit users on page 47
Creating a new user profile on page 48
Assigning a Service Profile to an administered user on page 49

Assigning a Service Profile to implicit users

Before you begin

You must create the Service Profile before it can be assigned.

Procedure

1. On System Manager, in **Elements**, click **Avaya Breeze™**.

2. In the left navigation pane, click **Configuration** > **Implicit User Profiles.**

3. Click **New** to create a new rule, or select a pattern and click **Edit** to change an existing rule.

4. In the **Service Profile** field select the Service Profile for these users.

5. In the **Pattern** field, specify the pattern as defined for Session Manager and Communication Manager digit routing.

   For non-SIP users, the dial pattern should be the same pattern format as used in the Routing Policy Dial pattern. The range includes users of the Service Profile. For SIP users, as a best practice use E.164 patterns to scope the SIP users either singularly or as a range. If that is not desired, use the Communication Address defined on **User** > **User Management** > **Manage Users** User Profile **Communication Profile** tab. The pattern range used can include both SIP and non-SIP users.

   The pattern must match, or be a subset of, the pattern administered for implicit sequencing.

   Enter "x" patterns at the end of the number as wildcards to match multiple users. For example, for a single user using E.164 format, enter +13035551212, alternatively enter +1303555xxxx to match all users with the +1303555 prefix.

   If multiple patterns match implicit user profile rules when a snap-in is invoked, the closest matching pattern is used.

6. Optionally revise the **Min** and **Max** values for the number of digits from the pattern to match. These fields auto-populate based on the pattern.

7. Type a description of the rule, typically a description of the group of users the rule defines.

8. Click **Commit** to save your changes.
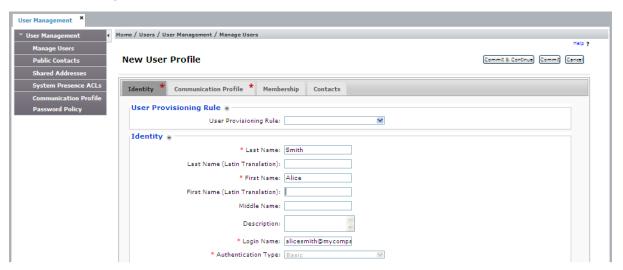
Related links

Creating a new user profile

Use this procedure to create a new explicit user in System Manager. This procedure is not required if you are using an implicit user profile rule to assign a Service Profile to users. It also is not required for users already administered as explicit users.

Procedure

1. On the System Manager **Home** page, under **Users**, select **User Management** > **Manage Users**.

2. Click **New**.

3. Click the **Identity** tab.

4. Enter the user's Last, First, and Login names.

   The login name is in the form of `handle@domain`.

5. Click the **Communication Profile** tab.

6. Enter the **Communication Profile Password** and confirm the password.

7. Create a new Communication Address.

   a. In the **Communication Address** table, click **New**.

   b. In the **Type** drop-down menu, select `Avaya E.164` or `Avaya SIP`.

   c. In the first part of the **Fully Qualified Address** field, enter a number that matches the **Pattern** in the Implicit User Rule page. E.164 numbers can have a maximum of fifteen digits and are usually written with a + prefix, for example, +15553091337.

This is the pattern that you created when administering implicit sequencing. Your user must fall in the implicit sequencing pattern range so that Avaya Breeze™ is invoked when a call is received or sent.

d. In the second field, select the domain for this user from the drop-down menu.

e. Click **Add**.

Assigning a Service Profile to an administered user

Before you begin

You must create the Service Profile before it can be assigned.

Procedure

1. On the System Manager web console, click **Users** > **User Management**.

2. In the left navigation pane, click **Manage Users**.

3. Select the check box by the appropriate user name.

4. Click **Edit**.

5. On the **Communication Profile** tab, scroll to the middle of the screen and select the **Avaya Breeze™ Profile** check box.

6. Select the **Service Profile** from the drop-down menu.

7. Click **Commit**.

Chapter 5: HTTP Security Administration

Administering HTTP Security

Administering a whitelist for HTTP Security

Procedure

1. On System Manager, in **Elements**, click **Avaya Breeze™**.

2. In the navigation pane, click **Configuration** > **HTTP Security**.

3. Select the cluster.

   > ⊛ **Note:**
   >
   > For Avaya Breeze™ Release 3.0 or earlier, select the **Legacy** option in the **Cluster** field. This option displays the preconfigured Whitelists.

4. Click the Whitelist tab.

5. Select the **Whitelist Enabled** check box.

   If you do not select the **Whitelist Enabled** check box, Avaya Breeze™ accepts HTTP or HTTPS requests from any system.

6. To add a new IP address to the Whitelist table:

   a. Click **New**.

   b. In the new row, type values in the **IP address** and the **Subnet Bits** fields.

7. Click **Commit**.

Related links

[HTTP Security field descriptions](#) on page 78

Administering client certificate challenge for HTTPS

Procedure

1. On System Manager, in **Elements**, click **Avaya Breeze™**.

2. In the navigation pane, click **Configuration** > **HTTP Security**.

3. Select the cluster.

4. Click the Whitelist tab.

5. Select the **Client Certificate Challenge Enabled** check box.

   The client certificate must be signed by a trusted certificate authority.

6. Click **Commit**.

Related links

HTTP Security field descriptions on page 78

Administering HTTP CORS security

Procedure

1. On System Manager, in **Elements**, click **Avaya Breeze™**.

2. In the navigation pane, click **Configuration** > **HTTP Security**.

3. Select the cluster.

   ⊛ **Note:**

   For Avaya Breeze™ Release 3.0 or earlier, select the **Legacy** option in the **Cluster** field. This option displays the preconfigured HTTP CORS.

4. Click the HTTP CORS tab.

5. Perform one of the following:

   • Select the **Allow Cross-origin Resource Sharing for all** check box to allow any server to make requests.

   • Clear the **Allow Cross-origin Resource Sharing for all** check box to limit access to administered servers.

6. Limit the receipt of requests by adding authorized servers to the **Host Address** list:

   a. Verify that the **Allow Cross-origin Resource Sharing for all** check box is cleared.

   b. Click **New**.

   c. In the **Host address** field, type the complete origin address of the server that you want Avaya Breeze™ to have access permission to.

      For example, if the origin is `xyz.com`, add `xyz.com` as an origin in the CORS list. If the origin is `ip:port`, add `ip:port` as an origin in the CORS list.

7. Click **Commit**.

Related links

HTTP Security field descriptions on page 78

Chapter 6: JDBC Resource Administration

JDBC Resource administration

JDBC resource providers and data source

Create and manage JDBC providers to create data sources for pre-existing, external snap-in database. Use the JDBC providers to upload drivers to the Avaya Breeze™ clusters, which enables the use of multiple database variants like Oracle, MySQL.

As a user, download the JDBC driver jar file that is compatible with the database version. Download this file from the database vendor website.

✳ **Note:**

JDBC providers or data sources created by using incorrect or incompatible jar files fail. Ensure that you use the correct jar file and the appropriate implementation class for the jar.

Use the JDBC jar file to create the JDBC provider resource. The JDBC provider creates the JDBC provider service, which is displayed on the Service Management page. Select and install the JDBC provider service on your cluster. After you install the provider, create the JDBC data source by using the provider. Ensure that you specify a unique JNDI name for the data source. You can access the data source using the JNDI name.

❗ **Important:**

After you create or modify a JDBC provider or a data source, you must restart all the Avaya Breeze™ servers in the cluster. To restart a server, on the Server Administration page, select the servers that you want to restart and click **Shutdown System** > **Reboot**.

Administering JDBC providers

Adding a JDBC provider resource

Procedure

1. On System Manager, in **Elements**, click **Avaya Breeze™**.

2. In the left navigation pane, click **Configuration** > **JDBC Provider**.

3. Click **New**.

4. On the JDBC Provider Editor page, configure the JDBC provider details.

5. Click **Commit**.

Related links

[JDBC Provider Editor field descriptions](#) on page 82

Editing a JDBC provider resource

Procedure

1. On System Manager, in **Elements**, click **Avaya Breeze™**.

2. In the left navigation pane, click **Configuration** > **JDBC Provider**.

3. Select the JDBC source provider that you want to edit.

4. Click **Edit**.

5. On the JDBC Provider Editor page, edit the provider details.

   ⊛ **Note:**

   You cannot edit all the fields in this page. For example, you cannot modify the jar path.

6. Click **Commit** to save the changes.

Related links

[JDBC Provider Editor field descriptions](#) on page 82

Deleting JDBC provider resources

Procedure

1. On System Manager, in **Elements**, click **Avaya Breeze™**.

2. In the left navigation pane, click **Configuration** > **JDBC Provider**.

3. On the JDBC Provider page, select the providers that you want to delete.

   ⊛ **Note:**

   You cannot delete a JDBC provider if the provider is installed on a cluster through a snap-in.

4. Click **Delete**.

Administering JDBC data source

Adding a JDBC data source

About this task

Use the **JDBC Source** option to configure the:

• JDBC resource used for the data source.

• Database properties for the data source.

- JNDI name for the data source.

Procedure

1. On System Manager, in **Elements**, click **Avaya Breeze™**.

2. In the left navigation pane, click **Configuration** > **JDBC Source**.

3. Click **New**.

4. On the JDBC Data Source Editor page, enter the details of the data source.

5. Click **Commit** to add the data source.

Related links

[JDBC Data Source Editor field descriptions](#) on page 83

Editing a JDBC data source

Procedure

1. On System Manager, in **Elements**, click **Avaya Breeze™**.

2. In the left navigation pane, click **Configuration** > **JDBC Source**.

3. Select the JDBC data source that you want to edit.

4. Click **Edit**.

5. On the JDBC Data Source Editor page, edit the data source details.

   You cannot edit all the fields on this page.

6. Click **Commit** to save the changes.

   ✱ **Note:**

   After you edit the data source for a cluster, you must restart all the servers in the cluster. On the Server Administration page, select the servers that belong to the cluster you need to restart. Click **Shutdown System** > **Reboot**.

Related links

[JDBC Data Source Editor field descriptions](#) on page 83

Deleting a JDBC data source

Procedure

1. On System Manager, in **Elements**, click **Avaya Breeze™**.

2. In the left navigation pane, click **Configuration** > **JDBC Source**.

3. Select the JDBC data source that you want to delete.

4. Click **Delete**.

Testing the connection using query validation

About this task

Use **Test Connection** to determine whether the data source you created is reachable. When you click **Test Connection**, the validation query that you have defined for the data source is executed.

Procedure

1. On System Manager, in **Elements**, click **Avaya Breeze™**.

2. In the left navigation pane, click **Configuration** > **JDBC Source**.

3. Select the JDBC data source whose connection you want to test.

4. Click **Test Connection**.

   The system displays a success or failure response after the validation query is executed.

Chapter 7: Geo Redundancy

Avaya Breeze™ with System Manager Geographic Redundancy

Terminology

The geographic redundancy section applies only if you use the System Manager geographic redundancy feature.

1. Element: An *element* is an instance of an Avaya Aura® network entity. System Manager manages elements such as a Session Manager server or a Avaya Breeze™ server in an Avaya Aura® network.

   > ✳ **Note:**
   >
   > A Avaya Breeze™ server is *managed* by either the primary System Manager instance or the secondary System Manager instance in a geographically redundant solution. This means that you can use the System Manager interface to administer Avaya Breeze™ clusters, administer Avaya Breeze™ platforms, load snap-ins, uninstall snap-ins, and run on demand maintenance tests.

2. Primary server: The first or the master System Manager server in a Geographic Redundancy set up that serves all the requests. The primary System Manager server is always in the *active* mode unless you turn off the server. In fail back cases, the primary System Manager instance might not be in the active mode.

3. Secondary server: The System Manager server that functions as a backup to the primary System Manager server. The normal mode of operation of the secondary System Manager server is the *standby* mode.

4. Active server: The mode of operation of the System Manager server where the server provides the full System Manager functionality.

5. Standby server: The mode of operation of the System Manager server where the server serves only authentication and authorization requests. In the standby mode of operation, the system supports limited Geographic Redundancy configuration and the inventory service.

6. *Geographic Redundancy-aware* elements are those elements of the Avaya Aura® solution that support the **Geographic Redundancy** feature, such as Avaya Breeze™ Release 3.0.

7. *Geographic Redundancy-unaware* elements are those elements of the Avaya Aura® solution that do not support the **Geographic Redundancy** feature, such as Avaya Breeze™ instances earlier than Release 3.0.

8. Geographic Redundancy replication: Geographic The Geographic Redundancy feature provides the following replication mechanisms to ensure consistency of data between the primary and the secondary System Manager servers: database replication, file replication, and LDAP replication. For more information, see *Administering Avaya Aura System Manager*.

Managing Avaya Breeze™ in a Geographic Redundancy solution

Either the primary or the secondary System Manager server manages Avaya Breeze™ servers in different geographic redundancy scenarios. It is important to understand which System Manager server manages each Avaya Breeze™ server. For more information, see *Geographic Redundancy Scenarios* in *Administering Avaya Aura System Manager*.

1. Determining the System Manager that manages each Avaya Breeze™ server:

Avaya Breeze™ release 3.0:

To view the System Manager server that manages a particular Avaya Breeze™ server, see the **Managed By** column in the **Inventory** > **Manage Elements** webpage. The status can be *Primary*, *Secondary*, or *Unknown*. The *Unknown* value indicates that the System Manager instance cannot get the status from the Avaya Breeze™ server. Select a Avaya Breeze™ server and click **Get Current Status** to refresh the status for that Avaya Breeze™ server.

Avaya Breeze™ earlier than release 3.0:

Avaya Breeze™ servers earlier than release 3.0 are not Geographic Redundancy-aware. These Avaya Breeze™ servers can be managed only by the primary System Manager. For these Avaya Breeze™ servers, the **Inventory** > **Managed Elements** webpage displays **Not Supported** in the **Managed By** column.

Related links

Avaya Breeze™ administration in a geographic redundancy environment

This section provides information about the Avaya Breeze™ administration for different Geographic Redundancy scenarios. This section also covers the considerations when you make administration changes such as loading, installing, and uninstalling snap-ins, managing clusters, and loading Service Profiles. See the *Applicability* section for a full list of the administration webpages that are applicable.

Sunny day scenario

In this case, the primary System Manager manages all the Avaya Breeze™ instances. The primary System Manager replicates administration changes to all the Avaya Breeze™ instances. The secondary server is in the standby mode and you cannot make any administration changes using the secondary server.

Rainy day scenario

In this case, the secondary System Manager manages all the Avaya Breeze™ servers. The secondary System Manager replicates the administration changes to all the Avaya Breeze™ servers. The primary server is offline and you cannot make any administration changes using the primary server.

Split-network scenario

In this case the primary and the secondary servers run in the active mode. The primary and secondary servers do not communicate with each other due to a network outage. Before making administration changes, the administrator must confirm the group membership using the **Inventory** > **Managed Elements** webpage. The administrator must perform the administration changes on the primary System Manager for the Avaya Breeze™ instances that the primary server manages. Similarly, the administrator must perform the administration changes on the secondary System Manager for the Avaya Breeze™ instances that the secondary server manages. Each System Manager replicates the administration changes to the respective Avaya Breeze™ servers. Administration changes must also be compatible with non-Avaya Breeze™ elements in the split network. For example, a SIP user added on System Manager should have Avaya Breeze™ Profile, Session Manager Profile and CM Endpoint Profile that reference the Avaya Breeze™, Session Manager, and Communication Manager elements managed by the same System Manager. In other words, the elements are all on the same side of the network split.

⚠️ **Caution:**

Before making administration changes, you must assess the extent of the enterprise network split. The network split results in partitioning of Avaya Breeze™ servers and other elements into two groups. The primary System Manager manages one group and the secondary System Manager manages the other group.

✴ **Note:**

After a split-network scenario you can restore changes made only in one of the two System Manager servers.

Split-network warning messages

The Avaya Breeze™ Server Administration page displays a warning message when the System Manager server detects that the administrator is configuring for a split-network scenario. The primary System Manager can detect the possibility of a split-network configuration if:

- The primary System Manager does not manage all the Avaya Breeze™ instances.
- The secondary System Manager is not reachable on the network.
- The secondary System Manager is active.

The secondary System Manager can detect the possibility of a split-network configuration if:

- The secondary System Manager is active.
- The secondary server does not manage all the Avaya Breeze™ instances.

When the system displays a warning message, click the **Avaya Breeze™ Management Status** link to go to the **Inventory** > **Manage Elements** webpage. In this webpage, view the status of the System Manager that manages each Avaya Breeze™ server. Click **Minimize** to hide the warning message.

Applicability

The following table lists all the Avaya Breeze™ administration related functionalities for the respective webpages. When you make administration changes using any of these pages, System Manager replicates these changes only to those Avaya Breeze™ servers that the System Manager manages.

Web page	Functionality	Notes
Avaya Breeze™ > **Server Administration**.	Add, edit, delete the Avaya Breeze™ servers.	
Avaya Breeze™ > **Cluster Administration**>	Add, edit, view, and delete Avaya Breeze™ clusters.	
Avaya Breeze™ > **Service Administration**	Load, install, uninstall and delete services.	
Avaya Breeze™ > **Configuration**	Change the Service Profile configuration, attributes configuration, Avaya Aura® Media Server configuration, HTTP requests configuration.	
Inventory > **Manage Elements**	Add, edit, or delete the Avaya Breeze™ servers	
User Management > **Manage Users**	Change the Service Profile.	

Related links

[Managing Avaya Breeze in a Geographic Redundancy solution](#) on page 57

Avaya Breeze™ Status and Maintenance

This section provides information on using a System Manager to view the Avaya Breeze™ status and perform the maintenance operations on Avaya Breeze™. For example, you can view the status of a Avaya Breeze™ on the **Avaya Breeze™** > **Dashboard** webpage, or run the maintenance tests on a Avaya Breeze™ server from the **Avaya Breeze™** > **System Tools** > **Maintenance Tests** webpage.

Sunny day scenario

Using the primary System Manager, view the Avaya Breeze™ system status and perform the maintenance operations. You cannot use the secondary server to view the Avaya Breeze™ system status or to perform the maintenance operations.

Rainy day scenario

Use the secondary System Manager to view the Avaya Breeze™ system status and to perform the maintenance operations. You cannot use the primary server to view the Avaya Breeze™ system status or to perform the maintenance operations.

Split-network scenario

You must view the Avaya Breeze™ status and perform the maintenance operations from the System Manager server that manages the Avaya Breeze™ server.

Applicability

The following table lists all the system status functions of Avaya Breeze™ and maintenance operation functions for the respective webpages. The functions listed are only available for the Avaya Breeze™ servers that the System Manager manages.

Web page	Functionalities	Notes
Avaya Breeze™ > Dashboard	• View the Avaya Breeze™ system status. • Accept or deny new services.	
Session Manager > **System Tools**	• Run the maintenance tests for Avaya Breeze™ instances. • Download zipped copy of the Avaya Breeze™ related SNMP MIBs..	
Inventory > **Manage Elements**	View and edit the trusted certificate configuration and the identify certificate configuration of a Avaya Breeze™ instance by clicking the **More Actions** button.	

Related links

[Managing Avaya Breeze in a Geographic Redundancy solution](#) on page 57

Fault management (alarming and logging) in a geographic redundant environment

This section provides information on viewing the Avaya Breeze™ alarms and logs in the primary and secondary System Manager servers.

Sunny day scenario

Both the primary and the secondary System Manager servers collect alarms from all the Avaya Breeze™ instances. You can view all the Avaya Breeze™ related alarms from the **Events** > **Alarms** webpage on the primary System Manager.

Collect logs for a Avaya Breeze™ server from the **Events** > **Logs** > **Log Harvester** webpage on the primary System Manager.

View Avaya Breeze™ audit logs from the **Events** > **Logs** > **Log Viewer** webpage on the primary System Manager. These logs provide the details of the administration changes made on the primary System Manager.

The secondary System Manager is offline. During the Sunny day scenario you cannot view or collect any logs on the secondary System Manager.

Rainy day scenario

The secondary System Manager collects alarms from all the Avaya Breeze™ instances. After you configure the secondary System Manager into the active state, view the following alarms from the **Events** > **Alarms** webpage:

- Alarms collected when the secondary server was in the standby mode.
- New Avaya Breeze™ related alarms.

Collect logs from a Avaya Breeze™ server by navigating to the **Events** > **Logs** > **Log Harvester** webpage on the secondary System Manager.

View the Avaya Breeze™ audit logs from the secondary System Manager by navigating to the **Events** > **Logs** > **Log Viewer** webpage. These logs provide details of the administration changes made after the activation of the secondary System Manager.

The primary System Manager is offline. During the rainy day scenario you cannot view or collect alarms from the primary System Manager.

Split-network scenario

In the split-network scenario, both the primary and the secondary System Manager collect alarms from any Avaya Breeze™ that are reachable on the enterprise network. View these alarms from the **Events** > **Alarms** webpage. If a Avaya Breeze™ server cannot connect to a System Manager because of the network split, the Avaya Breeze™ forwards all the logs to that System Manager when the network connectivity restores. Go to the **Inventory** > **Manage Elements** webpage to view the status of the network connectivity from the current System Manager to each Avaya Breeze™ instance.

View the logs collected from a Avaya Breeze™ server by navigating to the **Events** > **Logs** > **Log Viewer** webpage of either the primary or the secondary System Manager, whichever manages the Avaya Breeze™ server. You cannot collect logs from a Avaya Breeze™ that the current System Manager does not manage.

View the Avaya Breeze™ audit logs from both the primary and secondary System Manager by navigating to the **Events** > **Logs** > **Log Viewer** webpage. Each System Manager displays audit logs for the administration changes made on that System Manager after that server became active.

Related links

[Managing Avaya Breeze in a Geographic Redundancy solution](#) on page 57

Performance management in a geographic redundant environment

This section provides information on the performance data collection and the performance data analysis of Avaya Breeze™.

Sunny day scenario

The primary and the secondary System Manager collect the performance data from all the Avaya Breeze™ servers based on the configuration settings. The configuration settings are available on the **Avaya Breeze™** > **Performance** > **Data Collection** webpage of the primary System Manager. Analyze the data in the primary System Manager from the **Avaya Breeze™** > **Performance** webpage. You cannot analyze the performance data collected from the secondary System Manager.

Rainy day scenario

The secondary System Manager collects the performance data from all the Avaya Breeze™ servers based on the configuration settings on the **Avaya Breeze™** > **Performance** > **Data Collection** webpage of the secondary System Manager. Analyze the data on the secondary System Manager from the **Avaya Breeze™** > **Performance** webpage. You cannot analyze the performance data collected from the primary System Manager.

Split-network scenario

The primary and the secondary System Manager collect the performance data from all the Avaya Breeze™ servers that are reachable on the enterprise network. The system performs the performance data collection on each System Manager based on the settings configured on the **Avaya Breeze™** > **Performance** > **Data Collection** webpage of the System Manager.

> ✱ **Note:**
>
> You cannot collect the performance data from a Avaya Breeze™ server that is not reachable on the network from the System Manager. When the connectivity restores, the system resumes the performance data collection. Go to the **Inventory** > **Manage Elements** webpage to view the status of the connectivity from the current System Manager to each Avaya Breeze™ server.
>
> Both the primary and the secondary System Manager servers can analyze the performance data using the **Avaya Breeze™** > **Performance** webpage. A System Manager server cannot collect the performance data from a Avaya Breeze™ server that is not reachable. This results in data gaps for the unobtainable data until the connection to all the Avaya Breeze™ servers restores.

Related links

[Managing Avaya Breeze in a Geographic Redundancy solution](#) on page 57

Geographic Redundancy Replication and data restoration

Geographic Redundancy Replication

The Geographic Redundancy feature provides the following replication mechanisms to ensure consistency of data between the primary and the secondary System Manager servers:

- Database replication
- File replication
- LDAP (Directory) replication

The primary System Manager server continuously replicates the data with the secondary System Manager server. If the system does not replicate the data for a specific period of time that is configured in **Services** > **Configurations** > **Settings** > **SMGR** > **HealthMonitor**, the primary and the secondary System Manager servers raise alarms.

For more information on replication, see *Administering Avaya Aura® System Manager*.

Data restoration

In a Geographic Redundancy set up you must restore data when the primary System Manager server or the site fails. Restore the data from an old primary server or from the secondary server. In addition you may perform data restoration while replacing the primary or the secondary server, or while recovering the primary server from disaster. For more information on data restoration, see *Administering Avaya Aura® System Manager*.

> 😎 **Note:**
>
> When the primary server comes up after the server returns to the sunny day scenario, the alarms raised by the secondary server persist. You must manually clear the alarms raised by the secondary server in the rainy day scenario.

Related links

[Managing Avaya Breeze in a Geographic Redundancy solution](#) on page 57

Performing system verification tests

About this task

Use this procedure to verify that a Geographic Redundancy-enabled system is operating correctly in the *sunny day scenario*.

Procedure

1. To check the Geographic Redundancy status of the system, Go to the Geographical Redundancy webpage of the primary System Manager server and verify the configuration settings.

2. To view the Geographic Redundancy status, go to the **Geographic Redundancy** > **GR Health** webpage of the primary System Manager.

   For more information, see *Geographic Redundancy Health Monitoring* in *Administering Avaya Aura® System Manager*.

3. On the **Avaya Breeze™** dashboard, verify the status of each Avaya Breeze™ server.

4. Optionally, run the System Manager maintenance tests and the Avaya Breeze™ maintenance tests on the primary System Manager server. To run the maintenance tests, go to the **Avaya Breeze™** > **System Tools** > **Maintenance Tests** webpage.

   For more information, see *Maintenance Tests* in *Maintaining and Troubleshooting Avaya Breeze™*.

Chapter 8: User Interface description

Attribute Configuration field descriptions

Use this page to configure global attributes for a service, to configure attributes for a service within a service profile, or to configure attributes for a cluster.

Service Profiles tab

Use the fields on this tab to define values for attributes for a specific, selected Service Profile. The values that you specify in this tab overrides the default values specified in the cluster and global attributes.

Name	Description
Profile	The name of the service profile that will use the attributes configured on this page.
Service	A drop-down list of the services that are currently assigned to the selected profile.
Name	The names of the attributes that can be configured for this service.
Override Default	A check indicates you want to override the default value of the attribute. If the box is not checked, the default value is used.
Effective Value	If you override the existing value in this tab, the **Effective Value** displays the value you entered. Else the value displays the first of these to be set: the override value on the **Service Clusters** tab, the override value on the **Service Globals** tab or the default if there are no overrides.
Description	A description of the attribute.

> ✱ **Note:**
>
> If you override an attribute for a service at the cluster level for two different clusters, and the override is not at the service profile level, the system does not display the effective value. Instead the system displays the message *Effective value for the attribute cannot be displayed as it has been overridden for multiple clusters*.

Service Clusters tab

Use this tab to define the service attributes of the services installed on specific clusters. The values you specify in this tab will override the default values specified in the global service attributes.

Name	Description
Cluster	The name of the cluster that will use the attributes configured on this page.
Service	A drop-down list of the services that are currently assigned to the selected cluster.
Name	The names of the attributes that can be configured for this cluster.
Override Default	A check indicates you want to override the default value of the attribute. If the box is not checked, the default value is used.
Effective Value	If you override the existing value in this tab, the **Effective Value** displays the value you entered. Else the field either displays the override value on the **Service Globals** tab, or the default if there are no overrides.
Description	A description of the attribute.

Service Globals tab

Use this tab to define the service attributes of all the service profiles that use this service. When you install a service for the first time, the factory default value is used for each attribute of the service profile. Override the factory default value by using the **Service Globals** tab. You can override the service attribute values either at the service profile level or at the cluster level by configuring the attributes in the respective tabs.

Name	Description
Service	A drop-down list of the services you can select for which you can configure attributes.
Name	The names of the attributes that can be configured for this service.
Override Default	Select the check box to override the default value of the attribute. If the box is not checked, the default value is used.
Effective Value	If you override the existing value in this tab, this field displays the value you entered. Otherwise the system displays the default value.
Description	The description of the attribute.

Buttons

Button	Description
Cancel	If you navigated to this page from the Service Profile Editor page, clicking cancel returns you to that page. Otherwise, it resets the page forms and selections.
Commit	Saves changes made to both tabs of the Attribute Configuration page.

Related links

Avaya Aura® Media Server Configuration field descriptions

Use this page to assign the Media Server URI and to configure licenses for the Avaya Aura® Media Server.

✱ **Note:**

For complete instructions for deploying the Avaya Aura® Media Server, see *Deploying Avaya Breeze™.*

Name	Description
Media Server URI	The URI used by Avaya Breeze™ to connect to the Avaya Aura® Media Server.
Server IP	The IP address of each Avaya Aura® Media Server licensed for Avaya Breeze™.
License Status	Displays one of the following states: • Attempting Connection: Displayed any time a connection is being attempted to the Avaya Aura® Media Server. This could be for checking the license state or for attempting to set the license key. • Installed: A successful connection was made to the server and the license key was found. • Not Installed: A successful connection was made to the Avaya Aura® Media Server and the license key was not found. • Unable to Connect: There was a failure in attempting to connect to the Avaya Aura® Media Server.

Button	Description
New	Creates a new row in the Licensing table so that a new server IP address can be added.
Delete	Marks the selected server for deletion.
Reinstall License	Reinstalls the license with the current license file.
Commit	Saves any modifications to the Media Server URI. If a new Server IP address was added to the Licensing

Table continues…

Button	Description
	list, then an attempt is made to create the license key and install it on the server. Any Server IPs marked for deletion attempt to connect to the Avaya Aura® Media Server to remove the license key and are then removed from the list.

Cluster administration field descriptions

Name	Description
Details	The details of the cluster. You can view the Avaya Breeze™ instances and services assigned to the cluster.
Cluster Name	The unique name of the cluster.
Cluster IP	The IP address of the cluster. The **Cluster IP** value is applicable only for HTTP/HTTPS.
Cluster Profile	The type of cluster that you want to choose. The options are: • **Context Store** • **Core Platform** • **Engagement Assistant Speech** • **General Purpose** • **General Purpose Large** • **Work Assignment**
Cluster State	The state of the cluster. The options are: • Accepting state: The cluster can serve service requests. • Denying state: The cluster cannot serve services or calls.
Alarms	The number of alarms for the cluster. This value is displayed in the following format: *<critical + major alarm count>/<minor alarm count>/<warning alarm count>*.
Activity	The sum of active SIP, HTTP, and other custom-defined sessions of all the snap-ins installed on the Avaya Breeze™ servers in the cluster.

Table continues…

Name	Description
Cluster Database	The High Availability status between the active Avaya Breeze™ server and the standby Avaya Breeze™ server in a cluster. • A green background indicates that the connection between the active and the standby servers is up. • A yellow background indicates that the standby server is getting ready to take over if the need arises. • A red background indicates that the connection between the active and the standby server is down. • No background color and the **Disabled** value indicates that the cluster database is disabled. The **Cluster Database** displays: • The number of active components and the disk consumption in the following format: *<number of active connections>/<disk consumption>*. • **- - - -** if the server does not report the disk consumption. • **Disabled** if the cluster database is disabled.
Data Replication	The aggregated data replication status between all Avaya Breeze™ servers in a cluster and System Manager. The options are: • Green check mark: Indicates that the replication is successful. • Red cross icon: Indicates that one or more nodes have failed replication.
Service Install Status	The aggregated service installation status of all the Avaya Breeze™ servers in a cluster. Theoptions are: • Green check mark: Indicates that all snap-ins are installed. • Yellow exclamation icon: Indicates that the snap-in is either queued for installation or for downloading to Avaya Breeze™. If downloading to Avaya Breeze™ fails, the column displays a red cross with the `Transfer has failed` message. • Red cross icon: Indicates that one or more snap-ins have failed to initialize, run, or deploy.

Table continues…

Comments on this document? infodev@avaya.com

Name	Description
Tests Pass	The aggregated maintenance test result for all Avaya Breeze™ servers in the cluster. A green check mark indicates that all Avaya Breeze™ servers in the cluster have passed the maintenance tests.
Data Grid Status	The aggregate status of the data grid in the cluster. The options are: • Green: Indicates that the data grid status is up. • Yellow: Indicates that the status of one or more servers in the cluster is down. • Red: Indicates that the data grid status is down.
Overload Status	The overload status of the Avaya Breeze™ cluster. The options are: • Green check mark: Indicates that none of the servers in the cluster are in the overloaded state. • Red cross icon: Indicates that one or more servers are in the overloaded state.
Service URL	The list of cut-through URLs for the services installed on the Avaya Breeze™ cluster. If you have administered the cluster IP, that IP is used as the host for the URL. If not, one of the Avaya Breeze™ server IP is used as the host for the URL.

Server details

On the Cluster Administration page, click **Show** for a cluster to view the details of each server in the cluster.

Name	Description
Server Name	The name of the Avaya Breeze™ server.
Security Module	The status of the security module for the server.
Server Version	The version of the Avaya Breeze™ server.
Server State	Indicates whether the server is in the accepting or the denying state. not parallel
Alarms	The number of alarms for the server. This value is displayed in the following format: *<critical + major alarm count>/<minor alarm count>/<warning alarm count>*.
Activity	The sum of active SIP, HTTP, and other custom-defined sessions of all the snap-ins installed on the Avaya Breeze™ server.

Table continues…

Name	Description
Cluster Database	The state of the server in a High Availability database setup. This column is highlighted in: • Green when the active server, standby server, and the idle server are ready. • Yellow when the standby server is preparing. • Red when the active server and the standby server fail. • No background color and displays **---** when cluster database is disabled.
Cluster Database Connection	The status of the connection between the active server and the standby server in a high availability database scenario. • A green check mark indicates that the connection between the active and the standby servers is up. • A yellow exclamation mark indicates that the standby server is getting ready to take over if the active server goes down. • A red cross indicates that the connection between the active and standby servers is down. • No background color with the value **---** indicates that the cluster database is disabled.
Data Replication	The status of data replication between the Avaya Breeze™ server and System Manager. • A green check mark indicates that the replication is successful. • A red cross indicates that the replication failed.
Service Install Status	The service install status for the Avaya Breeze™ server. • Green check mark: Indicates that all the snap-ins are installed. • Yellow exclamation icon: Indicates that the snap-in downloading to Avaya Breeze™ is in progress. If downloading fails, the column displays the red cross icon with the `Transfer has failed` message. • Red cross icon: Indicates that one or more snap-ins failed to initialize, run, or deploy.
Tests Pass	The maintenance test result for the Avaya Breeze™ server.

Table continues…

Administering Avaya Breeze™
Comments on this document? infodev@avaya.com

Name	Description
Data Grid Status	The data grid status of the Avaya Breeze™ server. The status of the server is either Up or Down for the server.
Overload Status	The overload status of the Avaya Breeze™ server: • A green tick mark indicates that the server is not overloaded. • A red cross icon indicates that the server is in an overloaded state.

Button	Description
New	Adds a new Avaya Breeze™ cluster.
Edit	Displays or modifies the Avaya Breeze™ cluster attributes or modifies the cluster profile.
Delete	Deletes the Avaya Breeze™ cluster. You cannot delete legacy clusters.
Certificate Management > Install Trust Certificate (All Avaya Breeze™ Instances)	Opens the Install Trusted Certificate page, where you can download a trusted certificate to install Avaya Breeze™ servers in a cluster.
Certificate Management > Use Demo SIP CA (Security Module)	Assigns the demo SIP CA identity certificate for all Avaya Breeze™ servers in a cluster. **❗ Important:** The demo certificate is meant for lab setups and nonproduction environments only. Therefore, Avaya recommends that you do not use the demo certificate for the production system.
Cluster State > Accept New Service	Allows incoming calls and requests for the cluster that you select.
Cluster State > Deny New Service	Blocks incoming calls and requests for the cluster that you select.
Filter: Enable	Enables filtering of clusters on the basis of the cluster name, IP address, profile, state, alarms, and activity.
Refresh icon	Refreshes the values in the **Cluster Administration** table.

Icon	Description
	Indicates that the server is one of the lookup servers.
	Indicates that the server is the active load balancer.

Table continues…

Icon	Description
	Indicates that the server is the active load balancer, but it is unable to connect to the standby server.
	Indicates that this server is the standby load balancer.
	Indicates that the load balancing server is: • Transitioning over to the standby server. • Experiencing a connection failure. • In an error state.
A	Indicates an active cluster database.
S	Indicates a standby cluster database.

Cluster Editor field descriptions

General tab

Name	Description
Cluster Profile	The type of cluster. Possible values are: • **Context Store**: Product specific cluster profile for the Context Store snap-in. Minimum of 2 Avaya Breeze™ servers are required for this profile. • **Core Platform**: Closed cluster that supports up to 10 Avaya Breeze™ servers. Snap-ins that might be installed on this cluster profile include Presence Services and Call Park and Page. • **Engagement Assistant Speech**: Product specific cluster profile for the Engagement Assistant snap-in. • **General Purpose**: General purpose cluster profile. Minimum of 1 Avaya Breeze™ server is required for this profile. • **General Purpose Large**: An open cluster that supports up to 5 Avaya Breeze™ servers. This cluster profile mainly supports the Engagement Call Control solution. • **Work Assignment**: Product specific cluster for the Work Assignment snap-in.
Cluster Name	The unique name that you wish to provide for the cluster.

Table continues…

Name	Description
Cluster IP	The unique IP address assigned to the cluster. The IP address is used for HTTP load balancing. This field is mandatory if you select the load balancer check box. The **Cluster IP** field is optional if you do not enable load balancing.
Enable Cluster Database	The check box to enable Cluster Database. ✱ **Note:** You cannot clear the check box if snap-ins are installed on the cluster that require Cluster Database.
Enable Database Auto Switchover	The check box to enable auto switch over of clusters with two or more servers in a high availability database scenario. Select this check box if you want the standby server to automatically take over as the active server whenever the active server is down. ✱ **Note:** If you do not select this check box, you must manually enable the standby server to take over whenever the active server is down.
Description	The cluster description.

Cluster Attributes

Name	Description
The URL of the announcement to play during failover	Specify the URL of the announcement that is to be played during a failover.
Grid Password	The internal grid password.
Use secure grid?	Select this check box to secure all the grid communication.
Http or Https limit on connections	The maximum number of HTTP or HTTPS connections at a given time per client. For General Purpose Large clusters, this value must be larger than 3.
Http or Https traffic rate limit in bytes/sec	The rate limit on the HTTP or HTTPS traffic served per connection. For General Purpose Large clusters, this value must be larger than 300,000 bytes/second.
Only allow Https traffic	Select this check box to serve only HTTPS requests. By default this check box is selected.

Table continues…

Name	Description
Is load balancer enabled	Select this check box to enable load balancing for the cluster. Use load balancing if you want to scale the HTTP services without targeting a particular Avaya Breeze™ server.
Is session affinity enabled	Select this check box to enable session affinity for the cluster. With session affinity, a particular client is always served by the same back end server.
Default Identity for special make call cases	The default identity that is used for calls generating from Avaya Breeze™. If a user does not specify an identity then the value in this field is used.
The maximum number of Avaya Breeze Servers allowed in Cluster	The maximum number of Avaya Breeze™ servers that you can add to a cluster.
List of optional snap-ins including version	The list of optional snap-ins for a specific cluster profile type. The version of each optional snap-in is also included. This attribute applies to the **Core Platform** and **Work Assignment** cluster profiles only.
List of required snap-ins including version	The list of required snap-ins for a specific cluster profile type. The minimum required versions of each snap-in is also included.
Default SIP Domain	The default SIP domain for the cluster. If an Avaya Breeze™ snap-in does not include a domain in the addresses that the snap-in sends to the Call Manipulation API, this domain is appended to the address.
Use secure signaling for platform initiated SIP calls	Select this check box to use secure signaling to initiate WebRTC Snap-incalls, calls from snap-ins to individuals for playing announcements, and for snap-ins that initiate two party calls. This attribute is not applicable for call intercept scenarios.
Preferred Minimum Session Refresh Interval (secs)	The minimum periodic refresh interval for the SIP session.
Use early pre-answer media?	The cluster attribute that defines the pre-answer media mode. Select the checkbox to use *Early* pre-answer mode. Choose this setting to send a 183 session progress response in the early media phase. If you do not select this checkbox, *Connected* pre-answer mode is chosen. This is the default setting. *Connected* setting sends a 200 OK SIP response in the early media phase. This field is applicable for the General Purpose and General Purpose Large clusters only.

Table continues…

Name	Description
Use short replication interval?	Select this check box to use a short replication interval.
Work Flow Engine name	The name of the Engagement Designer snap-in Workflow Engine. This field is applicable only for the **General Purpose** cluster.

Servers tab

This tab has the following columns in two tables: **Assigned Servers** and **Unassigned Servers**. When you add a server to a cluster, the system displays the server under the **Assigned Servers** table for that cluster.

Name	Description
Name	The name of the Avaya Breeze™ server.
Version	The version of the Avaya Breeze™ server.
Description	The description of the Avaya Breeze™ server.

Services tab

Name	Description
Name	The name of the snap-in which may already be installed in a cluster, or available in the database.
Version	The snap-in version.
Action Pending	The actions that are pending for the snap-in. If no actions are pending, the system displays **None**.
Uninstall icon	The uninstall icon. If you select a snap-in and click **Uninstall**, then the snap-in is removed from the cluster after all the activity ceases.
Force Uninstall icon	The force uninstall icon. If you select a snap-in and click **Force Uninstall**, the snap-in is forcefully removed from the cluster without waiting to complete any pending actions.

Button	Description
Commit	Adds the cluster or saves the changes to the cluster attributes.
Cancel	Cancels your action. The system displays the previous page.

Avaya Breeze™ Instance Editor field descriptions

Use this page to create a new Avaya Breeze™ instance, or to edit the properties of an existing instance.

Name	Description
SIP Entity	The name of the Avaya Breeze™ SIP entity. For a new instance, select the SIP entity from the pull-down menu. For information about how to create the SIP Entity, see *Deploying the Avaya Breeze™*. ⊛ **Note:** You can edit the IP address of the SIP entity only from the **Routing** > **SIP Entity Administration** page.
Description	Your description of the Avaya Breeze™ SIP entity.
UCID Network Node ID	The unique, numeric node ID that is assigned to each Avaya Breeze™ server provisioned. As part of the Avaya Aura architecture, Avaya Breeze™ will add a Universal Call ID (UCID) on calls. The nodes that generate the UCIDs must have a unique node ID assigned to them.
Management Network Interface: **FQDN or IP Address**	The IP Address of the Avaya Breeze™ Management Network Interface. This is the same IP address entered during OVA deployment. For more information, see *Deploying the Avaya Breeze™*.
Security Module: **SIP Entity IP Address**	The IP address of the Avaya Breeze™ Security Module.
Network Mask	The Network Mask of the Avaya Breeze™ Security Module.
Default Gateway	The Default Gateway of the Avaya Breeze™ Security Module.
Call Control PHB	The Call Control PHB value for the Avaya Breeze™ instance. Valid entry can range between 0 to 63. The default value is 34. Call Control PHM provides scalable service discrimination in the Internet without per-flow state and signaling at every hop.
VLAN ID	The VLAN ID of the Avaya Breeze™ Security Module.

Event catalog configuration field descriptions

Name	Description
Family	The family to which the event belongs.
Family Display Name	The name of the Event Catalog family as it is displayed in the Avaya Engagement Designer.
Type	The type of the event.
Type Display Name	The name of the Event Catalog type as it is displayed in the Avaya Engagement Designer.
Version	The version of the event.
Schema Name	The name of the event schema. You can use the same schema for multiple event types.
Schema Type	The schema type. JSON is supported for this release.

Button	Description
View	Displays the details of the event.
Edit	Displays the edit custom event page for you to edit the details of the event.
New	Creates a new event.
Delete	Deletes a custom event.

Event Catalog Editor field descriptions

Name	Description
Family	The family to which the event belongs. The default families include Call Events, System Events, and Eventing Framework Events.
Family Display Name	The name of the Event Catalog family as it is displayed in the Avaya Engagement Designer.
Type	The type of the event. The type name must be unique within a family.
Type Display Name	The name of the Event Catalog type as it is displayed in the Avaya Engagement Designer.
Version	The version of the schema.
Schema Name	The name of the schema.
Schema Type	The schema type. JSON is supported for this release.
Schema	The schema for the default or the custom event.

Button	Description
Commit	Adds an event or edits the changes to a custom event.

HTTP Security field descriptions

Use this page to configure access permissions for HTTP requests to Avaya Breeze™.

Name	Description
Cluster	If you select a cluster from the **Cluster** drop-down list on HTTP Security page, the system lists all the configured hosts for the Whitelist tab and the HTTP CORS tab if any. If you configure any new hosts for selected cluster, the new hosts will be applicable only for the Avaya Breeze™ for that cluster. ✱ **Note:** The **Legacy** option shown in the **Cluster** drop-down list can be used to administer the existing configured Whitelist and HTTP CORS for Avaya Breeze™ Release 3.1 or earlier. For Legacy clusters on Avaya Breeze™ Release 3.1 or earlier, the configured trusted hosts for other clusters (white-list) will also be applicable as trusted hosts.

Whitelist tab

Name	Description
Whitelist Enabled	If you select this check box, Avaya Breeze™ for the selected cluster accepts HTTP or HTTPS requests only from the IP Addresses listed in the table. If you do not select this check box, Avaya Breeze™ for the selected cluster accepts any HTTP or HTTPS request that passes the optional client certificate challenge.
Client Certificate Challenge Enabled	If you select this check box, Avaya Breeze™ for the selected cluster accepts an HTTPS request only when a valid client certificate is presented. The client certificate must be signed by a trusted certificate authority.
Host Address	An IP address from which Avaya Breeze™ for the selected cluster will accept HTTP requests when Whitelist Enabled is checked.

Table continues…

Name	Description
Subnet Bits	The subnet bits used when a range of clients need to access Avaya Breeze™ for the selected cluster through HTTP. Subnet bits vary based on the value in the **IP Address** field.

HTTP CORS tab

Name	Description
Allow Cross-origin Resource Sharing for all	Select this check box to enable cross-origin resource sharing, where any JavaScript from any application server can send HTTP or HTTPS requests to Avaya Breeze™ for the selected cluster. You must use this setting only in the lab environment.
Host Address	The authorized IP addresses or domain names that generate HTTP requests to Avaya Breeze™ for the selected cluster using JavaScript.

Button	Description
New	Adds an IP address or a domain name.
Delete	Marks the selected IP addresses or domain names for deletion.

Related links

[Administering a whitelist for HTTP Security](#) on page 50

Implicit User Profile Rule Editor field descriptions

Use the Implicit User Profile Rule Editor page to define the dialing pattern parameters of the implicit users who are to be assigned to a Service Profile.

Name	Description
Service Profile	The name of the Service Profile used to invoke call intercept snap-ins for this group of implicit users.
Pattern	The pattern defined as Implicit Users in Session Manager. The Service Profile is linked with this pattern for call-intercept snap-in invocation. For non-SIP users, the dial pattern should be the same pattern format as used in the Routing Policy Dial pattern. For SIP users, as a best practice use E. 164 patterns to scope the SIP users either singularly

Table continues…

Name	Description
	or as a range. If that is not desired, use the Communication Address defined on **User** > **User Management** > **Manage Users** User Profile **Communication Profile** tab.
	Enter "x" patterns at the end of the string as wildcards to match multiple users.
	The pattern range can include both SIP and non-SIP users.
Min	The minimum number of digits to be matched from the pattern. Value is auto-populated based on the pattern.
Max	The maximum number of digits to be matched from the pattern. Value is auto-populated based on the pattern.
Desc	A description of the rule, typically a description of the group of users the rule defines.

Button	Description
Commit	Saves new profile or changes to the existing profile.

Related links

Implicit User Profiles field descriptions

Use Implicit User Profiles to assign groups of users to a service profile whether or not they are explicitly administered on System Manager . This allows you to invoke call intercept snap-ins for non-SIP users without adding them as users on System Manager.

Name	Description
Service Profile	The name of the Service Profile used to invoke call intercept snap-ins for this group of implicit users.
Pattern	The pattern as defined for Session Manager and Communication Manager digit routing. The range includes users to add to the Service Profile.
Min	The minimum number of digits to be matched from the pattern. Value is auto-populated based on the pattern.

Table continues…

Name	Description
Max	The maximum number of digits to be matched from the pattern. Value is auto-populated based on the pattern.
Desc	A description of the rule, typically a description of the group of users the rule defines.

Button	Description
Edit	Modifies the selected Implicit User Profile Rule.
New	Creates a new Implicit User Profile Rule.
Delete	Deletes the selected Implicit User Profile Rule.

Install Trusted Certificate field descriptions

Use this page to retrieve a trust certificate that will be used for all the Avaya Breeze™ clusters listed on the Cluster Administration page.

Name	Description
Select Store Type to install trusted certificate	Lists the different locations where the trusted certificate can be applied.
Please select a file	The trust certificate you have selected.

Button	Description
Browse	Click to browse to the location where the trusted certificate is stored.
Retrieve Certificate	Click to retrieve the certificate and view the certificate details on this page.

JDBC provider field descriptions

Name	Description
Name	The name of the resource provider.
Class	The name of the class file.
Jar	The JDBC jar file or library that you have uploaded.
Desc	The description of the resource provider as specified in the configuration page.

Button	Description
Edit	Edits the JDBC provider details.
New	Adds a new JDBC provider resource.
Delete	Deletes the JDBC provider that you select.
Filter: Enable	Filters the JDBC providers according to name, class, jar, or description.

JDBC Provider Editor field descriptions

Name	Description
Provider	The name of the JDBC provider
Class Name	The name of the class file in the jar.
Select Jar File	The jar file that contains the JDBC drivers. Select **Browse...** to upload the jar file from your local computer.
Description	The description for the JDBC provider.

Button	Description
Commit	Adds the JDBC provider or saves the changes to the JDBC configuration.
Cancel	Cancels the add or edit action.

JDBC data source field descriptions

Name	Description
Name	The name of the data source.
Cluster	The cluster with which the data source is associated.
JDBC Provider	The JDBC resource provider used for the data source.
JNDI Name	The JNDI name for the data source.
URL	The database URL for which the data source is created.
Description	The description for the data source.

Button	Description
Edit	Edits the JDBC data source details.
New	Adds a new JDBC data source.
Delete	Deletes the JDBC data source that you select.
Filter: Enable	Filters the data source according to name, cluster, provider resource, JNDI, URL and description.
Test Connection	Displays the success or failure response after you execute a validation query.

JDBC Data Source Editor field descriptions

Name	Description
Name	The name of the JDBC data source.
Cluster	The cluster on which the snap-in using the JDBC data source is installed.
JDBC Provider	The JDBC resource provider used for the data source. Select the JDBC provider from the list of the uploaded JDBC providers.
JNDI Name	The JNDI name for the data source.
URL	The database URL for which the data source is created.
User Name	The database server user name.
Password	The database server password.
Validation Query	The validation query for the data source. This is the query that is tested when you click **Test Connection** for a data source.
Description	The description for the data source.

Custom Properties

Add custom attributes for your data source by using this section. Click the **+** symbol to add an attribute. Click the **-** symbol to delete an attribute.

Name	Description
Name	The name of the custom attribute that you want to add for the data source.
Value	The value for the custom attribute.

Button	Description
Commit	Adds or edits the JDBC data source.
Cancel	Cancels the add or edit action.

Maintenance Tests field descriptions

Use this page to run maintenance tests. For a description of the tests, see *Maintaining and Troubleshooting Avaya Breeze™.*

Name	Description
Select Avaya Breeze™ to test	The name of the Avaya Breeze™ instance that you are testing. Select the instance from the drop-down menu.
Test Description	The name of the maintenance test.
Test Result	Indicates whether the test was successful or failed.
Test Result Time Stamp	When the test completed.

Button	Description
Execute All Tests	Click to run all maintenance tests in the list.
Execute Selected Tests	Click to run only the maintenance tests you have selected from the list.

Server Administration field descriptions

Use this page to:

- Add or edit an Avaya Breeze™ server.

- Shutdown or restart an Avaya Breeze™ server.

- Assign trust and identity certificates to the Avaya Breeze™ servers.

- Access information about the service status and maintenance tests for each Avaya Breeze™ server.

Name	Description
Name	The name of the Avaya Breeze™ server. Click the name to navigate to the Avaya Breeze™ Instance Editor page.
Cluster Name	The name of the cluster to which this Avaya Breeze™ server belongs.
Service Install Status	The status of the installed services. • A green check mark icon indicates all services have been installed. • An orange triangle icon indicates the service is in the process of installing or uninstalling.

Table continues…

Name	Description
	• A red X icon indicates a service has not downloaded properly or is not installed. Click on an icon to navigate to the **Service Status** page.
Tests pass	Maintenance test result. A green check mark indicates the test or tests passed. A red X indicates a test failed. Click the check mark or X to navigate to the **Maintenance Tests** page.
Alarms	The number of alarms raised for the Avaya Breeze™ server. This value is in the format <critical + major alarm count>/<minor alarm count>/<warning alarm count>.
System State	The current state of the Avaya Breeze™ server. The system states are: • Accepting • Denying
Security Module	The state of the Security Module. The states are Up, Down, and - - - (unknown).
Activity	The sum of active SIP, HTTP, and other custom defined sessions of all the snap-ins installed on the Avaya Breeze™ server.
License mode	The license mode of the Avaya Breeze™ server. It is mandatory that all the Avaya Breeze™ servers be in compliance with the license file, including the major release and the total number of Avaya Breeze™ servers. The possible license modes are: • ✅ **License Normal Mode**: A valid license file is installed. License errors are not found. The complete functionality is present for the Avaya Breeze™ instance. • ⚠️ **License Error Mode**: License error is seen in this mode. The Avaya Breeze™ instance is in a 30 day grace period during this mode. Complete functionality is available during the grace period. The system displays the warning icon along with the date and time of the grace period expiration in the **License Mode** column. • ❌ **License Restricted Mode**: The Avaya Breeze™ instance goes in to the restricted mode after the 30 day grace period expires. The Avaya Breeze™ server goes in to the Deny New Service mode. The

Table continues…

Name	Description
	server automatically returns to service when the server returns to the License Normal mode. For more information on determining and troubleshooting the license errors, see *Maintaining and Troubleshooting Avaya Breeze™*.
Overload Status	The overload status of the Avaya Breeze™ server. • A green check mark indicates that the server is not in an overloaded state. • A red cross icon indicates that the server is in an overloaded state.
Version	The version of the Avaya Breeze™ software that is installed on the Avaya Breeze™ server.

Button	Description
Edit	Edits the selected Avaya Breeze™ server. It launches the Avaya Breeze™ Instance Editor page.
New	Adds a new Avaya Breeze™ server. It launches the Avaya Breeze™ Instance Editor page.
Delete	Deletes the selected Avaya Breeze™ server.
System State > Accept New Service	Allows incoming calls or requests for the Avaya Breeze™ server you select.
System State > Deny New Service	Blocks incoming calls or requests for the Avaya Breeze™ server you select.
Shutdown System > Shutdown	Shuts down the Avaya Breeze™ server you select.
Shutdown System > Reboot	Reboots the Avaya Breeze™ server you select.

Icon	Description
	Indicates that the Avaya Breeze™ server is one of the lookup servers.
	Indicates that the Avaya Breeze™ server is the active load balancer.
	Indicates that the Avaya Breeze™ server is the active load balancer, but it is unable to connect to the standby server.
	Indicates that this Avaya Breeze™ server is the standby load balancer.
	Indicates that this load balancing server is: • transitioning over to the standby server • experiencing a connection failure

Table continues…

Icon	Description
	• in an error state
A	Indicates that the Avaya Breeze™ server is the Active server in a cluster database.
S	Indicates that the Avaya Breeze™ server is the Standby server in a cluster database.

Avaya Breeze™ Instance Status field descriptions

Use this page to check the status of the service for each Avaya Breeze™ instance and to see which Service Profiles include this service.

Service Status tab

Name	Description
Name	The name of the Avaya Breeze™ instances that are associated with the service.
Service Install Status	The status of the service on the listed Avaya Breeze™ instance.
Details	A description of any problems the service is having with running on the Avaya Breeze™ instance.
Last Audit	The time and date of the last successful service install audit.

Service Profiles Summary tab

Name	Description
Service Profiles	The names of the Service Profiles that include this service.

Related links

Service Management field descriptions

Use this page to load, install, uninstall, start, stop and delete a snap-in.

Name	Description
Name	The names of all snap-ins that have been loaded to the System Manager database.

Table continues…

Name	Description
Version	The version number of the snap-in. You can not install versions of the same snap-in if the version number is identical.
Preferred Version	The preferred version of a snap-in. In a cluster, if you choose a preferred version of a snap-in, that particular version is used by default. Even if you install a newer version of the snap-in, the preferred version is continued.
State	Indicates if the service is LOADED or INSTALLED. Loaded snap-ins have been loaded to the System Manager database. Installed indicates that a request has been sent to install the snap-in to the Avaya Breeze™ instances. This state is an aggregated state across various clusters. To check the actual status of the service installation, see the **Service Install Status** column on the Avaya Breeze™ Instance Status page.
Deployment Type	The snap-in deployment type. Possible values include Java, Workflow. JDBC Provider is the custom defined type. The deployment type value is stored in the database. You can filter and sort snap-ins based on the deployment type.
License Mode	The license mode that the snap-in is currently in. The possible license modes are: • **License Normal Mode**: The snap-in has a valid license file for normal operation of the snap-in. License errors are not present. • **License Error Mode**: License error is seen in this mode. The snap-in is in the thirty day grace period. There are no restrictions on the functionalities. You must install a valid license file for the snap-in to get it back to the normal mode. This column displays the grace period when the snap-in is in the error mode. After the grace period expires, the snap-in enters the restricted mode. • **License Restricted Mode**: The snap-in has exceeded the license grace period. If you do not install a valid license file, the snap-in is uninstalled from the Avaya Breeze™ clusters. The element manager raises a critical alarm. If you install the license file the snap-in returns to the License Normal mode. You must manually re-install the

Table continues…

Name	Description
	snap-in to any cluster from which the snap-in was uninstalled. • **Not Applicable**: Many services do not require a license file. The value for these services is **Not Applicable**.
Avaya Signed	Indicates whether the snap-in is Avaya signed. The column displays a green tick mark if the snap-in is signed by Avaya. Else, the column displays **Not Signed**. The supplier id for Avaya provided snap-ins is 10000000. The Supplier id uniquely identifies the supplier of a particular snap-in offered through the Avaya Snapp-store. All the snap-ins from a given supplier will have the same Supplier Id. This is mandatory for the snap-ins offered through the Avaya Snapp-store and is optional for other snap-ins.
Log Size(MB)	The size of the log file in MB.

Button	Description
Load	Launches the Load Service window so you can browse to the location of a service and load it. Acceptable services have a file extension of .svar.
Install	Queues up the selected service be installed on all the administered Avaya Breeze™ instances. Depending on the number of instances, it may take a few minutes to install on all instances
Uninstall	Uninstalls the selected service from all the Avaya Breeze™ instances. A dialog will display to ask if you want to force uninstall or not. A force uninstall terminates all active connections immediately. Not checking this will cause the service to wait for all active connections to drop before uninstalling the service.
Delete	Deletes the selected service. An **Installed** service can not be deleted. It must first be uninstalled. ⚠️ **Caution:** Deleting the last version of a service completely deletes all attribute settings and profile configuration of that service from the system.
Set Preferred Version	Sets the preferred version of a service. The preferred version of any service is cluster specific. You can set

Table continues…

Button	Description
	the same version of a service as the preferred version across several clusters.
Start	Starts or restarts the snap-in. Start snap-in is used after installing a higher version of a snap-in, or after making some configuration changes to the snap-in.
Stop	Stops the snap-in. Stop snap-in is used while installing a higher version of a snap-in.

Related links

Service Ports field descriptions

> ✳ **Note:**
>
> If you modify the port configuration for an Avaya-developed snap-in, you must start and stop the snap-in for the change to take effect.

Name	Description
Service	The list of Avaya-developed snap-ins that have default ports specified. Select the snap-in whose ports you want to configure.
Cluster	The list of clusters that are available.

Selected Service Ports

Name	Description
Port Name	The name of the assigned ports for the snap-in.
Override Default	Select this check box to override the default port value that is assigned to the snap-in.
Effective Port Value	The effective port value. When you specify an override value, that value becomes the effective port value.
Description	The description for the assigned ports.

All Service Used/System Reserved Ports

The table lists all the assigned ports for all the Avaya-developed snap-ins, both at the snap-in level and cluster level.

Name	Description
Port Name	The name of the port that is assigned to the snap-in.
Port Number	The port number of the port that is assigned to the snap-in.
Default Port Number	The default port number that is assigned to the snap-in.
Port Type	The port type. This port type can be **snapin** or **reserved**.
Service	The snap-in for which you have configured the ports.
Cluster	The cluster in which the snap-in with the assigned port is installed. If the port is assigned at the snap-in level, this field is blank.
Description	The description for the reserved or assigned port.

Button	Description
Commit	Assigns the port you have chosen to the snap-in.
Cancel	Cancels the port configuration action.

Service Profile Configuration field descriptions

Use this page to create, edit or delete a Service Profile.

Name	Description
Name	The administered name of the Service Profile.
Description	A description of the Service Profile.

Button	Description
Edit	Click to edit the selected Service Profile. Launches the Service Profile Editor page.
New	Click to create a new Service Profile. Launches the Service Profile Editor page.
Delete	Click to delete the selected Service Profile. You cannot delete a Service Profile if it still has a user assigned to it.

Related links

Creating a Service Profile on page 35

Service Profile Editor field descriptions

Use this page to create or edit a Service Profile, to add or remove services in a Service Profile and to define the invocation order of services in the profile.

Identity

Name	Description
Name	The name of the service profile.
Description	The description of the service profile.

All Services tab

Name	Description
Remove from Service Profile	Click the X in this column to remove a service from the service profile.
Name	The name of each service in the service profile.
Version	The version of each service in the service profile.
Description	The description of the service.

Service Invocation Details

Includes fields for: Calling Service Invocation Order; Called Service Invocation Order; and Service Not in an Invocation Order.

Name	Description
Order: First to Last	Provides arrows used to move services up and down in the invocation order. You can include up to five Call Intercept (calling or called party) services in a service profile.
Name	The name of each service in the service profile.
Version	The version of each service in the service profile.
Description	The description of the service.

Available Service to Add to this Service Profile

Name	Description
Add to Service Profile	Click **+** to add the latest version of a service to the service profile. Click **Advanced** to select the version of a service to add to the service profile. You can also set the preferred version of a service to a service profile from the **Add Service- Advanced** pop-up dialog box.

Table continues…

Name	Description
Name	The names of services that can be added to the service profile.
Description	The descriptions of services that can be added to the service profile.

Service Status field descriptions

Use this page to check the status of the snap-ins associated with the Avaya Breeze™ server you selected on the Server Administration page.

Name	Description
Name	The name of each snap-in that is associated with the selected Avaya Breeze™ sever.
Service Version	The snap-in version.
Service Install Status	The status of each snap-in. • A green check mark icon indicates that the snap-in is installed. • A yellow triangle icon indicates that the snap-in has been queued to be installed or uninstalled. • A red X icon indicates that the snap-in has failed to install or uninstall.
Service Checksum	A green check mark indicates that the checksum on System Manager matches the checksum on the Avaya Breeze™ server. A red X indicates that it does not.
Activity	The sum of active SIP, HTTP, and other custom defined sessions of a specific snap-in installed on a specific Avaya Breeze™ server.

Button	Description
Reinstall Service	Reinstalls the snap-in you selected.

SNMP MIB Download field descriptions

Use this page to download the SNMP MIB to a selected location.

Name	Description
File Name	The name of the SNMP MIB file.
Description	A description of the file and its contents.

Button	Description
Download	Launches a File Download window from which you can select a location to save the SNMP MIB file.

Index

Administering Avaya Breeze™