IP Office™ Platform 10.1

IP Office Resilience Overview

Issue 02a - (05 July 2017)

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 by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. 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 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. Refer to your sales agreement 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 You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

"Hosted Service" means a 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 IF YOU PURCHASE A 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 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. YOUR USE OF THE HOSTED SERVICE SHALL BE LIMITED BY THE NUMBER AND TYPE OF LICENSES PURCHASED UNDER YOUR CONTRACT FOR THE HOSTED SERVICE, PROVIDED, HOWEVER, THAT FOR CERTAIN HOSTED SERVICES IF APPLICABLE, YOU MAY HAVE THE OPPORTUNITY TO USE FLEX LICENSES, WHICH WILL BE INVOICED ACCORDING TO ACTUAL USAGE ABOVE THE CONTRACT LICENSE LEVEL. CONTACT AVAYA OR AVAYA'S CHANNEL PARTNER FOR MORE INFORMATION ABOUT THE LICENSES FOR THE APPLICABLE HOSTED SERVICE, THE AVAILABILITY OF ANY FLEX LICENSES (IF APPLICABLE), PRICING AND BILLING INFORMATION, AND OTHER IMPORTANT INFORMATION REGARDING THE HOSTED SERVICE.

Licenses
THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, UNDER THE LINK "AVAYA SOFTWARE LICENSE TERMS (Avaya Products)" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. "Software" means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Instance" means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine ("VM") or similar deployment.

License type(s)
Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "Unit" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

Database License (DL). End User may install and use each copy or an Instance of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than one Instance of the same database.

CPU License (CP). End User may install and use each copy or Instance of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee.

Named User License (NU). You may: (i) install and use each copy or Instance of the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use each copy or Instance of the Software on a Server so long as only authorized Named Users access and use the Software. "Named User", means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickthrough" license accompanying or applicable to the Software ("Shrinkwrap License").

Heritage Nortel Software
"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at https://support.avaya.com/LicenseInfo under the link "Heritage Nortel Products" or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

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

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

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

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

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

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

Customer acknowledges and agrees that it is responsible for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: https://support.avaya.com or such successor site as designated by Avaya.

Security Vulnerabilities

Information about Avaya’s security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security. Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

Downloading Documentation

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

Contact Avaya Support

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

Contents

1. IP Office Server Edition Resilience

2. Design Considerations

3. Configuring General Resilience

4. Configuring IP Phone Resilience

5. Configuring Voicemail Resilience

6. Configuring one-X Portal for IP Office Resilience

7. Configuring DECT Resilience

8. Configuring DECT Master Resilience

9. Configuring Trunk Resilience

10. Configuring Media Preservation

11. Monitoring Resilience

12. Document History

Chapter 1.

IP Office Server Edition Resilience

1. IP Office Server Edition Resilience

An IP Office Server Edition network can consist of multiple servers, each hosting different services and spread over multiple locations. Resilience refers to a set of features intended to ensure some degree of continued operation when any of those services or servers becomes unavailable for some reason.

Resiliency refers to a failure of normal operation. It indicates an issue in the network such as the loss of a service, server or network connection. The cause may be a temporary event due to maintenance activity or it may indicate a more serious failure. During resilience, the priority must always be to resolve the cause of why resilient mode was invoked.

- **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.

1.1 Glossary

- **Alternate Gatekeeper**
  For IP telephones, the system to which they attempt to register during failover.
- **Backup**
  The system to which the user, phone, application or server is supported when failover occurs.
- **Fallback**
  Another term for 'failover'. The confusion between fallback and failback is utterly unfortunate.
- **Failback**
  The process whereby, when an original server or service recovers or becomes accessible again, it resumes operation from any failover servers or services.
- **Failover**
  The process whereby, if a server or service fails or is no longer accessible, another one takes over its operation.
- **Home**
  The server from which the user, phone, application or service is supported during normal operation.
- **Normal Operation**
  The state of the network when no applications, services or servers are in failover.
- **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.

1.2 Resilience Features

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

Resiliency Feature	Summary	IP Office Server Edition	IP Office Select
Call Resilience 12	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.	Yes	Yes
User Resilience 11	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.	Yes	Yes
Hunt Group Resilience 15	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.	Yes	Yes
IP Phone Resilience (Basic) 13	Avaya IP phones registered with one system can automatically reregister with another system when resilience is required.	Yes	Yes
IP Phone Resilience (Select) 14	Building on standard IP phone resilience, in IP Office Select mode, IP Phone resilience above can be to another expansion system based on location settings.	–	Yes
Voicemail Resilience 19	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's users during resilience.	Yes	Yes
DECT Resilience 14	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.	Yes	Yes
DECT Master Resilience 15	Each DECT R4 system includes one base station configured as the master base station. Base station mirroring allows two base stations to be configured as the master. Whilst only one is active at any time, the other becomes active if the existing master is not available for some reason.	Yes	Yes
one-X Portal Resilience 16	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.	–	Yes
Virtualized Server Resilience 18	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.	Yes	Yes
Hardware Resilience 18	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.	Yes	Yes
Trunk Resilience 17	Through individual system configuration, systems can fallback to using alternative trunk groups.	Yes	Yes

1.2.1 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.

- 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, essentially the user's name, extension number, login code, home system and current (if hot desked) system. This is sufficient for other systems to correctly route calls to other 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 doesn't 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.

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 failback occur?

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

The failback delay allows certainty that the home system has recovered and is stable if it was the cause of 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.

1.2.2 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.

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.

Media Connection Preservation (MCP)

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:

- **9608**
- **9611**
- **9621**
- **9641**

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 reregister 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.

1.2.3 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.

- Failover is intended to only provide basic call functionality while the cause of failover is fixed. User changes to their settings during failover are lost after failback.
- Calls through the system are disconnected by failover. Direct media calls may continue but this is not guaranteed. See Call Resilience 12.
- 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 indefinitely as a "guest". The guest phones do not consume any licenses.
- 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	SIP		SIP Softphones[2]	DECT R4
• 1600 Series • 9600 Series	• 1120[1] • 1140[1] • 1220[1] • 1230[1]	• E129 • B179[2] • H175[1] • J129	• Avaya Communicator for Windows • one-X Mobile Preferred for Android • one-X Mobile Preferred for iOS	• All supported Avaya DECT R4 handsets.

1. These phones obtain their failover address via the IP Office auto-generated settings files.
2. These Avaya SIP Phones cannot obtain their failover address from the IP Office system at restart. Instead they require manual configuration.
3. SIP softphone clients also require one-X Portal for IP Office resilience 16 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, that failover system begins allowing the IP phones to re-register with it. Phones with existing calls using media connection preservation 12 which 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?

Once 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 referred to as "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.

1.2.4 IP Phone Resilience (Select)

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

Building on standard IP phone resilience, in IP Office Select mode, IP Phone resilience above can be to another expansion system based on location settings.

Location based resilience is supported on Avaya 1600 and 9600 series phones and all SIP endpoints.

1.2.5 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 15 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 DECT phones (3720, 3725, 3740, 3745 and 3749) 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 56.

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 56. In that case, control of failback is through System Status Application 78.

1.2.6 DECT Master Resilience

Each DECT R4 system includes one base station configured as the master base station. Base station mirroring allows two base stations to be configured as the master. Whilst only one is active at any time, the other becomes active if the existing master is not available for some reason.

For base station resiliency, two base stations are configured to act as 'mirrored' master base stations. One becomes the active master base station whilst the other becomes a standby master base station. 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 non-master 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 14 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.

1.2.7 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.

1.2.8 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 13 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 phone failover.

When Does Hunt Group Failback Occur?

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

1.2.9 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.

For IP Office Release 10, 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 mode. Portal resilience can also be configured when using 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:
  - Portal browser access.
  - one-X Communicator clients.
  - one-X Mobile Preferred clients.
  - Portal call assistant.
  - SoftConsole presence indication.
- Whilst resilience may appear to work between servers running different levels of portal software this is not supported. 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.

When Does Portal Failover Occur?

- **On primary server portal failure**
  If the primary server's portal service stops for some reason, the portal service on the secondary server automatically becomes available.
  - Users who were logged into the portal on the primary are able to 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 referred as "Standalone Mode".

When Does Portal Failback Occur?

- **On primary server portal recovery:**
  When the primary server's portal service is available again, the portal service on the secondary server stops supporting 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.

1.2.10 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.

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 68.

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 69.

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.

See Configuring Break Out Controls 67.

1.2.11 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.

1.2.12 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's 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 severs 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 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 severs. 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 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?

Once the server is available again, failback occurs once all active voicemail calls have ended and server SMTP synchronization is complete. 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 28.

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. See Configuring Voicemail Resilience 44.

1.3 When Does Failover Occur

Resiliency Feature	When does failover occur
User Resilience 11	If the home system is not visible to its failover system for at least 3 minutes.
Hunt Group Resilience 15	Hunt group failover occurs at the same time as IP phone failover.
IP Phone Resilience 13	If the home system is no longer visible to the failover system for at least 3 minutes, that failover system begins allowing the IP phones to re-register with it. Phones with existing calls using media connection preservation 12 which do not failover until that call ends.
Voicemail Resilience 19	Voicemail failover is automatically triggered by IP Phone failover coming into operation. It can also be manually triggered through System Status Application using the **Activate Backup Server** button.
DECT Resilience 14	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 56.
DECT Master Resilience 15	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 16	The failover portal becomes active immediately the primary portal is stopped or not visible.

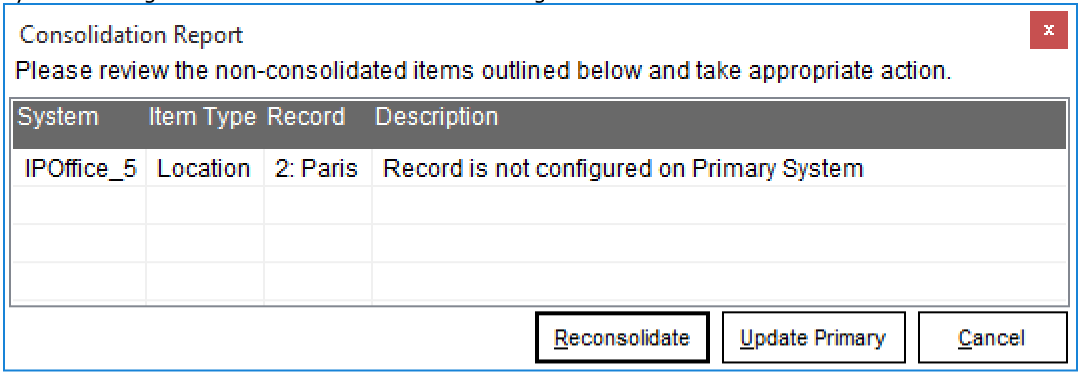
1.4 When Does Failback Occur

Resiliency Feature	When does failback occur
User Resilience 11	Once the home system has been visible again for more than 10 minutes.
Hunt Group Resilience 15	Hunt group failback occurs at the same time as IP phone failback.
IP Phone Resilience 13	Once 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 referred to as "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.
Voicemail Resilience 19	Once the server is available again, failback occurs once all active voicemail calls have ended and server SMTP synchronization is complete. However, manual failback or failback after a set time can be configured. Manual failback in control using System Status Application.
DECT Resilience 14	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 56. In that case, control of failback is through System Status Application 78.
DECT Master Resilience 15	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 16	The secondary portal returns control to the primary portal once it is available or visible again.

1.5 System Configuration During Failover

The following configuration limitations are applied during failover:

- **User telephony changes**
  Any telephony setting changes (forward number, DND, etc.) made during failover are lost following failback.
- **one-X Portal for IP Office Configuration**
  Any portal configuration changes a user make whilst logged into the secondary portal during resilience are lost following failback.
- **DECT Configuration**
  No changes to the DECT configuration or additional handset subscriptions are allowed during failover.
- **IP Office Configuration**
  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 via the secondary server. Following failover, when the configurations are next loaded, IP Office Manager highlights unsynchronized configuration changes. Guest users and extensions supported by a system during failover are not visible in the configuration of their failover host.



Consolidation Report

Please review the non-consolidated items outlined below and take appropriate action.

System	Item Type	Record	Description
IPOffice_5	Location	2: Paris	Record is not configured on Primary System

  - **Reconsolidate**
    Update the configuration of all servers in the network.
  - **Update Primary**
    Update the configuration of just the primary server.

Chapter 2. Design Considerations

2. Design Considerations

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

2.1 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 the additional users and extension but also the additional calls, hunt groups, etc. For system capacity details, refer to the "Avaya IP Office Platform Capacity Planning Guidelines" 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. That also includes any other systems in resilience to that remote server at the same time. Extensions and users beyond the support capacity do not receive resilience support. See System Capacities 24.

- **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 support capacities. That also includes any other systems in resilience to that remote server at the same time. Extensions and users beyond the support capacity do not receive resilience support. See System Capacities 24.

2.2 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.

To install Avaya root certificates on secondary servers and clients:

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. **Subject Name:** IP Office's fully qualified domain name (FQDN).
   b. **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. **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. Click the link in the message to download and save the certificate in the ***.p12*** format.
5. 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**.
6. Now, log in to the primary server's web control menus and download the root certificate.
7. Install this root certificate in the systems where required.

2.3 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/IP Office Select network relies on the customer's own data network over which the traffic of the IP Office lines is routed. However, the routes between sites within that data network may not necessarily match the configured IP Office lines. This can cause scenarios where failover occurs but the resilience features are not accessible to some users, or users attempt to use resilience features when they are not invoked.

- **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.

  - **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 a site B and so starts failover support for site B.

    - At site B, the result depend 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 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.

2.4 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.

2.5 Licensing

If the license 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 failover servers acting as hosts guest users and extensions during failover do not require any licenses. They inherit the guest users and extensions licenses for the duration of failover or until restarted.

Chapter 3. Configuring General Resilience

3. Configuring General Resilience

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

3.1 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. That also includes any other systems in resilience to that remote server at the same time. Extensions and users beyond the support capacity do not receive resilience support. See System Capacities 24.

- **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 31.

- **WARNING**
  Using the resiliency administration wizard overrides any lines configured for location based administration 40.

To configure resilience using the IP Office Manager wizard:

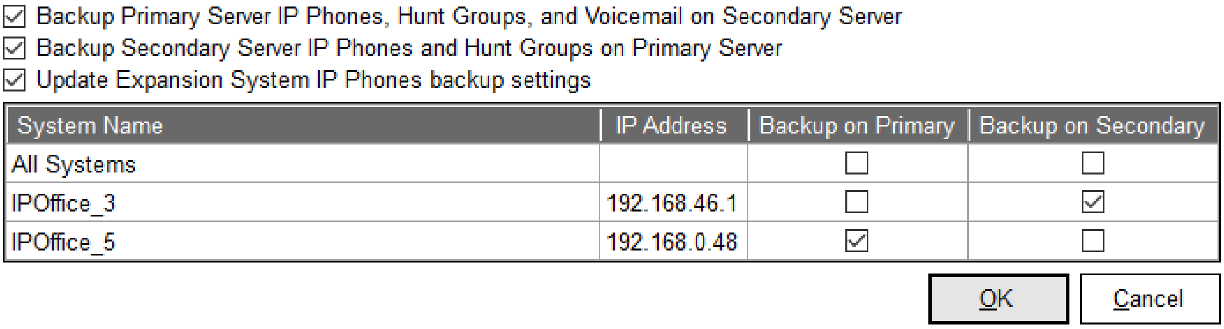
1. Using IP Office Manager, receive the configuration from the primary server. The configuration opens at the solution page. If already in the configuration, click on **Solution** in the navigation tree on the left.

2. Check that all the expected servers are listed as having there configuration present at the bottom of the screen and that each has a **Bothway** link to the primary and, if present, secondary server. If otherwise, resolve those issues before configuring resilience.

3. 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.

4. Select the general resilience options that you want applied between systems in the network.

   - **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

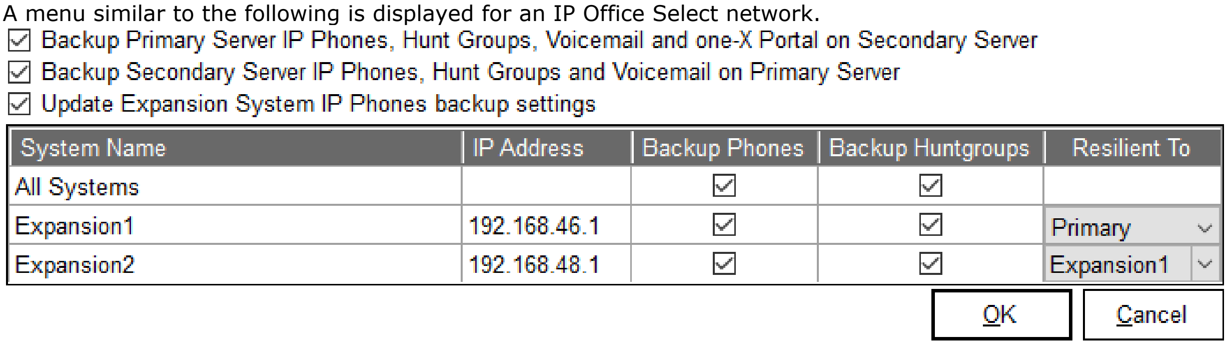
System Name	IP Address	Backup on Primary	Backup on Secondary
All Systems		☐	☐
IPOffice_3	192.168.46.1	☐	☑
IPOffice_5	192.168.0.48	☑	☐

- **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 56. 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 56. 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.

- **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		☑	☑	
Expansion1	192.168.46.1	☑	☑	Primary
Expansion2	192.168.48.1	☑	☑	Expansion1

  - **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 56, portal support also requires configuring one-X Portal for IP Office resilience 50. 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 requires configuring DECT trunk resilience 56, portal support also requires configuring one-X Portal for IP Office resilience 50. 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 30, then selection of another expansion is also possible. Not selecting an option disables those resilience settings for the expansion system.

5. Click **OK**.

6. Save the changes.

3.2 Adding Expansion to Expansion Lines

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.

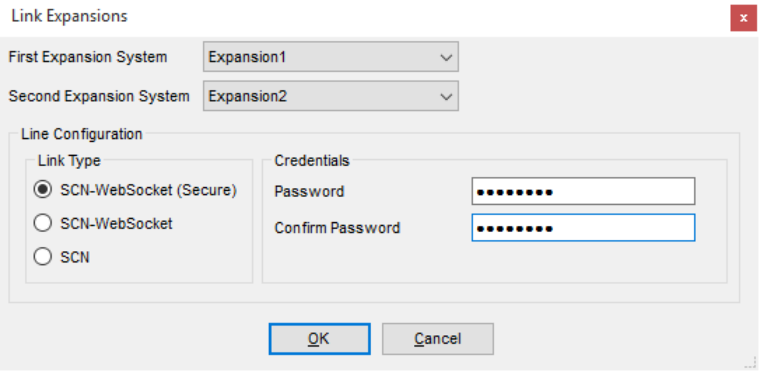
You must still ensure that the failover system has sufficient capacity 24 to host the additional extensions and users during failover.

To link expansion systems:

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

1. Open Manager and log in to the primary server.

2. On the **Solution** page, on the left under **Link** click **Expansion System**.



Link Expansions

First Expansion System: Expansion1

Second Expansion System: Expansion2

Line Configuration

Link Type

● SCN-WebSocket (Secure)

○ SCN-WebSocket

○ SCN

Credentials

Password: ••••••••

Confirm Password: ••••••••

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 76 to confirm the operation of the new lines between the two expansion systems.

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

3.3 Using the Individual System Line Settings

The solution wizard 28 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.

3.3.1 ... Using IP Office Manager

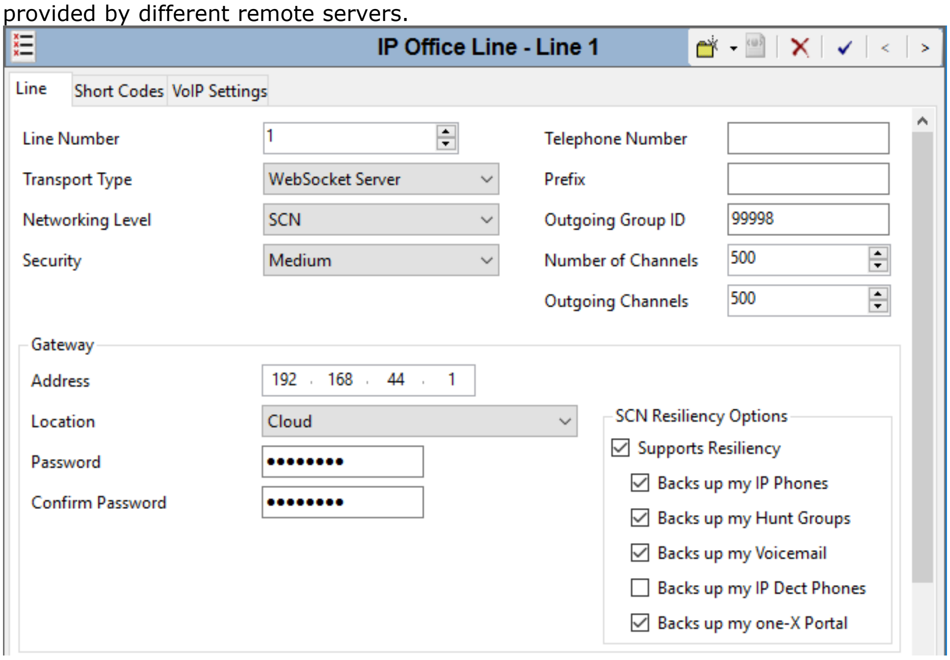
To configure resilience using the IP Office Manager line settings:

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.



IP Office Line - Line 1

Line | Short Codes | VoIP Settings

Line Number: 1
Transport Type: WebSocket Server
Networking Level: SCN
Security: Medium
Telephone Number:
Prefix:
Outgoing Group ID: 99998
Number of Channels: 500
Outgoing Channels: 500

Gateway
Address: 192 . 168 . 44 . 1
Location: Cloud
Password: ••••••••
Confirm Password: ••••••••

SCN Resiliency Options
☑ Supports Resiliency
☑ Backs up my IP Phones
☑ Backs up my Hunt Groups
☑ Backs up my Voicemail
☐ Backs up my IP Dect Phones
☑ Backs up my one-X Portal

5. Select the resilience options required.

- **Supports Resiliency**
  Enables support for failover to the remote system on this line. The remote system maintains a backup copy of this system's user records (see User Resilience 11). It begins monitoring the availability of this system in order to determine when to enable failover. Note that this control enables or disables all the available resilience options when clicked. Selecting just this option and none of the below is used when configuring additional lines to support location based resilience 40.

  - **Backs up my IP Phones** 13
    Use the remote system to support this system's Avaya IP telephones during resiliency. Users of SIP softphone client's may also require one-X Portal for IP Office resilience for this to work for them.

    - **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. That also includes any other systems in resilience to that remote server at the same time. Extensions and users beyond the support capacity do not receive resilience support. See System Capacities 24.

    - **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.

  - **Backs up my Hunt Groups** 15
    Use the remote system to support this system's hunt groups during resiliency. This setting requires **Backs up my IP Phones** to also be enabled.

- **Backs up my Voicemail** 19
  Use the remote system to support this system's voicemail during resiliency. This option is only available on lines to the primary and secondary servers.

- **Backs up my IP Dect Phones** 13
  Use the remote system to support this system's DECT R4 telephones during resiliency. This option also requires the DECT R4 system to be configured for DECT Trunk Resilience 56. Use of this setting is subject to the same capacity limits as IP Phone resilience plus the separate total IP DECT extension support limits of the remote server.

  - **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 support capacities. That also includes any other systems in resilience to that remote server at the same time. Extensions and users beyond the support capacity do not receive resilience support. See System Capacities 24.

- **Backs up my one-X Portal** 16
  Use the remote system to support this system's one-X Portal for IP Office users during resiliency.

6. Click **OK**.

7. Repeat the process for any other systems in the network.

8. Save the configuration changes.

3.3.2 ... Using IP Office Web Manager

The solution wizard 28 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.

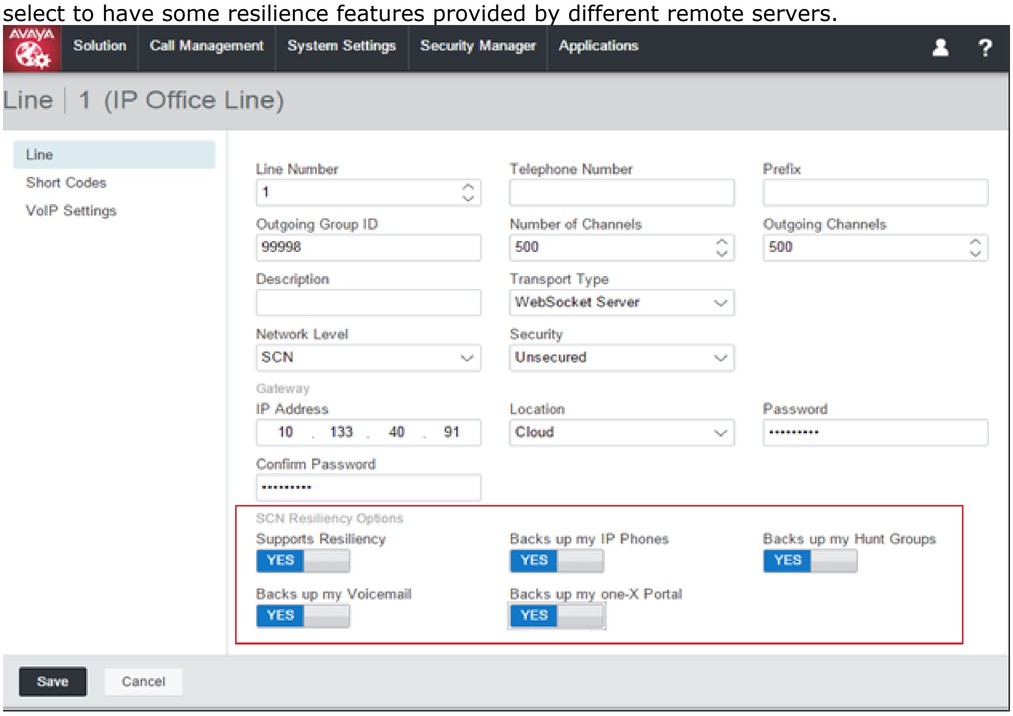
To configure resilience using the IP Office Manager line settings:

1. Using IP Office Web Manager, receive the configuration from the primary server.

2. Select **System Settings**.

3. Select **Line**.

4. Select the line you want to edit. Only one line providing resilience is supported on each system, ie. you cannot select to have some resilience features provided by different remote servers.



Line Number: 1
Telephone Number:
Prefix:
Outgoing Group ID: 99998
Number of Channels: 500
Outgoing Channels: 500
Description:
Transport Type: WebSocket Server
Network Level: SCN
Security: Unsecured
Gateway
IP Address: 10 . 133 . 40 . 91
Location: Cloud
Password: •••••••••
Confirm Password: •••••••••
SCN Resiliency Options
Supports Resiliency: YES
Backs up my IP Phones: YES
Backs up my Hunt Groups: YES
Backs up my Voicemail: YES
Backs up my one-X Portal: YES

5. Select the resilience options required.

   - **Supports Resiliency**
     Enables support for failover to the remote system on this line. The remote system maintains a backup copy of this system's user records (see User Resilience 11). It begins monitoring the availability of this system in order to determine when to enable failover. Note that this control enables or disables all the available resilience options when clicked. Selecting just this option and none of the below is used when configuring additional lines to support location based resilience 40.

- **Backs up my IP Phones** 13
  Use the remote system to support this system's Avaya IP telephones during resiliency. Users of SIP softphone client's may also require one-X Portal for IP Office resilience for this to work for them.

  - **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. That also includes any other systems in resilience to that remote server at the same time. Extensions and users beyond the support capacity do not receive resilience support. See System Capacities 24.

  - **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.

- **Backs up my Hunt Groups** 15
  Use the remote system to support this system's hunt groups during resiliency. This setting requires **Backs up my IP Phones** to also be enabled.

- **Backs up my Voicemail** 19
  Use the remote system to support this system's voicemail during resiliency. This option is only available on lines to the primary and secondary servers.

- **Backs up my IP Dect Phones** 13
  Use the remote system to support this system's DECT R4 telephones during resiliency. This option also requires the DECT R4 system to be configured for DECT Trunk Resilience 56. Use of this setting is subject to the same capacity limits as IP Phone resilience plus the separate total IP DECT extension support limits of the remote server.

  - **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 support capacities. That also includes any other systems in resilience to that remote server at the same time. Extensions and users beyond the support capacity do not receive resilience support. See System Capacities 24.

- **Backs up my one-X Portal** 16
  Use the remote system to support this system's one-X Portal for IP Office users during resiliency.

6. Click **OK**.

7. Repeat the process for any other systems in the network.

8. Save the configuration changes.

3.4 Configuration Update Scenarios

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

3.4.1 Adding an Expansion Server

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

To set the resilience settings for a new expansion sever:

1. Run the general resilience configuration wizard 28.
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.

3.4.2 Adding a Secondary Server

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

To set the resilience settings for a new expansion sever:

1. **Check the voicemail server settings** 44
   Adding a secondary server allows voicemail resilience to be deployed. This requires the two voicemail servers to be synchronized using SMTP connections.
2. **Configure DECT resilience** 50 *(IP Office Select only)*
   For IP Office Select networks, 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 28.
   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.

3.4.3 IP Office Server Edition Upgrade to R10.0

In upgrading to Release 10.0, IP Office Server Edition networks with both primary and secondary servers gain the option to have one-X Portal for IP Office resilience. See Configuring one-X Portal for IP Office Resilience 50.

3.4.4 IP Office Select Upgrade to 10

In upgrading to Release 10.0, IP Office Select networks with both primary and secondary servers gain the option to have one-X Portal for IP Office resilience. See Configuring one-X Portal for IP Office Resilience 50.

The existing voicemail resilience (one active server, one standby) can also be changed to dual active voicemail. See Configuring Voicemail Resilience 44.

Chapter 4. Configuring IP Phone Resilience

4. 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.

- Failover is intended to only provide basic call functionality while the cause of failover is fixed. User changes to their settings during failover are lost after failback.
- Calls through the system are disconnected by failover. Direct media calls may continue but this is not guaranteed. See Call Resilience 12.
- 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 indefinitely as a "guest". The guest phones do not consume any licenses.
- 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	SIP	SIP Softphones[2]	DECT R4
• 1600 Series • 9600 Series	• 1120[1] • 1140[1] • 1220[1] • 1230[1] • E129 • B179[2] • H175[1] • J129	• Avaya Communicator for Windows • one-X Mobile Preferred for Android • one-X Mobile Preferred for iOS	• All supported Avaya DECT R4 handsets.

1. These phones obtain their failover address via the IP Office auto-generated settings files.
2. These Avaya SIP Phones cannot obtain their failover address from the IP Office system at restart. Instead they require manual configuration.
3. SIP softphone clients also require one-X Portal for IP Office resilience 16 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, that failover system begins allowing the IP phones to re-register with it. Phones with existing calls using media connection preservation 12 which 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?

Once 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 referred to as "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.

Configuring IP Phone Resilience

Basic IP phone resilience is configured as part of the general resilience settings. See Configuring General Resilience 28.

- For SIP phone resiliency, all systems in the IP Office Server Edition network must use the same SIP Domain settings (**System | LAN | VoIP**) and these should not be set to IP addresses. The SIP Domain is not the same as the IP Office fully qualified domain name. They are not synonymous but can be related through DNS SRV A records. A single SIP Domain can include multiple SIP servers.

- Resiliency is not supported on remote worker phones which are not on the customer premises. This is in contrast to Remote Worker phones with a remote Primary Gateway address. The use of the alternate gateway's private/public address is determined by the remote extension's configuration setting 38.

- For Avaya Communicator for Windows:

  - The backup server in the application settings is set to the failirover server's FQDN.

  - The domain must be set through the applications user settings (**User Settings | Domain**).

  - The user must login using their extension number.

4.1 Configuring the H323 Failback Mode

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.

To configure the phone failback mode:

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 Fallback** 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**.

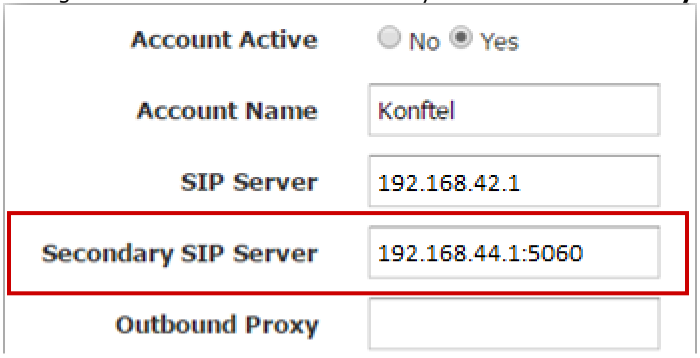
6. Save the configuration.

4.2 B179 Phone Configuration

The B179 phone cannot obtain details of the failover system directly from its home system. Instead it must be configured manually.

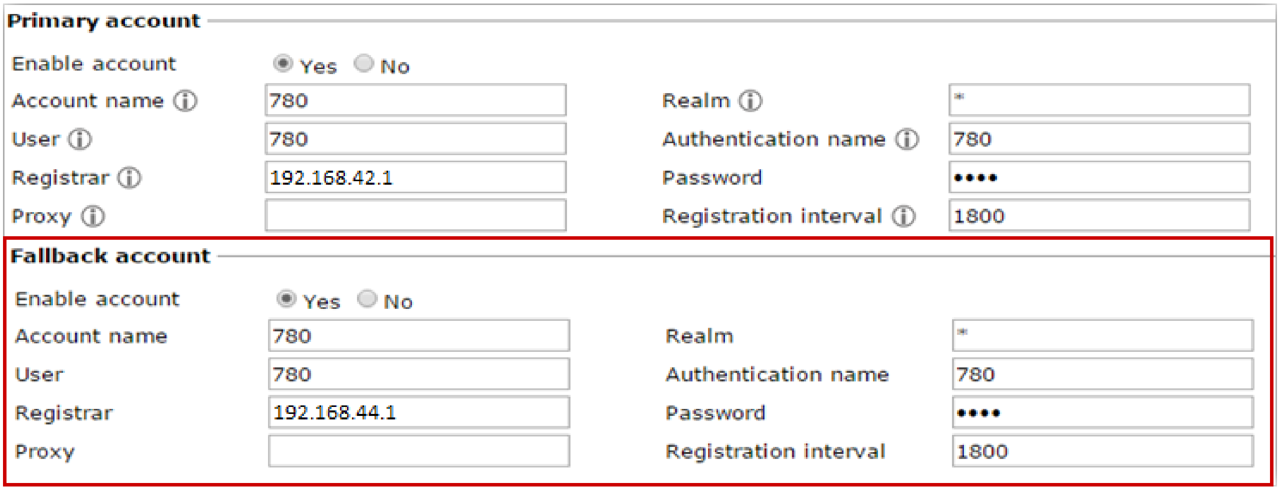
Use the phone's web interface:

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



Account Active	○ No ● 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	● Yes ○ No		
Account name ⓘ	780	Realm ⓘ	*
User ⓘ	780	Authentication name ⓘ	780
Registrar ⓘ	192.168.42.1	Password	••••
Proxy ⓘ		Registration interval ⓘ	1800

Fallback account

Enable account	● Yes ○ No		
Account name	780	Realm	*
User	780	Authentication name	780
Registrar	192.168.44.1	Password	••••
Proxy		Registration interval	1800

4.3 H323 Remote Worker Configuration

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.

To configure the remote worker failback mode:

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.

4.4 Configuring Expansion to Expansion Resilience

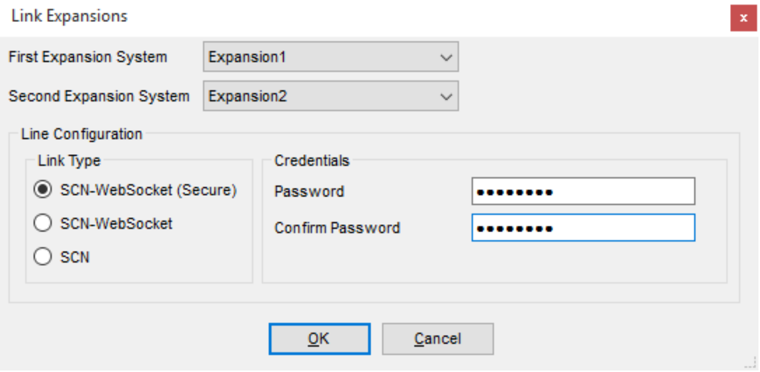
For IP Office Select, you can link expansion systems and enable resiliency between those systems. Note that this assumes that the customer also has data routing between the sites.

You must still ensure that the failover system has sufficient capacity 24 to host the additional extensions and users during failover.

To link expansion systems:

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

1. Open Manager and log in to the primary server.
2. On the **Solution** page, on the left under **Link** click **Expansion System**.



Link Expansions

First Expansion System: Expansion1

Second Expansion System: Expansion2

Line Configuration

Link Type

● SCN-WebSocket (Secure)

○ SCN-WebSocket

○ SCN

Credentials

Password: ••••••••

Confirm Password: ••••••••

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 76 to confirm the operation of the new lines between the two expansion systems.
10. You can now use the resilience wizard or individual line settings to configure resilience between expansion systems.

4.5 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 fallover 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 30.
- 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.

Process summary:

These processes assume that locations have already been created.

1. **Creating Locations** 40
2. **Setting a System's Location** 40
   For location based resilience, the normal host and failover systems must have their system location's set. In general, the location of each system in the network should be set
3. **Configuring a Line for Location Based Resilience** 41
4. **Adjusting a System's Location for Resilience** 41
   Configure the failover destination for extensions in that location to override the systems main resilience line.
5. **Setting Extension Locations** 41

4.5.1 Creating Locations

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 behaviour 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.

To create a Location:

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.
5. You can use the **Subnet** settings to have phones registering with IP addresses in the same range automatically associated with to the matching location.
6. Click **OK**.
7. Create other locations for each system as required.
8. Save the configuration changes.

4.5.2 Setting a System's Location

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 41 or if its IP address matches another location's **Subnet** settings.

To configure the Location of a system:

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 system's in the network.
6. Save the configuration.

4.5.3 Configuring a Line for Location Based Resilience

In a correctly configured network, the primary and secondary servers have 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 30 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 28.

To configure an IP Office for location based resilience:

1. Using IP Office Manager, receive the configuration from the primary server.
2. If not already done, use the expansion link wizard 30 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.

4.5.4 Adjusting a Location for Resilience

This process adjusts the previously created location records 40 to override that system's resilience settings for any extensions in the same location and registered on that system.

To change the failover destination of a Location:

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 41.
6. Click **OK**.
7. Save the configuration changes.

4.5.5 Setting an Extension's Location

This process sets the location for a specific extension. This overrides the system location 40 if set.

- **Hint**
  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.

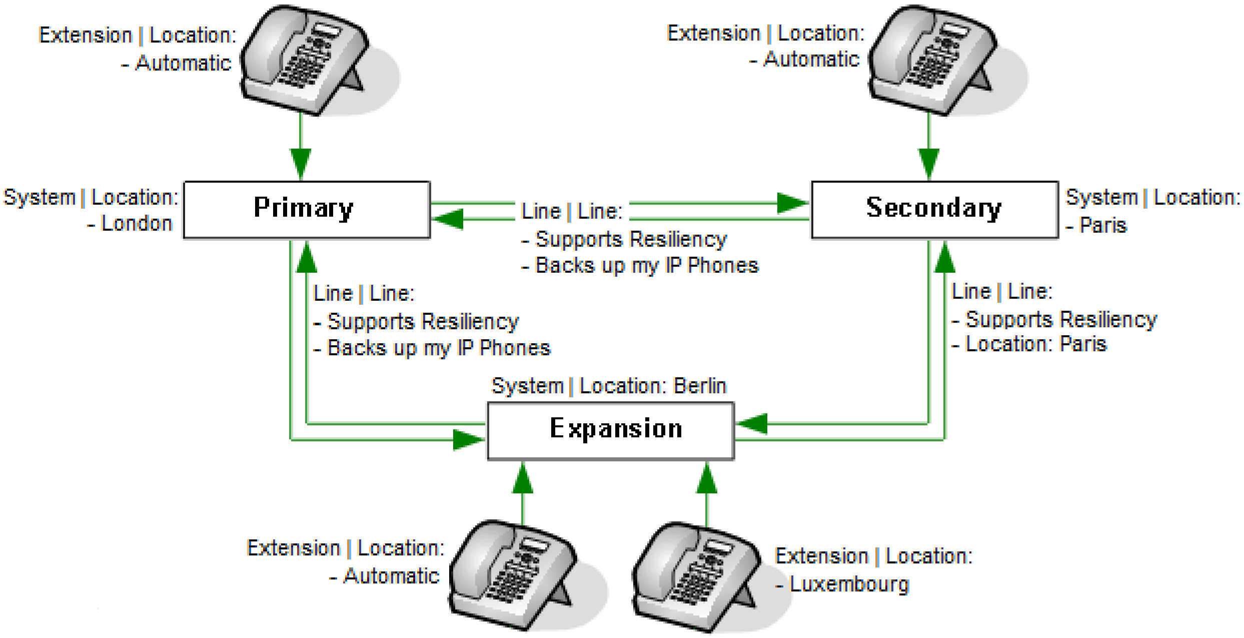
To set the Location for a specific extension:

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.

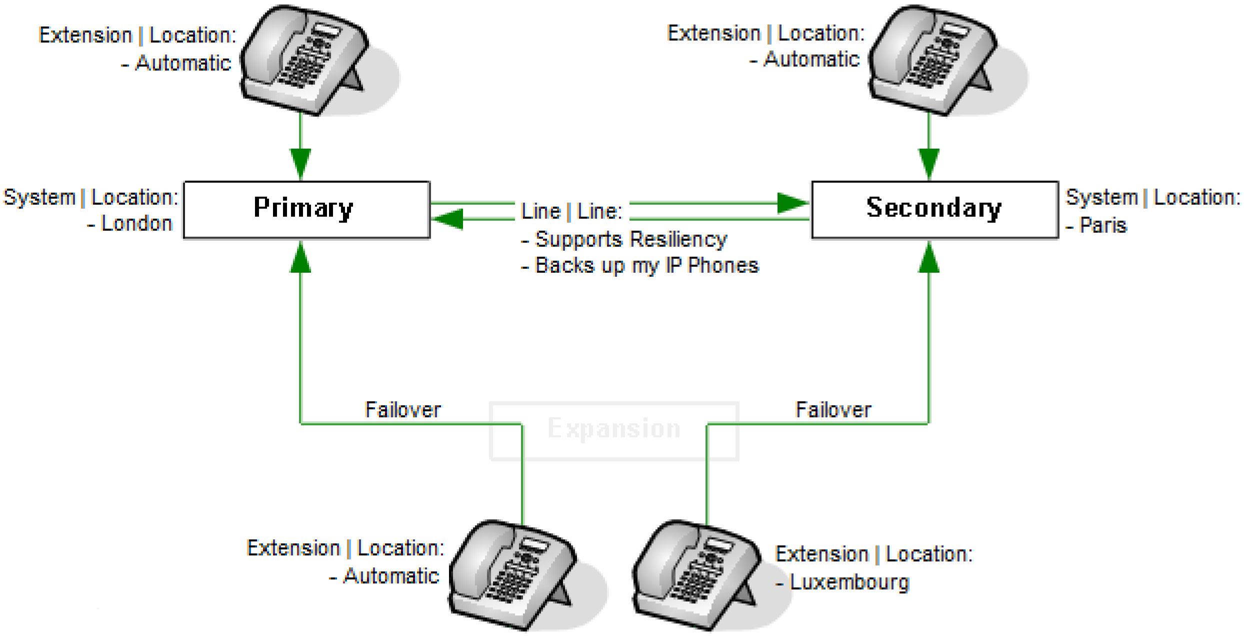
4.5.6 Example

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***.



Expansion Loss Failover

Chapter 5. Configuring Voicemail Resilience

5. 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's 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 severs 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 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 severs. 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 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?

Once the server is available again, failback occurs once all active voicemail calls have ended and server SMTP synchronization is complete. 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 28.

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. See Configuring Voicemail Resilience 44.

Process Summary

1. **Check the system voicemail settings** 45
   Check the voicemail settings of the primary and secondary IP Office systems.

2. **Check the voicemail server SMTP settings** 46
   Check the SMTP sender settings of the primary and secondary servers. These are used for the server synchronization.

3. **Configure the voicemail failback method** 47
   When the server is available again, by default failback occurs once all active voicemail calls have ended and server SMTP synchronization is complete. However, manual failback or failback after a set time can be configured.

4. **Configure voicemail resilience** 28
   Use the general resilience settings to enable voicemail resilience between the servers.

5.1 Checking the System Voicemail Settings

The voicemail settings of the server's within the network are largely 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. All other servers are configured to redirect their voicemail needs to the primary. The primary server is configured with the address of the secondary server as its failover destination.
- In an IP Office Select 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. When the later is the case, each expansion server is configured to redirect its voicemail needs to either the primary or secondary. The primary server is configured with the address of the secondary server as its failover destination and vice versa.

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

IP Office Server Edition Settings/IP Office Select 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*

IP Office Select 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*

To view and change the voicemail settings:

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 the changes.

5.2 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 severs. 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.

5.2.1 Configuring the SMTP Sender

To change the voicemail server's SMTP sender:

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. The first entry in the list of servers should be as follows:
   - **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 ***vmpro1.example.com***. Any incoming messages where the recipient mail domain does not match are ignored.
   - **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 the 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.
6. After making any changes, click **OK**.
7. Click **Save & Make Live**.

5.2.2 Configuring the SMTP Receiver

To change the voicemail server's SMTP receiver:

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.
   - **SMTP Receiver**
     Set this to ***Internal***.
   - **Port**
     Set this to ***25***.
   - **Domain**
     Set this to match the server's fully qualified domain name.
5. After making any changes, click **OK**.
6. Click **Save & Make Live**.

5.3 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. However, manual failback or failback after a set time can be configured.

5.3.1 ... using the Voicemail Client

To set the voicemail server failback method using the Voicemail Pro client:

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, when providing resilient support, the servers should return control of voicemail services to the other server. Failback is only considered once the two voicemail servers have started their synchronization operation (SMTP exchange of messages, etc.).
    - **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 is complete.
    - **Automatic**
      The failover server initiates failback either after the specified timeout period (maximum 60 minutes) or after all the active voicemail calls on the failover server come to an end, whichever occurs first. It does not wait for server SMTP synchronization to be completed.
5. After making any changes, click **OK**.
6. Click **Save & Make Live**.

5.3.2 ... using Web Manager

To set the voicemail server failback method using web manager:

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, when providing resilient support, the servers should return control of voicemail services to the other server. Failback is only considered once the two voicemail servers have started their synchronization operation (SMTP exchange of messages, etc.).
    - **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 is complete.
    - **Automatic**
      The failover server initiates failback either after the specified timeout period (maximum 60 minutes) or after all the active voicemail calls on the failover server come to an end, whichever occurs first. It does not wait for server SMTP synchronization to be completed.
5. After making any changes, click **Update**.
6. When asked to confirm the changes, click **Yes**.

5.4 Configuring Recording Archiving

If a call recording archiving application such as IP Office Media Manager or Call Recorder for IP Office is being used with the primary voicemail server, then during resiliency the backup voicemail server performs the call recording and places any VRL recordings in its 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.

To change the voicemail server's SMTP sender:

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 enter the details of an administrator account on the primary voicemail server.
5. For the **Remote FTP Location** enter either:
   - **If using IP Office Media Manager:** Enter */opt/vmpro/MM/VRL*
   - **If using Call Recorder for IP Office:** Enter */opt/vmpro/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**.

Chapter 6.
Configuring one-X Portal for IP Office Resilience

6. 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.

For IP Office Release 10, 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 mode. Portal resilience can also be configured when using 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:
    - Portal browser access.
    - one-X Communicator clients.
    - one-X Mobile Preferred clients.
    - Portal call assistant.
    - SoftConsole presence indication.
- Whilst resilience may appear to work between servers running different levels of portal software this is not supported. 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.

When Does Portal Failover Occur?

- **On primary server portal failure**
  If the primary server's portal service stops for some reason, the portal service on the secondary server automatically becomes available.
    - Users who were logged into the portal on the primary are able to 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 referred as "Standalone Mode".

When Does Portal Failback Occur?

- **On primary server portal recovery:**
  When the primary server's portal service is available again, the portal service on the secondary server stops supporting 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.

Process Summary

1. **Enable centralized CTI link mode** 52
   Allow the portal servers to automatically create and change provider settings.
2. **Configure the portal services** 53
   Configure the portal servers with the required address information of the other IP Office and portal servers.

3. **Enable portal resilience** 52
   Use the general resilience settings to enable voicemail resilience between the servers.

6.1 Configuring the IP Office Systems

The IP Office lines between the primary and secondary IP Office severs need to have the setting for portal backup enabled. This can be done through the configuring general resilience 28 options.

Enable Portal Backup on Network Trunks

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.

6.2 Enabling Centralized CTI Link Mode

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.

To check and enable Centralized CTI Link Mode

1. Login to the primary portal's administrator menus.
2. Select **Confi**guration.
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.

6.3 Configuring the one-X Portal for IP Office Servers

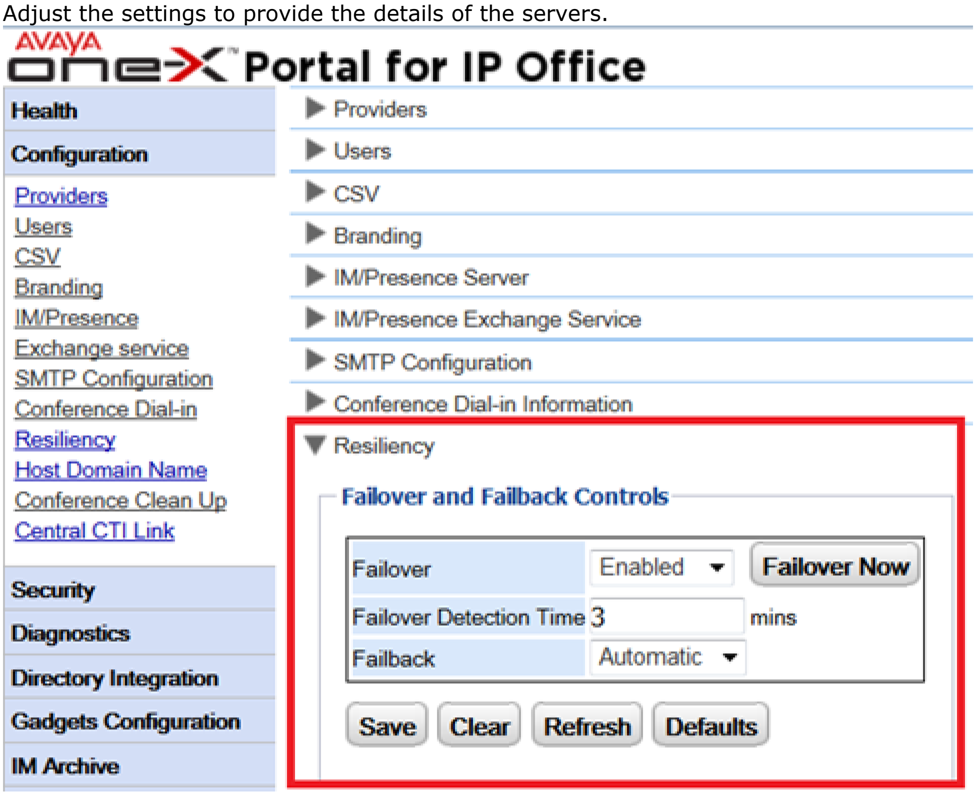
To enable portal server resilience:

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.



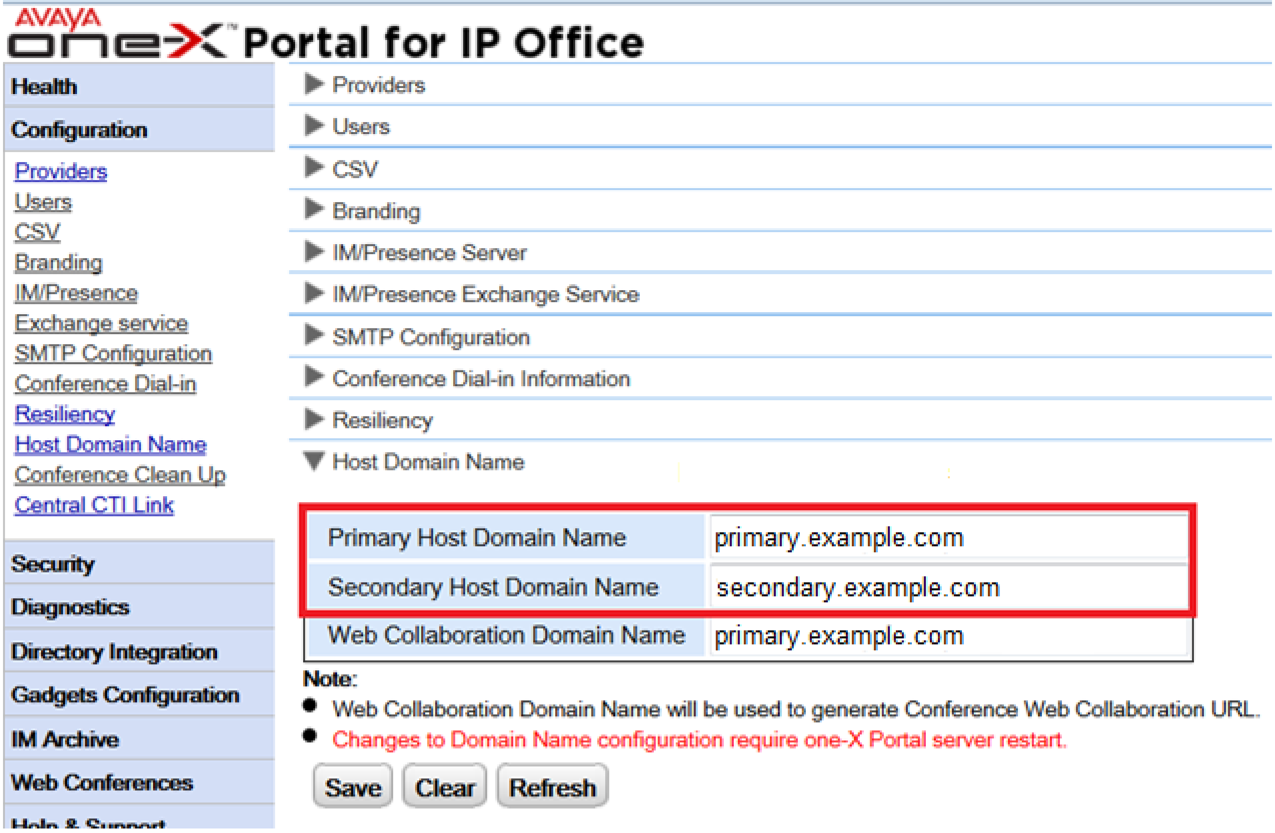
Failover	Enabled
Failover Detection Time	3 mins
Failback	Automatic

- **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.



Primary Host Domain Name	primary.example.com
Secondary Host Domain Name	secondary.example.com
Web Collaboration Domain Name	primary.example.com

Note:
- Web Collaboration Domain Name will be used to generate Conference Web Collaboration URL.
- Changes to Domain Name configuration require one-X Portal server restart.

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 52.

Chapter 7. Configuring DECT Resilience

7. 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 15 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 DECT phones (3720, 3725, 3740, 3745 and 3749) 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 56.

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 56. In that case, control of failback is through System Status Application 78.

Process Summary

1. **Configure the Master Base Station** 57
   Enter details of the failover IP Office system into the master base stations configuration.

2. **Configure the IP Office System** 59
   Configure the IP Office system to support DECT resilience.

3. **Configure IP DECT Phone Resilience** 28
   Use the general resilience settings to enable voicemail resilience between the servers.

7.1 Provisioned Base Station Configuration

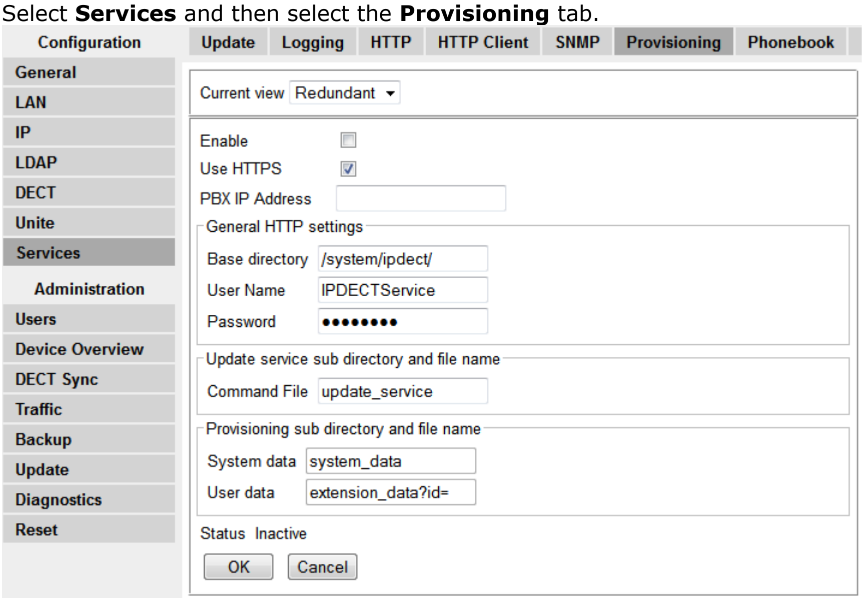
For a provisioned installation, the master base station needs to be configured to accept a provisioning connection from the failover system.

To configure the provisioned master base station for IP Office resilience:

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.



Current view: Redundant

Enable: □

Use HTTPS: ☑

PBX IP Address:

General HTTP settings

Base directory: /system/ipdect/

User Name: IPDECTService

Password: ••••••••

Update service sub directory and file name

Command File: update_service

Provisioning sub directory and file name

System data: system_data

User data: extension_data?id=

Status: Inactive

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.

7.2 Non-Provisioned Base Station Configuration

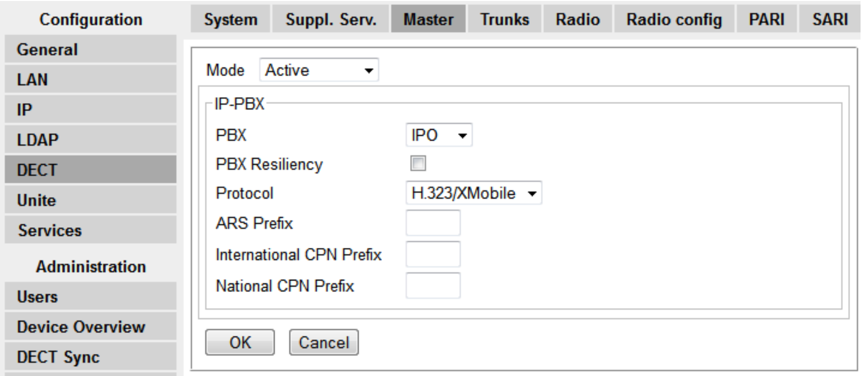
For non-provisioned systems, the master base station needs to be configured with details of a redundant trunk connection to the failover IP Office and when to use that trunk.

To configure the non-provisioned master base station for IP Office resilience:

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.



Mode: Active

IP-PBX

PBX: IPO

PBX Resiliency: □

Protocol: H.323/XMobile

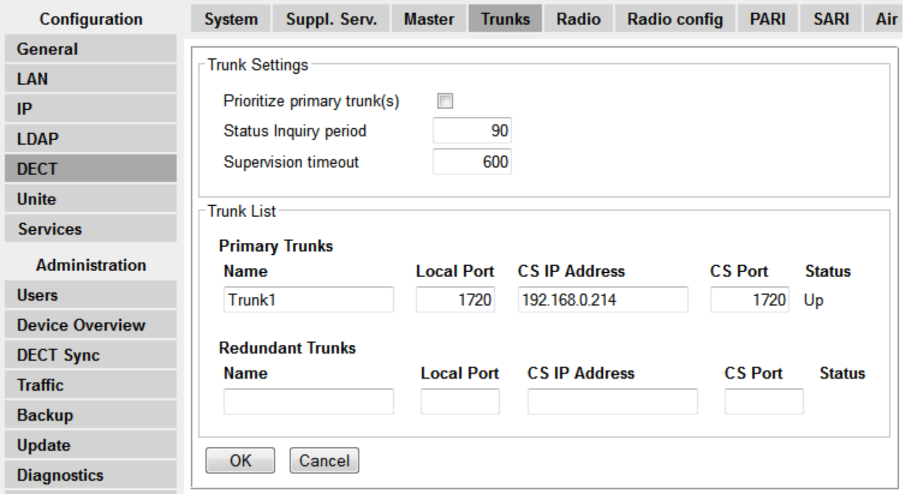
ARS Prefix:

International CPN Prefix:

National CPN Prefix:

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 displayed.



Trunk Settings

Prioritize primary trunk(s): □

Status Inquiry period: 90

Supervision timeout: 600

Trunk List

Primary Trunks

Name	Local Port	CS IP Address	CS Port	Status
Trunk1	1720	192.168.0.214	1720	Up

Redundant Trunks

Name	Local Port	CS IP Address	CS Port	Status

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 78.

   - **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 59 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.

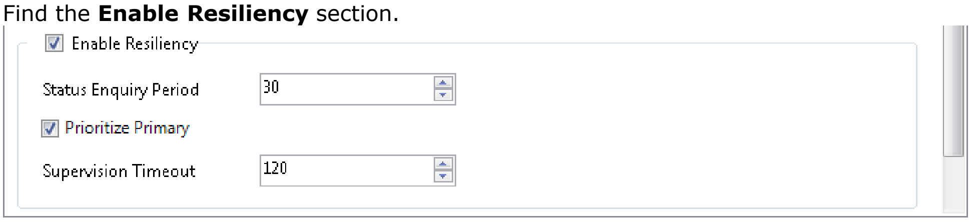
   b. Click **OK**. Depending on your base station, wait for the lower LED to return to solid blue or solid green.

7.3 IP Office Configuration for DECT Resilience

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 57.

To configure the IP Office for DECT resilience:

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.



☑ Enable Resiliency

Status Enquiry Period 30

☑ Prioritize Primary

Supervision Timeout 120

6. Select **Enable Resiliency**.
7. Only 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 78.
   - **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.

Chapter 8.
Configuring DECT Master Resilience

8. Configuring DECT Master Resilience

Each DECT R4 system includes one base station configured as the master base station. Base station mirroring allows two base stations to be configured as the master. Whilst only one is active at any time, the other becomes active if the existing master is not available for some reason.

For base station resiliency, two base stations are configured to act as 'mirrored' master base stations. One becomes the active master base station whilst the other becomes a standby master base station. 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 non-master 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 14 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.

Process Summary

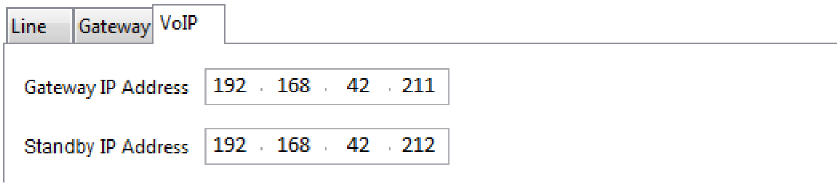
1. **Configure the IP Office** 62
   Enter the address of the failover IP Office system.
2. **Configure the Mirrored Base Stations** 63
   Configure the two base stations to act as mirrors of each other.
3. **Activate the Master Base Station** 64
   Select which of the mirrored base station is the currently active master base station.

8.1 Configuring the IP Office

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

To configure the IP Office for mirroring:

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.



Gateway IP Address: 192 . 168 . 42 . 211

Standby IP Address: 192 . 168 . 42 . 212

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

   b. Save the changes.

8.2 Configuring the Mirrored Base Stations

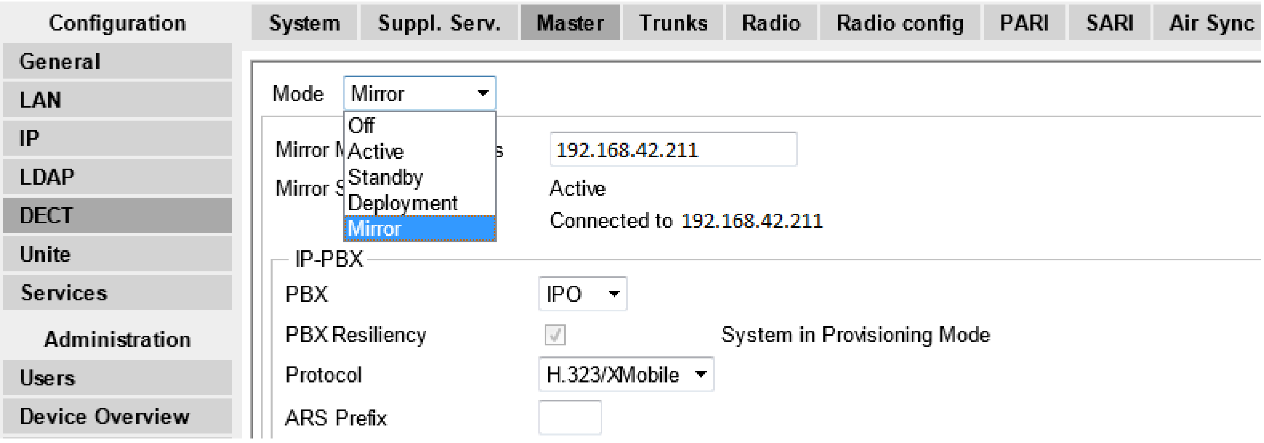
Use the following process to configure the master base station and its mirror.

To configure the mirrored base stations:

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

1. Login to the first master base station.

2. Select **DECT** and then select the **Master** tab.



Mode: Mirror

Mirror M...s: 192.168.42.211

Mirror S...: Active

Connected to 192.168.42.211

IP-PBX

PBX: IPO

PBX Resiliency: ☑ System in Provisioning Mode

Protocol: H.323/XMobile

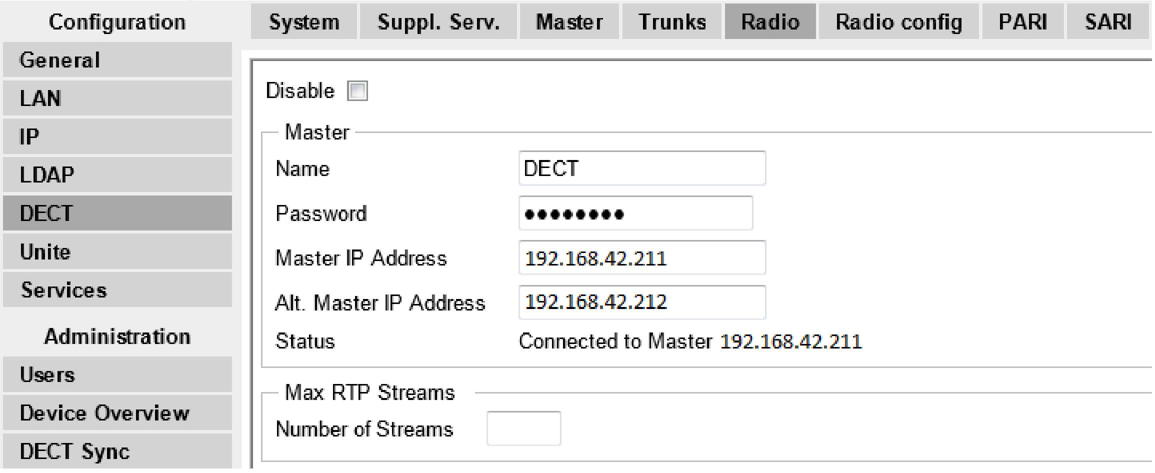
ARS Prefix:

   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.



Disable □

Master

Name: DECT

Password: ●●●●●●●●

Master IP Address: 192.168.42.211

Alt. Master IP Address: 192.168.42.212

Status: Connected to Master 192.168.42.211

Max RTP Streams

Number of Streams:

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

5. Repeat this process for the other mirrored base station.

8.3 Activating the Master Base Station

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.

To select the active mirror:

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

1. Login to one of the mirrored master base stations.
2. Select **DECT** and then select the **Master** tab.
3. Click **Activate mirror**. That base station is made the currently active master base station in the mirrored pair.

Chapter 9. Configuring Trunk Resilience

9. Configuring 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.

9.1 Configuring Breakout Controls

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.

To add a break out button:

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 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.

To add a break out short code:

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.

9.2 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 be able to use those trunks on the secondary when necessary.

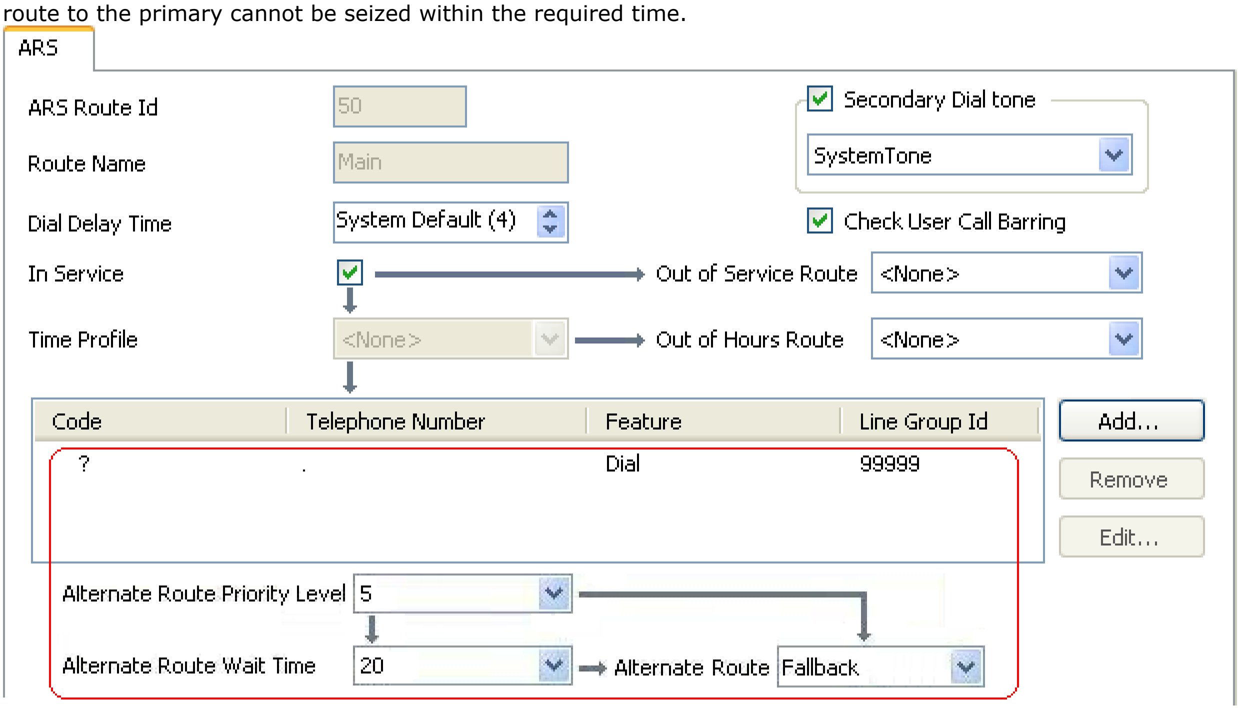
Note that these examples are useable in both normal and failover operation. They are not using specific resilience failover features.

The simplest method is to add a **?/./Dial/99998** short code to the primary system's existing ARS form. However, that method provides very little control 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 will apply a delay to them using a secondary trunk when the primary trunks are not available.

9.2.1 ARS Alternate Route Overflow

To configure primary ARS fallback to the secondary server:

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.



ARS

ARS Route Id: 50

Route Name: Main

Dial Delay Time: System Default (4)

In Service: ☑ → Out of Service Route: <None>

Time Profile: <None> → Out of Hours Route: <None>

☑ Secondary Dial tone: SystemTone

☑ Check User Call Barring

Code	Telephone Number	Feature	Line Group Id
?	.	Dial	99999

Alternate Route Priority Level: 5

Alternate Route Wait Time: 20 → Alternate Route: Fallback

   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.

9.2.2 ARS Out of Service Routing

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.

To configure primary ARS out of service fallback to the secondary server:

1. Using IP Office Manager, receive the configuration from the primary server.

2. Expand the configuration of the primary server and select ARS.

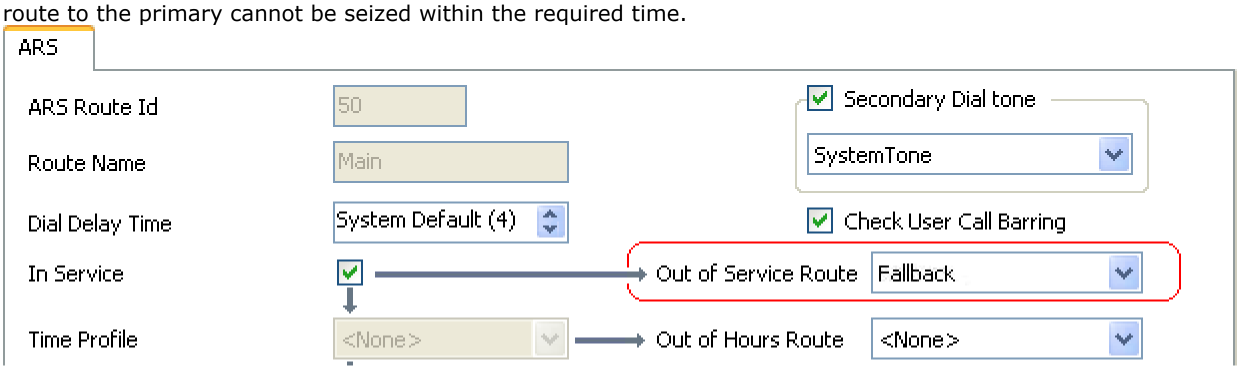
3. Click on the icon to add a new ARS record.

   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.



ARS

ARS Route Id: 50

Route Name: Main

Dial Delay Time: System Default (4)

In Service: ☑

Time Profile: <None>

☑ Secondary Dial tone: SystemTone

☑ Check User Call Barring

Out of Service Route: Fallback

Out of Hours Route: <None>

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.

Chapter 10. Configuring Media Preservation

10. 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:

- **9608**
- **9611**
- **9621**
- **9641**

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 reregister 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.

Process Summary

1. **Configuring the System Settings** 73.
2. **Configuring SIP Line Settings** 73.

10.1 Configuring the System Setting

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[73] separately.

To configure the system call preservation setting:

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.

10.2 Configuring the SIP Line Setting

By default, all SIP trunks use the same setting applied to the system[73]. However, each trunk can be configured separately to use its own setting.

To configure the setting for a SIP trunk:

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[73].
    - **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.

Chapter 11. Monitoring Resilience

11. Monitoring Resilience

11.1 Resilence Indication on Phones

The following indicators may appear on phones during failover scenarios:

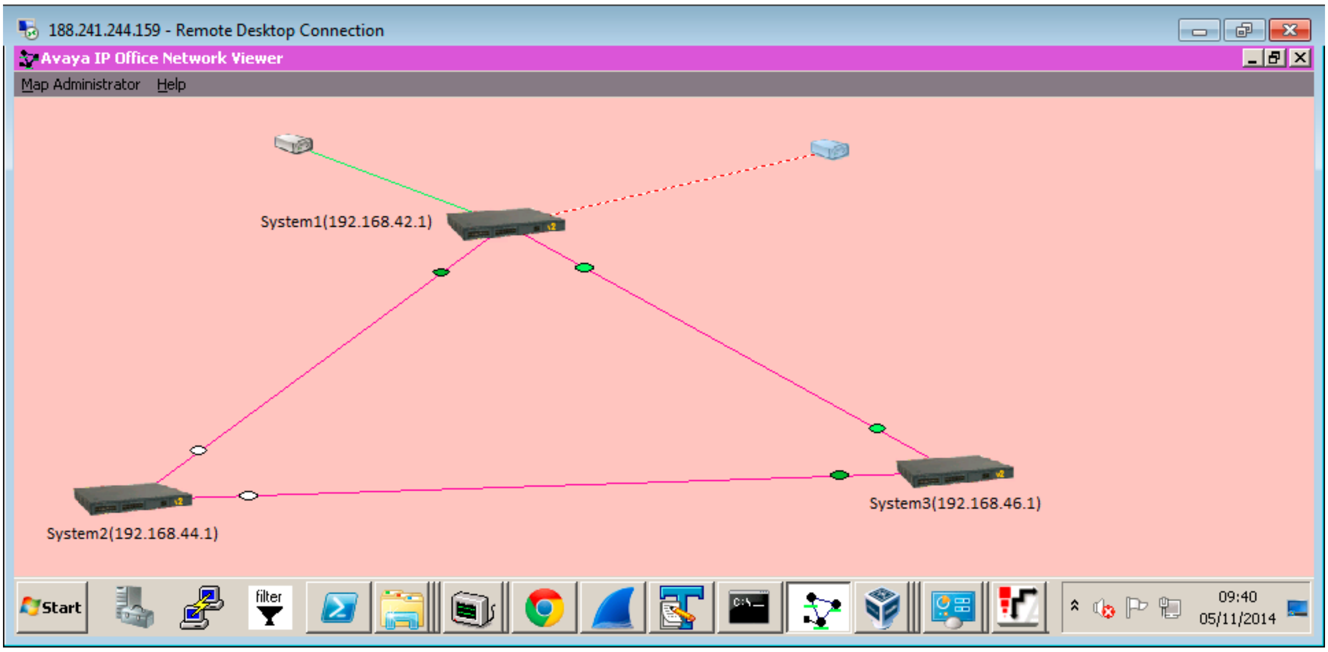
- **R: IP Phone Resilience Indication**
  An **R** is displayed on phones when they are operating in resilient mode. This is supported by 1600 and 9600 Series phones and on 3720, 3725, 3740, 3745 and 3749 DECT phones (if provisioned).

- **!: 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 normal settings. This is supported by 1600 and 9600 Series phones.

11.2 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 colour 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)

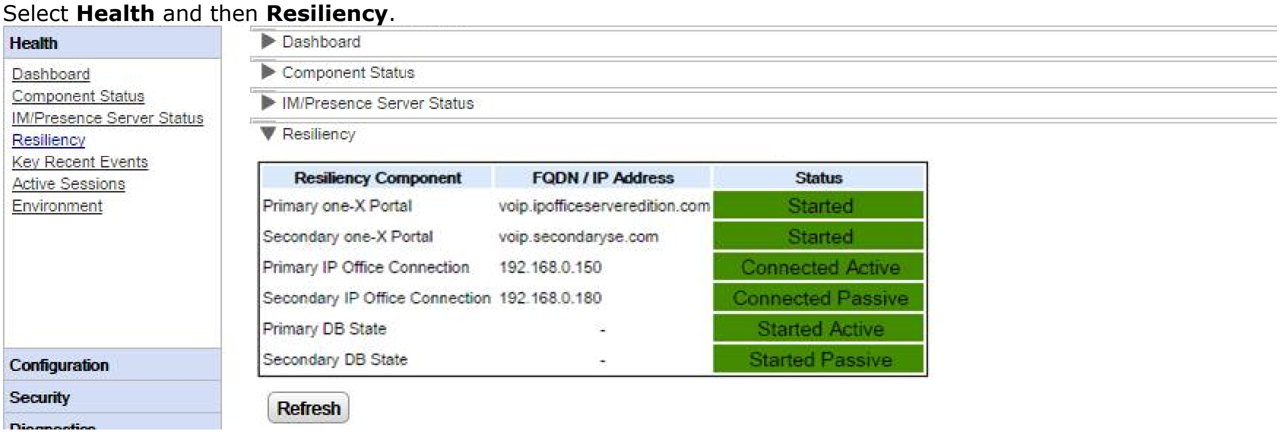
11.3 one-X Portal for IP Office Status

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

To view the portal resiliency status:

1. Login to the portal administrator menus.

2. Select **Health** and then **Resiliency**.



Resiliency Component	FQDN / IP Address	Status
Primary one-X Portal	voip.ipofficeserveredition.com	Started
Secondary one-X Portal	voip.secondaryse.com	Started
Primary IP Office Connection	192.168.0.150	Connected Active
Secondary IP Office Connection	192.168.0.180	Connected Passive
Primary DB State	-	Started Active
Secondary DB State	-	Started Passive

In this example, the primary is running and providing portal services ('active'). The secondary is also running but not currently providing portal services ('passive').

- **Started**
  Indicates that the server or service is running.

- **Stopped**
  Indicates that the server or service is not running.

- **Connected**
  Indicates that a connected to the server is available.

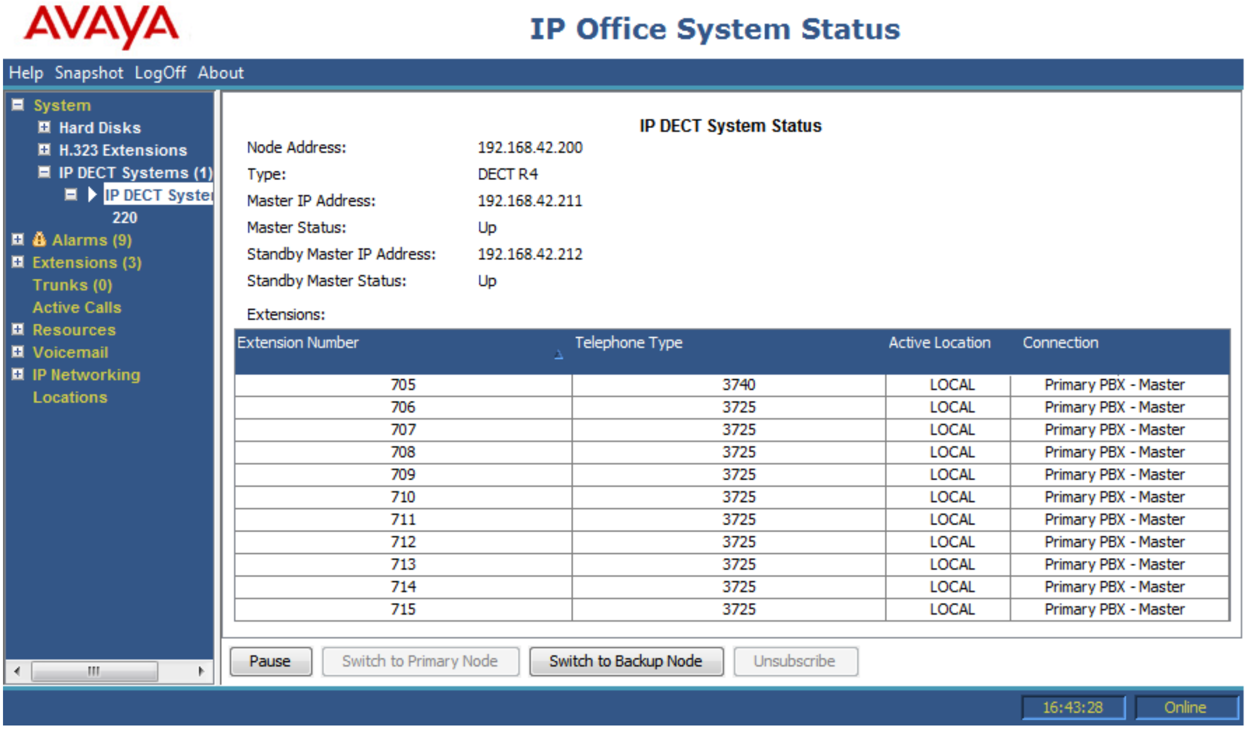
- **Active**
  Indicates that the server or connection is running and is currently being used to support portal users.

- **Passive**
  Indicates that the server or connection is running but is not currently being used to support portal users.

11.4 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.



IP DECT System Status

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

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 Trunk Resilience 56.

Chapter 12. Document History

12. Document History

Date	Issue	Change Summary
5th July 2017	**02a**	• Release 10.1 branded. • Clarification around configuration of voicemail resiliency settings. • Additional of Voicemail Recording system preference settings if using a call archiving application. • 1100/1200 Phones • Clarification on IP phone resilience configuration. [IPOFFICE-121102]

Index

Template: 26th January 2016