



IP Office Resilience Overview

Release 12.0
Issue 12
April 2024

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

"Hosted Service" means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, [HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO](https://support.avaya.com/licenseinfo) UNDER THE LINK "Avaya Terms of Use for Hosted Services" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE, BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE

TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

The Global Software License Terms ("Software License Terms") are available on the following website <https://www.avaya.com/en/legal-license-terms/> or any successor site as designated by Avaya. These Software License Terms are applicable to anyone who installs, downloads, and/or uses Software and/or Documentation. By installing, downloading or using the Software, or authorizing others to do so, the end user agrees that the Software License Terms create a binding contract between them and Avaya. In case the end user is accepting these Software License Terms on behalf of a company or other legal entity, the end user represents that it has the authority to bind such entity to these Software License Terms.

Copyright

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

Virtualization

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

Third Party Components

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

Service Provider

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

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 LLC.

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

Contents

| | |
|--|----|
| Chapter 1: IP Office Resilience | 7 |
| Resilience Features..... | 7 |
| When Does Failover Occur..... | 9 |
| When Does Failback Occur..... | 10 |
| System Configuration During Failover..... | 10 |
| Chapter 2: Resilience Features | 12 |
| User Resilience..... | 12 |
| Call Resilience (Media Preservation)..... | 13 |
| Hunt Group Resilience..... | 14 |
| System Conference Resilience..... | 15 |
| Fallback Twinning..... | 15 |
| IP Phone Resilience..... | 15 |
| Advanced IP Phone Resilience..... | 17 |
| DECT Resilience..... | 18 |
| DECT R4 Master Base Station Resilience..... | 19 |
| Hardware Resilience..... | 19 |
| one-X Portal for IP Office Resilience..... | 20 |
| Trunk Resilience..... | 21 |
| Virtual Server Resilience..... | 22 |
| Voicemail Resilience..... | 23 |
| Chapter 3: Design Considerations | 25 |
| System Capacities..... | 25 |
| Certificates and Domains..... | 26 |
| Installing Avaya root certificates on secondary servers and clients..... | 26 |
| Network Considerations..... | 27 |
| Emergency Call Routing..... | 28 |
| Licensing..... | 28 |
| Chapter 4: Configuring General Resilience | 30 |
| Using the Resilience Administration Wizard..... | 30 |
| Configuring resilience using the IP Office Manager wizard..... | 31 |
| IP Office Server Edition Options..... | 31 |
| IP Office Select Options..... | 32 |
| Adding Expansion to Expansion Lines..... | 33 |
| Using the Individual System Line Settings..... | 33 |
| Configuring resilience using the IP Office Manager line settings..... | 34 |
| Using IP Office Web Manager..... | 34 |
| SCN Resiliency Options..... | 34 |
| Configuration Update Scenarios..... | 37 |
| Adding an Expansion Server..... | 38 |

| | |
|--|-----------|
| Adding a Secondary Server..... | 38 |
| Chapter 5: Configuring IP Phone Resilience..... | 40 |
| Configuring the H323 Failback Mode..... | 42 |
| H323 Remote Worker Configuration..... | 42 |
| Vantage/Avaya Workplace Resilience..... | 43 |
| B179 Phone Configuration..... | 43 |
| B199 Phone Configuration..... | 44 |
| SIP Remote Extension Resilience..... | 45 |
| Configuring Expansion to Expansion Resilience..... | 45 |
| Chapter 6: Configuring the Location Based Resilience..... | 47 |
| Creating Locations..... | 47 |
| Setting a System's Location..... | 48 |
| Configuring a Line for Location Based Resilience..... | 49 |
| Adjusting a Location for Resilience..... | 49 |
| Setting an Extension's Location..... | 50 |
| Example..... | 50 |
| Chapter 7: Configuring Voicemail Resilience..... | 53 |
| Topology of voicemail resilience..... | 54 |
| Checking the System Voicemail Settings..... | 56 |
| Viewing and changing the voicemail settings..... | 57 |
| Checking the SMTP Settings..... | 58 |
| Configuring the SMTP Sender..... | 58 |
| SMTP Sender options..... | 59 |
| Configuring the SMTP Receiver..... | 59 |
| Configuring the Voicemail Failback Method..... | 60 |
| Setting the voicemail server failback method using the Voicemail Pro client..... | 60 |
| Setting the voicemail server failback method using web manager..... | 61 |
| Configuring Recording Archiving..... | 61 |
| IP500 V2 SCN Network..... | 62 |
| Chapter 8: Configuring one-X Portal for IP Office Resilience..... | 63 |
| Topology of portal resiliency..... | 64 |
| Configuring the IP Office Systems..... | 66 |
| Enabling Centralized CTI Link Mode..... | 66 |
| Configuring the one-X Portal for IP Office Servers..... | 67 |
| Chapter 9: Configuring WebRTC Resiliency..... | 68 |
| Chapter 10: Configuring DECT Resilience..... | 69 |
| Provisioned Base Station Configuration..... | 70 |
| Non-Provisioned Base Station Configuration..... | 71 |
| IP Office Configuration for DECT Resilience..... | 72 |
| Chapter 11: Configuring DECT Master Resilience..... | 73 |
| Configuring the IP Office..... | 73 |
| Configuring the Mirrored Base Stations..... | 74 |

| | |
|---|-----------|
| Activating the Master Base Station..... | 75 |
| Chapter 12: Configuring External Trunk Resilience..... | 76 |
| Configuring Breakout Controls..... | 76 |
| Adding a break out short code..... | 77 |
| Primary ARS Fallback to Secondary Trunks..... | 77 |
| ARS Alternate Route Overflow..... | 78 |
| ARS Out of Service Routing..... | 78 |
| Chapter 13: Configuring Media Preservation..... | 80 |
| Configuring the System Setting..... | 81 |
| Configuring the SIP Line Setting..... | 81 |
| Adjusting the Media Connection Preservation Time..... | 82 |
| Chapter 14: Monitoring Resilience..... | 83 |
| Resiliency Alarms..... | 83 |
| Resilience Indication on Phones..... | 83 |
| IP Office Line Status..... | 84 |
| one-X Portal for IP Office Status..... | 85 |
| DECT Trunk Resilience..... | 86 |
| Chapter 15: Additional Help and Documentation..... | 87 |
| Additional Manuals and User Guides..... | 87 |
| Getting Help..... | 87 |
| Finding an Avaya Business Partner..... | 88 |
| Additional IP Office resources..... | 88 |
| Training..... | 89 |

Chapter 1: IP Office Resilience

Resiliency refers to providing continued access to features during a failure of normal operation. This may occur due to an issue in the network such as the loss of a service, server, or network connection. The cause may be a temporary event, or it may indicate a more serious failure.

Important:

- When the use of resilience features occurs, the priority must always be to resolve why resilient mode was invoked.

This document mainly covers the set of features supported in an IP Office network using Linux-based primary and secondary servers. These features are supported in IP Office Server Edition , IP Office Select and IP Office Subscription networks.

Definitions

- **Resilience:**
 - The ability of a system to return to its normal state following a disturbance. It can also refer to the ability of the system to maintain some operation during the disturbance.
- **Failover:**
 - The process whereby, if a server or service fails or is no longer accessible, another one takes over its operation.
- **Failback:**
 - The process whereby, when an original server or service recovers or becomes accessible again, it resumes operation from any failover servers or services.

Related links

[Resilience Features](#) on page 7

[When Does Failover Occur](#) on page 9

[When Does Failback Occur](#) on page 10

[System Configuration During Failover](#) on page 10

Resilience Features

The following are the main resiliency features discussed in this document.

| Resiliency Feature | Summary |
|--------------------------------------|--|
| Call Resilience | Phones and trunks using direct media may be able to continue existing calls when resilience first occurs. Additional settings can be configured to ensure that the start of resilient mode operation does not interrupt those calls. |
| User Resilience | Information about the users on each system is distributed within the network. This allows users to resume activity when their normal home system is not visible for some reason. |
| Hunt Group Resilience | For hunt groups containing members from other systems in the network or members who have hot desked to other systems, hunt group resilience allows those members to still receive group calls even when the group's host system is not available for some reason. |
| Conference Resilience | For system conferences configured on a primary server, the secondary server hosts the conferences when the primary server is not available. |
| IP Phone Resilience (Basic) | Avaya IP phones registered with one system can automatically reregister with another system when resilience is required. |
| IP Phone Resilience (Select) | In addition to standard IP phone resilience, in IP Office Select and IP Office Subscription mode, IP Phone resilience can be to another expansion system based on location settings. Supported on IP Office Select only. |
| Voicemail Resilience | The IP Office Server Edition network can include two voicemail servers, one on the primary server and one on the secondary server. The two servers automatically synchronize during normal operation and can provide voicemail support for the other users during resilience. |
| DECT Resilience | DECT R4 uses an IP DECT trunk between the host IP Office server and the DECT master base station. DECT resilience allows the DECT system to be configured with an additional trunk to another IP Office server in the network. If the host server becomes unavailable for some reason, the failover trunk and server become active, allowing continued DECT operation. |
| DECT Master Resilience | Each DECT R4 system includes a configured as the master base station. Base station mirroring allows two base stations to be configured as the master. Whilst only one is active master, the other becomes active if the existing master becomes unavailable. |
| one-X portal Resilience | Both the primary and secondary server host copies of portal service with the service on the primary normally being the active one. However, in failback scenarios the secondary's service can become active until the systems recover. Supported on IP Office Select only. |
| WebRTC Resilience | On systems with Avaya one-X® Portal for IP Office resilience configured, resilience is also supported for user's using an Avaya WebRTC client to make and answer calls. Supported on IP Office Select only. |
| Virtualized Server Resilience | Virtual servers can use all of the standard IP Office resilience features. In addition, in IP Office Select mode they can alternatively use VMware's High Availability option. |
| Hardware Resilience | Servers hosted on PC platforms can use the PC manufacturer's supported options such as redundant power supplies, RAID drive configurations, etc. In addition, equipment and phones can use UPS support to continue operation. |
| External Trunk Resilience | Through individual system configuration, systems can use alternative routes for outgoing external calls. |

Related links

[IP Office Resilience](#) on page 7

When Does Failover Occur

| Resiliency Feature | When does failover occur |
|--------------------------------|--|
| User Resilience | <p>If the home system is not visible to its failover system for at least 3 minutes and IP desk phone resilience has begun.</p> <p>The failover delay ensures that resilience is not invoked when it is not required, for example when the home system is simply being rebooted to complete configuration changes.</p> |
| Hunt Group Resilience | Hunt group failover occurs at the same time as IP desk phone failover. |
| Conference Resilience | Conference resilience occurs at the same time as IP desk phone failover. |
| IP Phone Resilience | If the home system is no longer visible to the failover system for at least 3 minutes, the failover system will allow IP phones to re-register with it. This requires at least one physical IP desk phone to trigger failover. Phones with existing calls using media connection preservation do not failover until that call ends. |
| Voicemail Resilience | Voicemail failover is automatically triggered by IP desk phone failover coming into operation. It can also be manually triggered through System Status Application using the Activate Backup Server button. |
| DECT Resilience | The master base station regularly polls its normal IP Office server, by default every 30 seconds. If that IP Office is not visible for some reason, then by default, after 2 minutes the master base station switches to using its failover IP Office system. These timings can be adjusted, see Configuring DECT Resilience on page 69. |
| DECT Master Resilience | The standby master regularly polls the active master. If the active master becomes invisible for some reason, the standby master automatically becomes the active master. |
| one-X Portal Resilience | The failover portal becomes active immediately the primary portal is stopped or not visible. |

Related links

[IP Office Resilience](#) on page 7

When Does Failback Occur

| Resiliency Feature | When does failback occur |
|--------------------------------|--|
| User Resilience | After the home system has been visible again for more than 10 minutes. The failback delay helps ensure that the home system has fully recovered and is stable before starting failback. |
| Hunt Group Resilience | Hunt group failback occurs at the same time as IP desk phone failback. |
| IP Phone Resilience | After the home system has been visible again for more than 10 minutes, any idle phones begin to re-register with the home system. If for some reason, a phone is unable to connect to the home system, there is a 5-minute grace period, where the phone can be logged in to either the home or failover system. This is called "homeless prevention". Automatic failback to the home system is the default mode. For H323 IP phones, manual failback can be selected. In manual mode, the phone does not failback until either logged out or rebooted. |
| Conference Resilience | System conference failback occurs at the same time as IP desk phone failback. Existing active system conferences continue on the secondary, but new conferences start on the primary. |
| Voicemail Resilience | After the server is available again, failback occurs once all active voicemail calls have ended, and server SMTP synchronization is completed. However, manual failback or failback after a set time can be configured. Manual failback in control using System Status Application. |
| DECT Resilience | When the original IP Office system returns to normal operation, by default DECT control is automatically returned to it. The operation can be set to manual control if necessary, see Configuring DECT Resilience on page 69. In that case, control of failback is through the System Status Application. |
| DECT Master Resilience | When the active master is available again, it resumes control, and the other base station returns to being the standby master. |
| one-X Portal Resilience | The secondary portal returns control to the primary portal once it is available or visible again. |

Related links

[IP Office Resilience](#) on page 7

System Configuration During Failover

The following configuration limitations are applied during failover:

| Configuration Method | Details | | | | | | | | | | | | | | | | |
|--|---|----------|--|--------|-------------|------------|----------|----------|--|--|--|--|--|--|--|--|--|
| User telephony changes: | <ul style="list-style-type: none"> • During resilience, Avaya Workplace Client users configured for both mobile and internal twinning, cannot switch from mobile to internal twinning. • Any telephony setting changes, for example forward numbers and do not disturb, made during failover are lost following failback. | | | | | | | | | | | | | | | | |
| one-X Portal for IP Office Configuration: | <ul style="list-style-type: none"> • Any portal configuration changes a user makes whilst logged into the secondary portal during resilience are lost following failback. | | | | | | | | | | | | | | | | |
| DECT Configuration: | <ul style="list-style-type: none"> • No changes to the DECT configuration or additional handset subscriptions are allowed during failover. | | | | | | | | | | | | | | | | |
| IP Office Configuration: | <ul style="list-style-type: none"> • During failover of any system, you can still configure the remaining servers in the network. If the primary is in failover, this can be done through the secondary server. However, guest users and extensions supported by a system during failover are not visible in the configuration of their failover host. • Following failover, the system will prompt you as to what action to perform on unsynchronized configuration changes: <div data-bbox="506 768 1461 1096" style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p>Consolidation Report ✕</p> <p>Please review the non-consolidated items outlined below and take appropriate action.</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>System</th> <th>Item Type</th> <th>Record</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>IPOffice_5</td> <td>Location</td> <td>2: Paris</td> <td>Record is not configured on Primary System</td> </tr> <tr> <td> </td> <td> </td> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> <td> </td> <td> </td> </tr> </tbody> </table> <div style="text-align: right; margin-top: 10px;"> <input type="button" value="Reconsolidate"/> <input type="button" value="Update Primary"/> <input type="button" value="Cancel"/> </div> </div> <ul style="list-style-type: none"> - Reconsolidate: Update the configuration of all servers in the network. - Update Primary: Update the configuration of just the primary server. | System | Item Type | Record | Description | IPOffice_5 | Location | 2: Paris | Record is not configured on Primary System | | | | | | | | |
| System | Item Type | Record | Description | | | | | | | | | | | | | | |
| IPOffice_5 | Location | 2: Paris | Record is not configured on Primary System | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | |

Related links

[IP Office Resilience](#) on page 7

Chapter 2: Resilience Features

The following sections provide a summary of the operation of the main resiliency features discussed in this document.

Related links

- [User Resilience](#) on page 12
- [Call Resilience \(Media Preservation\)](#) on page 13
- [Hunt Group Resilience](#) on page 14
- [System Conference Resilience](#) on page 15
- [Fallback Twinning](#) on page 15
- [IP Phone Resilience](#) on page 15
- [Advanced IP Phone Resilience](#) on page 17
- [DECT Resilience](#) on page 18
- [DECT R4 Master Base Station Resilience](#) on page 19
- [Hardware Resilience](#) on page 19
- [one-X Portal for IP Office Resilience](#) on page 20
- [Trunk Resilience](#) on page 21
- [Virtual Server Resilience](#) on page 22
- [Voicemail Resilience](#) on page 23

User Resilience

Information about the users on each system is distributed within the network. That allows users to resume activity when their home system is not available.

- The system on which the user record was created holds their full user setting. That includes their telephony settings, personal directory and call log. This is that users' home system.
- All other systems in the network receive basic details of the users on other systems: the user's name, extension number, login code, home system and current (if hot-desked) system. This information is sufficient for other systems to correctly route calls to users when required.
- When a user logs in at another system, that system requests their full user settings for their home system.
- User resilience is configured by the **Backs up my IP Phones** settings, even if the system does not host any IP phones.

How does resilience affect this

- When the line from a system to a remote system is set to support IP phone resilience, then during normal operation that remote switch also receives a backup copy of all the system's user settings. That is regardless of the user's currently associated phone type.
- If for some reason, the user's home system is no longer visible on the network, after 3 minutes the failover system begins supporting any requests for the other system's user records.
 - For IP phone users, this allows them to continue using their phone once it has re-registered with the failover system.
 - For all users, it allows them to hot desk onto any phone on the failover system with their full settings. It also allows them to hot desk with their full settings onto phones on any other systems that are still in the network with the failover server.

When does user failover occur?

If the home system is not visible to its failover system for at least 3 minutes and IP desk phone resilience has begun.

The failover delay ensures that resilience is not invoked when it is not required, for example when the home system is simply being rebooted to complete configuration changes.

When does user fallback occur?

After the home system has been visible again for more than 10 minutes.

The fallback delay helps ensure that the home system has fully recovered and is stable before starting fallback.

Limitations

- Resilience fails if the failover server is restarted during failover. The backup user settings received by the failover server during normal operation are held in its non-permanent memory. If during failover operation the server is rebooted, those records are lost.
- Internal twinning is not supported during resilience failover.
- Fallback twinning is supported during failover. However, only after the phone has registered with the failover server.

Related links

[Resilience Features](#) on page 12

Call Resilience (Media Preservation)

Phones and trunks using direct media may be able to continue existing calls when resilience first occurs. Additional settings can be configured to ensure that the start of resilient mode operation does not interrupt those calls.

When using direct media, the audio part of the call is no longer routed via the telephone system. The telephone system is only involved when any of the parties in the call requires call signaling. This means that the call audio can continue without requiring the telephone system. So long as

the call data routing remains in place, the call may continue even if the telephone system is no longer visible for some reason. However, this is not guaranteed.

On calls involving links between systems, the invoking of resilience mode can potentially interrupt existing calls as re-registration occurs. Media connection preservation can help prevent this if required. This feature is supported for the following telephones on IP Office Release 9.1 or higher. It can be applied to calls between systems and via SIP trunks:

- IP Office Release 9.1+ : 9608, 9611, 9621, 9641
- IP Office Release 11.0+ : J139, J159, J169, J179, J189, Avaya Workplace Client

On those phones, if a call experiences end-to-end signaling loss or refresh failures but still has an active media path, call preservation allows the call to continue. While preserving a call, the phone does not attempt to re-register with its call server or attempt to failover to a standby call server until the preserved call has ended. The maximum duration of a preserved call is two hours after which it is automatically ended.

Calls on hold and calls to hunt groups are not preserved. Only the following call types are preserved:

- Connected active calls.
- Two-party calls where the other end is a phone, trunk or voicemail.
- Conference calls.

During a preserved call the only permitted action is to continue speaking and then end the call. The phone's softkey actions and feature menus do not work. Call preservation can be enabled at the system level and for individual trunks. The system level setting control use of call preservation on the system's IP Office lines and H.323 IP phones. All systems in the network must be configured for call preservation to ensure end to end connection support. By default, the system setting is also automatically applied to all SIP trunks. However, the trunk setting for each trunk can be individually altered.

When does media connection preservation occur?

This is an immediate feature applied to all qualifying calls currently in progress. It ends when the call ends.

Configuring media connection preservation

See [Configuring Media Preservation](#) on page 80.

Related links

[Resilience Features](#) on page 12

Hunt Group Resilience

For hunt groups containing members from other systems in the network or members who have hot desked to other systems, hunt group resilience allows those members to still receive group calls even when the group's host system is not available for some reason.

The trigger for hunt group failover is IP phone failover. Therefore, IP phone resilience must be configured for the system, regardless of whether the system has any registered IP phones.

When Does Hunt Group Failover Occur?

Hunt group failover occurs at the same time as IP desk phone failover.

When Does Hunt Group Failback Occur?

Hunt group failback occurs at the same time as IP desk phone failback.

Related links

[Resilience Features](#) on page 12

System Conference Resilience

For system conferences configured on a primary server, the secondary server hosts the conferences when the primary server is not available.

When Does Conference Failover Occur?

Conference resilience occurs at the same time as IP desk phone failover.

When Does Conference Failback Occur?

System conference failback occurs at the same time as IP desk phone failback. Existing active system conferences continue on the secondary, but new conferences start on the primary.

Related links

[Resilience Features](#) on page 12

Fallback Twinning

This feature is not linked to system resiliency. When enabled, fallback twinning redirects calls to the user's mobile twinning number when their host system cannot connect to their normal registered extension.

In system resiliency scenarios, fallback twinning is still supported for users failing over to another system but only after their extension has registered with the failover system.

Related links

[Resilience Features](#) on page 12

IP Phone Resilience

Avaya IP phones registered with one system can automatically reregister with another system when resilience is required.

IP Phone failover to an alternate gatekeeper is a native feature of many IP phones. However, it only works if the alternate gatekeeper allows registration. During normal operation, registration to the alternate gatekeeper is blocked. During failover it is allowed.

! Important:

- IP phone resilience requires at least 1 physical phone (H323 or SIP). It will not operate using just softphone clients. The failover registration of IP phones is also the trigger for user, hunt group and voicemail resilience.
- User changes to their settings during failover are lost after failback. In addition, the call history for calls during failover is also lost after failback.
- Calls through the system are disconnected by failover. Direct media calls may continue but this is not guaranteed. See [Call Resilience \(Media Preservation\)](#) on page 13.
- Resilience fails if the failover server is restarted during failover. The backup user and registered phone settings received by the failover server during normal operation are held in its non-permanent memory. If during failover operation the server is rebooted, those records are lost.
- Failover features require that the phones local to each system are still able to route data to the failover system.
- When an IP phone fails over, the failover system allows it to operate as a "guest". The guest phones do not consume any licenses.
- The features for user resilience are applied to the phone user.
- Hot desked users are automatically logged out. When their base extension fails back to the home system, the hot desked user is automatically logged in on that extension.
- For secure communication using TLS/SRTP, all IP Office systems must have an identity certificate that has been signed by the same trusted root CA.

Supported Telephones

| | |
|-------------------------------------|---|
| H.323 | 1600 Series, 9600 Series. |
| SIP | 1120, B179 ^[1] , 1140, B199 ^[1] , 1220, H175, 1230, J100 Series, K100 Series. |
| SIP Softphones^[2] | Avaya Workplace Clients |
| Others | All supported Avaya DECT R4 handsets. IP Office WebRTC SDK Clients ^[3] |

1. These Avaya SIP Phones require some manual configuration for resilience operation.
2. Softphone resiliency requires physical IP desk phone resiliency to have occurred.
3. Requires Avaya one-X[®] Portal for IP Office resilience to be configured.

When Does IP Phone Failover Occur?

If the home system is no longer visible to the failover system for at least 3 minutes, the failover system will allow IP phones to re-register with it. This requires at least one physical IP desk phone to trigger failover. Phones with existing calls using media connection preservation do not failover until that call ends.

The failover delay ensures that resilience is not invoked when it is not required, for example when the home system is simply being rebooted to complete configuration changes.

When Does IP Phone Failback Occur?

After the home system has been visible again for more than 10 minutes, any idle phones begin to re-register with the home system. If for some reason, a phone is unable to connect to the home system, there is a 5-minute grace period, where the phone can be logged in to either the home or failover system. This is called "homeless prevention".

Automatic failback to the home system is the default mode. For H323 IP phones, manual failback can be selected. In manual mode, the phone does not failback until either logged out or rebooted.

DHCP Resilience

When an IP Office provides extension data to the system that will back up the extensions it also provides DHCP data. The failover IP Office will provide DHCP service to the failover IP Phones - even if that system's DHCP is disabled. This operation relies on DHCP forwarding be allowed between networks or on the two servers being on the same subnet. A likely requirement is to have different SSONs for the two sets of phones.

Simultaneous Clients

If a user is in simultaneous mode on their home server when failover occurs, both their phones failover.

Limitations

- Resilience fails if the failover server is restarted during failover. The backup user settings received by the failover server during normal operation are held in its non-permanent memory. If during failover operation the server is rebooted, those records are lost.
- Internal twinning is not supported during resilience failover.
- Fallback twinning is supported during failover. However, only after the phone has registered with the failover server.

Related links

[Resilience Features](#) on page 12

Advanced IP Phone Resilience

Avaya IP phones registered with one system can automatically reregister with another system when resilience is required.

In addition to standard IP phone resilience, in IP Office Select and IP Office Subscription mode, IP Phone resilience can be to another expansion system based on location settings.

Related links

[Resilience Features](#) on page 12

DECT Resilience

DECT R4 uses an IP DECT trunk between the host IP Office server and the DECT master base station. DECT resilience allows the DECT system to be configured with an additional trunk to another IP Office server in the network. If the host server becomes unavailable for some reason, the failover trunk and server become active, allowing continued DECT operation.

Resilience operation occurs when the master base station cannot detect its normal host IP Office system, that is the IP Office system configured with an IP DECT line to it. During resilience, the failover IP Office system takes control and hosts the DECT extensions and users that were previously on its normal host system. However, no changes to the DECT configuration or additional handset subscriptions are allowed.

The failover IP Office system can host its own DECT R4 system using its own IP DECT line and master base station. When that is the case, it can only support failover from another system up to its maximum capacity of DECT users including its own DECT users (maximum 384 on an IP500 V2, 400 on a Linux based system).

DECT trunk resilience and base station mirroring can be combined.

For a provisioned installation

- The centralized phone book is still supported after failover. However, this does not apply to the phone book if being provided by an AIWS.
- An R is displayed on the 3700 Series DECT phones when they are in failover.
- By default DECT control and extensions automatically return to the primary IP Office system when it is available again.

For a non-provisioned installation

- The centralized phonebook is not supported during failover.
- The handsets do not display any indication that the system is in failover.

When Does DECT Failover Occur?

The master base station regularly polls its normal IP Office server, by default every 30 seconds. If that IP Office is not visible for some reason, then by default, after 2 minutes the master base station switches to using its failover IP Office system. These timings can be adjusted, see [Configuring DECT Resilience](#) on page 69.

When Does DECT Failback Occur?

When the original IP Office system returns to normal operation, by default DECT control is automatically returned to it. The operation can be set to manual control if necessary, see [Configuring DECT Resilience](#) on page 69. In that case, control of failback is through the System Status Application.

Related links

[Resilience Features](#) on page 12

DECT R4 Master Base Station Resilience

Each DECT R4 system includes a configured as the master base station. Base station mirroring allows two base stations to be configured as the master. Whilst only one is active master, the other becomes active if the existing master becomes unavailable.

For base station resiliency, two base stations are configured to function as 'mirrored' master base stations. One becomes the active master whilst the other becomes a standby master. If for any reason, the active master base station becomes unavailable, the standby master base station becomes the active master and continues DECT operation.

- The standby master base station is still able to handle call connections in the same way as normal base stations.
- Mirroring is not supported between compact and non-compact base stations. However, it is supported between a DECT Gateway and non-compact base station.
- Base station mirroring and DECT trunk resilience can be combined.

When Does DECT Master Failover Occur?

The standby master regularly polls the active master. If the active master becomes invisible for some reason, the standby master automatically becomes the active master.

When Does DECT Master Failback Occur?

When the active master is available again, it resumes control, and the other base station returns to being the standby master.

Related links

[Resilience Features](#) on page 12

Hardware Resilience

Servers hosted on PC platforms can use the PC manufacturer's supported options such as redundant power supplies, RAID drive configurations, etc. In addition, equipment and phones can use UPS support to continue operation.

Refer to the PC manufacturer's documentation for details of supported resilience option and their configuration.

In addition, the use of uninterruptible power supplies (UPS) can be considered. However, if doing so ensure that the UPS support also includes the data network and any PoE supplies.

Related links

[Resilience Features](#) on page 12

one-X Portal for IP Office Resilience

Both the primary and secondary server host copies of portal service with the service on the primary normally being the active one. However, in failback scenarios the secondary's service can become active until the systems recover.

The portal service is also installed by default on the IP Office Server Edition secondary server. This allows that secondary server to act as the portal server for users when, for some reason, the primary server is not available.

- Portal resilience is supported in IP Office Select and IP Office Subscription modes. That includes an IP Office Application Server in place of the primary or secondary server's portal service.
- Portal resilience is supported by the following client applications:
 - Avaya one-X[®] Portal for IP Office browser access.
 - Avaya one-X[®] Portal for IP Office call assistant.
 - IP Office SoftConsole presence indication.
- Resilience is only supported between primary and secondary servers running the same version of portal software.
- During normal operation (both servers running and connected), user and administrator changes made on the primary server are automatically synchronized to the secondary server. However, during resilience, changes made on either server are not synchronized and may be lost when the servers return to normal operation.
 - Scheduled conferences are currently an exception to the above. Conferences scheduled on the primary do not occur when running in failover. Conferences scheduled on the secondary are lost when failback occurs.

When Does Portal Failover Occur?

- If the primary server's portal service is not available, the portal service on the secondary server automatically becomes available.
- Users who were logged into the portal on the primary can login again on the secondary server.
 - If the primary IP Office service is still running, those portal users are automatically redirected.
 - If the user has not previously accessed the secondary portal server, they may need to accept the security certificate or create an exception which will interrupt automatic re-connection.
- The same applies for users who were logged into one of the portal clients such as the Outlook Plug-in
- New users wanting to login will have to use the address of the secondary server.
- On primary server IP Office failure: If the primary server's IP Office service stops for some reason, portal services are automatically transferred to the secondary server as above. Users belonging to that IP Office cannot update or delete personal contacts from the portal directory gadget.

- On network failure: If the network connection between the primary and secondary server fails for some reason, both portal servers become active and can be logged into. Again, user and admin changes on secondary portal server are not copied to primary when the network connection recovers. This is called "Standalone Mode".

When Does Portal Failback Occur?

- When the primary server's portal service is available again, the portal service on the secondary server stops supporting user login.
 - Users who were logged into the portal on the secondary are automatically re-directed to login again on the primary server.
 - Users who were logged into one of the portal clients such as the Outlook Plug-in are automatically connected to the primary server.
 - New users wanting to log in are redirected to the primary.
- On primary server IP Office recovery: When the primary server's IP Office service is available again, portal service support also returns to the primary server as above.

Related links

[Resilience Features](#) on page 12

Trunk Resilience

It is difficult to provide trunk guidance for resilience as the configuration of the external trunk routing and usage of every network varies greatly. We can only discuss general principles and factors that need to be considered, and show examples of the different methods that can be used.

- Special consideration must be given to the correct routing of emergency calls and indication of the caller location.
- Outgoing caller ID must be assessed. Rerouted calls may be blocked if the ID used to call out on an alternate trunk or site is not accepted by the line provider.

Default Call Routing

In an IP Office Server Edition deployment with no other changes than the addition of SIP trunks to the primary server:

- The default short code/ARS configuration on the primary server routes all external calls to any trunk/channel in outgoing line group 0.
- If a secondary server is present, its default short code/ARS configuration route all external calls to outgoing line group 99999 (to the primary).
- For any expansion server's present, their default short code/ARS configuration routes all external calls to outgoing line group 99999 (to the primary) if available, else to outgoing line group 99998 (to the secondary).

The above provides only minimal resilience. Expansion systems unable to see the primary but able to see the secondary can still make external calls if the secondary can still access the primary. In the case above, the simplest method of adding some further resilience would be to also add SIP trunks to the secondary server. The secondary server's ARS would be reconfigured to

use the outgoing line group of its own SIP trunks. Expansion systems unable to see the primary can then still make external calls using the secondary's SIP trunks.

Obviously, further resilience can be achieved by providing each location with its own trunks. This also simplifies the configuration of emergency call routing.

Using ARS Short Codes

By default, the short codes in an ARS form are used in the order entered in order to seize an available external trunk. Adding an additional short code however does not allow any further control, that route is automatically and immediately used if the preceding short code route is not available.

Using ARS Fallback

ARS forms can include an alternate route which redirects calls to another ARS form. See [ARS Alternate Route Overflow](#) on page 78.

Using ARS Out of Service

The out of service features of ARS allows calls to be redirected when it is known in advance that the trunks used by that ARS will not be available, for example for maintenance. See [ARS Out of Service Routing](#) on page 78

Using Breakout

The Breakout action is potentially useful during failover scenarios. It allows a telephone user to make a call as if dialing the digits on another system on the network and thus have their dialing routed by that system. The action can be assigned to short codes and to programmable buttons.

Related links

[Resilience Features](#) on page 12

Virtual Server Resilience

Virtual servers can use all of the standard IP Office resilience features. In addition, in IP Office Select mode they can alternatively use VMware's High Availability option.

VMware High Availability (HA) allows a virtual machine to be automatically re-established on another host machine if its normal host fails or detects a potential failure. For example:

- Host failures include power failure and ESXi kernel panic.
- A Linux operating system crash on the host server.

Backup is started up after a failure has been detected and takes approximately 10 minutes to complete. During the switch any unsaved data and active calls are lost.

Use of this feature is only supported for IP Office Select mode systems. It requires the customer data center to include multiple host servers and for those hosts to have access to the same separate datastore.

HA cannot be combined with the general IP Office resiliency features as they conflict. For example, if HA is enabled for a Server Edition primary server, no primary resources (phones,

hunt groups, voicemail server) can be supported using IP Office resilience failover to a Server Edition secondary.

Related links

[Resilience Features](#) on page 12

Voicemail Resilience

The IP Office Server Edition network can include two voicemail servers, one on the primary server and one on the secondary server. The two servers automatically synchronize during normal operation and can provide voicemail support for the other users during resilience.

By default, the primary and secondary servers each include the voicemail service. The method by which these are used depends on the type of network:

- **IP Office Server Edition:** In this mode, the voicemail server on the primary is active and provides voicemail services for the whole network during normal operation. The voicemail server on the secondary remains in standby mode. However, during resilience, the voicemail server on the secondary can become active and provide voicemail services. When the primary voicemail is available again, by default the secondary voicemail returns to standby mode.
- **IP Office Select:** For IP Office Select the voicemail services on the primary and secondary servers can be used in two ways as follows:
 - **Single active server/standby server:** The voicemail services are configured to operate in the same way as for IP Office Server Edition above. The secondary acts as the failover server for the primary.
 - **Dual active voicemail servers:** The voicemail services on both servers can be configured to be active at the same time during normal operation (this requires the secondary server to be configured with the appropriate voicemail licenses, etc.). In this mode, each server provides voicemail services for its own extensions and trunks. Each expansion system is configured to use either the primary or secondary voicemail server. Each voicemail server can act as the failover server for the others voicemail.

During resilience, the IP Office system informs Avaya one-X[®] Portal for IP Office and other applications which voicemail server to use. The same information is also applied to all user voicemail access.

Both voicemail servers are constantly synchronizing settings, callflow configurations and mailboxes during normal operation. This is done using SMTP connections between the two voicemail servers. Following resilience, the same connections are used to re-synch the servers. Following any voicemail resilience, normal operation is not resumed until SMTP synchronization has restarted.

When does voicemail failover occur?

Voicemail failover is automatically triggered by IP desk phone failover coming into operation. It can also be manually triggered through System Status Application using the **Activate Backup Server** button.

When does voicemail failback occur?

After the server is available again, failback occurs once all active voicemail calls have ended, and server SMTP synchronization is completed. However, manual failback or failback after a set time can be configured. Manual failback in control using System Status Application.

How is resilient voicemail operation configured?

1. The settings of the IP Office lines between the primary and secondary are used to indicate whether resilience is required. See [Configuring General Resilience](#) on page 30 .
2. The SMTP settings of the voicemail servers are configured to ensure synchronization of settings between the servers during normal operation.
3. The method by which a server providing active resilience returns to non-resilient mode operation (manual, graceful or automatic) is configurable through the voicemail server settings.

Related links

[Resilience Features](#) on page 12

Chapter 3: Design Considerations

The following factors should be kept in mind when planning the resilience operation of a network.

- The failover registration of IP phones is also the trigger for user, hunt group and voicemail resilience. That IP phone resilience requires at least 1 physical phone (H323 or SIP). It will not operate using just softphone clients.

Related links

[System Capacities](#) on page 25

[Certificates and Domains](#) on page 26

[Network Considerations](#) on page 27

[Emergency Call Routing](#) on page 28

[Licensing](#) on page 28

System Capacities

When using a server as the failover destination, you must ensure that it has sufficient supported capacity for that role. That includes not just capacity to support the additional users and extensions when providing resilience but also the additional calls, hunt groups, etc. This is all in addition to its existing normal capacity requirements.

For system capacity details, refer to the [Avaya IP Office™ Platform Guidelines: Capacity](#) document.

Failover Server Total IP Phone Capacity

When added to the remote server's extensions and users during resilience, the total numbers must be within the remote server's total supported capacity (and any other specific limit for the extension type). That also includes any other systems in resilience to that remote server at the same time. Extensions and users beyond the supported capacity do not receive resilience support.

Failover Server Total IP DECT Capacity

When added to the remote server's local extensions and users during resilience, the total numbers must be within the remote server's IP DECT and total supported capacities. That also includes any other systems in resilience to that remote server at the same time. Extensions and users beyond the supported capacity do not receive resilience support.

Related links

[Design Considerations](#) on page 25

Certificates and Domains

For resilience to work, all servers within the network must be part of the same domain.

For secure communication using TLS/SRTP, all IP Office systems must have an identity certificate that has been signed by the same trusted root Certificate Authority (CA).

Note:

It is important that the certificate created by a root CA has entries for DNS:<mySIPDomain>,DNS:<myFQDN.com>,IP:<IP address>, URI:sip:<IP address>, DNS:<IP address>.

You can also install Avaya root certificates on the secondary server and client computers to establish Avaya Inc. as a trusted CA.

Related links

[Design Considerations](#) on page 25

[Installing Avaya root certificates on secondary servers and clients](#) on page 26

Installing Avaya root certificates on secondary servers and clients

Procedure

1. Using a web browser, log in to your primary IP Office server's web control menus (browse to **Platform View** within web management).
2. Click **Settings**.
3. Under **Certificates**, select the **Create certificate for another machine** check box and provide the following information:
 - a. In **Subject Name** enter the IP Office's fully qualified domain name (FQDN).
 - b. In **Subject Alternative Names** provide the following information, separated by a comma: DNS: <FQDN>, IP: <IP address of IP Office LAN1>, IP: <IP address of IP Office LAN2 or public IP address if remote clients are involved>.

For example: DNS:abc.avaya.com, IP:123.123.1.1, IP:321.321.2.2
 - c. In **Password** export password for the identity certificate.

This password is required later when uploading the certificate to the designated server.
4. Click **Generate** to create the certificate.

A pop-up message appears.

5. Click the link in the message to download and save the certificate in the .p12 format.
6. You need to upload the saved certificate file to the IP Office secondary server.
 - a. In IP Office Manager, go to the security settings of the secondary and then navigate to **System > Certificates**.
 - b. Click **Set** and then, in the **Certificate Source** dialog box select **Import** certificate from file and click **OK**.
 - c. Select the saved .p12 certificate, click **OK**, and then click **Save**.
7. Log in to the primary server's web control menus and download the root certificate.
8. Install this root certificate in the systems where required.

Related links

[Certificates and Domains](#) on page 26

Network Considerations

The default arrangement of IP Office lines in an IP Office Server Edition and IP Office Select network is for each server to have a line to the primary server and, if present, a line to the secondary server. In return, the primary and secondary servers have lines to each expansion system. This is referred to as a 'double-star' configuration.

Data Routing vs IP Office Routing

The IP Office Server Edition network relies on the customer's data network which routes the traffic of the IP Office lines. However, the routes between sites within that data network may not necessarily match the configured IP Office lines. This can cause scenarios where when failover occur resilience features are not accessible to users.

- **Unable to access failover servers:**

The use of resilience features assumes that there is still a data network between sites even if the server at that site is in failover. If the cause of failover at a user's home server site also affects the data network, resilience features at the failover server are still invoked. However, users at the home site are isolated from the failover server and so receive no support.

For example:

- **Data Network Failure:**

The expansion server at site B host Avaya IP phones and is configured to failover to the primary server at site A. Suppose the data connection between the two sites fails for some reason.

- Site A cannot see the server at site B and so starts failover support for site B.

- At site B, the result depends on whether the data network failure is affect traffic with the site and or traffic to other sites.
 - If the IP phones can still see the server at site B, they continue operating with it. However, the users will not be able to access services provided from site A such as voicemail and Avaya one-X[®] Portal for IP Office.
 - If the IP phones cannot see the server at site B, they try to failover to site A. However, the lack of data network between sites prohibits that.

- **Network Blocked:**

There are scenarios where users can become network blocked. For example, if an IP phone is not able to see its home server it will attempt to reregister with its failover server. However, if the failover server is able to see the home server, it will not support failover of the phone.

Data Network Resilience

Resilience of the data network should be considered in conjunction with IP Office resilience. For example:

- Ensuring that the data network routes between sites are such that traffic has alternate routes.
- Ensuring that the data network equipment is supported by UPS and similar backup power supply options.

Related links

[Design Considerations](#) on page 25

Emergency Call Routing

- Special consideration must always be given to ensure the correct routing of emergency calls, especially in regard to identifying caller location.
- Outgoing caller ID must be assessed. Rerouted calls may be blocked if the ID used to call out on an alternate trunk or site is not accepted by the line provider.

Related links

[Design Considerations](#) on page 25

Licensing

If the license or subscription server being used by the network becomes unavailable for some reason, the individual systems within the network enter a 30-day grace period.

This operation is automatic and does not require any configuration. The server acting as host to guest users and extensions during failover does not require any additional licenses or subscriptions.

- **Voicemail Licenses:**

The primary server's voicemail license and subscription rights are honored by the secondary server's voicemail.

- IP Office Media Manager is not accessible during failover of the primary server. However, if running, the secondary voicemail will continue supporting VRL recording. Those recordings are collected from the secondary server by the primary following restoration of normal operation.
 - Note that for PLDS licenses dual active voicemail configurations, both the primary and secondary servers require a Media Manager license during normal operation for resilience support.
- For IP Office Select systems, during normal operation, the primary and secondary voicemail servers are assigned voicemail port licenses from the total pool available.

- **Extension and User Profile Licenses:**

During failover, users and extensions maintain their previously licensed or subscribed rights.

- **Other Licenses and Subscriptions:**

Other licenses and subscriptions are specific to the system to which they have been issued. They do not migrate during failover.

- **License Grace Period:**

If the primary server has failed, the license on all other servers enter the 30-day grace period state.

Related links

[Design Considerations](#) on page 25

Chapter 4: Configuring General Resilience

This section covers the application of general resiliency settings between systems.

Important:

User and phone resilience requires at least 1 physical phone (H323 or SIP) included in the configuration for resilience. User resilience will not operate using just softphone clients.

Related links

[Using the Resilience Administration Wizard](#) on page 30

[Adding Expansion to Expansion Lines](#) on page 33

[Using the Individual System Line Settings](#) on page 33

[Configuration Update Scenarios](#) on page 37

Using the Resilience Administration Wizard

The solution wizard allows quick selection of the general resilience settings for all servers in the network.

• Failover Server Total IP Phone Capacity:

When added to the remote server's extensions and users during resilience, the total numbers must be within the remote server's total supported capacity (and any other specific limit for the extension type). That also includes any other systems in resilience to that remote server at the same time. Extensions and users beyond the supported capacity do not receive resilience support. See [System Capacities](#) on page 25

• Reboot Required:

For 1600 and 9600 Series phones and Avaya SIP softphone clients, changing the failover server for IP phones requires the phone to be restarted in order to pick up changes to its failover server address.

• Manual Phone Configuration Required:

For 1100 and 1200 Series phones, B179 and H175 telephones; the telephone must be manually configured with the address details of its failover server.

• IP DECT Phone Resilience:

The solution wizard does not include the configuration of IP DECT resilience. To configure that configure resilience using the individual line settings

! Important:

- Using the resiliency administration wizard overrides any lines configured for location-based administration

Related links

[Configuring General Resilience](#) on page 30

[Configuring resilience using the IP Office Manager wizard](#) on page 31

[IP Office Server Edition Options](#) on page 31

[IP Office Select Options](#) on page 32

Configuring resilience using the IP Office Manager wizard

Procedure

- Using IP Office Manager, receive the configuration from the primary server.
- If already in the configuration, click on **Solution** in the navigation tree on the left.
- Check that all the expected servers are listed as having their configuration present at the bottom of the screen and that each has a **Bothway** link to the primary and, if present, secondary server.
- Click the **Resiliency Administration** link on the right. The options shown vary depending on the types of servers within the network, for example whether IP Office Select or not, and whether there are expansion servers.
- Select the general resilience options that you want applied between systems in the network. See [IP Office Server Edition Options](#) on page 31 or [IP Office Select Options](#) on page 32.
- Click **OK**.
- Save the changes.

Related links

[Using the Resilience Administration Wizard](#) on page 30

IP Office Server Edition Options

A menu similar to the following is displayed for an IP Office Server Edition network.

- Backup Primary Server IP Phones, Hunt Groups, and Voicemail on Secondary Server
- Backup Secondary Server IP Phones and Hunt Groups on Primary Server
- Update Expansion System IP Phones backup settings

| System Name | IP Address | Backup on Primary | Backup on Secondary |
|-------------|--------------|-------------------------------------|-------------------------------------|
| All Systems | | <input type="checkbox"/> | <input type="checkbox"/> |
| IPOffice_3 | 192.168.46.1 | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| IPOffice_5 | 192.168.0.48 | <input checked="" type="checkbox"/> | <input type="checkbox"/> |

- Backup Primary Server IP Phones, Hunt Groups and Voicemail on Secondary Server:**
If selected, this enables IP phone, hunt group and voicemail resilience from the primary

server to the secondary. Note that IP DECT support also requires configuring DECT trunk resilience . If not selected, all server resilience settings are disabled.

- **Backup Secondary Server IP Phones and Hunt Groups on Primary Server:** If selected, this enable IP phone and hunt group resilience from the secondary server to the primary. Note that IP DECT support also requires configuring DECT trunk resilience . If not selected, all server resilience settings are disabled.
- **Update Expansion System IP Phones backup settings:** When selected, the resilience settings of the existing expansion systems can also be seen and adjusted. This allows the selection of either the primary or secondary server as the remote server for each expansion's resilience. Selecting a server enables IP Phone (standard and IP DECT) and hunt group resilience. Not selecting an option disables all resilience settings for the expansion system.

Related links

[Using the Resilience Administration Wizard](#) on page 30

IP Office Select Options

A menu similar to the following is displayed for an IP Office Select network.

- Backup Primary Server IP Phones, Hunt Groups, Voicemail and one-X Portal on Secondary Server
- Backup Secondary Server IP Phones, Hunt Groups and Voicemail on Primary Server
- Update Expansion System IP Phones backup settings

| System Name | IP Address | Backup Phones | Backup Huntgroups | Resilient To |
|-------------|--------------|-------------------------------------|-------------------------------------|---|
| All Systems | | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | |
| Expansion1 | 192.168.46.1 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Primary <input type="button" value="v"/> |
| Expansion2 | 192.168.48.1 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Expansion1 <input type="button" value="v"/> |

- **Backup Primary Server IP Phones, Hunt Groups, Voicemail and one-X Portal on Secondary Server:** If selected, this enables IP phone, hunt group, voicemail and portal resilience from the primary server to the secondary. Note that IP DECT support also requires configuring DECT trunk resilience , portal support also requires configuring one-X Portal for IP Office resilience . If not selected, all resilience settings for the expansion are disabled.
- **Backup Secondary Sever IP Phones, Hunt Groups and Voicemail on Primary Server:** If selected, this enables IP phone, hunt group, voicemail and portal resilience from the secondary server to the primary. Note that IP DECT support also requires configuring DECT trunk resilience , portal support also requires configuring one-X Portal for IP Office resilience . If not selected, all resilience settings for the expansion are disabled.
- **Update Expansion System IP Phones backup settings:** When selected, the resilience settings of the existing expansion systems can also be seen and adjusted. This allows the selection of the primary or secondary server as the remote server for each expansion's resilience. If additional lines have been added between the expansion systems , then selection of another expansion is also possible. Not selecting an option disables those resilience settings for the expansion system.

Related links

[Using the Resilience Administration Wizard](#) on page 30

Adding Expansion to Expansion Lines

About this task

For IP Office Select, you can link expansion systems and enable resiliency between those systems. Note that this assumes that the customer also has data routing between the sites.

You must still ensure that the failover system has sufficient capacity to host the additional extensions and users during failover.

This process creates reciprocal IP Office lines between the selected expansion systems.

Procedure

1. Open Manager and log in to the primary server.
2. On the **Solution** page, on the left under **Link** click **Expansion System**.
3. Select the expansion systems to link.
4. Under **Line Type**, select the type of IP Office line:
 - **SCN-Websocket (Secure)**: Recommended for security and NAT traversal.
 - **SCN-Websocket**: Supports NAT traversal with limited security.
 - **SCN**: Legacy SCN line. Not recommended for new deployment.
5. If the **Link Type** is set to one of the web socket options, enter a web socket password.
6. Click **OK**.
7. The lines created in the configuration of each system are defaulted to medium security. If this needs to be changed, edit the individual line settings.
8. Save the configuration.
9. Use System Monitor to confirm the operation of the new lines between the two expansion systems.

Result

You can now use the resilience wizard or individual line settings to configure resilience between expansion systems.

Related links

[Configuring General Resilience](#) on page 30

Using the Individual System Line Settings

The solution wizard automatically applies the selected options to the appropriate IP Office lines within the configurations of each individual system. The configuration of those lines can also be checked and configured directly using the process below.

Related links

[Configuring General Resilience](#) on page 30

[Configuring resilience using the IP Office Manager line settings](#) on page 34

[Using IP Office Web Manager](#) on page 34

[SCN Resiliency Options](#) on page 34

Configuring resilience using the IP Office Manager line settings

Procedure

1. Using IP Office Manager, receive the configuration from the primary server.
2. Select the systems whose resilience settings you want to check or adjust.
3. Select Line.
4. Select the line to the system which you want to provide resilience support for the currently selected system.

Only one line providing resilience is supported on each system, ie. you cannot select to have some resilience features provided by different remote servers.
5. Select the resilience options required. See [SCN Resiliency Options](#) on page 34.
6. Click **OK**.
7. Repeat the process for any other systems in the network.
8. Save the configuration changes.

Related links

[Using the Individual System Line Settings](#) on page 33

Using IP Office Web Manager

The solution wizard automatically applies the selected options to the appropriate IP Office lines within the configurations of each individual system. The configuration of those lines can also be checked and configured directly using the process below.

Related links

[Using the Individual System Line Settings](#) on page 33

SCN Resiliency Options

Note:

- **Failover Server Total IP Phone Capacity**

When added to the remote server's extensions and users during resilience, the total numbers must be within the remote server's total supported capacity (and any other specific limit for the extension type). That also includes any other systems in resilience to that remote server at the same time. Extensions and users beyond the supported capacity do not receive resilience support. See [System Capacities](#) on page 25.

- **Reboot Required**

For 1600, 9600 and J100 Series phones and Avaya SIP softphone clients, changing the failover server for IP phones requires the phone to be restarted in order to pick up changes to its failover server address.

- **Manual Phone Configuration Required**


For 1100 and 1200 Series phones, B179 and H175 telephones; the telephone must be manually configured with the address details of its failover server.

| Field | Description |
|------------------------------|---|
| Supports Resiliency | <p>Default = Off.</p> <p>These fields are available when Networking Level is set to SCN. When selected, all the available options are defaulted to On.</p> |
| Backs up my IP Phones | <p>Default = Off.</p> <p>When selected, the local system shares information about the registered phones and users on those phones with the backup system. If the local system is no longer visible to the phones, the phones will reregister with the backup system. When phones have registered with the backup system, they show an R on their display.</p> <p>Note that while IP Office line settings are mergeable, changed to this setting require the IP phones to be restarted in order to become aware of the change in their failover destination.</p> <p>If the Phone Failback setting is set to Automatic, and the phone's primary server has been up for more than 10 minutes, the backup system causes idle phones to perform a failback recovery to the original system.</p> <p>If using resilience backup to support Avaya IP phones, Auto-create Extn and Auto-create User should not be left enabled after initial configuration or any subsequent addition of new extensions and users. Leaving auto-create options enabled on a system that is a failover target may cause duplicate extension/user records on the multi-site network under multiple failure scenarios.</p> |

Table continues...

| Field | Description |
|---------------------------------------|---|
| <p>Backs up my Hunt Groups</p> | <p>Default = Off.</p> <p>This option is available only on the IP Office Line connecting the Server Edition Primary server to the Server Edition Secondary server.</p> <p>When selected, any hunt groups the local system is advertising to the network are advertised from the backup system when fallback is required. The trigger for this occurring is desk phones registered with the local system registering with the backup system, therefore Backs up my IP Phones above must also be enabled.</p> <p>When used, the only hunt group members that will be available are as follows:</p> <ul style="list-style-type: none"> • If the group was a distributed hunt group, those members who were remote members on other systems are still visible within the network. • Any local members who have hot desked to another system still visible within the network. <p>When the local system becomes visible to the backup system again, the groups will return to be advertised from the local system.</p> |
| <p>Backs up my Voicemail</p> | <p>Default = Off.</p> <p>This option can be used if the local system is hosting the Voicemail Pro server being used by the network. If selected, when the local system is no longer visible to the voicemail server, the backup system acts as host for the voicemail server. In a Server Edition network, this option is only available on the trunk from the Primary Server to the Secondary Server. It is assumed to be on and is automatically set by the Resilience Administration tool.</p> <p>The option requires the backup system to have licenses for the Voicemail Pro features that are required to operate during any fallback period.</p> |

Table continues...

| Field | Description |
|-----------------------------------|---|
| Backs up my IP DECT Phones | <p>Default = Off.</p> <p>This option is used for Avaya IP DECT phones registered with the system. When selected, it will share information about the registered phones and users on those phones with the backup system.</p> <p>This option also requires the DECT R4 system to be configured for DECT Trunk Resilience.</p> <p>If the local system is no longer visible to the phones, the phones will reregister with the backup system. The users who were currently on those phones will appear on the backup system as if they had hot desked. Note that when the local system is restored to the network, the phones will not automatically re-register with it. A phone reset via either a phone power cycle or using the System Status Application is required. When phones have registered with the backup system, they will show an R on their display.</p> <p> Note:</p> <p>Only one IP Office Line can have this configuration parameter set to On.</p> <p>When added to the remote server's local extensions and users during resilience, the total numbers must be within the remote server's IP DECT and total supported capacities. That also includes any other systems in resilience to that remote server at the same time. Extensions and users beyond the supported capacity do not receive resilience support. See System Capacities on page 25.</p> |
| Backs up my one-X Portal | <p>Default = Off.</p> <p>This option is available on Server Edition Select deployments and only on the IP Office Line connecting the Server Edition Primary server to the Server Edition Secondary server.</p> <p>When set to On, this setting enables one-X Portal resiliency and turns on the backup one-X Portal on the Server Edition Secondary server.</p> |
| Backs up my Conferences | <p>Default = Off</p> <p>This option is available on the line from the primary to secondary server in Linux-based networks. If enabled, the secondary server will provide hosting for system meet-me conferences if the primary is not available.</p> |

Related links

[Using the Individual System Line Settings](#) on page 33

Configuration Update Scenarios

The following processes outline the steps that may be necessary when adding additional servers to an existing network.

Related links

[Configuring General Resilience](#) on page 30

[Adding an Expansion Server](#) on page 38

[Adding a Secondary Server](#) on page 38

Adding an Expansion Server

About this task

Add the new server as per the IP Office Server Edition deployment documentation and confirm normal operation. You can then proceed with configuring resilience.

Procedure

1. Run the general resilience configuration wizard.
2. Select **Update Expansion System IP Phones** backup settings (IP Office Server Edition) or **Update Expansion System IP Phones** backup settings (IP Office Select) to display the resilience settings of the expansion servers.
3. Select the resilience settings for the new expansion system.
4. Click **OK**.
5. Save the changes.

Related links

[Configuration Update Scenarios](#) on page 37

Adding a Secondary Server

About this task

Add the new server as per the IP Office Server Edition deployment documentation and confirm normal operation. You can then proceed with configuring resilience.

Procedure

1. Check the voicemail server settings. Adding a secondary server allows voicemail resilience to be deployed. This requires the two voicemail servers to be synchronized using SMTP connections.
2. For IP Office Select only:
 - a. Configure DECT resilience if required.
 - b. Adding a secondary server allows portal resilience to be deployed. This requires the portal servers to be configured with resilience settings.
3. Run the general resilience configuration wizard:
 - a. Select the resilience options required between the primary and secondary servers.
 - b. Select **Update Expansion System IP Phones backup settings** (IP Office Server Edition) or **Update Expansion System IP Phones backup settings** (IP Office Select) to display the resilience settings of the expansion servers.
 - c. Update the expansion server settings to use either the primary or secondary servers.

- d. Click **OK**.
- e. Save the changes.

Related links

[Configuration Update Scenarios](#) on page 37

Chapter 5: Configuring IP Phone Resilience

Avaya IP phones registered with one system can automatically reregister with another system when resilience is required.

IP Phone failover to an alternate gatekeeper is a native feature of many IP phones. However, it only works if the alternate gatekeeper allows registration. During normal operation, registration to the alternate gatekeeper is blocked. During failover it is allowed.

Important:

- IP phone resilience requires at least 1 physical phone (H323 or SIP). It will not operate using just softphone clients. The failover registration of IP phones is also the trigger for user, hunt group and voicemail resilience.
- User changes to their settings during failover are lost after failback. In addition, the call history for calls during failover is also lost after failback.
- Calls through the system are disconnected by failover. Direct media calls may continue but this is not guaranteed. See [Call Resilience \(Media Preservation\)](#) on page 13.
- Resilience fails if the failover server is restarted during failover. The backup user and registered phone settings received by the failover server during normal operation are held in its non-permanent memory. If during failover operation the server is rebooted, those records are lost.
- Failover features require that the phones local to each system are still able to route data to the failover system.
- When an IP phone fails over, the failover system allows it to operate as a "guest". The guest phones do not consume any licenses.
- The features for user resilience are applied to the phone user.
- Hot desked users are automatically logged out. When their base extension fails back to the home system, the hot desked user is automatically logged in on that extension.
- For secure communication using TLS/SRTP, all IP Office systems must have an identity certificate that has been signed by the same trusted root CA.

Supported Telephones

| | |
|-------------------------------------|---|
| H.323 | 1600 Series, 9600 Series. |
| SIP | 1120, B179 ^[1] , 1140, B199 ^[1] , 1220, H175, 1230, J100 Series, K100 Series. |
| SIP Softphones^[2] | Avaya Workplace Clients |

Table continues...

| | |
|---------------|---|
| Others | All supported Avaya DECT R4 handsets. IP Office WebRTC SDK Clients ^[3] |
|---------------|---|

1. These Avaya SIP Phones require some manual configuration for resilience operation.
2. Softphone resiliency requires physical IP desk phone resiliency to have occurred.
3. Requires Avaya one-X[®] Portal for IP Office resilience to be configured.

When Does IP Phone Failover Occur?

If the home system is no longer visible to the failover system for at least 3 minutes, the failover system will allow IP phones to re-register with it. This requires at least one physical IP desk phone to trigger failover. Phones with existing calls using media connection preservation do not failover until that call ends.

The failover delay ensures that resilience is not invoked when it is not required, for example when the home system is simply being rebooted to complete configuration changes.

When Does IP Phone Failback Occur?

After the home system has been visible again for more than 10 minutes, any idle phones begin to re-register with the home system. If for some reason, a phone is unable to connect to the home system, there is a 5-minute grace period, where the phone can be logged in to either the home or failover system. This is called "homeless prevention".

Automatic failback to the home system is the default mode. For H323 IP phones, manual failback can be selected. In manual mode, the phone does not failback until either logged out or rebooted.

DHCP Resilience

When an IP Office provides extension data to the system that will back up the extensions it also provides DHCP data. The failover IP Office will provide DHCP service to the failover IP Phones - even if that system's DHCP is disabled. This operation relies on DHCP forwarding be allowed between networks or on the two servers being on the same subnet. A likely requirement is to have different SSONs for the two sets of phones.

Simultaneous Clients

If a user is in simultaneous mode on their home server when failover occurs, both their phones failover.

Limitations

- Resilience fails if the failover server is restarted during failover. The backup user settings received by the failover server during normal operation are held in its non-permanent memory. If during failover operation the server is rebooted, those records are lost.
- Internal twinning is not supported during resilience failover.
- Failback twinning is supported during failover. However, only after the phone has registered with the failover server.

Related links

[Configuring the H323 Failback Mode](#) on page 42

[H323 Remote Worker Configuration](#) on page 42

[Vantage/Avaya Workplace Resilience](#) on page 43

[B179 Phone Configuration](#) on page 43

[B199 Phone Configuration](#) on page 44

[SIP Remote Extension Resilience](#) on page 45

[Configuring Expansion to Expansion Resilience](#) on page 45

Configuring the H323 Failback Mode

About this task

By default, all systems are set to use automatic failback for their IP phones when they recover from resilient operation. However, if necessary, manual failback can be configured for the system's H323 IP phones.

Manual failback requires the telephones to be unregistered or rebooted.

Procedure

1. Using Manager, log in to the home system for the resilient phones.
2. In the navigation pane on the left, select **System**.
3. In the details pane, click the **Telephony** tab.
4. In the **Phone Failback** field, select the required mode:
 - **Automatic**
Failback when system failback has occurred, and the phone has no call in progress.
 - **Manual**
Failback when the phone is restarted.
5. Click **OK**.
6. Save the configuration.

Related links

[Configuring IP Phone Resilience](#) on page 40

H323 Remote Worker Configuration

About this task

For H323 remote worker extensions, the failback server address provided by setting the general resilience settings may not be valid for them to access that server. In that case, the extension needs to use an alternate address.

Procedure

1. Using Manager, receive the configuration.
2. In the navigation pane on the left, select **Extension**.

3. Select the remote worker extension.
4. In the **Fallback As Remote Worker** field, select the required mode:
 - **Auto** - Use the failover address configured on the IP Office Line providing the service.
 - **No** - Use the alternate gateway private address.
 - **Yes** - Use the alternate gateway public address.
5. Click **OK**.
6. Save the configuration.

Related links

[Configuring IP Phone Resilience](#) on page 40

Vantage/Avaya Workplace Resilience

For all Avaya Vantage™ and Avaya Workplace Client, the address supplied for the failover server will either be the failover system's FQDN or its IP address.

- If the failover server FQDN address **System > LAN > VoIP** is set, that address is provided to the clients as the failover address. This requires that the failover server's FQDN is resolvable through the customer's network back to the IP address of the system in order for resiliency to work.
- If the failover FQDN is not set, then the system's IP address is provided to the clients as their failover server address.

Related links

[Configuring IP Phone Resilience](#) on page 40

B179 Phone Configuration

About this task

The B179 phone cannot obtain details of the failover system directly from its home system. Instead, it must be configured manually through the phone's web interface.

Procedure

1. Configure the address of the failback system as the **Secondary SIP Server** setting:

| | |
|----------------------|---|
| Account Active | <input type="radio"/> No <input checked="" type="radio"/> Yes |
| Account Name | Konftel |
| SIP Server | 192.168.42.1 |
| Secondary SIP Server | 192.168.44.1:5060 |
| Outbound Proxy | |

2. Enter details of the **Fallback Account** settings. These match the primary account except for the Registrar address which should be the failover server address.

| | | | |
|-------------------------|---|-----------------------|------|
| Primary account | | | |
| Enable account | <input checked="" type="radio"/> Yes <input type="radio"/> No | Realm | * |
| Account name | 780 | Authentication name | 780 |
| User | 780 | Password | •••• |
| Registrar | 192.168.42.1 | Registration interval | 1800 |
| Proxy | | | |
| Fallback account | | | |
| Enable account | <input checked="" type="radio"/> Yes <input type="radio"/> No | Realm | * |
| Account name | 780 | Authentication name | 780 |
| User | 780 | Password | •••• |
| Registrar | 192.168.44.1 | Registration interval | 1800 |
| Proxy | | | |

Related links

[Configuring IP Phone Resilience](#) on page 40

B199 Phone Configuration

About this task

For R11.1 and higher, using B199 1.0.1.0.9 firmware or higher, the B199 can automatically obtain many of its settings by requesting a avayab199.xml file from the IP Office. However, the following additional manual configuration steps are required to enable resilience support by the phone.

Before you begin

Procedure

1. Using a web browser, connect to the B199 phone's web menus and login using the phone's admin password.
2. Select the SIP tab.

3. In the Fallback Account section, set the follow values. These should match the same values as used for the Primary Account shown on the same menu.
 - a. Check that the **Registrar** and **Proxy** show the correct address for the failover IP Office system. These values are obtained automatically by the phone from the IP Office when the phone is started.
 - b. Enter the phone's extension number in the **User** and **Authentication Name** fields.
 - c. Enter the phone's extension password in the **Password** field.
4. Click **Save**.

Result

The phone is rebooted.

Related links

[Configuring IP Phone Resilience](#) on page 40

SIP Remote Extension Resilience

Remote SIP phones and softphones can support resilience. Refer to the [Deploying Remote IP Office SIP Phones with an ASBCE](#) manual.

Related links

[Configuring IP Phone Resilience](#) on page 40

Configuring Expansion to Expansion Resilience

About this task

For IP Office Select, you can link expansion systems and enable resiliency between those systems. Note that this assumes that the customer also has data routing between the sites.

This process creates reciprocal IP Office lines between the selected expansion systems.

Procedure

1. Open Manager and log in to the primary server.
2. On the **Solution** page, on the left under **Link** click **Expansion System**.
3. Select the expansion systems to link.
4. Under **Line Type**, select the type of IP Office line:
 - SCN-Websocket (Secure): Recommended for security and NAT traversal.
 - SCN-Websocket: Supports NAT traversal with limited security.

- SCN: Legacy SCN line. Not recommended for new deployment.
5. If the **Link Type** is set to one of the web socket options, enter a web socket password.
 6. Click **OK**.

The lines created in the configuration of each system are defaulted to medium security.
 7. Edit the individual line settings if required.
 8. Save the configuration.
 9. Use System Monitor to confirm the operation of the new lines between the two expansion systems.

Result

You can now use the resilience wizard or individual line settings to configure resilience between expansion systems.

Related links

[Configuring IP Phone Resilience](#) on page 40

Chapter 6: Configuring the Location Based Resilience

Locations can be used in the configuration of IP Office systems to group extensions and systems by their physical location. This then allows the application of location specific settings.

For IP Office Select mode networks, the location settings can also be used to configure IP phone failover:

- The location entry in each system's configuration can specify a failover system. When set, extensions with the same location use that system for failover rather than the system line configured for **Backs up my IP Phones**.
- The failover system can be an expansion system. Expansion failover requires the addition of an IP Office line between the expansion systems.
- Location based resilience is supported on Avaya 1600 and 9600 series phones and all Avaya SIP endpoints.
- The location of an extension can be specifically set or can be determined from its IP address (unless routed through an ASBCE).

Related links

[Creating Locations](#) on page 47

[Setting a System's Location](#) on page 48

[Configuring a Line for Location Based Resilience](#) on page 49

[Adjusting a Location for Resilience](#) on page 49

[Setting an Extension's Location](#) on page 50

[Example](#) on page 50


Creating Locations

About this task

In order to configure and use location-based resilience, a number of locations must first be configured and assigned to each system. Additional locations can also be added for use by sets of extensions that require different behavior from the location of their host system.

When viewed at the solution level, the location records do not include the Emergency ARS and Fallback System settings. These settings are available when the same location record is viewed at the individual system level as they can be set differently for each system.

Procedure

1. Using IP Office Manager, receive the configuration from the primary server.
2. Click **Location**.
3. Click  and select **Location**.
4. Enter an appropriate **Location Name** to identify the location.
 - You can use the Subnet settings to have phones registering with IP addresses in the same range automatically associated with to the matching location.
5. Click **OK**.
6. Create other locations for each system as required.
7. Save the configuration changes.

Related links

[Configuring the Location Based Resilience](#) on page 47

Setting a System's Location

About this task

This process sets the location of a system. Each extension registered on that system then also uses this location's settings unless it either has a different location set or if its IP address matches another location's **Subnet** settings.

Procedure

1. Using IP Office Manager, receive the configuration from the primary server.
2. In the navigation pane on the left, select **System**.
3. In the **Location** field, select the required location.
4. Click **OK**.
5. Repeat this process for all systems in the network.
6. Save the configuration.

Related links

[Configuring the Location Based Resilience](#) on page 47

Configuring a Line for Location Based Resilience

About this task

In a correctly configured network, the primary and secondary servers are reciprocally linked to each of the expansion systems. Those links can also be used for location-based resilience. If you also want to have location-based resilience between expansion systems, you must first use the expansion link wizard to create reciprocal lines between those systems.

The process below assumes enables an additional IP Office line for resilience support. This is in addition to the default resilience link configured during general resilience configuration

Procedure

1. Using IP Office Manager, receive the configuration from the primary server.
2. If not already done, use the expansion link wizard to create reciprocal lines between the expansion systems.
3. Select the system for which you want to setup location-based resilience.
4. Select the IP Office line from that system to the system which should support extensions for location-based resilience.
 - a. Set the **Location** field to match the location setting of the system to which it links.
 - b. In the **SCN Resiliency Options**, select **Supports Resiliency**. The other settings remain greyed out.
5. Save the changes to the configuration.

Related links

[Configuring the Location Based Resilience](#) on page 47

Adjusting a Location for Resilience

About this task

This process adjusts the previously created location records to override that system's resilience settings for any extensions in the same location and registered on that system.

Procedure

1. Using IP Office Manager, receive the configuration from the primary server.
2. Select the system for which you want to setup location-based resilience.
3. Click **Location**.
4. Select the location for which you want to configure location-based resilience.
5. In the **Fallback System** field, select the IP line that has been configured for resilience to the required system.

6. Click **OK**.
7. Save the configuration changes.

Related links

[Configuring the Location Based Resilience](#) on page 47

Setting an Extension's Location

About this task

This process sets the location for a specific extension. This overrides the system location if set.

Tip:

The process below sets the location of a single extension. To rapidly assign extensions to a location, in the group pane, double-click on the location. This displays a menu that allows the addition or deletion of extensions from the location.

Procedure

1. Using IP Office Manager, receive the configuration from the primary server.
2. In the navigation pane on the left, select **Extension**.
3. In the **Location** field, select the required location. **System** matches the system location as set above.
4. Click **OK**.
5. Save the configuration changes.

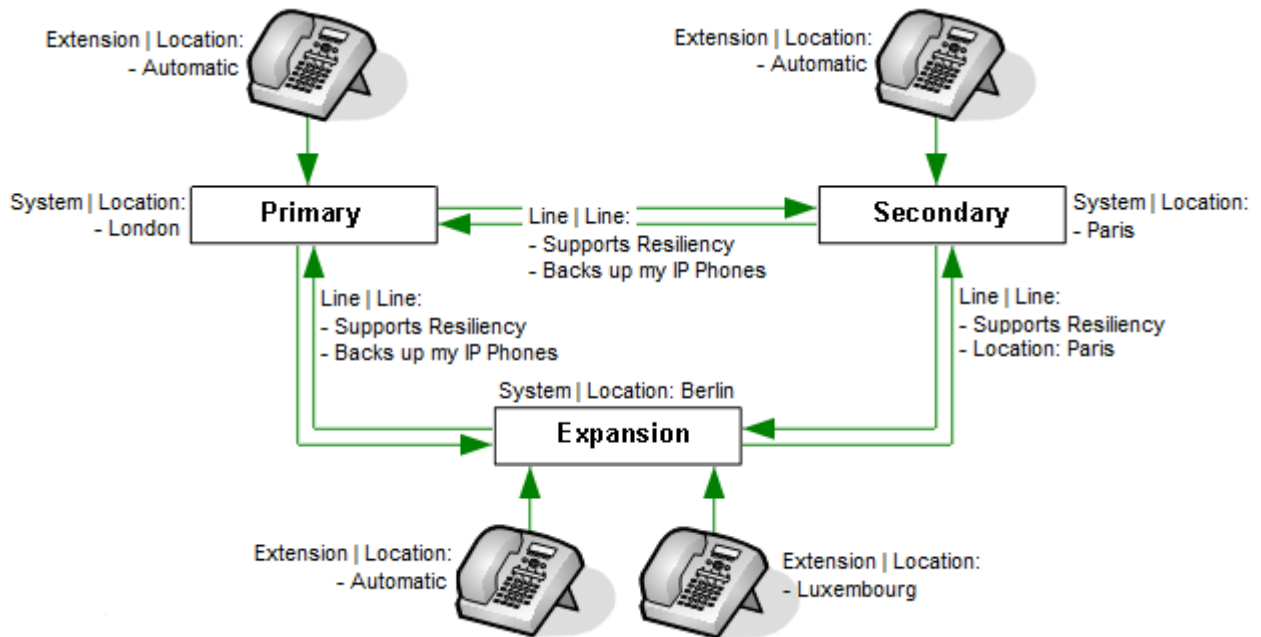
Related links

[Configuring the Location Based Resilience](#) on page 47

Example

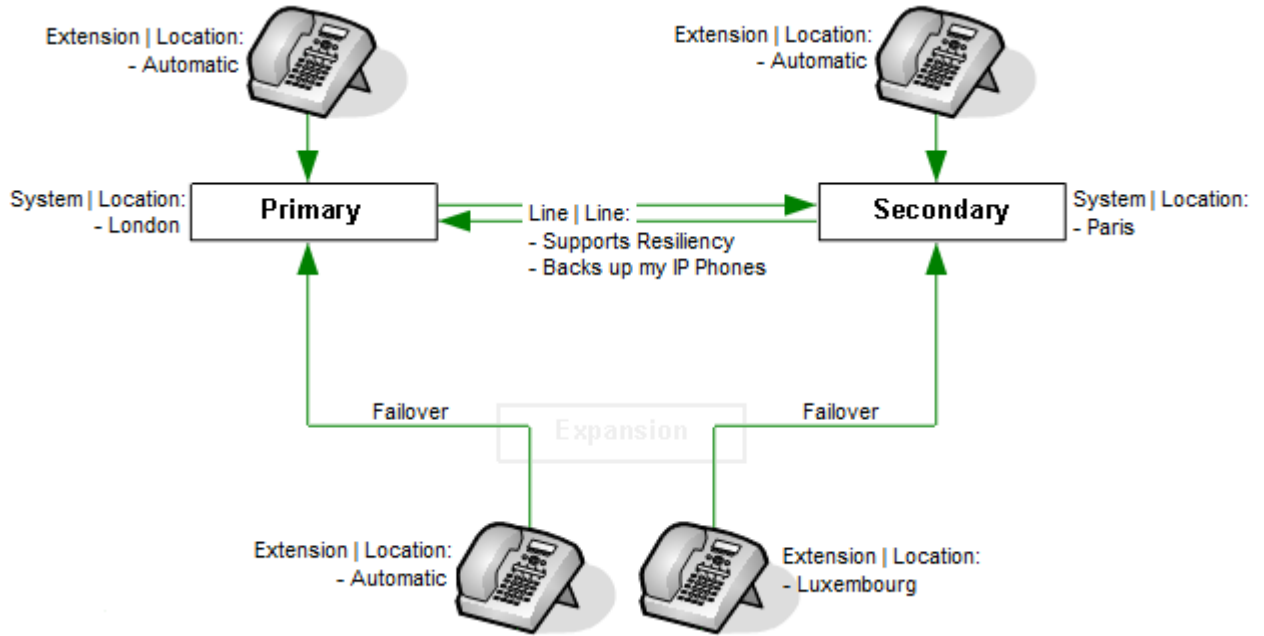
The Example Company has a multi-site IP Office Select network. Their primary server is located in London, the secondary server is located in Paris, and they have a third site with an expansion server located in Berlin. The Berlin site also supports a number of physically located in Luxembourg.

The resiliency administration wizard was used to configure resilience between the primary (London) and secondary (Paris) and from the expansion (Berlin) to the primary (London). However, the company wants those extensions located in Luxembourg to failover to the secondary (Paris) server rather than the primary (London). To achieve that:



1. At the solution configuration level, location records were created for London, Berlin, Luxembourg and Paris.
2. The location setting of each system was set as appropriate (London, Berlin and Paris).
3. In the configuration of the expansion system (Berlin) was adjusted as follows:
 - a. The location settings of the expansion system's IP Office lines were set to match their destination systems.
 - b. On the line to the secondary server (Paris), the **Supports Resilience** option was enabled.
 - c. In the system's copy of the Luxembourg location, the **Fallback Server** was set to the line to the secondary server (Paris).
 - d. For the extensions in Luxembourg, the **Location** was set to Luxembourg.

Configuring the Location Based Resilience



Related links

[Configuring the Location Based Resilience](#) on page 47

Chapter 7: Configuring Voicemail Resilience

The IP Office Server Edition network can include two voicemail servers, one on the primary server and one on the secondary server. The two servers automatically synchronize during normal operation and can provide voicemail support for the other users during resilience.

By default, the primary and secondary servers each include the voicemail service. The method by which these are used depends on the type of network:

- **IP Office Server Edition:** In this mode, the voicemail server on the primary is active and provides voicemail services for the whole network during normal operation. The voicemail server on the secondary remains in standby mode. However, during resilience, the voicemail server on the secondary can become active and provide voicemail services. When the primary voicemail is available again, by default the secondary voicemail returns to standby mode.
- **IP Office Select:** For IP Office Select the voicemail services on the primary and secondary servers can be used in two ways as follows:
 - **Single active server/standby server:** The voicemail services are configured to operate in the same way as for IP Office Server Edition above. The secondary acts as the failover server for the primary.
 - **Dual active voicemail servers:** The voicemail services on both servers can be configured to be active at the same time during normal operation (this requires the secondary server to be configured with the appropriate voicemail licenses, etc.). In this mode, each server provides voicemail services for its own extensions and trunks. Each expansion system is configured to use either the primary or secondary voicemail server. Each voicemail server can act as the failover server for the others voicemail.

During resilience, the IP Office system informs Avaya one-X[®] Portal for IP Office and other applications which voicemail server to use. The same information is also applied to all user voicemail access.

Both voicemail servers are constantly synchronizing settings, callflow configurations and mailboxes during normal operation. This is done using SMTP connections between the two voicemail servers. Following resilience, the same connections are used to re-synch the servers. Following any voicemail resilience, normal operation is not resumed until SMTP synchronization has restarted.

When does voicemail failover occur?

Voicemail failover is automatically triggered by IP desk phone failover coming into operation. It can also be manually triggered through System Status Application using the **Activate Backup Server** button.

When does voicemail failback occur?

After the server is available again, failback occurs once all active voicemail calls have ended, and server SMTP synchronization is completed. However, manual failback or failback after a set time can be configured. Manual failback in control using System Status Application.

How is resilient voicemail operation configured?

1. The settings of the IP Office lines between the primary and secondary are used to indicate whether resilience is required. See [Configuring General Resilience](#) on page 30 .
2. The SMTP settings of the voicemail servers are configured to ensure synchronization of settings between the servers during normal operation.
3. The method by which a server providing active resilience returns to non-resilient mode operation (manual, graceful or automatic) is configurable through the voicemail server settings.

Related links

[Topology of voicemail resilience](#) on page 54

[Checking the System Voicemail Settings](#) on page 56

[Viewing and changing the voicemail settings](#) on page 57

[Checking the SMTP Settings](#) on page 58

[Configuring the Voicemail Failback Method](#) on page 60

[Configuring Recording Archiving](#) on page 61

[IP500 V2 SCN Network](#) on page 62

Topology of voicemail resilience

One Active Voicemail Pro server

Server Edition supports one active Voicemail Pro server on the Server Edition Primary server. A backup Voicemail Pro server is supported on the Server Edition Secondary server for resiliency.

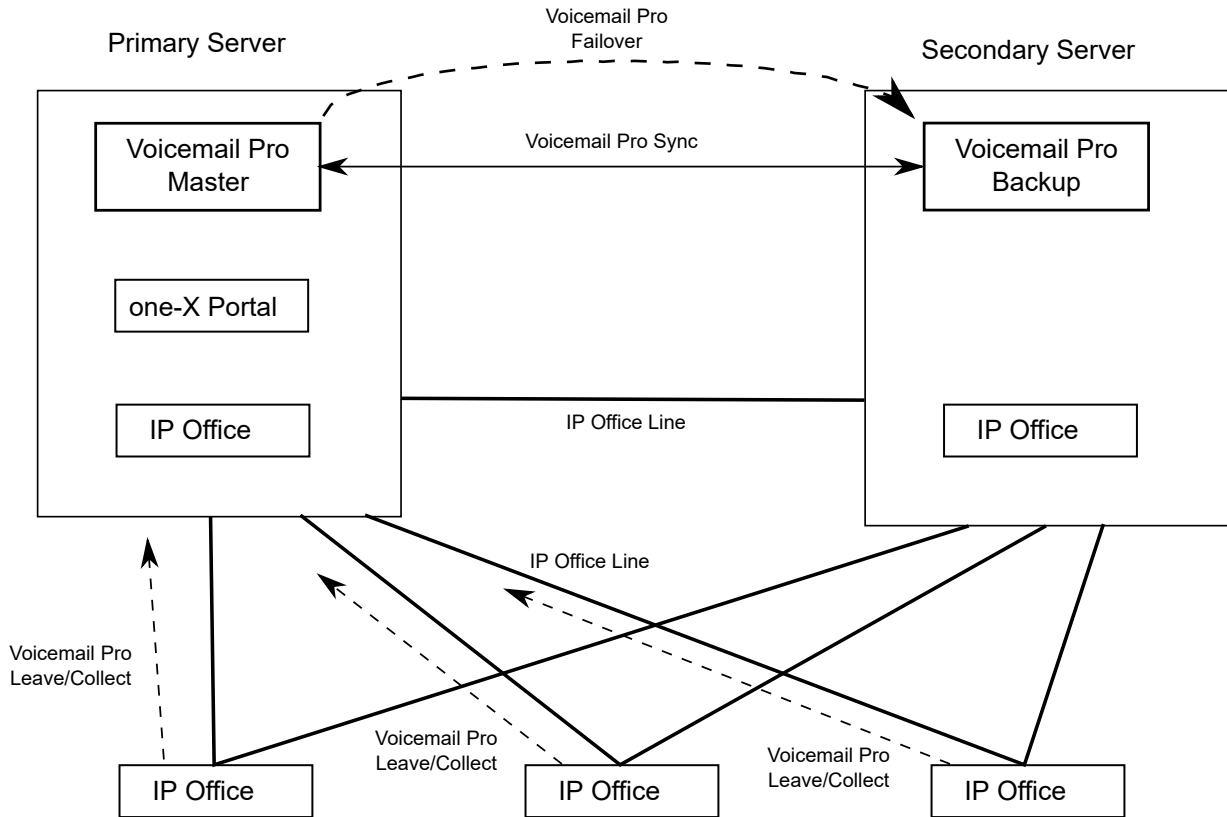


Figure 1: One active Voicemail Pro server

Dual Active Voicemail Pro servers

Server Edition Select and subscription deployments can support two active Voicemail Pro servers, doubling the maximum channel capacity and dual processing locations. Each expansion system and all contained users can be configured to use one or the other. Each Voicemail Pro server provides backup for the other. The two Voicemail Pro servers are both active for a configured subset of users. They share a common configuration and message store. Each can support all mailboxes, message waiting indicators (MWI) and call flows under failure conditions.

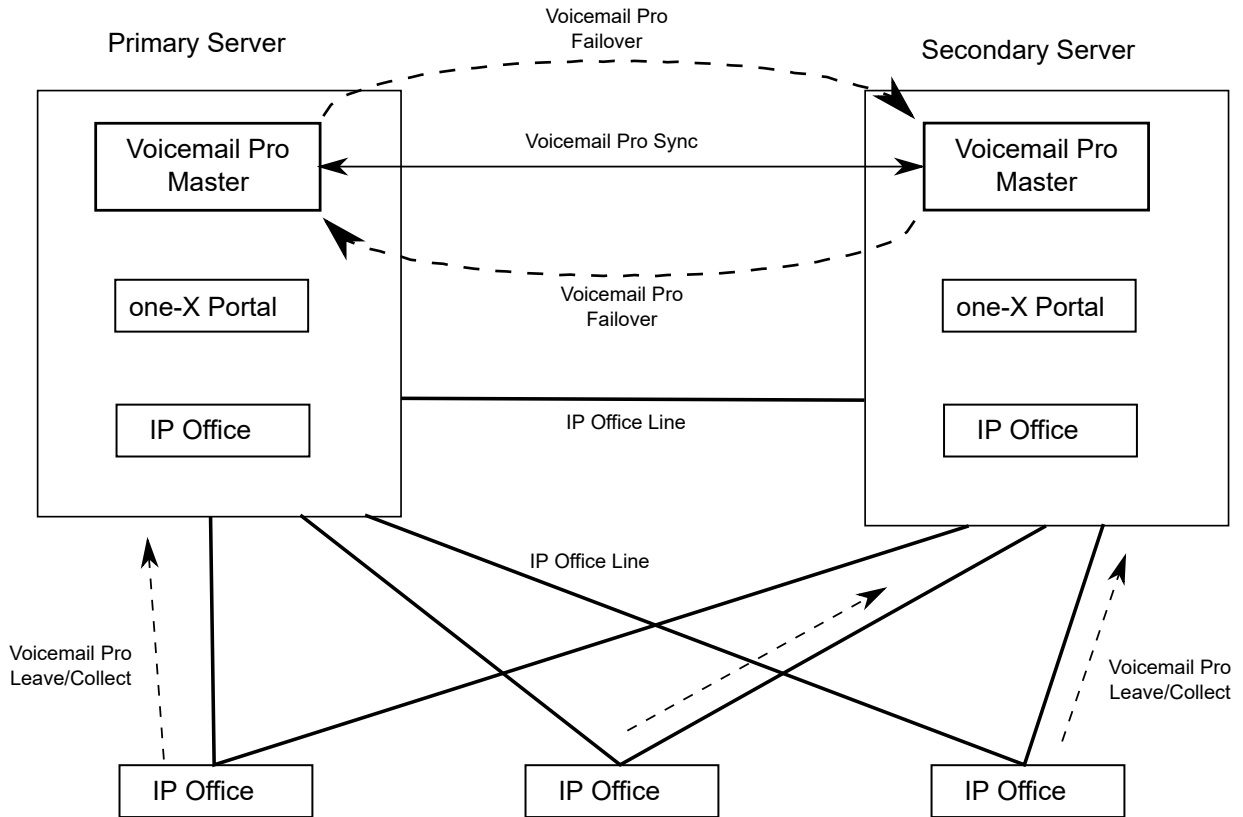


Figure 2: Dual Active Voicemail Pro servers

Related links

[Configuring Voicemail Resilience](#) on page 53

Checking the System Voicemail Settings

The voicemail settings of the server within the network are normally configured by default:

- In an IP Office Server Edition network, the primary server hosts the active voicemail service during normal operation whilst the voicemail service on the secondary is configurable but otherwise inactive.
 - The primary server is configured with the address of the secondary server as its failover destination.
 - The primary is licensed or subscribed for the voicemail features required, including Media Manager. Those rights pass to the secondary voicemail during resilience.
 - All other servers are configured to use the primary for voicemail. They are automatically redirected during resilience.

- In an IP Office Select or subscription network, the primary and secondary servers can be configured as above, or they can be configured to have both the primary and secondary voicemail services active simultaneously. In the latter case:
 - The primary server is configured with the address of the secondary server as its failover destination and vice versa.
 - The primary and secondary each require their own licenses/subscriptions for the voicemail features they require, including Media Manager.
 - Each expansion server is configured to use either the primary or secondary voicemail during normal operation.

The above appears in the **System > Voicemail** configuration settings of each server as follows:

Table 1: Single Active Server Settings

| Voicemail Setting | Primary Server | Secondary Server | Expansion Server |
|-----------------------------|-----------------------------|-----------------------|-----------------------|
| Voicemail Type | Voicemail Lite/Pro | Centralized Voicemail | Centralized Voicemail |
| Voicemail Destination | Not used | 99999 (primary) | 99999 (primary) |
| Voicemail IP Address | 127.0.0.1 | Not used | Not used |
| Backup Voicemail IP Address | Secondary server IP address | Not used | Not used |

Table 2: Dual Active Server Settings


| Voicemail Setting | Primary Server | Secondary Server | Expansion Server |
|-----------------------------|-----------------------------|---------------------------|---------------------------------------|
| Voicemail Type | Voicemail Lite/Pro | Voicemail Lite/Pro | Centralized Voicemail |
| Voicemail Destination | Not used | Not used | 99999 (primary) or 999998 (secondary) |
| Voicemail IP Address | 127.0.0.1 | 127.0.0.1 | Not used |
| Backup Voicemail IP Address | Secondary server IP address | Primary server IP address | Not used |

Related links

[Configuring Voicemail Resilience](#) on page 53

Viewing and changing the voicemail settings

Procedure

1. Using IP Office Manager, receive the configuration from the primary server.
2. Select the systems whose resilience settings you want to check or adjust.
3. Select  **System**.

4. Select the **Voicemail** tab. Check that the settings match those expected in the tables above.
5. If any changes have been made, click **OK**.
6. Check the settings for the other servers if necessary.
7. Save changes.

Related links

[Configuring Voicemail Resilience](#) on page 53

Checking the SMTP Settings

Both voicemail servers are constantly synchronizing settings, callflow configurations and mailboxes during normal operation. This is done using SMTP connections between the two voicemail servers. Following resilience, the same connections are used to re-synch the servers. Following any voicemail resilience, normal operation is not resumed until SMTP synchronization has restarted.

The SMTP connections are configured through the voicemail server preferences of each server. The first entry in the server's SMTP settings (**System > Voicemail > Email > SMTP Sender**) is its default SMTP server. This is the entry used for inter-voicemail server traffic for features such as resilience. This Domain and Server fields of this entry must be configured with the fully qualified domain name of voicemail server, they should not be set to local host.

Related links

[Configuring Voicemail Resilience](#) on page 53



[Configuring the SMTP Sender](#) on page 58

[SMTP Sender options](#) on page 59

[Configuring the SMTP Receiver](#) on page 59

Configuring the SMTP Sender

Procedure

1. Connect to the voicemail server using the Voicemail Pro client.
2. Click the **Preferences**  icon. Alternatively, from the **Administration** menu select **Preferences**.
3. Select the **Email** tab.
4. Select the **SMTP Sender** sub-tab.
5. After making any changes, click **OK**.
6. Click  **Save & Make Live**.

Related links

[Checking the SMTP Settings](#) on page 58



SMTP Sender options

| Option | Description |
|---------------------------------------|--|
| Mail Domain | Set this to match the server's fully qualified domain name. The voicemail service also uses the domain set to filter incoming SMTP mails received by the SMTP server. For this to work, the domain entered should be the fully-qualified name of the server on which the voicemail server is running, for example <code>vmpro1.example.com</code> . Any incoming messages where the recipient mail domain does not match are |
| Server | This specifies the IP address or fully-qualified domain name of the SMTP server to which messages are sent. Set this to the fully qualified domain name of the other voicemail server. |
| Port Number | Set this to 25. |
| Sender (Identifier) | Leave this blank. The voicemail server will insert a sender using either the e-mail address set for then voicemail mailbox user if set or otherwise using the best matching name it can resolve from the IP Office. |
| Server Requires Authentication | Leave these blank. |

Related links

[Checking the SMTP Settings](#) on page 58

Configuring the SMTP Receiver**Procedure**

1. Connect to the voicemail server using the Voicemail Pro client.
2. Click the  **Preferences** icon. Alternatively, from the **Administration** menu select **Preferences**.
3. Select the **Email** tab.
4. Select the **SMTP Receiver** sub-tab.
 - a. In **SMTP Receiver** set this to **Internal**.
 - b. In **Port** set to **25**.
 - c. In **Domain** set this to match the server's fully qualified domain name.
5. After making any changes, click **OK**.
6. Click  **Save & Make Live**.

Related links

[Checking the SMTP Settings](#) on page 58

Configuring the Voicemail Failback Method

Once the server is available again, by default failback occurs once all active voicemail calls have ended and server SMTP synchronization is complete. This is referred to as graceful failback. However, manual failback or automatic failback after a set time can be configured.

Related links


[Configuring Voicemail Resilience](#) on page 53

[Setting the voicemail server failback method using the Voicemail Pro client](#) on page 60

[Setting the voicemail server failback method using web manager](#) on page 61


Setting the voicemail server failback method using the Voicemail Pro client

Procedure

1. Connect to the voicemail server using the Voicemail Pro client.
2. Click the **Preferences**  icon. Alternatively, from the **Administration** menu select **Preferences**.
3. Select the required **General** tab.
4. Select the **Failback Option**. This field sets how the server should return control of voicemail services to the other server. Failback is only considered when the two voicemail servers have started SMTP synchronization.
 - **Manual**

The system administrator has to initiate failback operation from the **Voicemail** tab in System Status Application.
 - **Graceful** (Default)

The failover server initiates failback after all the active voicemail calls on the failover server have ended and server SMTP synchronization has finished.
 - **Automatic**

The failover server initiates failback either after the specified **Failback Timeout** period (maximum 60 minutes) or after all the active voicemail calls on the failover server end, whichever occurs first. It does not wait for server SMTP synchronization finish.
5. After making any changes, click **OK**.
6. Click  **Save & Make Live**.

Related links

[Configuring the Voicemail Failback Method](#) on page 60

Setting the voicemail server failback method using web manager

Procedure

1. Using a web browser, log into the web management menus.
2. Click **Applications** and select **Voicemail Pro - System Preferences**.
3. Select **General**.
4. Select the **Failback Option**. This field sets how the server should return control of voicemail services to the other server. Failback is only considered when the two voicemail servers have started SMTP synchronization.
 - **Manual**

The system administrator has to initiate failback operation from the **Voicemail** tab in System Status Application.
 - **Graceful** (Default)

The failover server initiates failback after all the active voicemail calls on the failover server have ended and server SMTP synchronization has finished.
 - **Automatic**

The failover server initiates failback either after the specified **Failback Timeout** period (maximum 60 minutes) or after all the active voicemail calls on the failover server end, whichever occurs first. It does not wait for server SMTP synchronization finish.
5. After making any changes, click **Update**.
6. When asked to confirm the changes, click **Yes**.

Related links

[Configuring the Voicemail Failback Method](#) on page 60


Configuring Recording Archiving

About this task

If a voice recording library (VRL) application such as IP Office Media Manager is being used with the primary voicemail server:

- For a single active voicemail configuration, then during resiliency the backup voicemail server performs call recording and places any VRL recordings in its own VRL folder. Once the primary voicemail server become active again, the secondary needs to transfer the recordings in its VRL folder to the primary server's VRL folder. This is done using the voicemail system preferences of the secondary voicemail server.
- For a dual active voicemail configuration, the configuration used during normal operation is also used during resilience. That requires the secondary voicemail to have its own Media Manager license or subscription.

Procedure

1. Connect to the secondary voicemail server using the Voicemail Pro client.
2. Click the **Preferences**  icon. Alternatively, from the **Administration** menu select **Preferences**.
3. Select the **Voicemail Recording** tab.
4. For the **FTP User Name** and **FTP Password** fields, enter the details of an administrator account on the primary voicemail server.
5. For the **Remote FTP Location**, enter `/opt/vmpro/MM/VRL`.
6. For the **Remote FTP Host** enter the FQDN or IP address of the primary voicemail server.
7. Click **Test Connection** and wait for a response.
8. If the connection is confirmed, click **OK**.

Related links

[Configuring Voicemail Resilience](#) on page 53

IP500 V2 SCN Network

The voicemail resilience features described in this manual apply to voicemail being provided by a primary/secondary pair of servers.

For voicemail being used in an SCN network of IP500 V2 systems, a number of alternate resilience features are supported:

| Option | Description |
|--------------------------------------|--|
| Distributed Voicemail Server: | Within the SCN, multiple voicemail servers are supported. One centralized server holds all messages and mailboxes, but other distributed servers can handle calls and perform recording before passing the resulting messages to the central server. |
| Backup IP Office Server: | The central voicemail server is controlled by a specified IP Office system. Another IP Office system can be specified as the backup IP Office which will take over control of voicemail if the original IP Office is not available for any reason. |
| Backup Voicemail Server: | An additional voicemail server can be configured to takeover if the centralized voicemail server is not available. |

For details, refer to the [Administering IP Office Voicemail Pro](#) manual.

Related links

[Configuring Voicemail Resilience](#) on page 53

Chapter 8: Configuring one-X Portal for IP Office Resilience

Both the primary and secondary server host copies of portal service with the service on the primary normally being the active one. However, in failback scenarios the secondary's service can become active until the systems recover.

The portal service is also installed by default on the IP Office Server Edition secondary server. This allows that secondary server to act as the portal server for users when, for some reason, the primary server is not available.

- Portal resilience is supported in IP Office Select and IP Office Subscription modes. That includes an IP Office Application Server in place of the primary or secondary server's portal service.
- Portal resilience is supported by the following client applications:
 - Avaya one-X[®] Portal for IP Office browser access.
 - Avaya one-X[®] Portal for IP Office call assistant.
 - IP Office SoftConsole presence indication.
- Resilience is only supported between primary and secondary servers running the same version of portal software.
- During normal operation (both servers running and connected), user and administrator changes made on the primary server are automatically synchronized to the secondary server. However, during resilience, changes made on either server are not synchronized and may be lost when the servers return to normal operation.
 - Scheduled conferences are currently an exception to the above. Conferences scheduled on the primary do not occur when running in failover. Conferences scheduled on the secondary are lost when failback occurs.

When Does Portal Failover Occur?

- If the primary server's portal service is not available, the portal service on the secondary server automatically becomes available.
- Users who were logged into the portal on the primary can login again on the secondary server.
 - If the primary IP Office service is still running, those portal users are automatically redirected.
 - If the user has not previously accessed the secondary portal server, they may need to accept the security certificate or create an exception which will interrupt automatic re-connection.

- The same applies for users who were logged into one of the portal clients such as the Outlook Plug-in
- New users wanting to login will have to use the address of the secondary server.
- On primary server IP Office failure: If the primary server's IP Office service stops for some reason, portal services are automatically transferred to the secondary server as above. Users belonging to that IP Office cannot update or delete personal contacts from the portal directory gadget.
- On network failure: If the network connection between the primary and secondary server fails for some reason, both portal servers become active and can be logged into. Again, user and admin changes on secondary portal server are not copied to primary when the network connection recovers. This is called "Standalone Mode".

When Does Portal Failback Occur?

- When the primary server's portal service is available again, the portal service on the secondary server stops supporting user login.
 - Users who were logged into the portal on the secondary are automatically re-directed to login again on the primary server.
 - Users who were logged into one of the portal clients such as the Outlook Plug-in are automatically connected to the primary server.
 - New users wanting to log in are redirected to the primary.
- On primary server IP Office recovery: When the primary server's IP Office service is available again, portal service support also returns to the primary server as above.

Related links

[Topology of portal resiliency](#) on page 64

[Configuring the IP Office Systems](#) on page 66

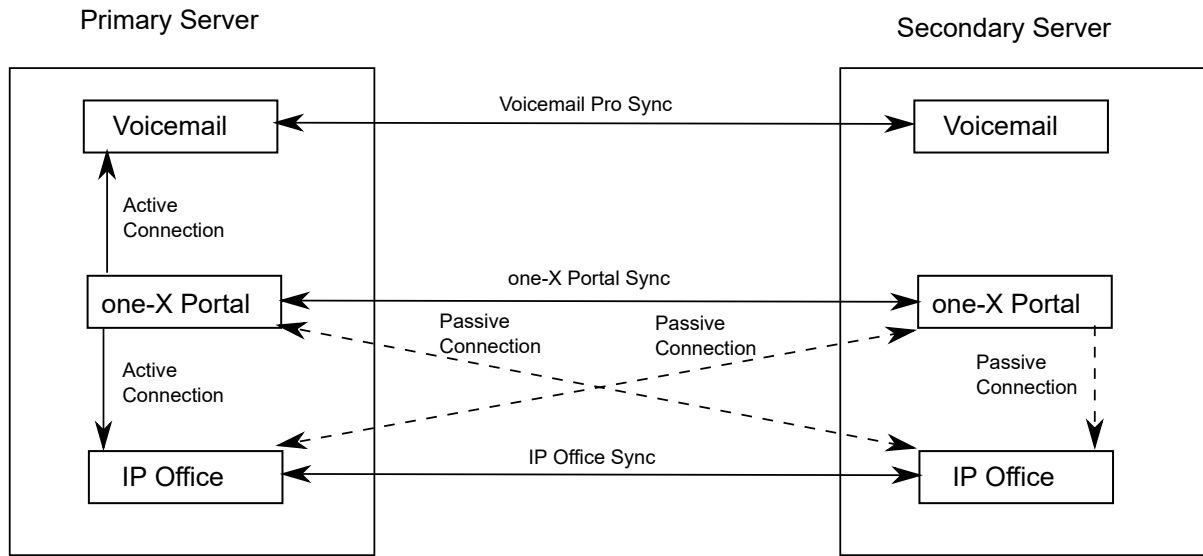
[Enabling Centralized CTI Link Mode](#) on page 66

[Configuring the one-X Portal for IP Office Servers](#) on page 67

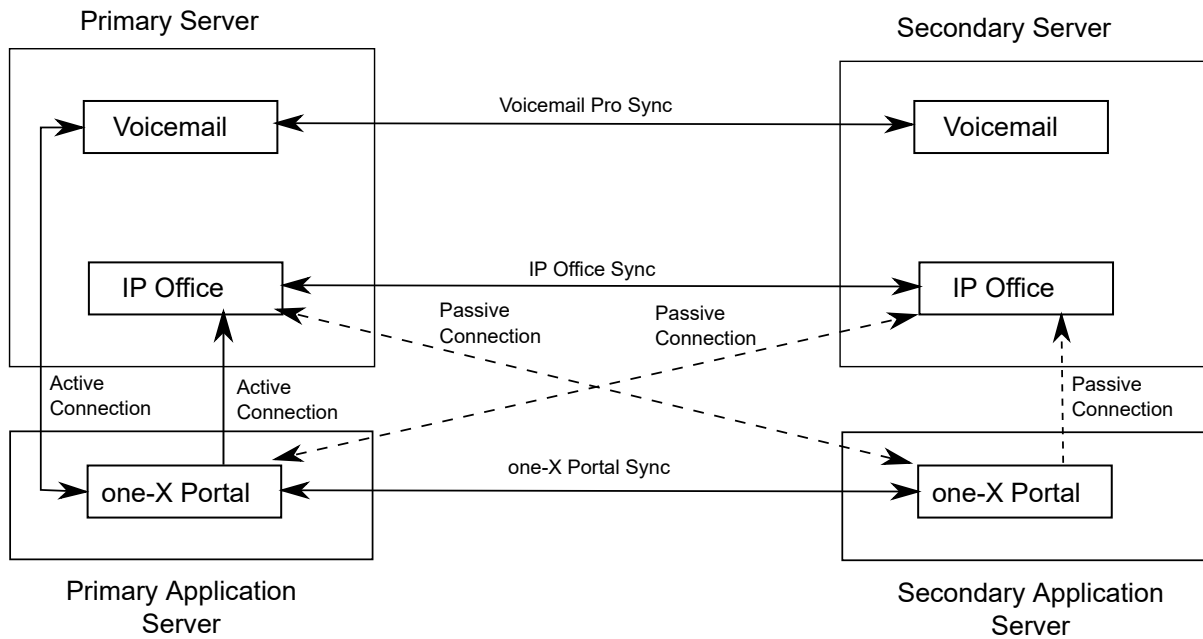
Topology of portal resiliency

Server Edition Select and subscription deployments support a backup portal server. The resilient portal server is installed by default on the secondary server though it can also be located on standalone application server associated with the secondary.

Resilient one-X Portal on the primary and secondary servers



Resilient portal on standalone application servers



Related links

[Configuring one-X Portal for IP Office Resilience](#) on page 63

Configuring the IP Office Systems

About this task

The IP Office lines between the primary and secondary IP Office servers need to have the setting for portal backup enabled. This can be done through the configuring general resilience options.

Procedure

1. Using IP Office Manager, load the configuration from the IP Office Server Edition IP Office systems.
2. In the settings of the primary, locate the IP Office line from the primary to the secondary IP Office system.
3. On the **Line** tab, in the **SCN Resiliency Options**, check that **Supports Resiliency** and **Backs up my one-X Portal** are selected.
4. Repeat the step above for the IP Office line from the secondary to the primary IP Office system.
5. Save the configuration changes.

Related links

[Configuring one-X Portal for IP Office Resilience](#) on page 63


Enabling Centralized CTI Link Mode

About this task

Both portal servers must be set to use centralized CTI link mode. That is the default for a new installation but must be manually enabled for existing systems upgraded to IP Office Release 10 or higher.

Configuration is done through the primary portal server. If setup correctly, this synch's its settings to the secondary portal server.

Procedure

1. Login to the primary portal's administrator menus.
2. Select **Configuration**.
3. Select **Central CTI Link**.
 - Systems upgraded from Release 9.1 display their original **Auto Provisioning** setting. Click on **Convert to Central CTI Link**.
 - Check the **Central CTI Link** is enabled.
4. Click **Save**.
5. If any changes have been made, restart the portal service by clicking on the  icon.

6. Repeat the process for the secondary portal.

Related links


[Configuring one-X Portal for IP Office Resilience](#) on page 63

Configuring the one-X Portal for IP Office Servers

About this task

The portal resiliency menu is not visible if the IP Office systems are not set to IP Office Select mode and configured for port resiliency, see [Configuring the IP Office Systems](#) on page 66 . If still not visible it may be necessary to restart the portal service.

Procedure

1. Login to the primary portal's administrator menus.
2. Select **Configuration**.
3. Select **Resilience**.
4. Adjust the settings to provide the details of the servers.
 - **Failover**: Select Enabled.
 - **Failover Detection Time**: Set the duration before which the failover process begins. This stops failover being initiated by minor maintenance actions and system restarts.
 - **Failback**: Select **Automatic** or **Manual**. If set to manual, failback is initiated by restarting the primary server.
5. Select **Host Domain Name**. Enter the fully qualified domain names of the primary and secondary portal servers.
6. Click **Save**.
7. If any changes have been made, restart the portal service by clicking on the  icon.
8. You can now enable support for portal resilience in the IP Office settings. See [Configuring the IP Office Systems](#) on page 66.

Related links

[Configuring one-X Portal for IP Office Resilience](#) on page 63

Chapter 9: Configuring WebRTC Resiliency

On systems with Avaya one-X® Portal for IP Office resilience configured, resilience is also supported for user's using an Avaya WebRTC client to make and answer calls.

This is supported for IP Office R11.0 and higher.

- Supported Clients: WebRTC resilience is only supported for clients that use the IP Office WebRTC SDK.

For failure of the Avaya one-X® Portal for IP Office services, auto-login is supported for existing active WebRTC clients. However, for IP Office service failure, manual re-login is required.

The primary and secondary server WebRTC Gateway services must use auto-configuration and be configured to use the same domain and certification settings. WebRTC resilience is not supported for external clients when the servers are behind a single ASBCE or NAT.

Chapter 10: Configuring DECT Resilience

DECT R4 uses an IP DECT trunk between the host IP Office server and the DECT master base station. DECT resilience allows the DECT system to be configured with an additional trunk to another IP Office server in the network. If the host server becomes unavailable for some reason, the failover trunk and server become active, allowing continued DECT operation.

Resilience operation occurs when the master base station cannot detect its normal host IP Office system, that is the IP Office system configured with an IP DECT line to it. During resilience, the failover IP Office system takes control and hosts the DECT extensions and users that were previously on its normal host system. However, no changes to the DECT configuration or additional handset subscriptions are allowed.

The failover IP Office system can host its own DECT R4 system using its own IP DECT line and master base station. When that is the case, it can only support failover from another system up to its maximum capacity of DECT users including its own DECT users (maximum 384 on an IP500 V2, 400 on a Linux based system).

DECT trunk resilience and base station mirroring can be combined.

For a provisioned installation

- The centralized phone book is still supported after failover. However, this does not apply to the phone book if being provided by an AIWS.
- An R is displayed on the 3700 Series DECT phones when they are in failover.
- By default DECT control and extensions automatically return to the primary IP Office system when it is available again.

For a non-provisioned installation

- The centralized phonebook is not supported during failover.
- The handsets do not display any indication that the system is in failover.

When Does DECT Failover Occur?

The master base station regularly polls its normal IP Office server, by default every 30 seconds. If that IP Office is not visible for some reason, then by default, after 2 minutes the master base station switches to using its failover IP Office system. These timings can be adjusted, see [Configuring DECT Resilience](#) on page 69.

When Does DECT Failback Occur?

When the original IP Office system returns to normal operation, by default DECT control is automatically returned to it. The operation can be set to manual control if necessary, see [Configuring DECT Resilience](#) on page 69. In that case, control of failback is through the System Status Application.

Related links

[Provisioned Base Station Configuration](#) on page 70

[Non-Provisioned Base Station Configuration](#) on page 71

[IP Office Configuration for DECT Resilience](#) on page 72

Provisioned Base Station Configuration

About this task

For a provisioned installation, the master base station needs to be configured to accept a provisioning connection from the failover system.

Procedure

1. Login to the master base station.

This process requires access to tabs and fields currently only visible when **Show Advanced Options** is selected.

2. Select **Services** and then select the **Provisioning** tab.

3. Set the **Current View** to **Redundant**.

- a. Select the **Enable** option.

- b. The IP Office security settings control whether HTTPS is supported between the master base station (by default it is supported) and the failover IP Office system.

- c. Set the **PBX IP Address** to match the failover IP Office system.

- d. In the **User Name and Password** fields, set the details that match the failover IP Office system's service user configured for IP DECT.

- e. Ensure that the **Base directory** is set to `/system/backupipdect/` instead of `/system/ipdect/`.

- f. Click **OK**.

4. Reset the base station.

- a. Click on **Reset** required if displayed. Otherwise, select **Reset** and then select the **Reset** tab.

- b. Click **OK**.

Depending on your base station, wait for the lower LED to return to solid blue or solid green.

Related links

[Configuring DECT Resilience](#) on page 69

Non-Provisioned Base Station Configuration

About this task

For non-provisioned systems, the master base station needs to be configured with details of a redundant trunk connection to the failover IP Office and when to use that trunk.

Procedure

1. Login to the master base station.

This process requires access to tabs and fields currently only visible when **Show Advanced Options** is selected.

2. Select **DECT** and then select the **Master** tab.
3. Enable the **PBX Resiliency** and click **OK**.
4. Select the **Trunks** tab.

Options for configuring the redundant trunk to the failover IP Office system are now

5. In the **Trunk Settings** section, configure how failover should operate:

- **Prioritize primary trunk:** If selected, when during failover the master base station detects that normal host system is available, it returns DECT control to that system. If not selected, the failover system retains control until it is manually returned using System Status Application
- **Status Inquiry Period:** This field set how frequently (in seconds) the master base station should check the status of the host system. This value and the **Status Enquiry Period** set in the host system configuration should match.
- **Supervision Timeout:** This option is only supported for a provisioned installation.

6. In the **Redundant Trunks** settings, set the port fields to **1720** and the **CS IP Address** to the IP address of the failover IP Office system.
7. Click **OK** and reset the base station.
 - a. Click on **Reset** required if displayed. Otherwise, select **Reset** and then select the **Reset** tab.
 - b. Click **OK**.

Result

Depending on your base station, wait for the lower LED to return to solid blue or solid green.

Related links


[Configuring DECT Resilience](#) on page 69

IP Office Configuration for DECT Resilience

About this task

For DECT switch resilience, the IP Office is configured as shown below. Only the host system needs this configuration. However, for provisioned systems, the security service user on the failover system must be enabled and configured to match the settings entered for the redundant provisioning connection

Procedure

1. Using IP Office Manager, retrieve the configuration from the IP Office system.
2. Click on **Line**. The list of existing lines is shown.
3. Click on the  icon and select IP DECT Line. The settings for an IP DECT line are displayed.
4. Select the **Gateway** tab.
5. Find the **Enable Resiliency** section.
6. Select **Enable Resiliency**.
7. Change the other values if necessary:
 - **Status Enquiry Period:** This field set how frequently (in seconds) the master base station should check the status of the primary IP Office. For a non-provisioned installation, this value should match the Status Inquiry Period set in the master base station.
 - **Prioritize Primary:** If selected, when during failover the primary IP Office returns to normal operation, DECT control is automatically returned to it. If not selected, the failover IP Office retains control until it is manually returned using System Status Application
 - **Supervision Timeout:** This field sets how long after contact is lost (in seconds) before the master base station should failover to the failover IP Office system. This option is only accessible here for a provisioned installation. For a non-provisioned installation the value is set through the master base station.
8. Click **OK**.
9. Save the settings back to the IP Office system.

Related links

[Configuring DECT Resilience](#) on page 69

Chapter 11: Configuring DECT Master Resilience

Each DECT R4 system includes a configured as the master base station. Base station mirroring allows two base stations to be configured as the master. Whilst only one is active master, the other becomes active if the existing master becomes unavailable.

For base station resiliency, two base stations are configured to function as 'mirrored' master base stations. One becomes the active master whilst the other becomes a standby master. If for any reason, the active master base station becomes unavailable, the standby master base station becomes the active master and continues DECT operation.

- The standby master base station is still able to handle call connections in the same way as normal base stations.
- Mirroring is not supported between compact and non-compact base stations. However, it is supported between a DECT Gateway and non-compact base station.
- Base station mirroring and DECT trunk resilience can be combined.

When Does DECT Master Failover Occur?

The standby master regularly polls the active master. If the active master becomes invisible for some reason, the standby master automatically becomes the active master.

When Does DECT Master Failback Occur?

When the active master is available again, it resumes control, and the other base station returns to being the standby master.

Related links

[Configuring the IP Office](#) on page 73

[Configuring the Mirrored Base Stations](#) on page 74


[Activating the Master Base Station](#) on page 75

Configuring the IP Office

About this task

In the IP Office system, the IP DECT line needs to be configured with the IP addresses of both of the mirrored base stations.

Procedure

1. Using IP Office Manager, retrieve the configuration from the IP Office system.
2. Click on **Line**. The list of existing lines is shown.
3. Click on the  icon and select **IP DECT Line**. The settings for an IP DECT line are displayed.
4. Select the IP DECT line and select the **VoIP** tab.

In the **Gateway IP Address** and the **Standby IP Address** fields, enter the IP addresses of the two base stations that will be mirrored.

5. Save the changes.

Related links

[Configuring DECT Master Resilience](#) on page 73

Configuring the Mirrored Base Stations

About this task

Use the following process to configure the master base station and its mirror.

This process requires access to tabs and fields currently only visible when **Show Advanced Options** is selected.

Procedure

1. Login to the first master base station.
2. Select **DECT** and then select the **Master** tab.
 - a. Set the **Mode** to **Mirror**.
 - b. Set the **Mirror Master IP** address field to the IP address of the other based station.
 - c. Click **OK**.
3. Select the **DECT > Radio** tab.
 - a. In the **Master IP Address** field, enter the base station's own IP address.
 - b. In the **Alt. Master IP Address** field, enter the IP address of the other master base station.
 - c. Click **OK**.
4. Reset the base station.
 - a. Click on **Reset required** if displayed. Otherwise, select **Reset** and then select the **Reset** tab.
 - b. Click **OK**.

Result

Depending on your base station, wait for the lower LED to return to solid blue or solid green.

Next steps

Repeat this process for the other mirrored base station.

Related links

[Configuring DECT Master Resilience](#) on page 73

Activating the Master Base Station

About this task

Only one base station in the mirrored pair acts as the master base station at any time. The initial selection is done through the base station menus of the selected member of the mirrored pair.

This process requires access to tabs and fields currently only visible when **Show Advanced Options** is selected.

Procedure

1. Login to one of the mirrored master base stations.
2. Select **DECT** and then select the **Master** tab.
3. Click **Activate** mirror.

Result

That base station is made the currently active master base station in the mirrored pair.

Related links

[Configuring DECT Master Resilience](#) on page 73

Chapter 12: Configuring External Trunk Resilience

It is difficult to provide trunk guidance for resilience as the configuration of the external trunk routing and usage of every network varies greatly. We can only discuss general principles and factors that need to be considered, and show examples of the different methods that can be used.

- Special consideration must always be given to ensure the correct routing of emergency calls, especially in regard to identifying caller location.
- Outgoing caller ID must be assessed. Rerouted calls may be blocked if the ID used to call out on an alternate trunk or site is not accepted by the line provider.

Related links

[Configuring Breakout Controls](#) on page 76

[Primary ARS Fallback to Secondary Trunks](#) on page 77

Configuring Breakout Controls

About this task

The **Breakout** action is potentially useful during failover scenarios. It allows a telephone user to make a call as if dialing the digits on another system on the network and thus have their dialing routed by that system. The action can be assigned to short codes and to programmable buttons.

Procedure

1. Using IP Office Manager, receive the configuration from the primary server.
2. Select the user or user rights to which you want to add a break out button and select the **Button Programming** tab.
3. Edit a button as follows:
 - a. Select the **Action** as **Select the Action as Advanced > Dial > Break Out**.
 - b. In the **Action Data** enter the system name or IP address of the remote server. Alternatively, if this field is left blank, display phones list the systems from which the use can select when the button is pressed.
4. Click **OK**.


5. Click **OK** again.
6. Save the configuration changes.

Related links

- [Configuring External Trunk Resilience](#) on page 76
- [Adding a break out short code](#) on page 77

Adding a break out short code

Procedure

1. Using IP Office Manager, receive the configuration from the primary server.
2. Select the type of short code you want to add, ie. a common system short code, specific system short code, user short code, user rights short code.
3. Click  and select Short Code.
4. Enter the short code details:
 - Code: Enter the dialing digits and short code characters that will trigger the short codes use.
 - Feature: Select **Break Out**.
 - Telephone Number: The IP address or the IP Office System name of the remote server. In IP addresses, use * characters in place of characters.
5. Click **OK**.
6. Save the configuration changes.

Related links

- [Configuring Breakout Controls](#) on page 76

Primary ARS Fallback to Secondary Trunks

In these examples, we assume that SIP trunks have been added to the secondary server. We want outgoing calls on the primary to use those trunks on the secondary when necessary.

- Note that these examples are useable in both normal and failover operation. They are not using specific resilience failover features.
- The simplest method is to add a `?/. /Dial/99998` short code to the primary system's existing ARS form. However, that method provides no or flexibility. Using an alternate ARS form allows a number of other features to be employed. For example, setting some users to a lower priority applies a delay to them using a secondary trunk when the primary trunks are not available.


Related links

- [Configuring External Trunk Resilience](#) on page 76
- [ARS Alternate Route Overflow](#) on page 78

[ARS Out of Service Routing](#) on page 78

ARS Alternate Route Overflow

Procedure

1. Using IP Office Manager, receive the configuration from the primary server.
2. Expand the configuration of the primary server and select ARS.
3. Click on the  icon to add a new ARS record.
 - a. Set the **Route Name** to something suitably descriptive such as **Fallback**.
 - b. Add a short code that will route calls from this ARS record to the secondary server: **?/Dial/.99998**
 - c. Click **OK**.
4. In the ARS record **50:Main** on the primary, we need to set the record to failover to using the fallback ARS when a route to the primary cannot be seized within the required time.
 - a. In the **Alternate Route** drop down select the fallback ARS created above.
 - b. Set the **Alternate Route Priority Level** to **5**.

This is the highest level of priority. It means that users with a lower priority need to wait for the Alternate Route Wait Time before calls overflow to the secondary when there are no available primary trunks. The default user priority is 5.
 - c. Click **OK**.
5. Save the configuration.

Related links

[Primary ARS Fallback to Secondary Trunks](#) on page 77


ARS Out of Service Routing

About this task

The use of alternate routing allows automatic overflow of calls when no primary trunks are available. The same alternate ARS can also be used to allow manual control of when the alternate ARS is used. This can be useful in scenarios where it is known that the primary trunks will be unavailable; for example for maintenance.

Once configured, the use of an out of service route can be enabled/disabled through IP Office Manager or using short codes with the **Disable ARS Form** and **Enable ARS Form** features.

Procedure

1. Using IP Office Manager, receive the configuration from the primary server.
2. Expand the configuration of the primary server and select ARS.
3. Click on the  icon to add a new ARS record.
 - a. Set the **Route Name** to something suitably descriptive such as **Fallback**.

- b. Add a short code that will route calls from this ARS record to the secondary server: **?/Dial/.99998**
 - c. Click **OK**.
4. In the ARS record 50:Main on the primary, we need to set the record to failover to using the fallback ARS when a route to the primary cannot be seized within the required time.
 5. In the **Alternate Route** drop down select the fallback ARS created above.
 6. Set the **Alternate Route Priority Level** to **5**.

This is the highest level of priority. It means that users with a lower priority need to wait for the **Alternate Route Wait Time** before calls overflow to the secondary when there are no available primary trunks. The default user priority is 5.
 7. Click **OK**.
 8. Save the configuration.

Related links

[Primary ARS Fallback to Secondary Trunks](#) on page 77

Chapter 13: Configuring Media Preservation

On calls involving links between systems, the invoking of resilience mode can potentially interrupt existing calls as re-registration occurs. Media connection preservation can help prevent this if required. This feature is supported for the following telephones on IP Office Release 9.1 or higher. It can be applied to calls between systems and via SIP trunks:

- IP Office Release 9.1+ : 9608, 9611, 9621, 9641
- IP Office Release 11.0+ : J139, J159, J169, J179, J189, Avaya Workplace Client

On those phones, if a call experiences end-to-end signaling loss or refresh failures but still has an active media path, call preservation allows the call to continue. While preserving a call, the phone does not attempt to re-register with its call server or attempt to failover to a standby call server until the preserved call has ended. The maximum duration of a preserved call is two hours after which it is automatically ended.

Calls on hold and calls to hunt groups are not preserved. Only the following call types are preserved:

- Connected active calls.
- Two-party calls where the other end is a phone, trunk or voicemail.
- Conference calls.

During a preserved call the only permitted action is to continue speaking and then end the call. The phone's softkey actions and feature menus do not work. Call preservation can be enabled at the system level and for individual trunks. The system level setting control use of call preservation on the system's IP Office lines and H.323 IP phones. All systems in the network must be configured for call preservation to ensure end to end connection support. By default, the system setting is also automatically applied to all SIP trunks. However, the trunk setting for each trunk can be individually altered.

When does media connection preservation occur?

This is an immediate feature applied to all qualifying calls currently in progress. It ends when the call ends.

Related links

[Configuring the System Setting](#) on page 81

[Configuring the SIP Line Setting](#) on page 81


[Adjusting the Media Connection Preservation Time](#) on page 82

Configuring the System Setting

About this task

Note that the default setting for SIP lines is to match the system setting set below. Therefore, if different operation of SIP trunks or a SIP trunk is required, the trunk must be configured separately.

Procedure

1. Using IP Office Manager, retrieve the configuration from the IP Office system.
2. Select **Configuration**.
3. Select the system from the navigation tree and click on  **System**.
4. Select Telephony and then select the **Telephony** sub-tab.
5. Change the **Media Connection Preservation** setting as required.
 - Disabled: If selected, call preservation is not attempted for any calls.
 - Enabled: If selected, call preservation is attempted for supported telephones and for IP Office lines.
6. Click **OK**.
7. Save the configuration.

Related links

[Configuring Media Preservation](#) on page 80

Configuring the SIP Line Setting

About this task

By default, all SIP trunks use the same setting applied to the system . However, each trunk can be configured separately to use its own setting.

Procedure

1. Using IP Office Manager, retrieve the configuration from the IP Office system.
2. Select **Configuration**.
3. Select the system from the navigation tree.
4. Click on **Line**. The list of existing lines is shown.
5. Select the SIP line that needs to be adjusted.
6. Select the **SIP Advanced** tab.
7. Change the **Media Connection Preservation** setting as required.
 - **System**: Apply the setting set for the system

- **Disabled:** If selected, call preservation is not attempted for any calls.
 - **Enabled:** If selected, call preservation is attempted for calls.
8. Click **OK**.
 9. Save the configuration.

Related links

[Configuring Media Preservation](#) on page 80

Adjusting the Media Connection Preservation Time

By default, active call connections are preserved for up to 120 minutes, after which they are automatically disconnected. Call connections on which the IP Office system cannot detect any activity are automatically disconnected after 10 minutes.

These timeouts can be adjusted using the following `NoUser` source numbers:

- **PRESERVED_CONN_DURATION=<Minutes (1 to 120)>**

When **System | Telephony | Telephony | Media Connection Preservation** is enabled, active calls are preserved for up to 120 minutes before being disconnected.. This `NoUser` source number can be used to adjust the duration in the range 1 to 120 minutes.

- **PRESERVED_NO_MEDIA_DURATION=<Minutes (1 to 120)>**

When **System | Telephony | Telephony | Media Connection Preservation** is enabled, calls on which no RTP, RTCP or speech is detected are disconnected after 10 minutes. This `NoUser` source number can be used to adjust the duration in the range 1 to 120 minutes.

Related links

[Configuring Media Preservation](#) on page 80

Chapter 14: Monitoring Resilience

There are a number of methods by which the different resilience features can be monitored.

Related links

- [Resiliency Alarms](#) on page 83
- [Resilience Indication on Phones](#) on page 83
- [IP Office Line Status](#) on page 84
- [one-X Portal for IP Office Status](#) on page 85
- [DECT Trunk Resilience](#) on page 86

Resiliency Alarms

For IP Office R11.0 and higher, the IP Office system providing resiliency support outputs an alarm when failover occurs.

- The alarm is generated whenever phones registered to another IP Office begin failing over to the system.
- A separate alarm is generated for each IP Office from which phones failover to the system.

The alarm is output as a standard system alarm configured through the **System > System Events** menu. Therefore, the alarm can be directed to System Status Application, email, Syslog and/or SNMP.

Related links

- [Monitoring Resilience](#) on page 83

Resilience Indication on Phones

The following indicators may appear on phones during failover scenarios:

- **R - IP Phone Resilience Indication:**

An **R** is displayed on phones when they are operating in resilient mode. This is supported by 1600, 9600 and J100 Series phones. If using DECT provisioning, it is also supported on 3700 Series DECT phones.

- **! - User Settings Retrieval Failure:**

If, when a user hots desk onto a phone on another system, it is not able to obtain their full settings from either their home or failover system, the phone displays !. They can still continue to use the phone to make and answer calls but will not have access to all their settings. This is supported by 1600, 9600 and J100 Series phones.

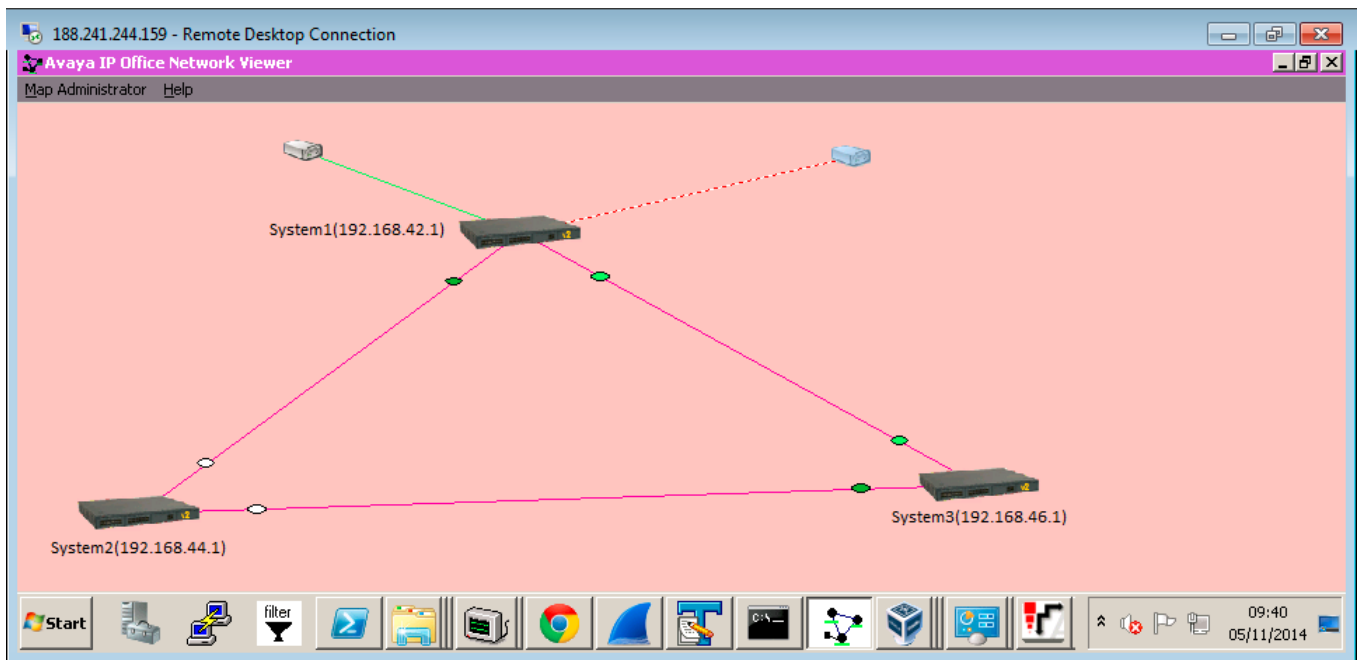
Related links

[Monitoring Resilience](#) on page 83

IP Office Line Status

The Network Viewer within System Monitor shows the IP Office lines between systems in a visual format. It also indicates the status of the lines.

Network view is currently not supported when using TCP, HTTP or HTTPS to connect System Monitor to the system.



The viewer indicates the status of each link by changing the color of the status dot next to the system hosting the line.

- Red = Link Down (non-resilient link)
- Light Green = Link Up (non-resilient link)
- White = Link Up (Resilient slave - "I provide Backup and I do not request Backup")
- Yellow = Link down (Resilient slave - "I am actively providing Backup")

- Dark Green = Link up (Resilient master)
- Orange = Link down - pending (Resilient slave)

Related links

[Monitoring Resilience](#) on page 83

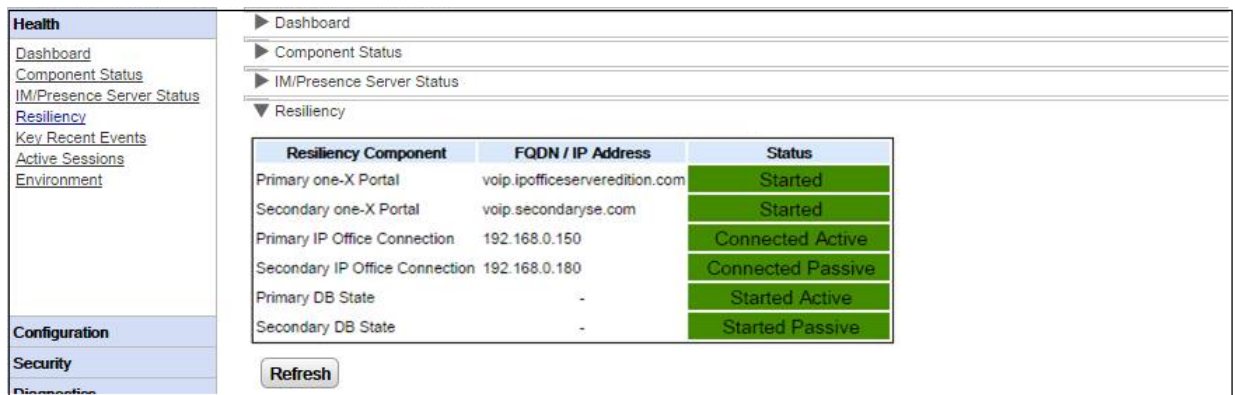
one-X Portal for IP Office Status

About this task

This menu is shown on IP Office Select network portal server. It shows the current status of the portal's server connections.

Procedure

1. Login to the portal administrator menus.
2. Select **Health** and then **Resiliency**.



- **Started:** Indicates that the server or service is running.
- **Stopped:** Indicates that the server or service is not running.
- **Connected:** Indicates that a connection to the server is available.
- **Active:** Indicates that the server or connection is running and is currently being used to support portal users.
- **Passive:** Indicates that the server or connection is running but is not currently being used to support portal users.

Related links

[Monitoring Resilience](#) on page 83

DECT Trunk Resilience

Using System Status Application you can view the status of both an IP Office system and also any DECT systems to which it is connected. This is done by selecting **System > IP DECT Systems**. Selecting the IP DECT System then displays details of the particular system and extensions being supported by that system.

The addresses and status of the mirrored master base stations is indicated. For the extensions, the connection being used is also indicated.

The screenshot shows the AVAYA IP Office System Status application. The left sidebar contains a navigation menu with options like System, Hard Disks, H.323 Extensions, IP DECT Systems (1), Alarms (9), Extensions (3), Trunks (0), Active Calls, Resources, Voicemail, IP Networking, and Locations. The main content area is titled 'IP DECT System Status' and displays the following information:

Node Address: 192.168.42.200
 Type: DECT R4
 Master IP Address: 192.168.42.211
 Master Status: Up
 Standby Master IP Address: 192.168.42.212
 Standby Master Status: Up

Extensions:

| Extension Number | Telephone Type | Active Location | Connection |
|------------------|----------------|-----------------|----------------------|
| 705 | 3740 | LOCAL | Primary PBX - Master |
| 706 | 3725 | LOCAL | Primary PBX - Master |
| 707 | 3725 | LOCAL | Primary PBX - Master |
| 708 | 3725 | LOCAL | Primary PBX - Master |
| 709 | 3725 | LOCAL | Primary PBX - Master |
| 710 | 3725 | LOCAL | Primary PBX - Master |
| 711 | 3725 | LOCAL | Primary PBX - Master |
| 712 | 3725 | LOCAL | Primary PBX - Master |
| 713 | 3725 | LOCAL | Primary PBX - Master |
| 714 | 3725 | LOCAL | Primary PBX - Master |
| 715 | 3725 | LOCAL | Primary PBX - Master |

At the bottom of the application, there are control buttons: Pause, Switch to Primary Node, Switch to Backup Node, and Unsubscribe. The status bar at the bottom right shows the time 16:43:28 and the system is Online.

The menu provides a number of controls:

- **Unsubscribe:** Force the selected extension to unsubscribe.
- **Switch to Backup Node:** Force the DECT connection to switch to the failover IP Office.
- **Switch to Primary Node:** Force the DECT connection to switch from the failover IP Office to the home IP Office. This option is required if the setting **Prioritize Primary** is not selected, see [Configuring DECT Resilience](#) on page 69.

Related links

[Monitoring Resilience](#) on page 83

Chapter 15: Additional Help and Documentation

The following pages provide sources for additional help.

Related links

[Additional Manuals and User Guides](#) on page 87

[Getting Help](#) on page 87

[Finding an Avaya Business Partner](#) on page 88

[Additional IP Office resources](#) on page 88

[Training](#) on page 89

Additional Manuals and User Guides

The [Avaya Documentation Center](#) website contains user guides and manuals for Avaya products including IP Office.

- For a listing of the current IP Office manuals and user guides, look at the [Avaya IP Office™ Platform Manuals and User Guides](#) document.
- The [Avaya IP Office Knowledgebase](#) and [Avaya Support](#) websites also provide access to the IP Office technical manuals and users guides.
 - Note that where possible these sites redirect users to the version of the document hosted by the [Avaya Documentation Center](#).

For other types of documents and other resources, visit the various Avaya websites (see [Additional IP Office resources](#) on page 88).

Related links

[Additional Help and Documentation](#) on page 87

Getting Help

Avaya sells IP Office through accredited business partners. Those business partners provide direct support to their customers and can escalate issues to Avaya when necessary.

If your IP Office system currently does not have an Avaya business partner providing support and maintenance for it, you can use the Avaya Partner Locator tool to find a business partner. See [Finding an Avaya Business Partner](#) on page 88.

Related links

[Additional Help and Documentation](#) on page 87

Finding an Avaya Business Partner

If your IP Office system currently does not have an Avaya business partner providing support and maintenance for it, you can use the Avaya Partner Locator tool to find a business partner.

Procedure

1. Using a browser, go to the [Avaya Website](#) at <https://www.avaya.com>
2. Select **Partners** and then **Find a Partner**.
3. Enter your location information.
4. For IP Office business partners, using the **Filter**, select **Small/Medium Business**.

Related links

[Additional Help and Documentation](#) on page 87

Additional IP Office resources

In addition to the documentation website (see [Additional Manuals and User Guides](#) on page 87), there are a range of website that provide information about Avaya products and services including IP Office.

- [Avaya Website](#) (<https://www.avaya.com>)

This is the official Avaya website. The front page also provides access to individual Avaya websites for different regions and countries.

- [Avaya Sales & Partner Portal](#) (<https://sales.avaya.com>)

This is the official website for all Avaya business partners. The site requires registration for a user name and password. Once accessed, you can customize the portal to show specific products and information type that you want to see.

- [Avaya IP Office Knowledgebase](#) (<https://ipofficekb.avaya.com>)

This site provides access to an online, regularly updated version of IP Office user guides and technical manual.

- [Avaya Support](#) (<https://support.avaya.com>)

This site provide access to Avaya product software, documentation and other services for Avaya product installers and maintainers.

- [Avaya Support Forums](https://support.avaya.com/forums/index.php) (<https://support.avaya.com/forums/index.php>)

This site provides forums for discussing product issues.

- [International Avaya User Group](https://www.iuag.org) (<https://www.iuag.org>)

This is the organization for Avaya customers. It provides discussion groups and forums.

- [Avaya DevConnect](https://www.devconnectprogram.com/) (<https://www.devconnectprogram.com/>)

This site provides details on APIs and SDKs for Avaya products, including IP Office. The site also provides application notes for third-party non-Avaya products that interoperate with IP Office using those APIs and SDKs.

- [Avaya Learning](https://www.avaya-learning.com/) (<https://www.avaya-learning.com/>)

This site provides access to training courses and accreditation programs for Avaya products.

Related links

[Additional Help and Documentation](#) on page 87

Training

Avaya training and credentials ensure our Business Partners have the capabilities and skills to successfully sell, implement, and support Avaya solutions and exceed customer expectations. The following credentials are available:

- Avaya Certified Sales Specialist (APSS)
- Avaya Implementation Professional Specialist (AIPS)
- Avaya Certified Support Specialist (ACSS)

Credential maps are available on the [Avaya Learning](#) website.

Related links

[Additional Help and Documentation](#) on page 87

Index

Numerics

| | |
|-------------------|---|
| 1100 Series | 30 , 34 |
| 1200 Series | 30 , 34 |
| 1600 Series | 30 , 34 |
| 3700 | 18 , 69 |
| 9600 Series | 30 , 34 |

A

| | |
|----------------------------|---|
| active master | 7 , 19 , 73 |
| active mirror | 75 |
| Administrator | 87 |
| alternate | |
| gatekeeper | 15 |
| route | 21 |
| alternate gatekeeper | 40 |
| alternate route | 78 |
| APIs | 88 |
| Application Notes | 88 |
| ARS | 21 , 78 |
| out of service | 78 |
| Avaya SIP softphones | |
| B179 | 30 |
| E129 | 30 |
| H175 | 30 |
| Avaya SIP Softphones | |
| B179 | 34 |
| E129 | 34 |
| H175 | 34 |

B

| | |
|-----------------------------------|---|
| B179 | 43 |
| backup voicemail IP Address | 56 |
| base station | 19 , 73 |
| master | 75 |
| status | 86 |
| switch | 86 |
| breakout | 21 , 76 |
| controls | 76 |
| business partner locator | 88 |

C

| | |
|------------------------|---|
| call assistant | 20 |
| capacities | 25 |
| certificates | 25 |
| conference | 15 , 80 |
| conference calls | 80 |
| configuration | |
| wizard | 30 , 34 |

| | |
|-----------------|--------------------|
| configuring | |
| B179 | 43 |
| voicemail | 53 |
| courses | 88 |

D

| | |
|------------------------------|--------------------|
| DECT capacity | 18 |
| DECT extension | 18 |
| DECT master resilience | 19 |
| DECT resilience | 18 |
| detect extension | 69 |
| DHCP | 40 |
| disable | |
| ARS form | 78 |
| domain | 25 |
| mail | 58 |
| during | |
| failover | 10 |

E

| | |
|----------------------------|---|
| enable | |
| ARS form | 78 |
| extension | |
| resilience | 15 , 40 |
| extension capacities | 25 |
| extension capacity | 18 , 30 , 34 , 69 |
| extensions maximum | 25 |
| external | |
| call resilience | 21 |
| external calls | 7 |

F

| | |
|---------------------|--------------------|
| Failback | 7 |
| failover | |
| configuration | 10 |
| Failover | 7 |
| forums | 88 |

H

| | |
|---------------------------|--------------------|
| hardware resilience | 19 |
| held calls | 80 |
| Help | 87 |
| hunt group | 19 |
| hunt groups | 34 |

I

| | |
|-------------------------|--------------------|
| internal twinning | 15 |
|-------------------------|--------------------|

| | | | |
|------------------------------|------------------------|---------------------------------|------------------------|
| IP DECT | 69 | resilience (<i>continued</i>) | |
| IP DECT phones | 34 | trunk | 7 |
| IP office | | virtual server | 7 |
| adding | 33 | WebRTC | 7 |
| status | 85 | Resilience | 7 |
| IP office line | 33, 45 | | |
| adding | 45 | | |
| IP phone | | S | |
| capacity | 25 | sales | 88 |
| resilience | 15 | SDKs | 88 |
| | | short code | |
| L | | ARS form | 78 |
| link to another | 33, 45 | short codes | 21 |
| | | SIP | |
| M | | domain | 25 |
| Manager | 34 | SMTP | |
| Manuals | 87 | receiver | 58 |
| monitoring | | sender | 58 |
| base station | 73 | support | 88 |
| | | switch | |
| O | | configuration | 10 |
| one-x portal | | switch to backup mode | 86 |
| IP office resilience | 20 | switch to primary node | 86 |
| IP office status | 85 | System Administrator | 87 |
| one-X portal | 34 | system conference | 15 |
| one-X resiliency | 64 | | |
| out of service routing | 21 | T | |
| outgoing calls | 21 | Technical Bulletins | 88 |
| | | topology | |
| P | | voicemail | 54 |
| passive master | 73 | training | 88, 89 |
| phone capacity | 30, 34 | trunk | |
| portal | | resilience | 21 |
| status | 85 | | |
| | | U | |
| Q | | unsubscribe | 86 |
| Quick Reference Guides | 87 | user | |
| | | settings | 10 |
| R | | User Guides | 87 |
| Reseller | 87 | | |
| resilience | 20, 56 | V | |
| base station | 7 | view | |
| call | 7 | DECT master | 86 |
| DECT | 7 | voice | |
| DHCP | 15 | SMTP | 58 |
| hardware | 7 | voicemail | 34 |
| hunt group | 7 | destination | 56 |
| IP phones | 7 | resilience | 53 |
| one-x portal | 7 | service | 53 |
| phone | 15 | type | 56 |

W

| | |
|----------------|--------------------|
| websites | 88 |
|----------------|--------------------|