Deploying Remote IP Office SIP Phones with an ASBCE

Release 12.1
Issue 17
March 2025

© 2020-2025, Avaya LLC
All Rights Reserved.

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

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

Copyright

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

Virtualization

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

Third Party Components

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

Service Provider

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Trademarks

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

Avaya is a registered trademark of Avaya LLC.

All non-Avaya trademarks are the property of their respective owners.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

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

Contact Avaya Support

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

Contents

Part 1: Supporting remote SIP extensions 7

Chapter 1: Supporting remote SIP extensions on IP Office 8

Example schematic 8

Security considerations 10

Chapter 2: IP Office configuration for remote SIP extensions 11

IP Office configuration checklist 11

Licenses and Subscriptions 12

IP Office SIP VoIP Setup 12

Setting the ASBCE details passed to remote extensions by the IP Office 14

Adding additional settings for remote extensions 16

Whitelisting the ASBCE 17

Chapter 3: Adding IP Office certificates to the ASBCE 18

ASBCE certificate checklist 18

Downloading the IP Office root certificate 19

Adding the IP Office root certificate to the ASBCE 20

Generating an ASBCE identity certificate using IP Office Web Manager 21

Generating an ASBCE identity certificate using Web Control (Platform View) 22

Splitting the ASBCE identity certificate 23

Adding the identity certificate to the ASBCE 24

Chapter 4: ASBCE Configuration for remote SIP extensions 26

ASBCE call flow summary 27

Clone vs. Add 29

ASBCE configuration checklist 29

Firewall configuration 31

Configure the external ASBCE interface 32

Configure the internal ASBCE interface 33

Creating a TLS client profile 35

Creating a TLS server profile 36

Creating an internal media interface 38

Creating an external media interface 39

Creating an internal signaling interface 40

Creating the external signaling interface 41

Creating a ASBCE server profile for the IP Office 42

Creating a server routing profile 44

Creating an ASBCE topology hiding policy 46

Creating an IP/URI blocklist 47

Creating an application rule 48

Creating a media rule 49

Creating an endpoint policy group 52

Configuring a user agents profile 53
Creating the subscriber flow 54
Creating a server flow 57
Adding reverse proxies for file requests 59
Chapter 5: Unanchoring call media from the ASBCE 64
Creating a session policy for a remote site 64
Creating a session flow for the remote site 66
Chapter 6: Supporting Avaya Workplace Client as a remote extension 68
Avaya Workplace Client SIP registration 68
Checking the remote settings 69
Chapter 7: Checking remote extension status in the ASBCE 71
Viewing ASBCE SIP statistics 71
Viewing ASBCE user statistics 72
Viewing ASBCE incidents 73
Part 2: Supporting IPv6 74
Chapter 8: Supporting IPv6 remote extensions 75
Remote extension IPv6 support 75
IPv6 Remote extension schematic 76
IPv6 Remote extension limitations 77
DNS configuration for IPv6 remote extension support 77
Certificate configuration for IPv6 remote extension support 77
Avaya cloud services configuration for IPv6 remote extension support 78
Configuration checklist for IPv6 remote extensions 78
Configuration checklist for combined IPv4 and IPv6 remote extensions 79
Part 3: Resilience 82
Chapter 9: ASBCE and IP Office resilience 83
Example resilience schematic 83
Generating an identity certificate for the secondary IP Office 84
Installing the secondary IP Office identity certificate 85
Configuring the IP Office for remote extension resilience 86
Configuring the Avaya one-X Portal 86
Configuring the ASBCE for resilience 87
Configuring DNS for resilience 87
Chapter 10: Checking the resilience configuration 88
Checking the resilience DNS routing 88
Viewing the ASBCE trace 89
Checking the Avaya one-X Portal responses 90
Part 4: Additional information 92
Chapter 11: Additional Help and Documentation 93
Additional Manuals and User Guides 93
Getting Help 93

Finding an Avaya Business Partner..... 94
Additional IP Office resources..... 94
Training..... 95
Chapter 12: Glossary..... 96

Part 1: Supporting remote SIP extensions

Chapter 1: Supporting remote SIP extensions on IP Office

This section provides an example process for supporting remote SIP extensions connecting to an IP Office through an Avaya Session Border Controller (ASBCE). The ASBCE provides a range of functions that provide additional security to the connection process.

- This document is based on IP Office R11.1.3.1 and ASBCE R10.1.2.
- For IP Office R11.1.3.1, the IP Office supports IPv6 iOS and Android Avaya Workplace Client remote extensions using IPv6. Otherwise, the IP Office only supports IPv4 remote extensions.

Supported remote SIP extensions

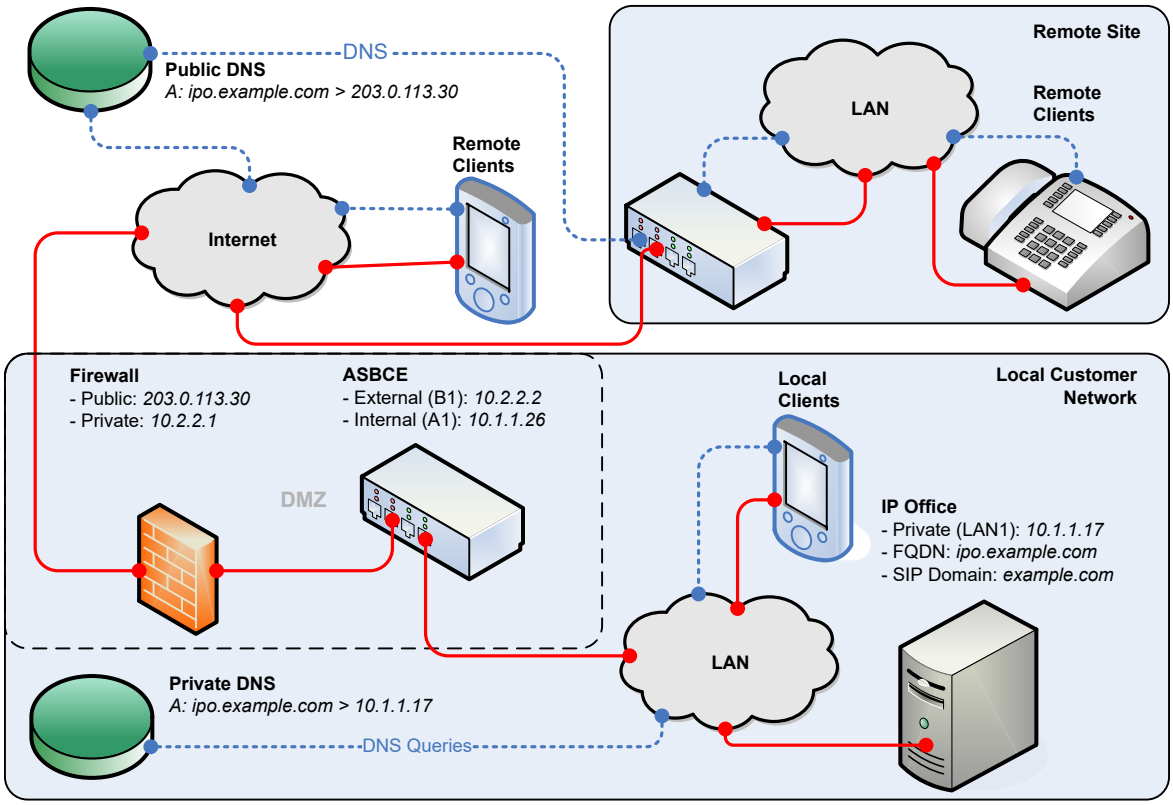
SIP Deskphones	SIP Softphones
• J100 Series Phones • K100 Series Phones (Avaya Vantage™)	• Avaya Workplace Client

Related links

Example schematic on page 8
Security considerations on page 10

Example schematic

This schematic shows the example scenario used in this document:



- For this scenario, the SIP extensions are J100 Series phones and Avaya Workplace Client softphones.
- The IP Office is the SIP registrar.
  - This example uses TLS for the SIP connections. That requires consideration of the IP Office certificates and provision of certificates for the ASBCE.
- The ASBCE has public and private IP interfaces. Using these, it acts as the gateway for SIP traffic between the customer's private network and the public internet.
  - When used internally, the SIP clients connect directly to the IP Office.
  - When used externally, the SIP clients connect to the IP Office through the ASBCE.
  - The ASBCE also routes requests for files used by the remote SIP extensions. For example, requests for the `.txt` and `.xml` files.
- The customer network includes a firewall between itself and the public internet. Avaya recommends this for improved security.
  - The firewall forwards traffic from remote extensions to the ASBCE.
- The customer's DNS solution provides Split DNS. That is:
  - On the customer's private network, DNS resolves the IP Office FQDN to the IP address of the IP Office.
  - On the public internet, DNS resolves the IP Office FQDN to the public IP address of the customer's firewall.

Related links

Supporting remote SIP extensions on IP Office on page 8

Security considerations

Any scenario where you connect the IP Office to the public internet must include consideration of security. IP Office security options and requirements are covered in the Avaya IP Office™ Platform Security Guidelines manual.

In this case, connecting using an ASBCE makes available a range of additional security options.

- **User Agent Matching**

  You can configure which user agent strings can connect through the ASBCE. This allows you to only support connections from known applications and devices. See Configuring a user agents profile on page 53.

- **Application Rules**

  You can use application rules to configure what type of media your connections support, the maximum number of connections, and the maximum number of connections per remote extension. See Creating an application rule on page 48.

- **IP/URL Blocklists**

  You can use these to block IP addresses or URLs that repeatedly fail username or password registration. See Creating an IP/URI blocklist on page 47.

Related links

Supporting remote SIP extensions on IP Office on page 8

Chapter 2: IP Office configuration for remote SIP extensions

This section provides a general summary of the IP Office configuration for supporting remote SIP extensions connection through an ASBCE.

Related links

IP Office configuration checklist on page 11
Licenses and Subscriptions on page 12
IP Office SIP VoIP Setup on page 12
Setting the ASBCE details passed to remote extensions by the IP Office on page 14
Adding additional settings for remote extensions on page 16
Whitelisting the ASBCE on page 17

IP Office configuration checklist

#	Action	Link/Notes	✔
1.	Check the SIP VoIP Settings	See IP Office SIP VoIP Setup on page 12.	
2.	Add setting for remote extensions	See Setting the ASBCE details passed to remote extensions by the IP Office on page 14.	
3.	Set the NoUser source numbers	See Adding additional settings for remote extensions on page 16.	
4.	Whitelist the ASBCE	Prevent the IP Office from blocking the ASBCE. See Whitelisting the ASBCE on page 17.	

Related links

IP Office configuration for remote SIP extensions on page 11

Licenses and Subscriptions

The IP Office does not require any additional licenses to support operation with an ASBCE. The phones and applications connected to the IP Office using an ASBCE use the same licenses or subscriptions as for local operation.

Related links

IP Office configuration for remote SIP extensions on page 11

IP Office SIP VoIP Setup

The following is the IP Office configuration used to support SIP extensions in the example scenario. This configuration is the same for both local and remote SIP extensions.

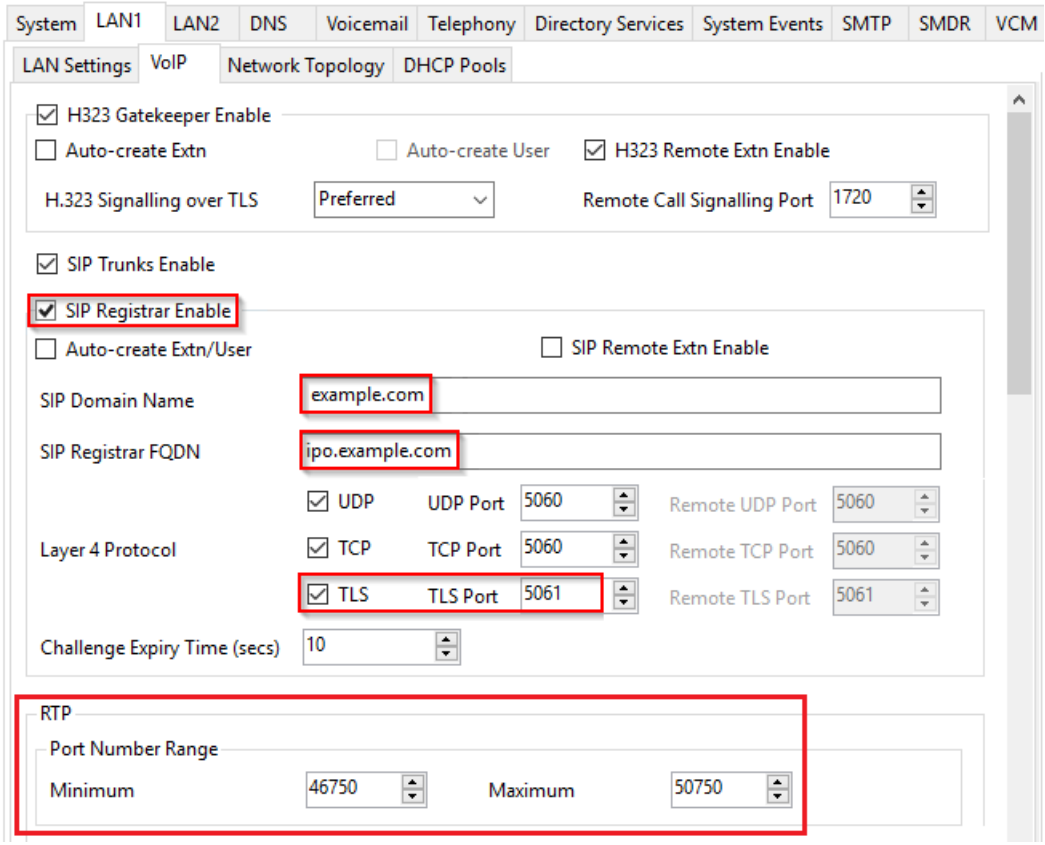
Important:

- Changing these settings requires an IP Office reboot.

Procedure

1. Log in to the IP Office using IP Office Manager or IP Office Web Manager.
2. Select **System** or **System Settings** > **System**.

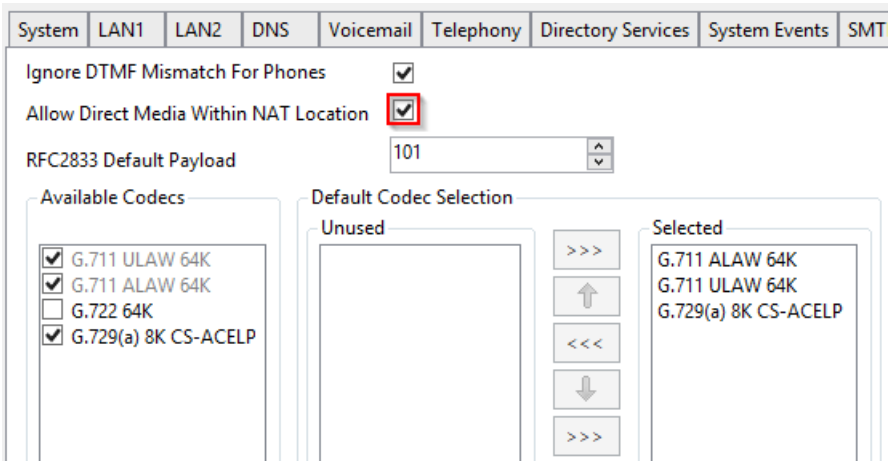
3. Select the **LAN1** tab.



Field	Description
SIP Registrar Enable	Allows SIP extensions to register with the IP Office.
SIP Remote Extn Enable	Disable. The ASBCE manages remote extension NAT connections.
SIP Domain Name	Sets the domain that SIP clients must use for registration.
SIP Registrar FQDN	Sets the fully-qualified domain name for routing SIP connections to the IP Office.
Layer 4 Protocol	Sets the Layer 4 protocols and ports on which the IP Office listens for SIP extension traffic.
Port Number Range	Sets the port number range the IP Office uses for RTP and RTCP traffic.

4. Select the **VoIP** sub-tab.

   Enable **Allow Direct Media With NAT Location** checkbox.



   - Enabling this allows direct media between devices reside on the same sub-net that connect to the IP Office using NAT. Supporting this through the ASBCE requires additional configuration in order for the ASBCE to unanchor itself from the call media, see Unanchoring call media from the ASBCE on page 64.

5. Click **OK** or **Update**.
6. Save the settings and reboot the IP Office system:
   - If using IP Office Manager, save the settings and reboot the system
   - If using IP Office Web Manager, click **Save to IP Office** and reboot the system.

Related links

IP Office configuration for remote SIP extensions on page 11

Setting the ASBCE details passed to remote extensions by the IP Office

Before registering with the IP Office, Avaya extensions request the `46xxsettings.txt` file. This file contains settings that the extensions use.

For remote extensions, the `46xxsettings.txt` file auto-generated by the IP Office needs to contain the addresses information that the remote extension can use to connect to the ASBCE.

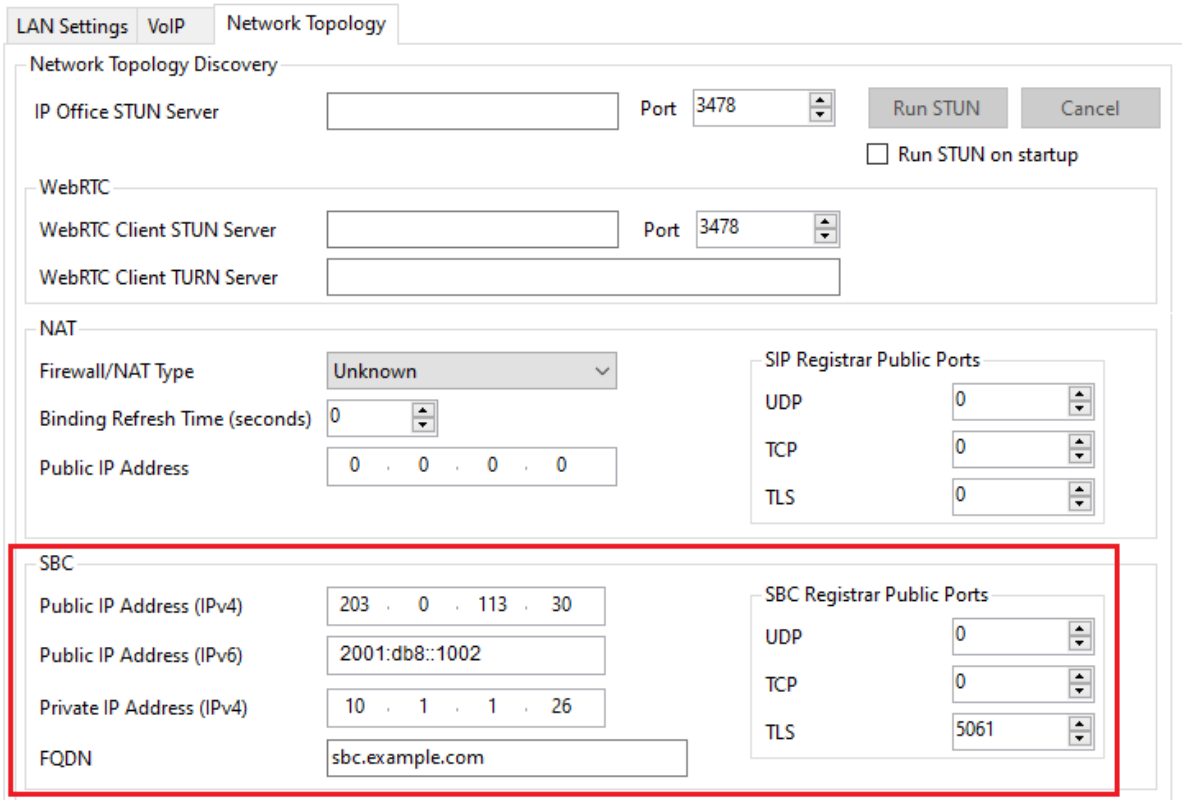
- Extensions request the `46xxsettings.txt` file when they first register with the IP Office.
- After receiving the `46xxsettings.txt` file, by default extensions request the file again every 24-hours to apply any changes.
- Extensions also request the file whenever they restart. You can restart them remotely using SysMonitor or System Status Application.

Important:

- Changing these settings requires an IP Office reboot.

Procedure

1. Log in to the IP Office using IP Office Manager or IP Office Web Manager.
2. Select **System** or **System Settings** > **System**.
3. Select the LAN (**LAN1** or **LAN2**) connected to the same network as the ASBCE.
4. Select **Network Topology**.
   - If using IP Office Web Manager, you can only change these settings in offline mode. Click the icon and select **Offline Mode**.
5. In the **SBC** section, enter the following information:



Setting	Description
Public IP Address (IPv4)	The public IPv4 address for incoming SIP client traffic into the customer network. • This is the public IPv4 address of the ASBCE or the internet facing service such as the customer firewall. • External DNS must resolve the IP Office FQDN to this address when requested by a IPv4 remote extension.

Table continues…

Setting	Description
Public IP Address (IPv6)	The public IPv6 address for incoming SIP client traffic into the customer network as above. For more details, see Supporting IPv6 remote extensions on page 75. • This is the public IPv6 address of the ASBCE or the internet facing service such as the customer firewall. • External DNS must resolve the IP Office FQDN to this address when requested by a IPv6 remote extension.
Private IP Address (IPv4)	The private/internal IPv4 address of the ASBCE. • Internal DNS must resolve the **FQDN** below to this address.
FQDN	The fully-qualified domain name of the ASBCE. DNS must resolve this FQDN to the IPv6 addresses being used (IPv4 uses the IP Office SIP Registrar FQDN).
SIP Registrar Public Ports	The public (external) **UDP**, **TCP** and/or **TLS** ports that external SIP clients must use to connect to the ASBCE.

6. Click **OK** or **Update**.
7. Save the settings and reboot the IP Office system:
   - If using IP Office Manager, save the settings and reboot the system
   - If using IP Office Web Manager, click **Save to IP Office** and reboot the system.

Related links

IP Office configuration for remote SIP extensions on page 11

Adding additional settings for remote extensions

You can use the following **NoUser** source numbers to have additional values set in the auto-generated `46xxsettings.txt` file the IP Office supplies to remote extensions.

Procedure

1. Log in to the IP Office using IP Office Manager or IP Office Web Manager.
2. Click **User** or **Call Management** > **User**.
3. Locate the settings for the user named *NoUser*.
4. Select **Source Numbers**.
5. Add the additional *NoUser* source numbers you require:
   - `SET_STIMULUS_SBC_REG_INTERVAL=<seconds>`

     This *NoUser* source number sets the registration interval used by J100 Series phones. The default is 3600 seconds (1 hour). When supporting phones through an ASBCE, the recommend value is 180 seconds. The supported range is 180 to 3600 seconds.
   - `PUBLIC_HTTP=<file server address>`

When using the **HTTP Server IP Address** and **HTTP Redirection** settings, the IP Office uses this value to set the public file server address given to remote extensions.

- `FORCE_SIP_SBC_TCP_SINGLE_PORT`

  Force the IP Office to open only one socket to the ASBCE for each client, regardless of the number of calls. Doing this has can resolve issues with calls giving one ring on client and then appearing as a missed call.

- `B_DISABLE_SIP_IPADDR`

  Disables the IP Office source IP address blacklisting. The ASBCE traffic control must be used instead.

6. Click **OK** or **Update**.
7. Save the settings and reboot the IP Office system:
   - If using IP Office Manager, save the settings and reboot the system
   - If using IP Office Web Manager, click **Save to IP Office** and reboot the system.

Related links

IP Office configuration for remote SIP extensions on page 11

Whitelisting the ASBCE

With remote extension connecting to the IP Office through the ASBCE, incorrect registration attempts can cause the IP Office to block the ASBCE IP address.

Procedure

1. Log in to the IP Office using IP Office Manager or IP Office Web Manager.
2. Select **System** or **System Settings** > **System**.
3. Select **VoIP** > **Access Control Lists**.
4. Add the internal IP address of the ASBCE to the **IP Whitelist**.
5. Click **OK** or **Update**.
6. If using IP Office Manager, save the settings to the IP Office system.

Related links

IP Office configuration for remote SIP extensions on page 11

Chapter 3: Adding IP Office certificates to the ASBCE

For the example scenario, the IP Office is using its self-signed certificate. In that case, the ASBCE needs:

- A copy of the IP Office root certificate. This is the Certificate Authority (CA).
- An identity certificate for the ASBCE issued by the IP Office.
  - **For IPv4:** The certificate must include the IP Office FQDN (CN or SAN) and IPv4 (SAN) address.
  - **For IPv6:** In addition to the IP Office FQDN and IPv4 address, the ASBCE identity certificate must include the ASBCE FQDN and IPv6 address.

Using third-party certificates

If the IP Office is using certificates issued by a third-party CA, then the root and identity certificates required for the ASBCE must be issued by that CA. However, the principles for the details required in the identity certificate remain the same as outlined in this section of the documentation.

Related links

ASBCE certificate checklist on page 18
Downloading the IP Office root certificate on page 19
Adding the IP Office root certificate to the ASBCE on page 20
Generating an ASBCE identity certificate using IP Office Web Manager on page 21
Generating an ASBCE identity certificate using Web Control (Platform View) on page 22
Splitting the ASBCE identity certificate on page 23
Adding the identity certificate to the ASBCE on page 24

ASBCE certificate checklist

#	Action	Link/Notes	✔
1.	Download the IP Office root certificate	See Downloading the IP Office root certificate on page 19.	

Table continues…

#	Action	Link/Notes	✔
2.	Add the root certificate to the ASBCE	See Adding the IP Office root certificate to the ASBCE on page 20.	
3.	Generate an identity certificate for the ASBCE	See Generating an ASBCE identity certificate using IP Office Web Manager on page 21.	
4.	Split the certificate	Extract separate certificate and private key files from the identity certificate. See Splitting the ASBCE identity certificate on page 23.	
5.	Add the files to the ASBCE	Add the identity certificate and private key files to the ASBCE See Adding the identity certificate to the ASBCE on page 24.	

Related links

Adding IP Office certificates to the ASBCE on page 18

Downloading the IP Office root certificate

Use this procedure to download a copy of the IP Office root certificate.

Procedure

1. Login to the IP Office using IP Office Web Manager.
   - For an IP500 V2, enter the system address followed by `:8443/WebMgmtEE/WebManagerment.html`.
   - For a Linux-based server, enter the system address followed by `:7070/WebManagement/WebManagement.html`.
2. Select **Security** > **Security Settings**.
3. If the IP Office is in a multi-site network, click the next to the required IP Office.
4. Select **Certificates**.
5. In the **Trusted Certificate Store**, locate the root certificate the IP Office system is using.
6. Click on the next to the certificate.
7. Click **Yes**.
8. Rename the file `IPO_RootCA.crt`.

Next steps

- Go to Adding the IP Office root certificate to the ASBCE on page 20.

Related links

Adding IP Office certificates to the ASBCE on page 18

Adding the IP Office root certificate to the ASBCE

Use this procedure to upload the copy of the IP Office root certificate to the ASBCE.

Before you begin

- Download the IP Office root certificate. See Downloading the IP Office root certificate on page 19.

Procedure

1. Go to **TLS Management** > **Certificates**.
2. Click **Install**.
3. Set the **Type** to **CA Certificate**.
4. Enter a descriptive name for the certificate.
5. Enable **Allow Weak Certificate/Key**.
6. Click **Choose File** and select the `IPO_RootCA.crt` file.
7. Click **Upload**. The menu displays a warning that this is a self-signed certificate.
8. Click **Proceed**. The menu displays the certificate.
9. Click **Install** .
10. Click **Finish**.

Next steps

- Use the IP Office to create an identity certificate for the ASBCE:
  - For subscription systems, see Generating an ASBCE identity certificate using IP Office Web Manager on page 21.
  - For other systems, see Generating an ASBCE identity certificate using Web Control (Platform View) on page 22.

Related links

Adding IP Office certificates to the ASBCE on page 18

Generating an ASBCE identity certificate using IP Office Web Manager

This process generates an identity certificate for the ASBCE using IP Office Web Manager.

- This process is for subscription mode IP Office systems using **Automatic Certificate Management**. For other systems, see Generating an ASBCE identity certificate using Web Control (Platform View) on page 22.

Procedure

1. Log in to the system using IP Office Web Manager.
   - For an IP500 V2, enter the system address followed by `:8443/WebMgmtEE/WebManagerment.html`.
   - For a Linux-based server, enter the system address followed by `:7070/WebManagement/WebManagement.html`.
2. Select **Security** > **Security Settings**.
3. If the IP Office is in a multi-site network, click the next to the required IP Office.
4. Select **Certificates**.
5. Click **Regenerate**.
6. Select **Create certificate for a different machine**.
7. In **Subject Name**, enter the FQDN of the ASBCE.
8. In **Subject Alternative Name(s)**, enter any additional values for other servers and services to which the ASBCE needs to connect.
   - **For IPv4:** The certificate must include the IP Office FQDN and IPv4 address.
   - **For IPv6:** In addition to the IP Office FQDN and IPv4 address, the ASBCE identity certificate must include the ASBCE FQDN and IPv6 address.
   - Use comma separate values for the required *DNS:<FQDN>* and *IP:<IP address>* entries.
   - If you are using different FQDNs for the Avaya one-X® Portal XMPP domain, enter all FQDNs as a comma separated list of DNS entries.
9. Click **OK**. Wait up to a minute whilst the IP Office generates the certificate.
10. When prompted, set an encryption password for the identity certificate and click **Yes**.
11. The browser will prompt you to download and save the certificate file.
12. Rename the downloaded file to `SBCE_ID.p12`.

Next steps

- See Splitting the ASBCE identity certificate on page 23.

Related links

Adding IP Office certificates to the ASBCE on page 18

Generating an ASBCE identity certificate using Web Control (Platform View)

This process generates an identity certificate for the ASBCE using the IP Office server's web control menus.

Procedure

1. Login to the IP Office Web Control menus by either:
   - From within IP Office Web Manager, select the primary server. Click on ☰ and select **Platform View**.
   - Browse to `https://<IP Office IP address>:7071` and log in.
2. Select the **Settings** tab and scroll down to **Certificates**.
3. Select **Create certificate for a different machine**.
4. Enter the following data:
5. In **Machine IP** enter the external IP address of the ASBCE.
6. In **Password** enter a password to encrypt the certificate and key.
7. In **Subject Name**, enter the FQDN of the ASBCE.
8. In **Subject Alternative Name(s)**, enter any additional values for other servers and services to which the ASBCE needs to connect.
   - **For IPv4:** The certificate must include the IP Office FQDN and IPv4 address.
   - **For IPv6:** In addition to the IP Office FQDN and IPv4 address, the ASBCE identity certificate must include the ASBCE FQDN and IPv6 address.
   - Use comma separate values for the required *DNS:<FQDN>* and *IP:<IP address>* entries.
   - If you are using different FQDNs for the Avaya one-X® Portal XMPP domain, enter all FQDNs as a comma separated list of DNS entries.
9. Click **Regenerate**.
10. Click on the link in the popup window and save the file.
11. Rename the downloaded file to `SBCE_ID.p12`.

Next steps

- See Splitting the ASBCE identity certificate on page 23.

Related links

Adding IP Office certificates to the ASBCE on page 18

Splitting the ASBCE identity certificate

The identity certificate created for the ASBCE by the IP Office is a single file. It contains both the certificate and private key. For the ASBCE configuration, you need to split the identity certificate into separate certificate and private key files.

Before you begin

- Use the IP Office to create an identity certificate for the ASBCE:
  - For subscription systems, see Generating an ASBCE identity certificate using IP Office Web Manager on page 21.
  - For other systems, see Generating an ASBCE identity certificate using Web Control (Platform View) on page 22.

Procedure

1. Using WinSCP, connect to the ASBCE management IP address using port 222 and the ipcs login.
2. Copy the IP Office identity certificate created for the ASBCE (`SBCE_ID.p12`) to the ASBCE **`/home/ipcs`** directory.
3. SSH to the ASBCE management IP using port 222 and ipcs login.
4. Enter the command **su root** or **su -root** and type the ASBCE root password.
5. Enter the following commands. The command to use depends on whether you generated the certificate using IP Office Web Manager or the web control (platform view) menus.

   Note:

   - When prompted for a password or PEM pass phrase, enter the password specified when generating the identity certificate for the ASBCE.
   - If the password includes special characters, you must prefix those with `\` when entering them on the command line. For example, on the command line, enter a `@` in the password as `\@`.

   - **IP Office Web Control Certificate:**

     Use the following steps with a certificate generated using the IP Office Web Control menus.

     ```
     openssl pkcs12 -in SBCE_ID.p12 -out SBCE_ID.crt -nokeys -clcerts
     openssl pkcs12 -in SBCE_ID.p12 -out SBCE_ID.key -nocerts
     ```

   - **IP Office Web Manager Certificate:**

Use the following steps with a certificate generated using IP Office Web Manager.

```
openssl enc -base64 -d -in SBCE_ID.p12 -out SBCE_ID_BIN.p12 -A
openssl pkcs12 -in SBCE_ID_BIN.p12 -out SBCE_ID.crt -nokeys -clcerts
openssl pkcs12 -in SBCE_ID_BIN.p12 -out SBCE_ID.key -nocerts
```

6. Copy the new `SBCE_ID.crt` and `SBCE_ID.key` files from the ASBCE to your PC
7. The `SBCE_ID.crt` file still contains the IP Office root CA certificate, private key and ASBCE ID certificate. To be able to import the file to the ASBCE, you must remove the CA certificate and the private key from the file.
   a. Open `SBCE_ID.crt` in WordPad on your PC.
   b. Remove all lines except those which are between the first **BEGIN CERTIFICATE** and **END CERTIFICATE** lines. For example:

```
-----BEGIN CERTIFICATE-----
MIIEYjCCA0qgAwIBAgIGYCZWOINgMA0GCSqGSIb3DQEBCwUAMIGtMQswCQYDVQQG
EwJVUzETMBEGA1UECAwKTmV3IEplcnNleTEWMBQGA1UEBwwNQmFza2lu2yBSaWRn
ZTESMBAGA1UECgwJQXZheWEgSW5jMQwwCgYDVQQLDANHQ1MxLTArBgNVBAMMJGlw
b2ZmaWNlLXJvb3QtMDAwQzI5RDJDRTQ2LmF2YXlhLmNvbTEgMB4GCSqGSIb3DQEJ
ARYRc3VwcG9ydEBhdmF5YS5jb20wHhcNMTUxMjA5MTMyNTQ5WhcNMjIxMjA5MTIy
NTQ5WjCBlzELMAkGA1UEBhMCVVMxEzARBgNVBAgMCk5ldyBKZXJzZXkxFjAUBgNV
BAcMDUJhc2tpbmcgUmlkZ2UxEjAQBgNVBAoMCUF2YXlhIEluYzEMMAoGA1UECwwD
R0NTMRcwFQYDVQQDDA5zYmNlLmJ1bmR5LmNvbTEgMB4GCSqGSIb3DQEJARYRc3Vw
cG9ydEBhdmF5YS5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDE
XivTfA4Q/w/oMlnojSnOyE51Yzk3dS4L1FPHtzfj6IZlfE3w0LAv/7uQl1AljRlc
diiZctJQw2puwnkdhsKzi+GQRaHzKoc+cb+tUhMRrrFBIvnnZ9yy0D1CW+iVp8z9
TO8Tce7G9vMgiRjRnZL7UfesqWigkuySpXMcDUKivlnTuYeOuP8znbu9620xrcCO
/w36qhOB2BcE3jGFn7Iv69hiol2ifHqAWhDcatwvQQahTf85Uka5hVoRetwdT9ys
mk1nnMJ913UyN8DlvXoqnWUav9rQVZKpnQMSOERw9w8n0sb5dXNOqxaV3G2zyHPq
psUHEYKc7bk2haooIvifAgMBAAGjgZswgZgwCQYDVR0TBAIwADALBgNVHQ8EBAMC
A/gwHwYDVR0RBBgwFoIOc2JjZS5idW5keS5jb22HBId88iIwHwYDVR0jBBgwFoAU
8AJiRrTa38gHJzRg4wpAX0Oc7SgwHQYDVR0OBBYEFApovB6QMB8amPZdmppIjaZ3
HO39MB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjANBgkqhkiG9w0BAQsF
AAOCAQEAOG2tfwKeBPaLX0aef35pDzdPjck6qFnZwV3BQFHCz3C3P0RxcLXdC+us
tk/UH71440h8yVhCqLwkQmHuoDK+8ofmuHOlvhnGK8d+lWPWJwImLrIk5PI5ZsXC
4n/9ZKQzibeylfblRQpiCgAaT6L2lvQvZfuETAfSYk4TwZUdMja8JGYDIkNqHBNp
FPb+W1/cPimututLyJYRVCGpkM6bGfmpyMbS3JDGtYWhb7uq19XqlMdZAVWtL5a1
Bxe1kwNfsYIOQGPDiOO9nO1s+9i2pcIUQ1BchpA2yUphvtwS2KrNMhOkG3mcpWHB
9a2PMn1DMM3PXMfyRh9vL00fMRSNVA==
-----END CERTIFICATE-----
```

Next steps

- Go to Adding the identity certificate to the ASBCE on page 24

Related links

Adding IP Office certificates to the ASBCE on page 18

Adding the identity certificate to the ASBCE

Use this process to upload the identity certificate to the ASBCE.

Before you begin

- Splitting the ASBCE identity certificate on page 23

Procedure

1. Go to **TLS Management** > **Certificates**.
2. Click **Install**.
3. In **Type**, select **Certificate**.

4. Enter a descriptive name for the certificate.
5. Click **Choose File** and select the `SBCE_ID.crt` file.
6. Select **Upload Key File**.
7. Click **Choose File** and select the `SBCE_ID.key` file.
8. Click **Upload**. The menu displays the certificate.
9. Click **Install**.
10. Click **Finish**.
11. Using SSH, access the ASBCE management IP address using port 222 and the ipcs login.
    a. Enter `su root` or `su -root` and the ASBCE root password.
    b. Enter the following commands, replacing `********` with the password set when generating the identity certificate:

```
cd /usr/local/ipcs/cert/key
enc_key SBCE_ID.key ********
```

    - You must prefix special characters in the password with a `\`. For example, to enter an `@`, type `\@`.

Related links

Adding IP Office certificates to the ASBCE on page 18

Chapter 4: ASBCE Configuration for remote SIP extensions

This section looks at the configuration of the ASBCE to route SIP calls between the remote extensions and the IP Office.

- **IPv6 Support:** For details regarding supporting IPv6 remote extensions, see Supporting IPv6 remote extensions on page 75.
  - **If only supporting IPv6 remote extensions:** Follow the configuration process in this section for IPv4, but replacing the external IPv4 addresses with IPv6 addresses where applicable.
  - **If supported IPv4 and IPv6 remote extensions:** You must perform additional configuration steps after completing the IPv4 configuration. See Configuration checklist for combined IPv4 and IPv6 remote extensions on page 79.

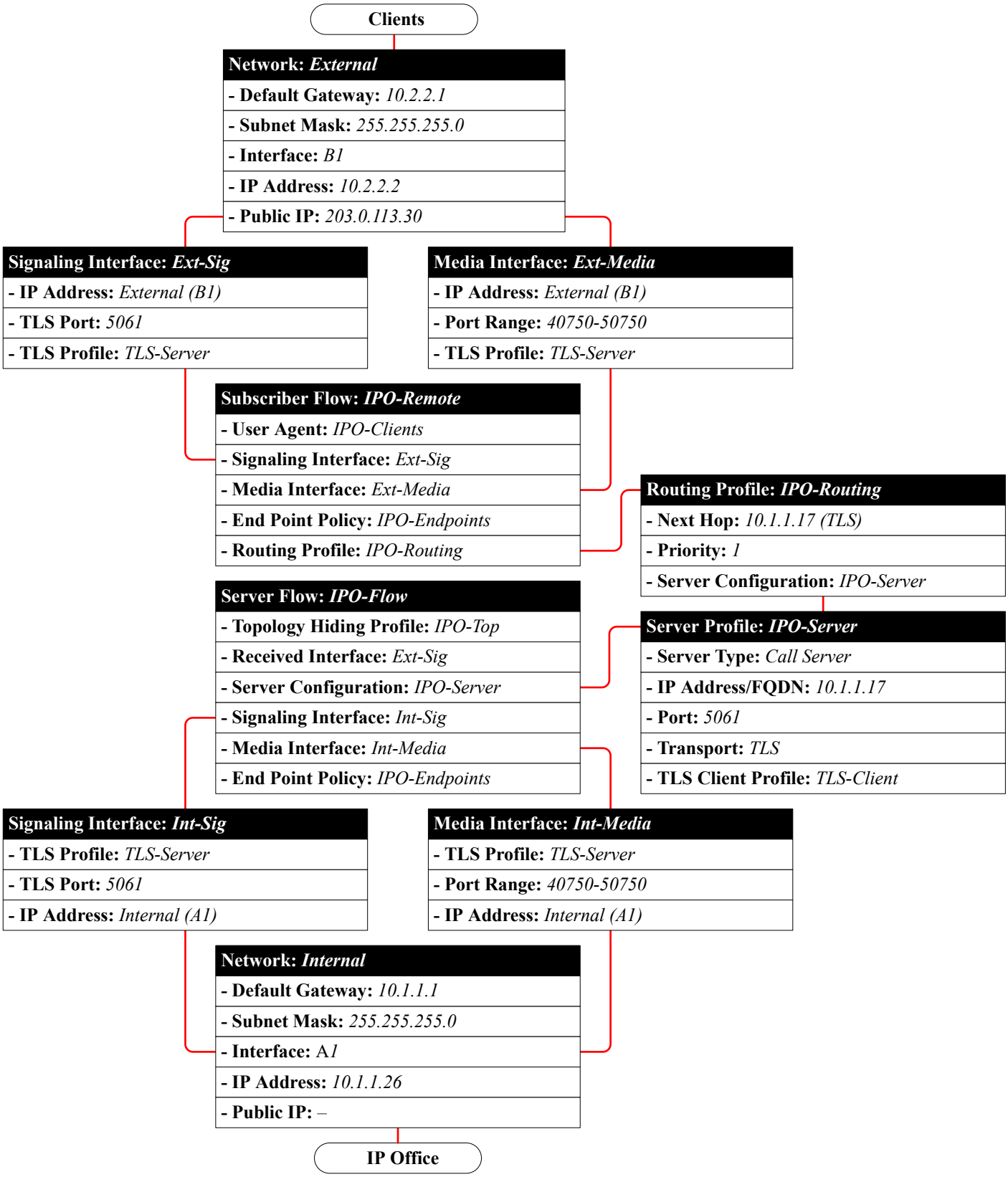
Related links

ASBCE call flow summary on page 27
Clone vs. Add on page 29
ASBCE configuration checklist on page 29
Firewall configuration on page 31
Configure the external ASBCE interface on page 32
Configure the internal ASBCE interface on page 33
Creating a TLS client profile on page 35
Creating a TLS server profile on page 36
Creating an internal media interface on page 38
Creating an external media interface on page 39
Creating an internal signaling interface on page 40
Creating the external signaling interface on page 41
Creating a ASBCE server profile for the IP Office on page 42
Creating a server routing profile on page 44
Creating an ASBCE topology hiding policy on page 46
Creating an IP/URI blocklist on page 47
Creating an application rule on page 48
Creating a media rule on page 49
Creating an endpoint policy group on page 52
Configuring a user agents profile on page 53

Creating the subscriber flow on page 54
Creating a server flow on page 57
Adding reverse proxies for file requests on page 59

ASBCE call flow summary

This image summarizes the ASBCE configuration components used for the connection between IPv4 remote extensions and the IP Office.


Clients
Network: External
- Default Gateway: 10.2.2.1
- Subnet Mask: 255.255.255.0
- Interface: B1
- IP Address: 10.2.2.2
- Public IP: 203.0.113.30
Signaling Interface: Ext-Sig
- IP Address: External (B1)
- TLS Port: 5061
- TLS Profile: TLS-Server
Media Interface: Ext-Media
- IP Address: External (B1)
- Port Range: 40750-50750
- TLS Profile: TLS-Server
Subscriber Flow: IPO-Remote
- User Agent: IPO-Clients
- Signaling Interface: Ext-Sig
- Media Interface: Ext-Media
- End Point Policy: IPO-Endpoints
- Routing Profile: IPO-Routing
Routing Profile: IPO-Routing
- Next Hop: 10.1.1.17 (TLS)
- Priority: 1
- Server Configuration: IPO-Server
Server Flow: IPO-Flow
- Topology Hiding Profile: IPO-Top
- Received Interface: Ext-Sig
- Server Configuration: IPO-Server
- Signaling Interface: Int-Sig
- Media Interface: Int-Media
- End Point Policy: IPO-Endpoints
Server Profile: IPO-Server
- Server Type: Call Server
- IP Address/FQDN: 10.1.1.17
- Port: 5061
- Transport: TLS
- TLS Client Profile: TLS-Client
Signaling Interface: Int-Sig
- TLS Profile: TLS-Server
- TLS Port: 5061
- IP Address: Internal (A1)
Media Interface: Int-Media
- TLS Profile: TLS-Server
- Port Range: 40750-50750
- IP Address: Internal (A1)
Network: Internal
- Default Gateway: 10.1.1.1
- Subnet Mask: 255.255.255.0
- Interface: A1
- IP Address: 10.1.1.26
- Public IP: –
IP Office

Related links

ASBCE Configuration for remote SIP extensions on page 26

Clone vs. Add

Important:

Several processes in this document instruct you to create a new items by cloning an existing template rather than adding a new entry. That is, to click **Clone** rather than **Add**.

- You must use **Clone** when indicated in a process, and you must clone the existing profile indicated in the instructions.
- Using **Add** will create a new entry that has different default settings from the expected clone. This will cause incorrect operation.

Related links

ASBCE Configuration for remote SIP extensions on page 26

ASBCE configuration checklist

#	Action	Link/Notes	✔
1.	Configure firewall port forwarding	Route external traffic from the clients to the ASBCE. See Firewall configuration on page 31.	
2.	Configure the external ASBCE network interface	Set the external IP addresses used by the ASBCE. See Configure the external ASBCE interface on page 32.	
3.	Configure the internal ASBCE network interface.	Set the internal IP addresses used by the ASBCE. See Configure the internal ASBCE interface on page 33.	
4.	Create a TLS client profile	This sets the TLS settings used by the ASBCE when it connects to the IP Office. See Creating a TLS client profile on page 35.	
5.	Create a TLS server profile	This sets the TLS settings used by the ASBCE when clients and the IP Office connect to it. See Creating a TLS server profile on page 36.	

Table continues…

#	Action	Link/Notes	✔
6.	Create an internal SIP media interface	Define the ports and addresses on which the ASBCE listens for SIP media from the IP Office. See Creating an internal signaling interface on page 40.	
7.	Create an external SIP media interface	Define the ports and addresses on which the ASBCE listens for SIP media for the remote extensions. See Creating the external signaling interface on page 41.	
8.	Create an internal SIP signaling interface	Define the ports and addresses on which the ASBCE listens for SIP call signaling from the IP Office. See Creating an internal signaling interface on page 40.	
9.	Create an external SIP signaling interface	Define the ports and addresses on which the ASBCE listens for SIP call signaling from the remote extensions. See Creating the external signaling interface on page 41.	
10.	Create a server profile	See Creating a ASBCE server profile for the IP Office on page 42.	
11.	Create server routing	See Creating a server routing profile on page 44.	
12.	Setup topology hiding	Define the conversions of SIP header information that the ASBCE needs to make. See Creating an ASBCE topology hiding policy on page 46.	
13.	Create an IP/URL blocklist.	Set the types of media supported and the maximum number of connections. See Creating an IP/URI blocklist on page 47.	
14.	Create an application rule	Set the type and number of media connections supported. See Creating an application rule on page 48.	
15.	Create a media rule	See Creating a media rule on page 49.	
16.	Create an endpoint policy	An endpoint policy groups the application and media rules. See Creating an endpoint policy group on page 52.	
17.	Add a user agent profile	Define the UA values for the remote extensions the ASBCE should allow to connect. See Configuring a user agents profile on page 53.	
18.	Create a subscriber flow	See Creating the subscriber flow on page 54.	

Table continues…

#	Action	Link/Notes	✔
19.	Create a server flow	See Creating a server flow on page 57.	
20.	Add a reverse proxy for Avaya Workplace Client	Route requests for settings files by the clients to the IP Office. See Adding reverse proxies for file requests on page 59.	

Related links

ASBCE Configuration for remote SIP extensions on page 26

Firewall configuration

You must configure the customer network equipment on the edge of their network to route external remote extension traffic to the ASBCE. The actual process varies depending on the customer network and equipment. The following are only guidelines.

Procedure

1. Enable **Layer 3 NAT** only.
2. Disable all SIP aware functionality such as ALG.
3. Forward the following ports to the IP address of the B1 interface of the ASBCE.
   - **For Avaya Workplace Client and J100 Series Phones:**

Transport/Application Protocol		Port	Usage
tcp	tls	5061	SIP TLS connection for registration.
	http	80	General and secure file requests from phones and clients if **Use Preferred Phone Ports** is not enabled on the IP Office.
	https	443	
	http	8411	General and secure file requests from phones and clients if **Use Preferred Phone Ports** is enabled on the IP Office.
	https	411	
udp	rtp	40750 to 50750	The port range used for call media (RTP) and call control (RTCP) traffic.
	rtcp		

Next steps

- Go to Configure the external ASBCE interface on page 32.

Related links

ASBCE Configuration for remote SIP extensions on page 26

Configure the external ASBCE interface

Add details for the customer network between the customer firewall and the ASBCE.

- **Dual IPv4/IPv6 Support:** To support IPv4 and IPv6 remote extensions, you must create separate entries for IPv4 and IPv6:
  - The **IP Address** for each must use the respective *B1* IPv4 or IPv6 address.

Important:

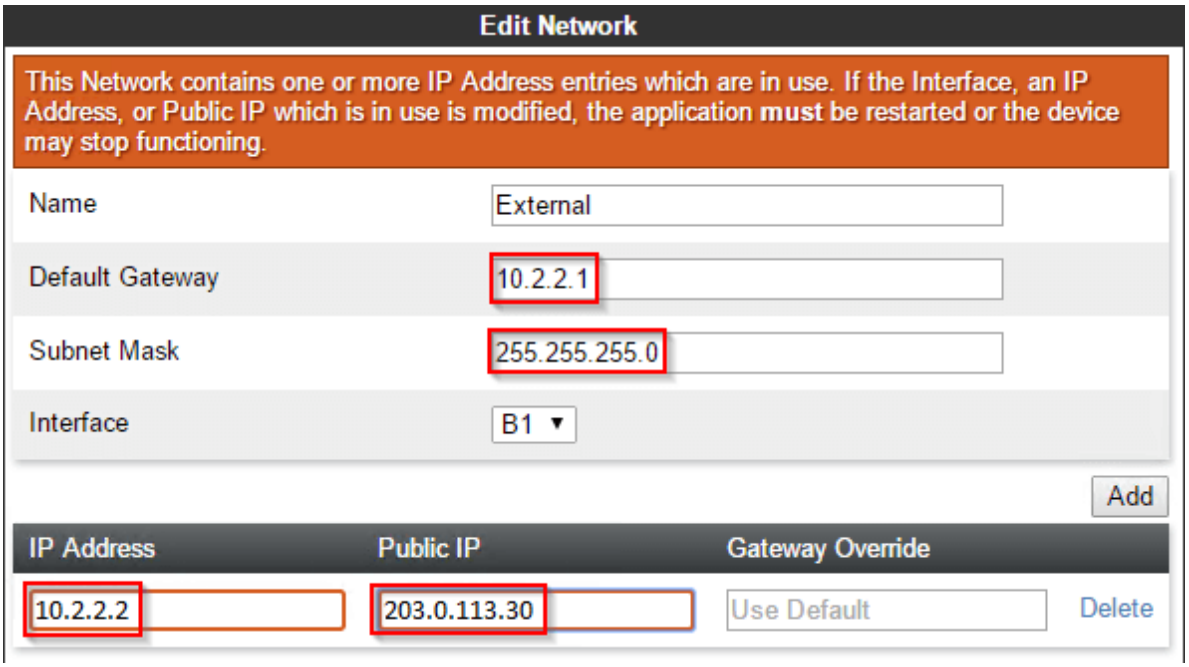
- This process requires you to restart the ASBCE. Doing that will end all current connections using the ASBCE.

Before you begin

- Firewall configuration on page 31

Procedure

1. Go to **Device Specific Settings** > **Network Management**.
2. Select the **Networks** tab and click **Add**.
3. Enter the following data:



Field	Description
Name	You use this name in other menus to select the network.
Default Gateway	The internal IP address of the equipment that routes traffic between the customer network and the public internet. For the example scenario, this is the internal address of the firewall.

Table continues…

Field	Description
Subnet Mask	The IP mask for the **Default Gateway** network.
Interface	Select the public interface of the ASBCE.

4. Click **Add** and enter an IP address the ASBCE uses on this network interface.

Field	Description
IP Address	Enter the IP address of the ASBCE interface connected to the firewall.
Public IP	Enter the public IP address of the firewall. This must match the IP address to which DNS directs remote extension when they perform DNS look-up of the IP Office fully-qualified domain name.

5. If supporting both IPv4 and IPv6 remote extensions, repeat the process to create the IPv6 entries.

Next steps

- Go to Configure the internal ASBCE interface on page 33.

Related links

ASBCE Configuration for remote SIP extensions on page 26

Configure the internal ASBCE interface

Add details for the customer network between the ASBCE and the IP Office.

- **Dual IPv4/IPv6 Support:** You can use the same entry for both IPv4 and IPv6 remote extensions.

Important:

- This process requires you to restart the ASBCE. Doing that will end all current connections using the ASBCE.

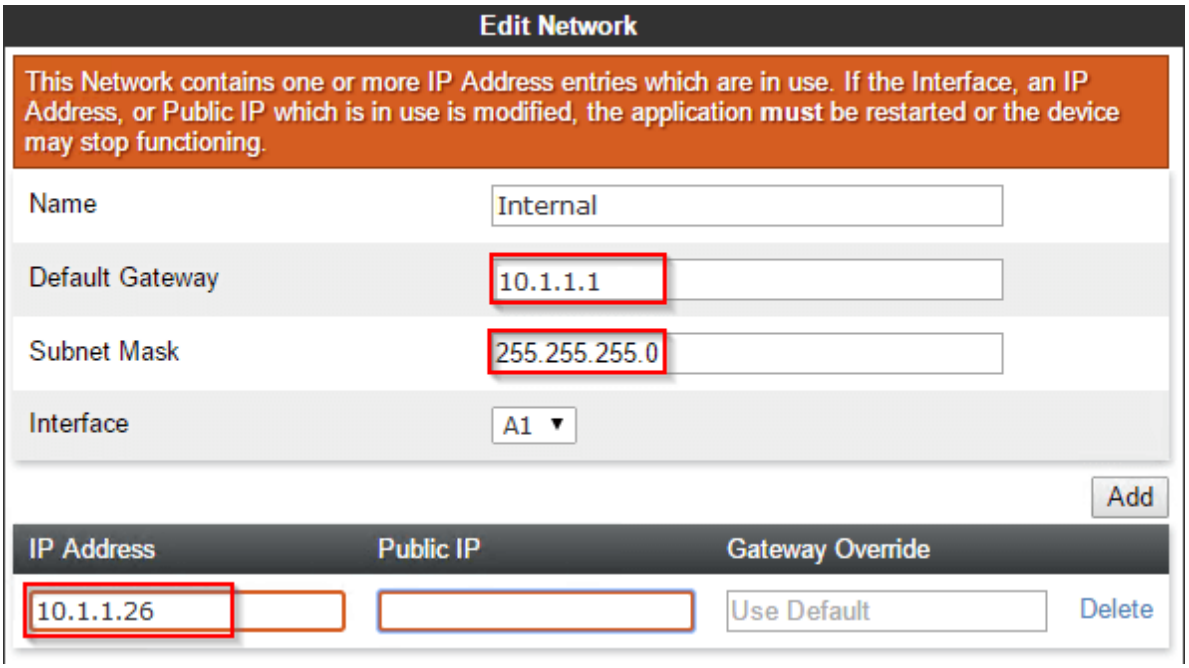
Before you begin

- Configure the external ASBCE interface on page 32

Procedure

1. Go to **Device Specific Settings** > **Network Management**.
2. Select the **Networks** tab and click **Add**.

3. Enter the following data:



Field	Description
Name	You use this name in other menus to select the network.
Default Gateway	The IP address and default gateway for traffic inside the customer network.
Subnet Mask	
Interface	Select the private interface of the ASBCE.

4. Click **Add** and enter an IP address the ASBCE uses on this network interface.

Field	Description
IP Address	Enter the IP address for the ASBCE interface connected to customer network. This is IP address of the A1 interface.

5. Go to **System Management** and click on **Restart Application**.

Next steps

- Go to Creating a TLS client profile on page 35.

Related links

ASBCE Configuration for remote SIP extensions on page 26

Creating a TLS client profile

For TLS connections from the ASBCE, it acts a as TLS client. For example, for connections to the IP Office and to the external clients. The TLS client profile used for each connection defines the certificates used and other TLS settings.

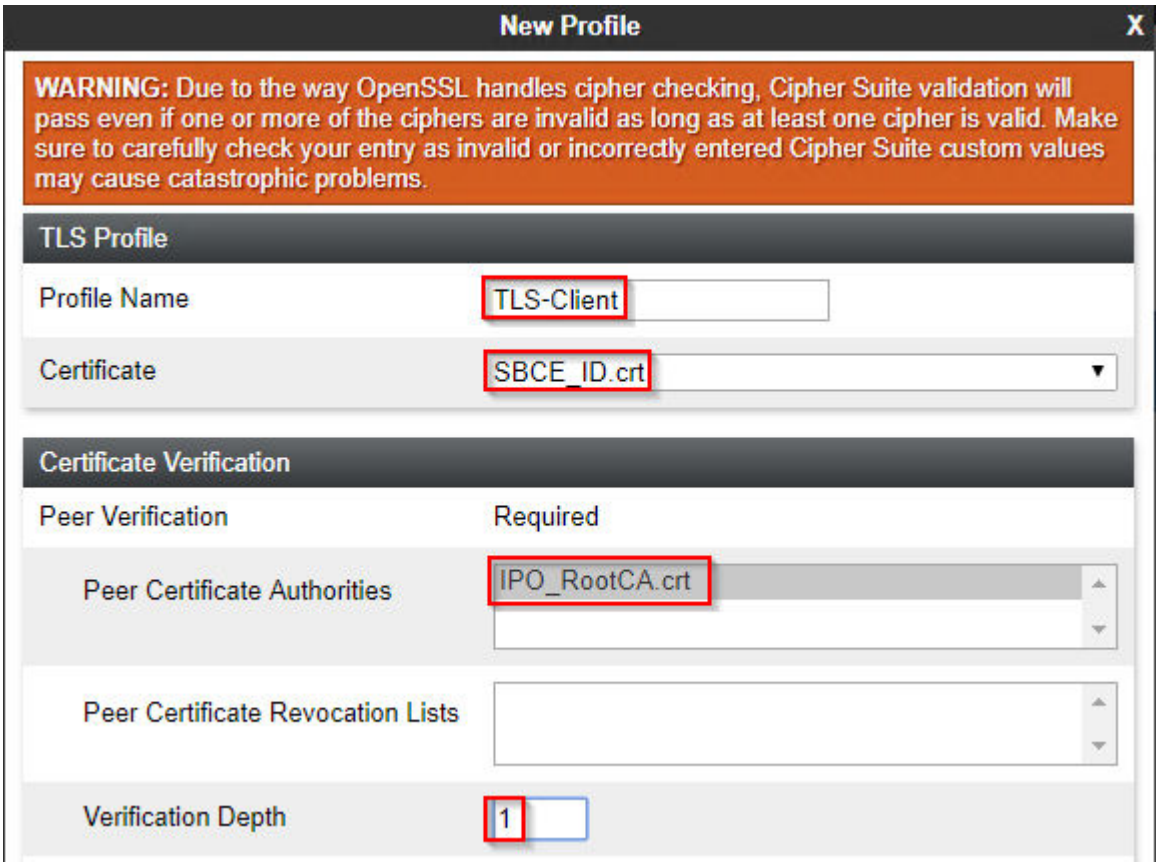
- **Dual IPv4/IPv6 Support:** You can use the same entry for both IPv4 and IPv6 remote extensions.

Before you begin

- Configure the internal ASBCE interface on page 33.

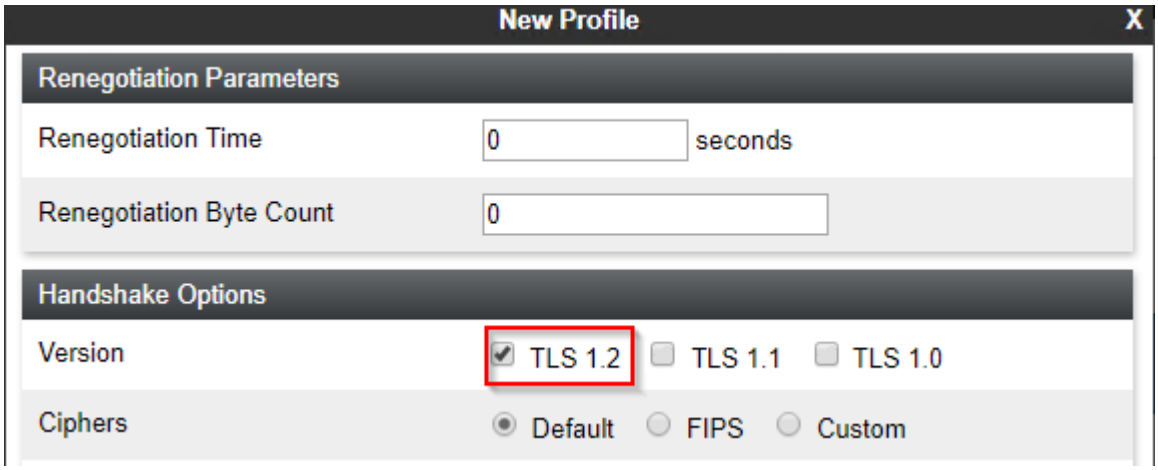
Procedure

1. Select **TLS Management** > **Client Profiles**.
2. Click **Add**.



3. Enter a name. You can then use this to select the policy in other menus.
4. In **Certificate**, select the identity certificate created for the ASBCE.
5. In **Peer Certificate Authorities**, select the root certificate used to create the identity certificate. For the example scenario, this is the `IPO_RootCA.crt` file uploaded to the ASBCE.

6. In **Verification Depth**, enter **1**.
7. Click **Next**.



8. Enable **TLS 1.2**.
9. Click **Finish**.

Next steps

- Go to Creating a TLS server profile on page 36.

Related links

ASBCE Configuration for remote SIP extensions on page 26

Creating a TLS server profile

For TLS connections to the ASBCE, it acts a as TLS server. For example, for connections from the IP Office and from external clients. The TLS client profile used for each connection defines the certificates used and other TLS settings.

- **Dual IPv4/IPv6 Support:** You can use the same entry for both IPv4 and IPv6 remote extensions.

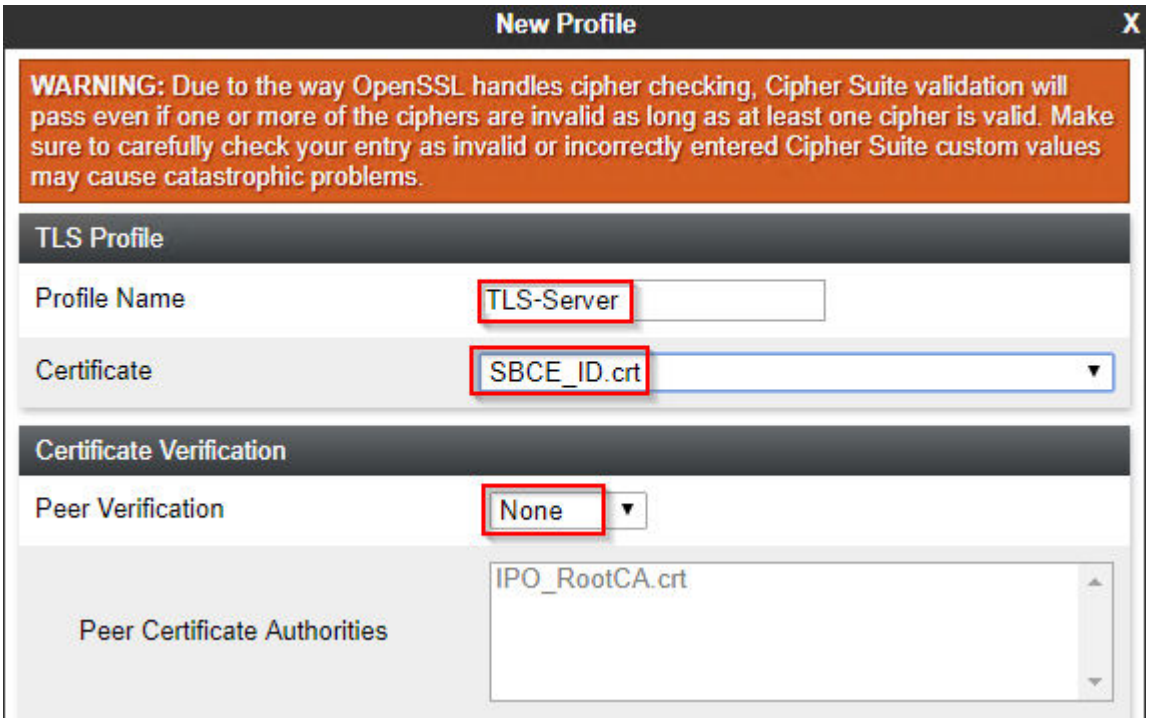
Before you begin

- Creating a TLS client profile on page 35.

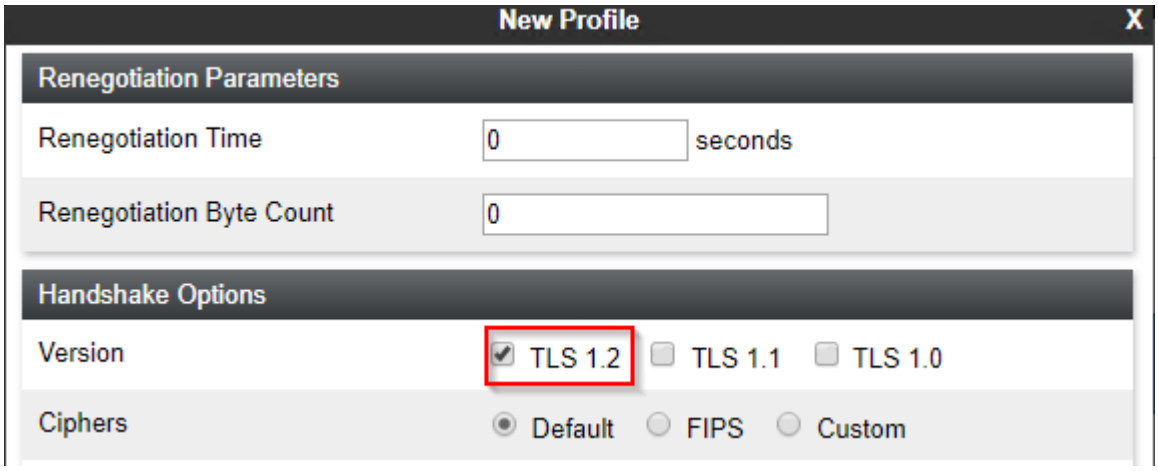
Procedure

1. Select **TLS Management** > **Client Profiles**.

2. Click **Add**.



3. Enter a name. You can then use this to select the policy in other menus.
4. In **Certificate**, select the identity certificate created for the ASBCE.
5. In **Peer Certificate Authorities**, select **None**.
6. Click **Next**.



7. Enable **TLS 1.2**.
8. Click **Finish**.

Next steps

- Go to Creating an internal media interface on page 38.

Related links

ASBCE Configuration for remote SIP extensions on page 26

Creating an internal media interface

You need to create an internal media interface. The ASBCE uses this to listen for SIP call media from the IP Office.

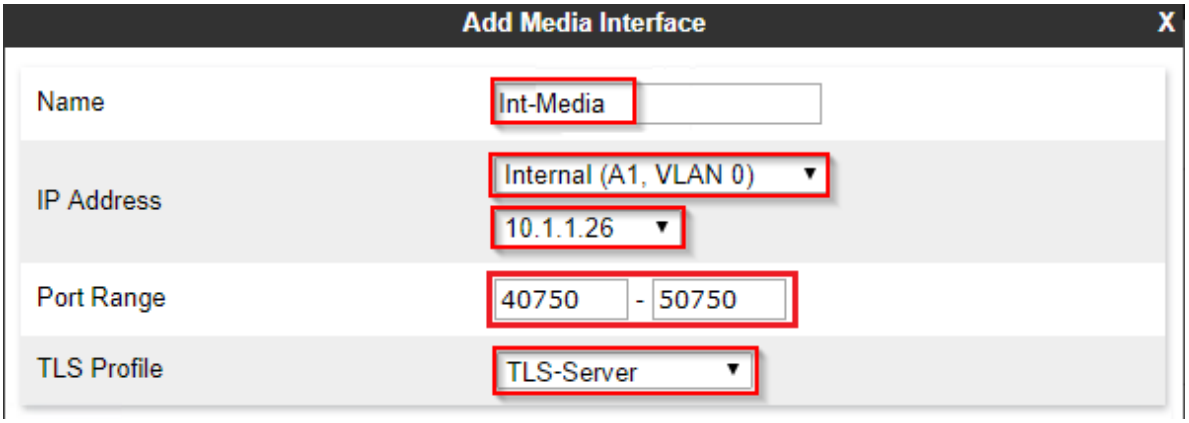
- **Dual IPv4/IPv6 Support:** You can use the same entry for both IPv4 and IPv6 remote extensions.

Before you begin

- Creating a TLS client profile on page 35.

Procedure

1. Select **Device Specific Settings** > **Media Interface**.
2. Click **Add**.



3. Enter a name. You can then use this to select the policy in other menus.
4. Select the internal interface of the ASBCE.
5. For **TLS Profile**, select the TLS server profile you created for traffic to the ASBCE.
6. Click **Finish**.

Next steps

- Go to Creating an external media interface on page 39.

Related links

ASBCE Configuration for remote SIP extensions on page 26

Creating an external media interface

You need to create an external media interface. The ASBCE uses this to listen for SIP call media from the remote extensions.

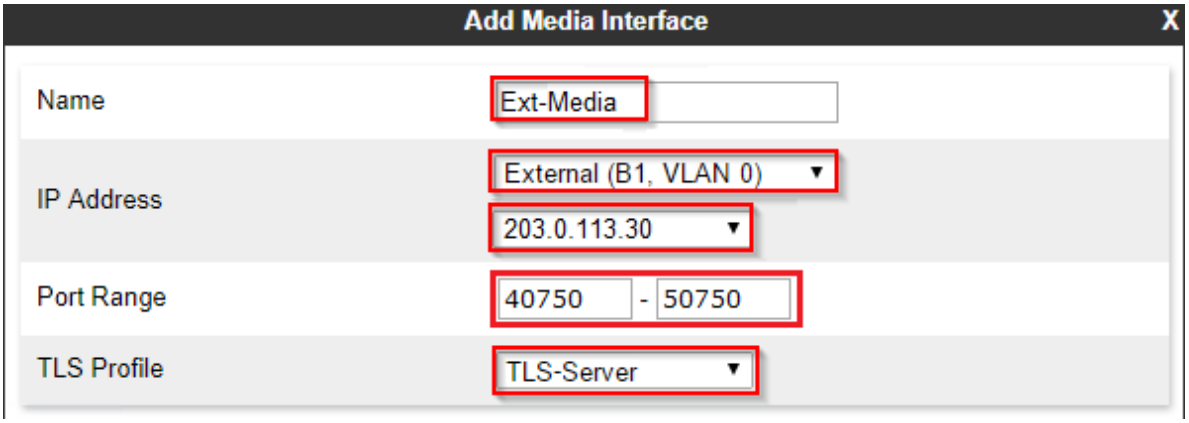
- **Dual IPv4/IPv6 Support:** To support IPv4 and IPv6 remote extensions, you must create separate entries for IPv4 and IPv6:
  - The **IP Address** for each must use the respective *B1* IPv4 or IPv6 address.

Before you begin

- Creating an internal media interface on page 38.

Procedure

1. Go to **Device Specific Settings** > **Media Interface**.
2. Click **Add**.



3. Enter a name. You can then use this to select the policy in other menus.
4. Select the external interface and IP address of the ASBCE.
5. For **TLS Profile**, select the TLS server profile you created for traffic to the ASBCE.
6. Click **Finish**.
7. If supporting both IPv4 and IPv6 remote extensions, repeat the process to create the IPv6 entries.

Next steps

- Go to Creating an internal signaling interface on page 40.

Related links

ASBCE Configuration for remote SIP extensions on page 26

Creating an internal signaling interface

You need to create an internal signaling interface. The ASBCE uses this to listen for SIP call signaling from the IP Office.

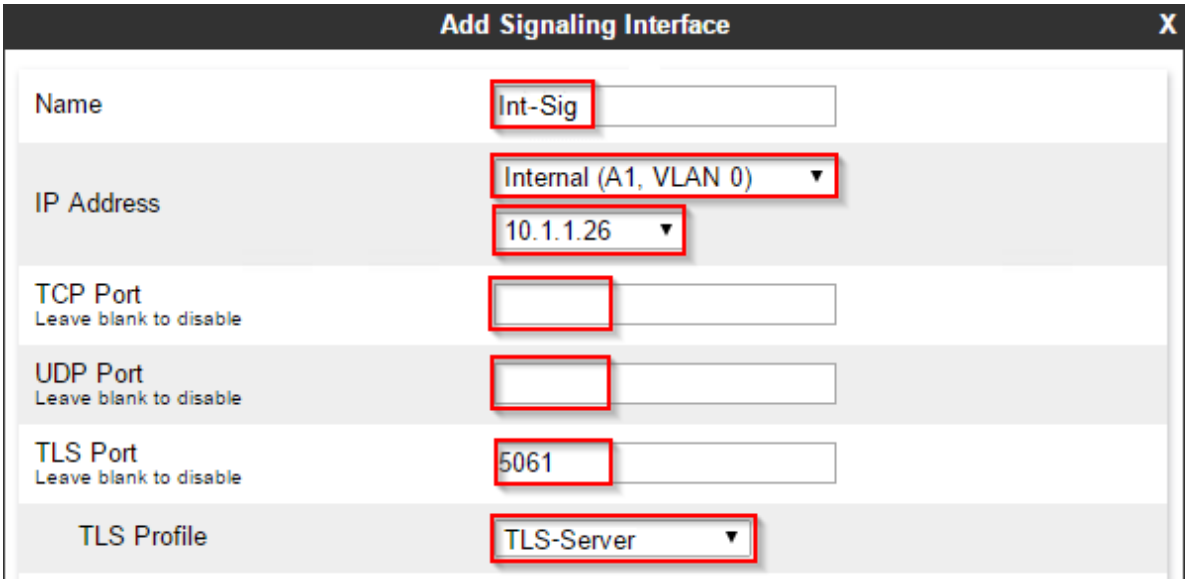
- **Dual IPv4/IPv6 Support:** You can use the same entry for both IPv4 and IPv6 remote extensions.

Before you begin

- Creating an external media interface on page 39.

Procedure

1. Select **Device Specific Settings** > **Signaling Interface**.
2. Click **Add**.



3. Enter a name. You can then use this to select the policy in other menus.
4. Choose *A1* from the **IP Address** drop-down list.
5. Leave the **TCP Port** blank to disable TCP.
6. Leave the **UDP Port** blank to disable UDP.
7. Set **TLS Port** to match the IP Office TLS port.
8. For **TLS Profile**, select the TLS server profile you created for traffic to the ASBCE.
9. Click **Finish**.

Next steps

- Go to Creating the external signaling interface on page 41.

Related links

ASBCE Configuration for remote SIP extensions on page 26

Creating the external signaling interface

You need to create an external signaling interface. The ASBCE uses this to listen for SIP registration messages from the remote extensions.

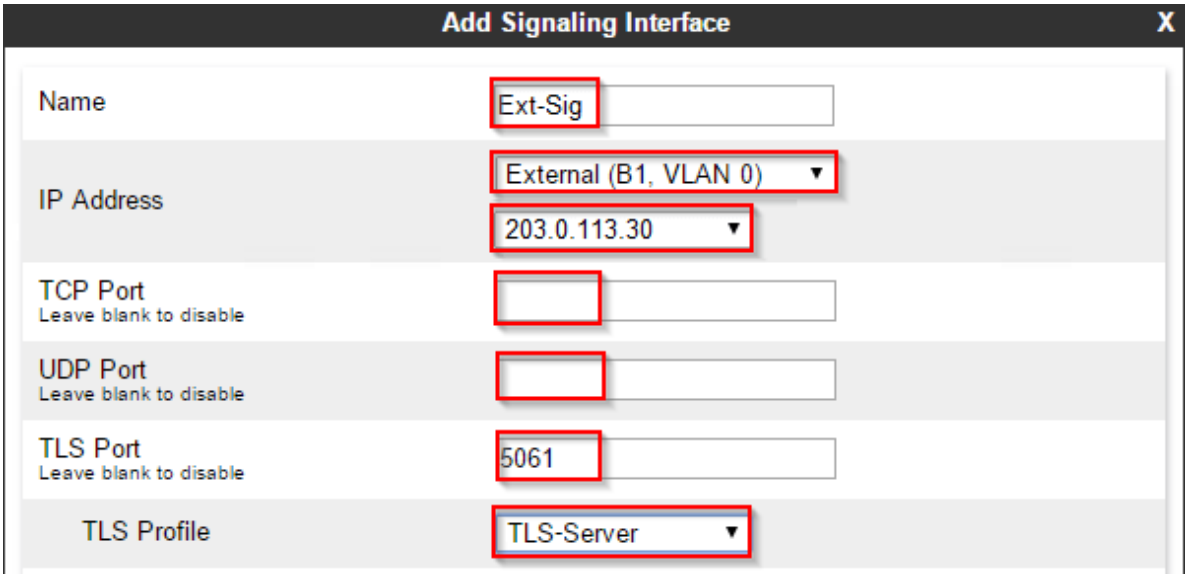
- **Dual IPv4/IPv6 Support:** To support IPv4 and IPv6 remote extensions, you must create separate entries for IPv4 and IPv6:
  - The **IP Address** for each must use the respective *B1* IPv4 or IPv6 address.

Before you begin

- Creating an internal signaling interface on page 40.

Procedure

1. Select **Device Specific Settings** > **Signaling Interface**.
2. Click **Add**.



3. Enter a name. You can then use this to select the policy in other menus.
4. Choose *B1* from the **IP Address** drop-down list.
5. Leave the **TCP Port** blank to disable TCP.
6. Leave the **UDP Port** blank to disable UDP.
7. Set **TLS Port** to match the IP Office TLS port.
8. For **TLS Profile**, select the TLS server profile you created for traffic to the ASBCE.
9. Click **Finish**.
10. If supporting both IPv4 and IPv6 remote extensions, repeat the process to create the IPv6 entries.

Next steps

- Go to Creating a ASBCE server profile for the IP Office on page 42.

Related links

ASBCE Configuration for remote SIP extensions on page 26

Creating a ASBCE server profile for the IP Office

You need to create a server profile on the ASBCE that matches the IP Office configuration, see IP Office SIP VoIP Setup on page 12.

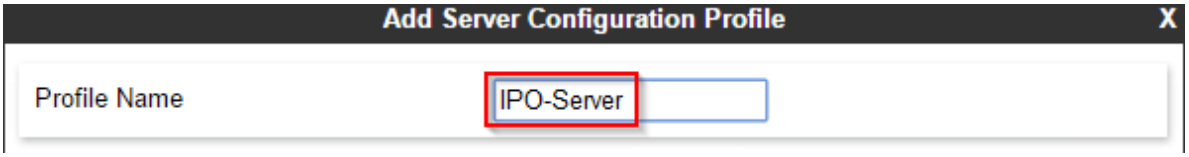
- **Dual IPv4/IPv6 Support:** You can use the same entry for both IPv4 and IPv6 remote extensions.

Before you begin

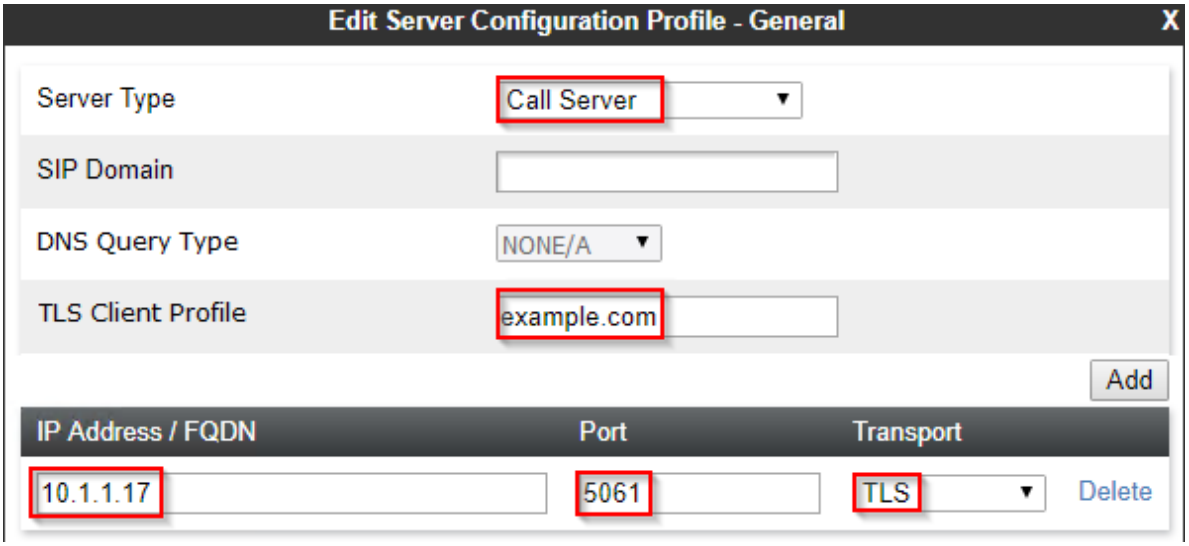
- Creating an internal signaling interface on page 40.

Procedure

1. Select **Global Profiles** > **Server Configuration**.
2. Click **Add**.
3. Enter a name. You can then use this to select the policy in other menus.



4. Click **Next**.



a. For the **Server Type** select **Call Server**.

b. Set the **SIP Domain** to match that used by the IP Office for SIP registration.

c. For the **TLS Client Profile** select the TLS client profile you created.

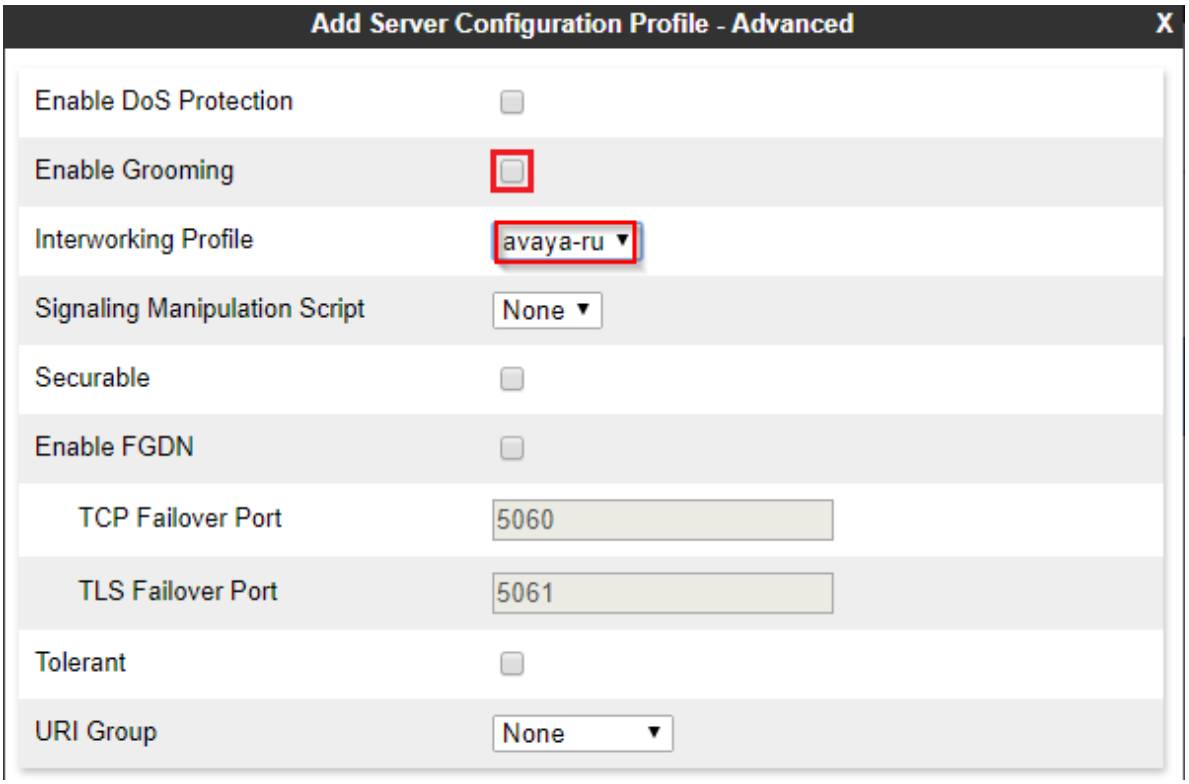
d. Click **Add** and enter the details for the layer 4 port SIP connections set in the IP Office configuration.

- Set the **IP Address/FQDN** to the IP address of the IP Office.
- Set the **Port** and **Transport** to match the IP Office settings.

e. Click **Next**.

5. Click **Next** to skip the **Authentication** settings.
6. Click **Next** to skip the **Heartbeat** settings.

7. Adjust the advanced settings as follows:



   a. Clear the **Enable Grooming** checkbox.
   b. Set **Interworking Profile** to *avaya-ru*.
8. Click **Finish**.

Next steps

- Go to Creating a server routing profile on page 44.

Related links

ASBCE Configuration for remote SIP extensions on page 26

Creating a server routing profile

The ASBCE uses a server routing profile to route matched incoming traffic to the appropriate server or servers. In this case you need to create a profile that routes traffic to the IP Office.

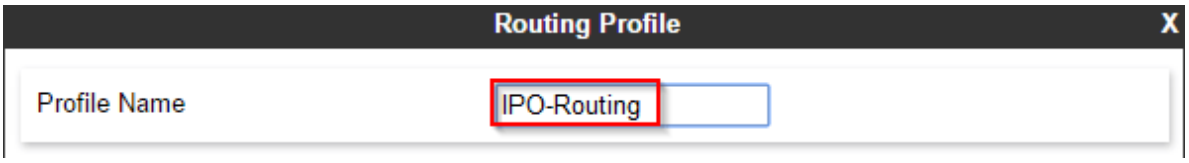
- **Dual IPv4/IPv6 Support:** You can use the same entry for both IPv4 and IPv6 remote extensions.

Before you begin

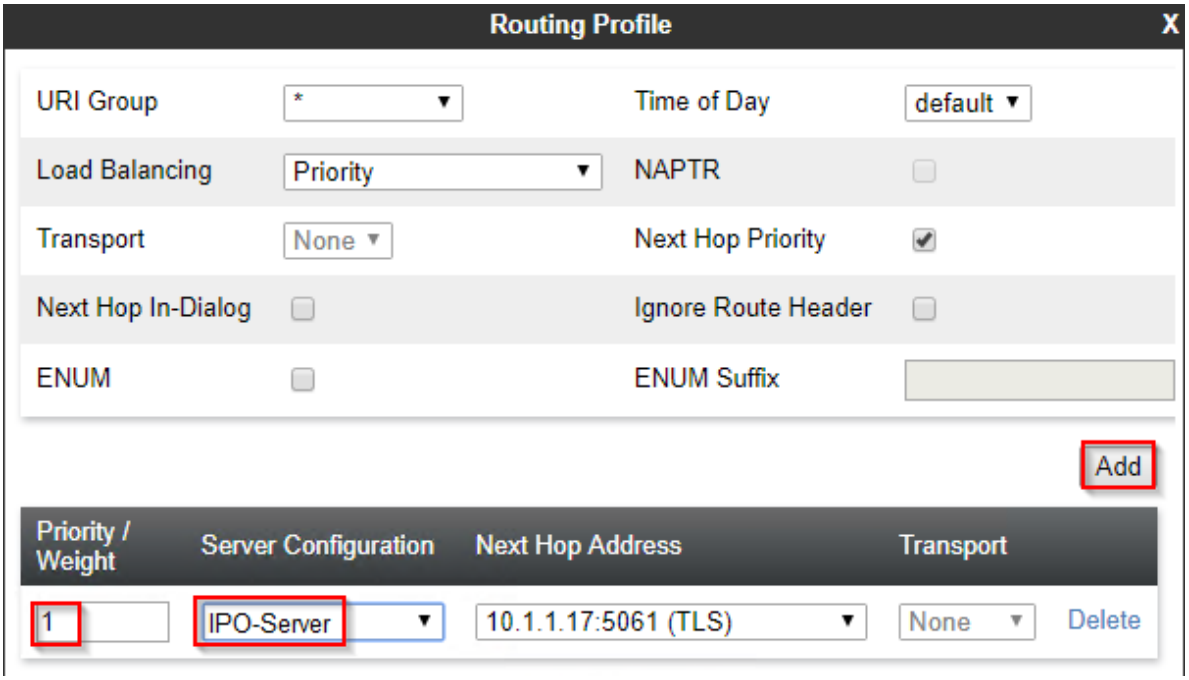
- Creating a ASBCE server profile for the IP Office on page 42.

Procedure

1. Select **Global Profiles** > **Routing**.
2. Click **Add**.
3. Enter a name. You can then use this to select the policy in other menus.



4. Click **Next**.



5. Click **Add**.
6. Set the **Priority** to 1.
7. Set the **Server Configuration** to the server profile created for the IP Office.
8. In the **Next Hop Address**, select the IP address of the IP Office.
9. Click **Finish**.

Next steps

- Go to Creating an ASBCE topology hiding policy on page 46.

Related links

ASBCE Configuration for remote SIP extensions on page 26

Creating an ASBCE topology hiding policy

The ASBCE can use topology hiding setting to remove or replace values in SIP messages. For example, replace an IP address in a SIP header with a required fully-qualified domain name.

- **Dual IPv4/IPv6 Support:** You can use the same entry for both IPv4 and IPv6 remote extensions.

Before you begin

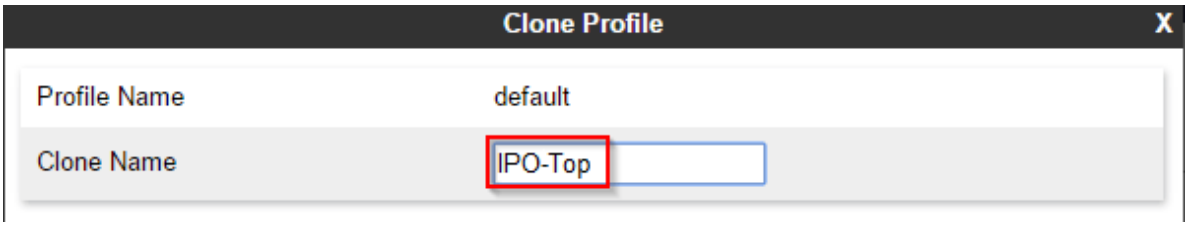
- Creating a server routing profile on page 44.

Procedure

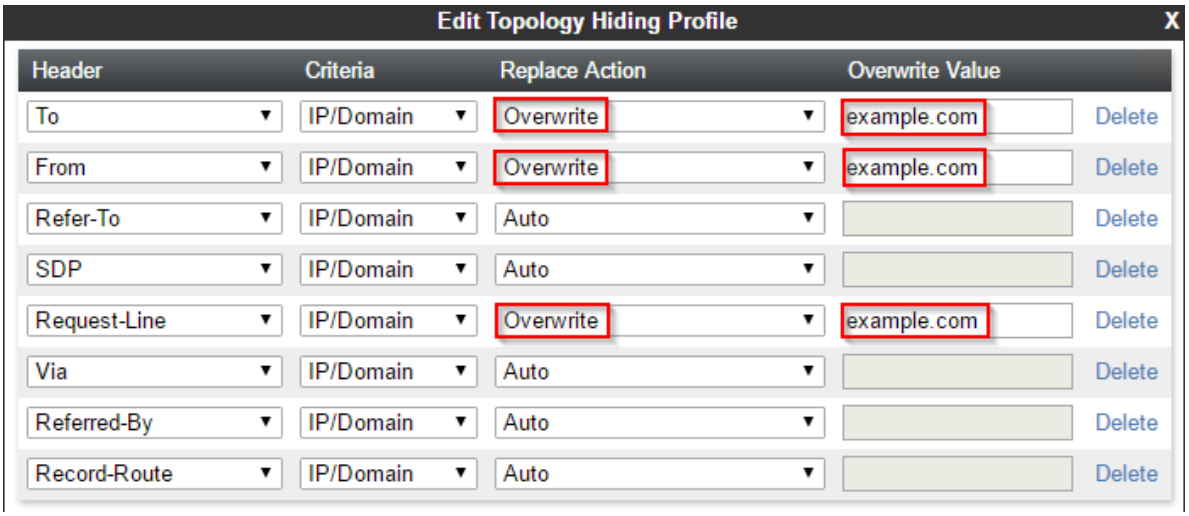
1. Select **Global Profiles** > **Topology Hiding**.
2. Select the default profile and click **Clone**.

   Important:

   - You must use **Clone** and the profile or policy indicated. Using **Add** will create a new profile or policy with different default settings.
3. Enter a name. You can then use this to select the policy in other menus.



4. Click **Finish**.
5. Select the new profile and click **Edit**.



6. For the **To**, **From**, **Refer-To**, **SDP**, and **Request-Line** fields:
   a. Set the **Replace Action** to **Overwrite**.
   b. Enter the IP Office domain as the **Overwrite Value**.
7. Click **Finish**.

Next steps

- Go to Creating an IP/URI blocklist on page 47.

Related links

ASBCE Configuration for remote SIP extensions on page 26

Creating an IP/URI blocklist

You can use a blocklist to have the ASBCE block IP addresses and URIs that are the source of failed registration requests. You can then add the blocklist to any subscriber flow and reverse proxies that you create.

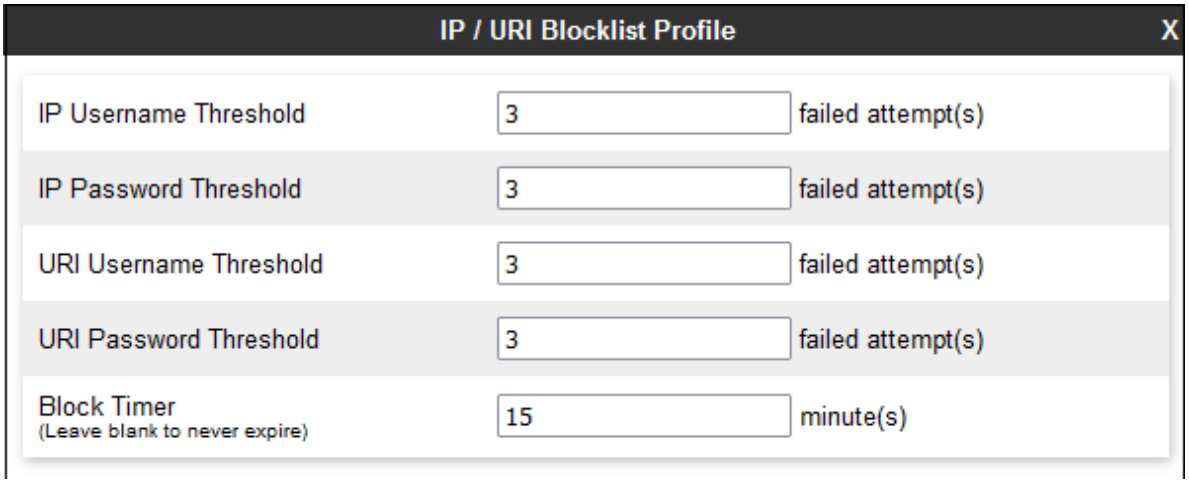
- **Dual IPv4/IPv6 Support:** You can use the same entry for both IPv4 and IPv6 remote extensions.

Before you begin

- Creating an ASBCE topology hiding policy on page 46.

Procedure

1. Select **Domain Policies** > **IP/URI Blocklist Profile**.
2. Click **Add**.



3. Enter a name. You can then use this to select the policy in other menus.
4. Set the number of failed name and password attempts allowed.

5. Set how long an IP address or URI is block after exceeding any of the limits set.
6. Click **Finish**.

Next steps

- Proceed to Creating an application rule on page 48.

Related links

ASBCE Configuration for remote SIP extensions on page 26

Creating an application rule

You can use an application rule to restrict the type of media connections the ASBCE allows. It can also set the maximum number of such connections and maximum connections per remote extension.

- **Dual IPv4/IPv6 Support:** You can use the same entry for both IPv4 and IPv6 remote extensions.

Before you begin

- Creating an IP/URI blocklist on page 47.

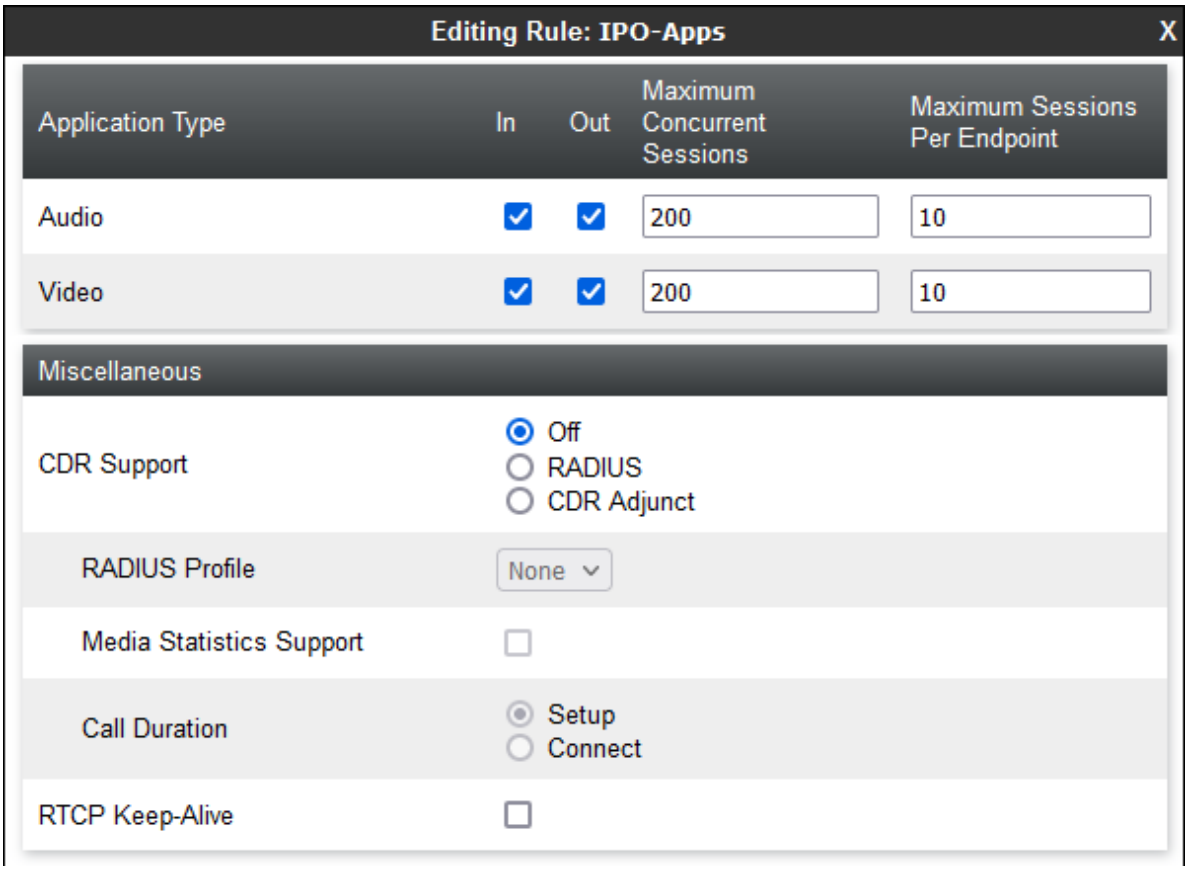
Procedure

1. Select **Domain Policies** > **Application Rules**.
2. Select the *default-low* policy and click **Clone**.

   Important:

   - You must use **Clone** and the profile or policy indicated. Using **Add** will create a new profile or policy with different default settings.
3. Enter a name. You can then use this to select the policy in other menus.
4. Click **Finish**.
5. Select the new policy and click **Edit**.

6. Select whether to allow **Audio** and/or **Video**.



7. For each of the above, set the **Maximum Concurrent Sessions** and **Maximum Sessions Per Endpoint**.
8. Click **Finish**.

Next steps

- Proceed to Creating a media rule on page 49.

Related links

ASBCE Configuration for remote SIP extensions on page 26

Creating a media rule

You can use a media rule to define various media settings.

- **Dual IPv4/IPv6 Support:** You can use the same entry for both IPv4 and IPv6 remote extensions.

Before you begin

- Creating an application rule on page 48.

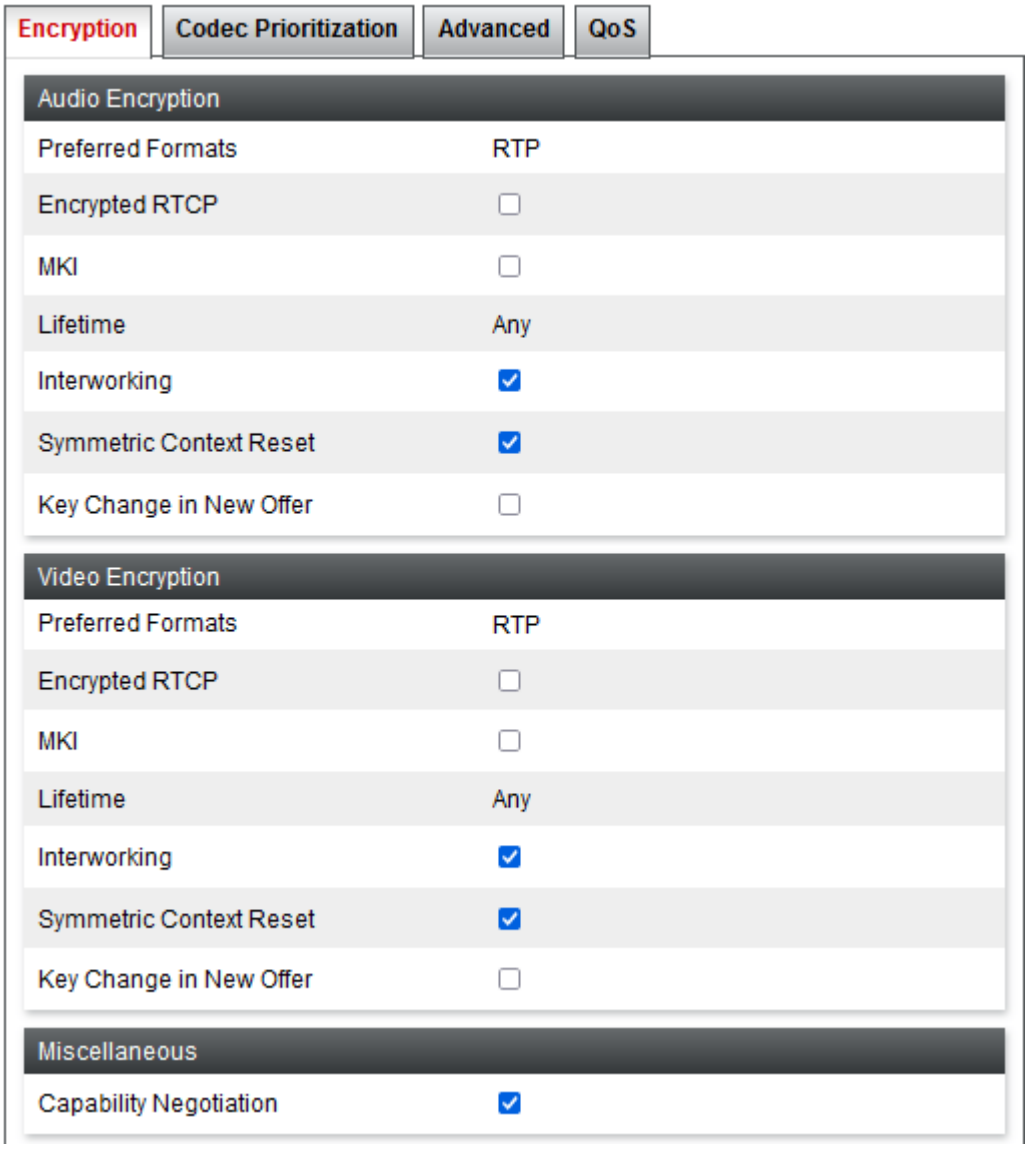
Procedure

1. Select **Domain Policies** > **Media Rules**.
2. Select the *avaya-low-med-enc* policy and click **Clone**.

   Important:

   - You must use **Clone** and the profile or policy indicated. Using **Add** will create a new profile or policy with different default settings.
3. Enter a name. You can then use this to select the policy in other menus.
4. Click **Finish**.
5. Select the new policy and click **Edit**.

6. For the **Audio Encryption** and **Video Encryption** options, set the **Preferred Formats** to *RTP*.



   - If using SRTP, set the **Preferred Formats** and **Encrypted RTCP** values to match the **VoIP Security** settings set on the IP Office.
7. Check that the **Advanced Options** > **ANAT Enabled** setting is not selected.
8. Click **Finish**.

Next steps

- Proceed to Creating an endpoint policy group on page 52.

Related links

ASBCE Configuration for remote SIP extensions on page 26

Creating an endpoint policy group

An endpoint policy groups rules such as media and applications rules. After creating an endpoint policy, you can associate it with the subscriber and server flows that you create.

- **Dual IPv4/IPv6 Support:** You can use the same entry for both IPv4 and IPv6 remote extensions.

Before you begin

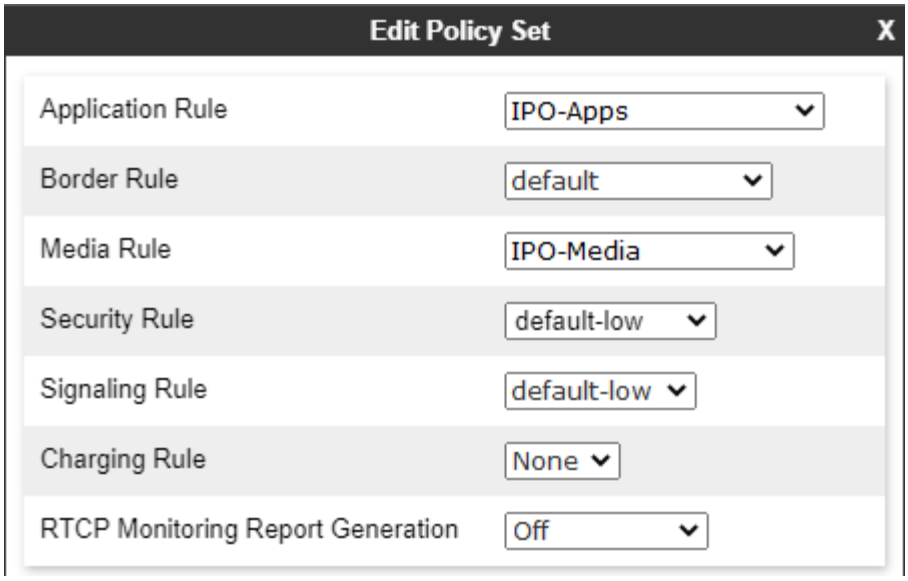
- Creating a media rule on page 49.

Procedure

1. Select **Domain Policies** > **Endpoint Policy Groups**.
2. Select the *default-low* policy and click **Clone**.

   Important:

   - You must use **Clone** and the profile or policy indicated. Using **Add** will create a new profile or policy with different default settings.
3. Enter a name. You can then use this to select the policy in other menus.
4. Click **Finish**.
5. Select the new policy and click **Edit**.
6. In **Application Rule**, select the application and media rules you created for the remote extensions.



7. In **Media Rule**, select the media rule you created.
8. Click **Finish**.

Next steps

- Proceed to Configuring a user agents profile on page 53.

Related links

ASBCE Configuration for remote SIP extensions on page 26

Configuring a user agents profile

You can use **User Agents** to restrict the ASBCE connection to those clients and phones that send a matching *User Agent* (*UA*) string. Otherwise, any phone or client can connect.

- **Dual IPv4/IPv6 Support:** You can use the same entry for both IPv4 and IPv6 remote extensions.

The following are example *UA* strings sent by Avaya clients.

Avaya Phone or Client	User Agent
Avaya 9600 Series Phones	*Avaya one-X Deskphone*
Avaya J159	*Avaya J159 IP Phone 4.0.10.3.2*
Avaya Workplace Client - Android	*Avaya Communicator Android/3.35.2 (FA-RELEASE80-BUILD.18; Pixel 8 Pro)*
Avaya Workplace Client - Windows	*Avaya Communicator/3.0 (3.33.0.96.6; Avaya SDK; Microsoft Windows NT 10.0.19045.0)*

- As shown in the examples above, the *UA* string can vary depending on the software version and/or platform.
- You can view the *UA* sent by a particular phone or softphone in SysMonitor after registering the phone or client.

The UA matching uses a Regular Expression (regex) string match. The following are example regex strings:

Regular Expression	Description
`Avaya.*`	Matches any *UA* beginning with *Avaya*. The . matches any character. The .* matches any number of characters.
`Avaya J1.*`	Matches the *UA* string of any J100 Series phone.
`Avaya (J1|Communicator).*`	Matches the *UA* string of both J100 Series phones and Avaya Workplace Client. The *( )* brackets enclose the potential matches, each potential match separated by a | character.
`Avaya Communicator\/3\.0 \(3\.33.*`	Matches the *UA* string of just the Windows 3.33 version of Avaya Workplace Client. The regex expression use the \ to prefix characters which would otherwise be treated as regex commands. For example . matches any character whilst \. matches just a literal . character.

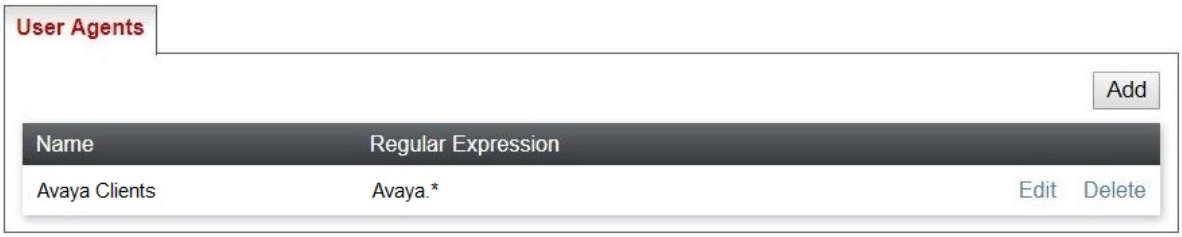
For more information on creating regex strings, see https://learn.microsoft.com/en-us/dotnet/standard/base-types/regular-expression-language-quick-reference and https://regex101.com.

Before you begin

- Creating an ASBCE topology hiding policy on page 46.

Procedure

1. Select **System Management** > **Global Parameters** > **User Agents**.
2. Click **Add**.



3. Enter a name. You can then use this to select the policy in other menus.
4. Enter the regular expression for the user agent string or strings that you want matched.
5. Click **Finish**.

Next steps

- Go to Creating the subscriber flow on page 54.

Related links

ASBCE Configuration for remote SIP extensions on page 26

Creating the subscriber flow

The ASBCE uses a subscriber flow to handling incoming connections from remote extensions.

- **Dual IPv4/IPv6 Support:** To support IPv4 and IPv6 remote extensions, you must create separate entries for IPv4 and IPv6:
  - The **Signaling Interface** and **Media Interface** interfaces for each must use the respective external IPv4 or IPv6 interfaces.

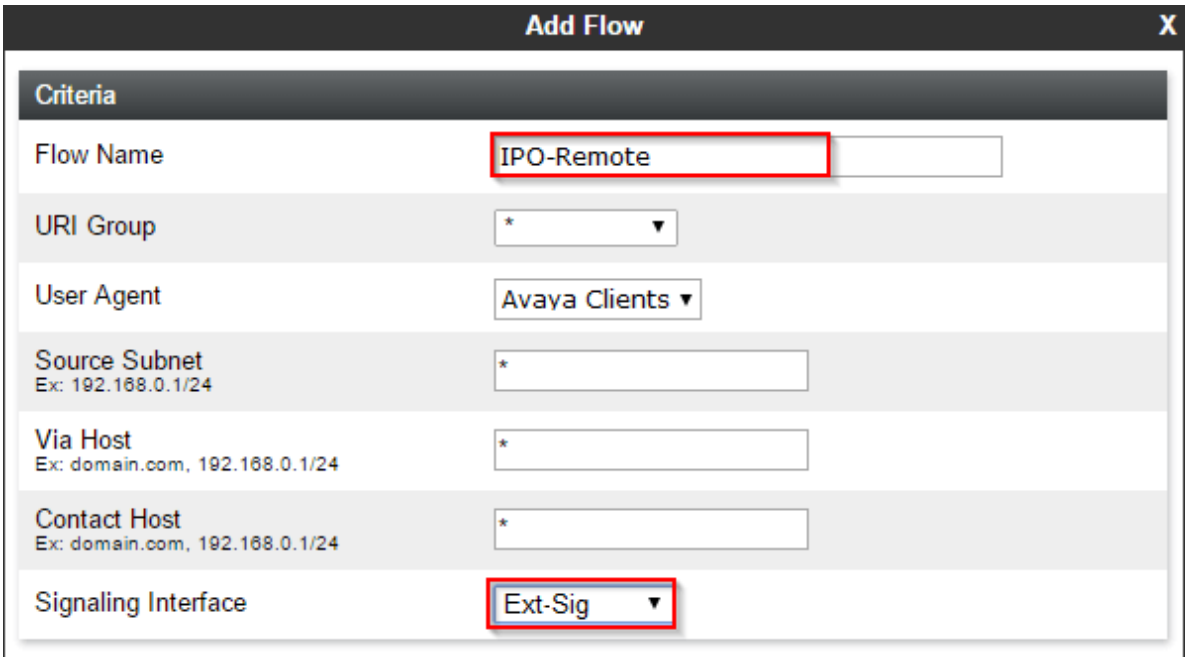
Before you begin

- Configuring a user agents profile on page 53.

Procedure

1. Select **Device Specific Settings** > **End Point Flows**.

2. Select **Subscriber Flows** tab and click **Add**.

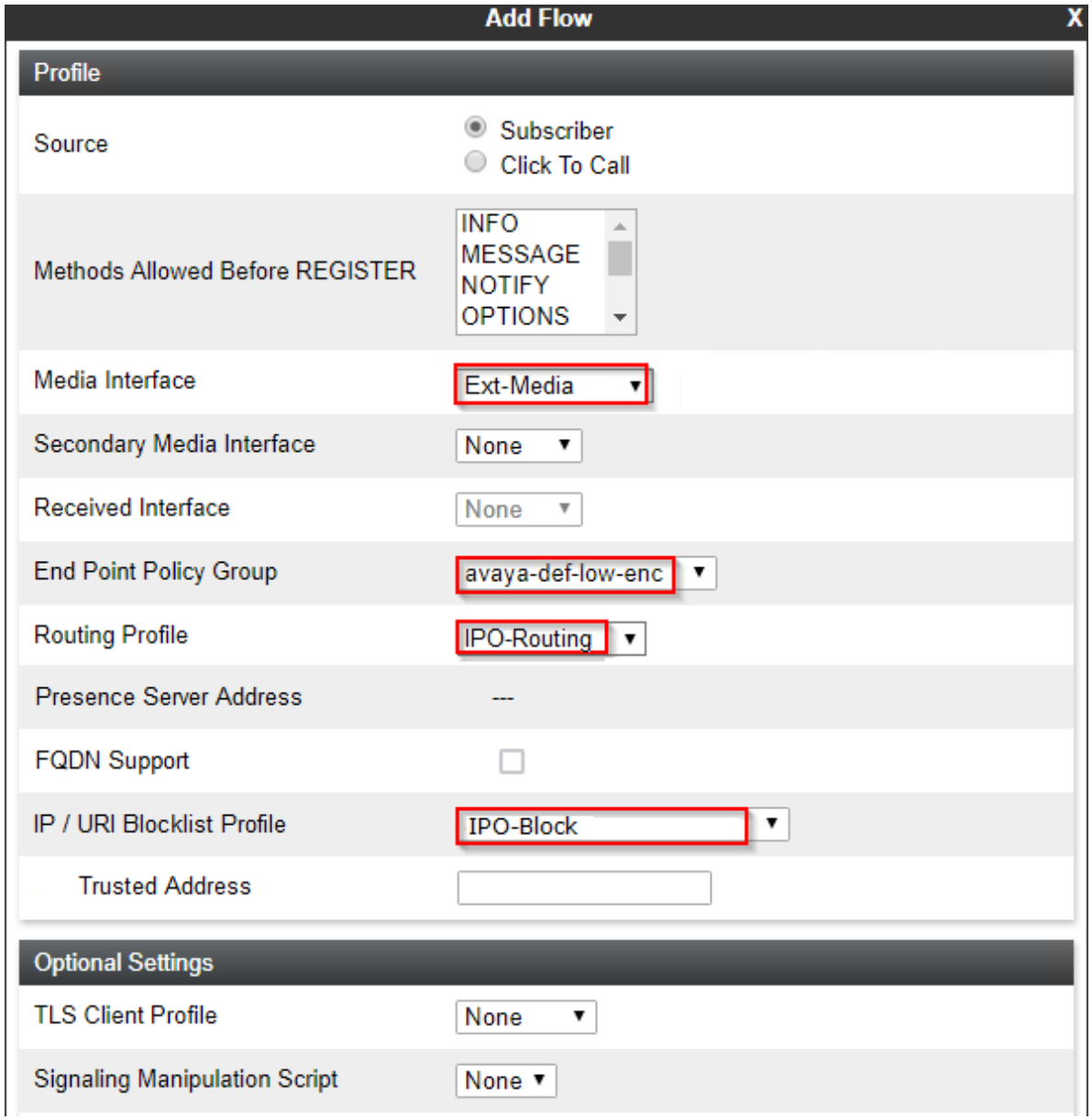


a. Enter a name. You can then use this to select the policy in other menus.

b. If required, select the **User Agent** profile you created to match the UA of clients allowed to use the subscriber flow.

c. Select the external **Signaling Interface** created for the remote extensions.

3. Click **Next**.



   a. In **Media Interface**, select the external media interface created for the remote extensions.
   b. In **End Point Policy Group**, select *avaya-def-low-enc*.
   c. In **Routing Profile**, select the server routing profile created for the IP Office.
   d. If you created a block list profile, select it using the **IP/URI Blocklist Profile** drop-down.

4. Click **Finish**.

5. If supporting both IPv4 and IPv6 remote extensions, repeat the process to create the IPv6 entries.

Next steps

- Go to Creating a server flow on page 57.

Related links

ASBCE Configuration for remote SIP extensions on page 26

Creating a server flow

The ASBCE uses a server flow to handling incoming connections from the IP Office server.

- **Dual IPv4/IPv6 Support:** To support IPv4 and IPv6 remote extensions, you must create separate entries for IPv4 and IPv6:
  - The **Received Interface** for each server flow must use the respective IPv4 or IPv6 external signaling interface.

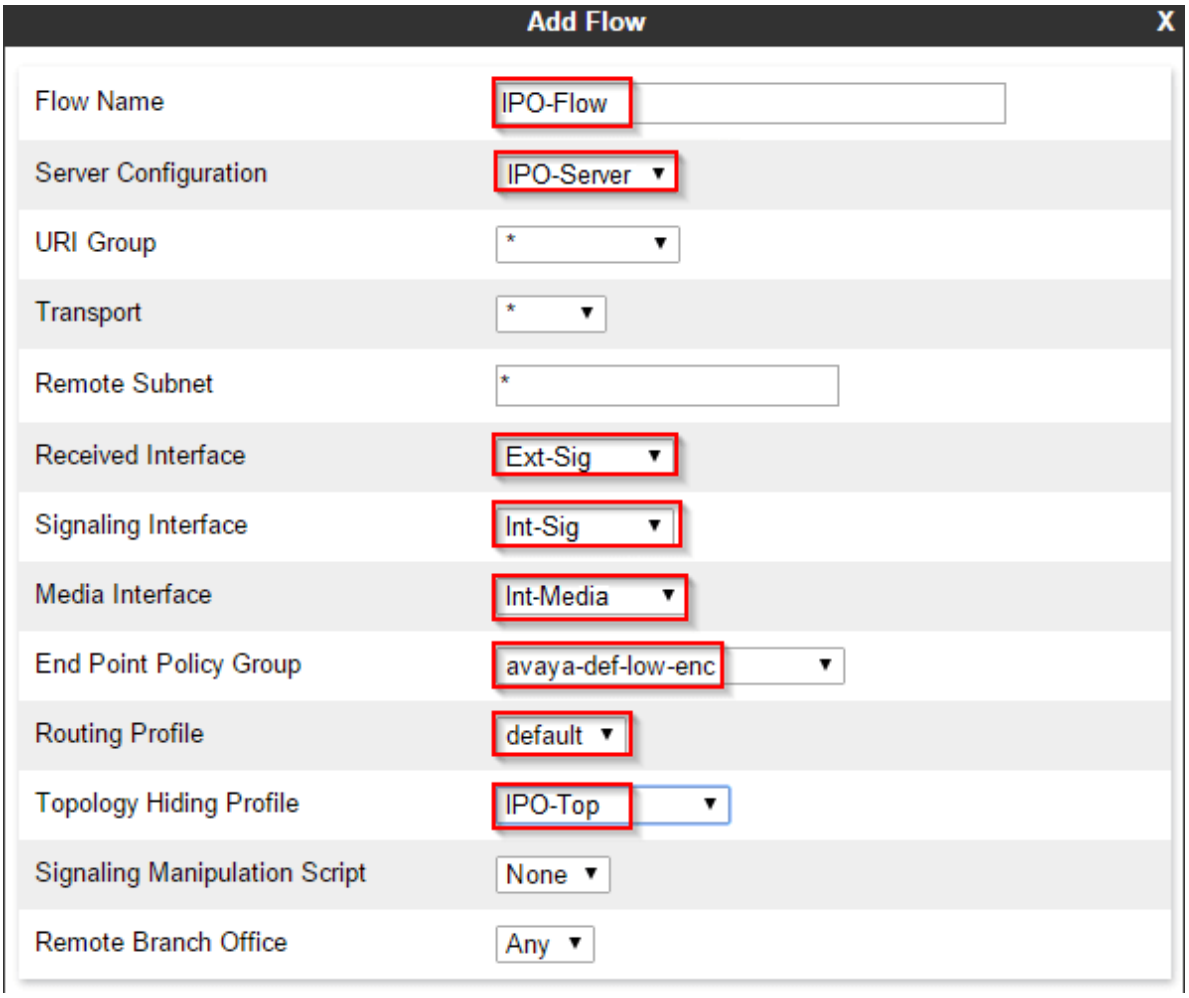
Before you begin

- Creating the subscriber flow on page 54.

Procedure

1. Select **Device Specific Settings** > **End Point Flows**.

2. Select **Server Flows** tab and click **Add**.



   a. In **Flow Name**, enter a descriptive name.
   b. In **Server Configuration**, select the server profile created for the IP Office server.
   c. In **Received Interface**, select the external signaling interface created for the remote extensions.
   d. In **Signaling Interface**, select the internal signaling interface created for the remote extensions.
   e. In **Media Interface**, select the internal media interface created for the remote extensions.
   f. In **End Point Policy Group**, select *avaya-def-low-enc*.
   g. In **Routing Profile**, select *default*.
   h. In **Topology Hiding Profile**, select the topology hiding profile created for IP Office remote extensions.

3. Click **Finish**.

4. If supporting both IPv4 and IPv6 remote extensions, repeat the process to create the IPv6 entries.

Next steps

- Go to Adding reverse proxies for file requests on page 59.

Related links

ASBCE Configuration for remote SIP extensions on page 26

Adding reverse proxies for file requests

The following is an example for creating reverse proxies for remote extensions. These allow the remote extensions to request files from the IP Office. For example, requesting the `46xxsettings.txt` and `46xxspecials.txt` files.

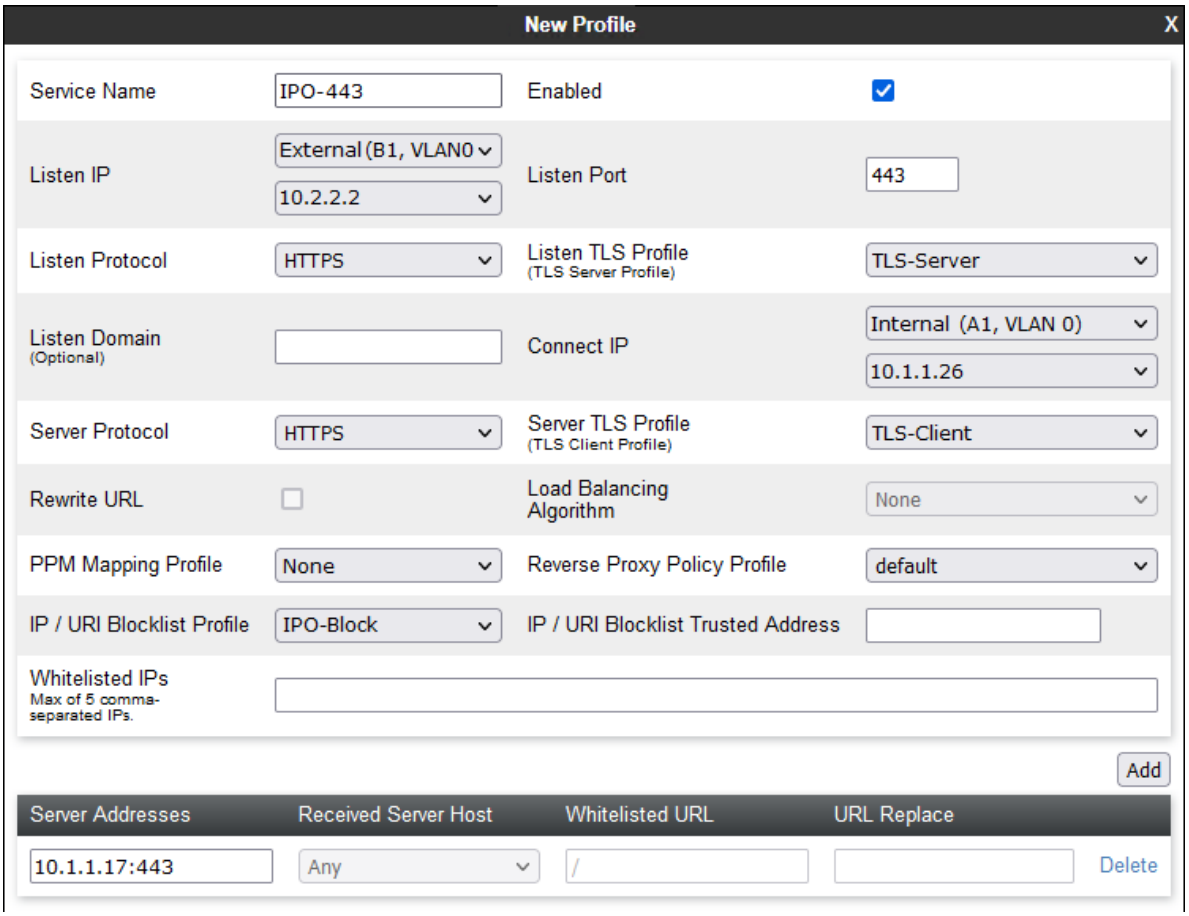
The ports and protocol required depend on the requirements of the type of remote extension.

- By default, for initial connection to the IP Office to request the `46xxsettings.txt` file, extensions use either `http` or `https`. The IP Office uses port `80` and port `443` respectively.
- The `46xxsettings.txt` settings tell the remote extension what ports and protocols to use for future connections.
- If **System** > **System** > **Use Preferred Phone Ports** is enabled, the `46xxsettings.txt` tells phones and clients to use port `8411` for HTTP and port `411` for HTTPS file requests, and those ports are enabled on the IP Office.
  - With **Use Preferred Phone Ports** enabled, the IP Office still allows connections on port `80` and port `443`. The IP Office requires this for initial connection and for legacy clients.
- **Dual IPv4/IPv6 Support:** To support IPv4 and IPv6 remote extensions, you must create separate entries for IPv4 and IPv6. Each using the respective IPv4 and IPv6 external interfaces.

Procedure

1. Select **Device Specific Settings** > **DMZ Services** > **Relay Services**.

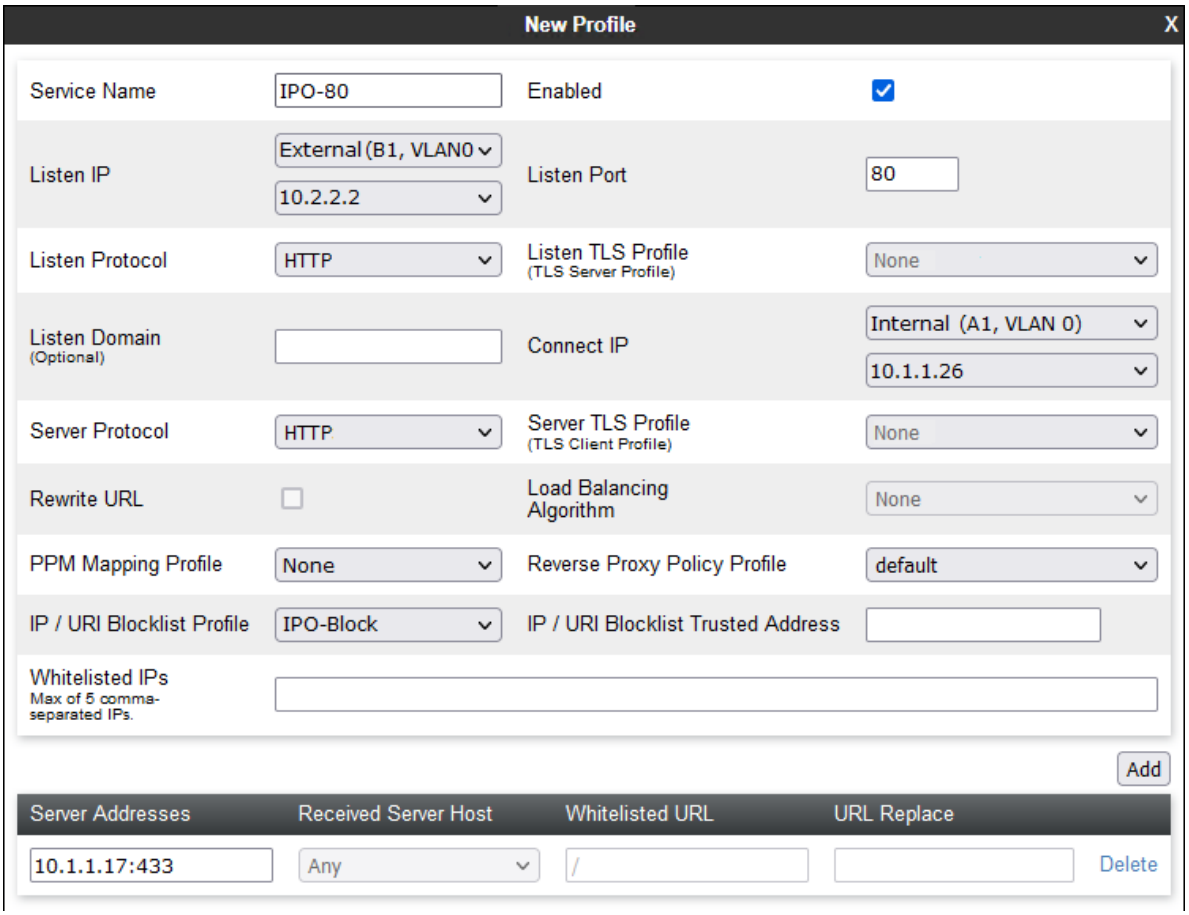
2. Select **Reverse Proxy** tab and click **Add**.



   a. In **Service Name** enter a descriptive name for the reverse proxy.
   b. In **Listen IP**, select the external *B1* interface and the IP address.
   c. Set the **Listen Port** to `443`.
   d. Set the **Listen Protocol** to **HTTPS**.
   e. In **Listen TLS Profile**, select the TLS server profile.
   f. In **Connect IP**, select the internal *A1* interface and IP address.
   g. In **Server Protocol**, select **HTTPS**.
   h. In **Server TLS Profile**, select the TLS client profile.
   i. If you created a blocklist, select it using the **IP/URI Blocklist Profile** drop-down.
   j. Click **Add**:
   k. For **Server Address**, enter the IP Office IP address followed by `:443`.

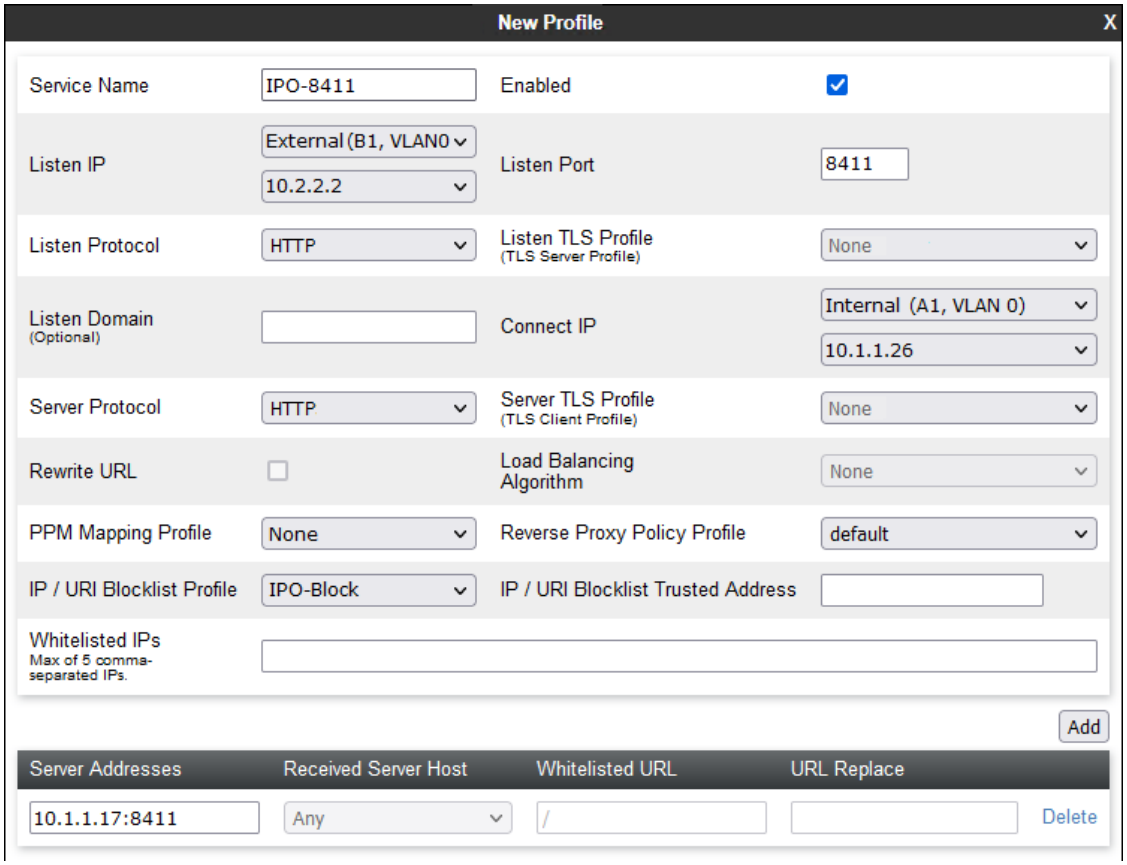
3. Click **Finish**.

4. Repeat the procedure to add a proxy for port `80` HTTP file requests. This proxy does not use any TLS profiles.

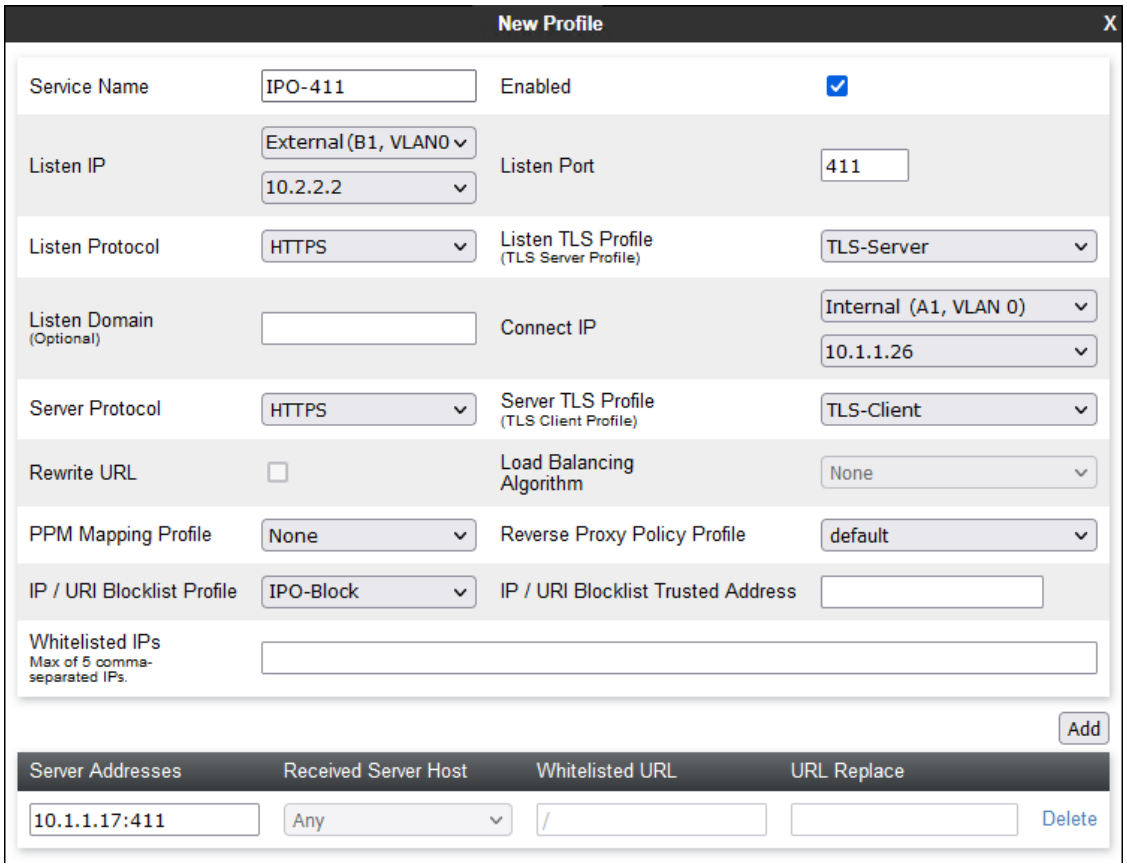


5. Click **Finish**.

6. If **Use Preferred Phone Ports** is enabled on the IP Office:
   a. Add a reverse proxy for HTTP on port `8411`.



b. Add a reverse proxy for HTTPS on port `411`.



7. If supporting both IPv4 and IPv6 remote extensions, repeat the process to create the IPv6 entries.

Related links

[ASBCE Configuration for remote SIP extensions](#) on page 26

Chapter 5: Unanchoring call media from the ASBCE

The ASBCE normally remains part of all calls it routes. All the call media and call signaling remains anchored to the ASBCE, and therefore requires bandwidth and processing from the ASBCE.

In scenarios where the networks involved support direct routing between all ends of the call, you can unanchor the call media from the ASBCE. Unanchoring reduces the bandwidth and resources required by the ASBCE. The ASBCE continues to handle the call signaling.

- For remote extensions on the same remote sub-net, unanchoring the ASBCE allows direct media between the remote extensions on that sub-net.
- You may also be able to use unanchoring in other scenarios. For example, between remote extensions on two separate sub-nets. For further information, see https://documentation.avaya.com/bundle/GUID-416B16B1-7DB4-4C01-A966-3E62EFEA4D43/page/Media_Unanchoring_scenarios.html.

Unanchoring uses the following additional ASBCE configuration items:

- **Session Flow**

  A session flow defines a pair of network address ranges and which session policy the ASBCE should apply for traffic between those networks. For direct media at a remote site, the sites address range is set for both networks in the session flow.

- **Session Policy**

  A session policy sets how the ASBCE should treat call media. You can use the same session policy for several session flows.

Related links

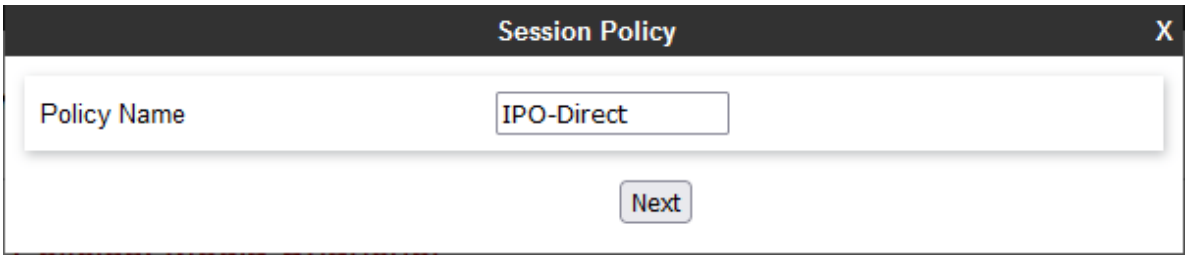
Creating a session policy for a remote site on page 64
Creating a session flow for the remote site on page 66

Creating a session policy for a remote site

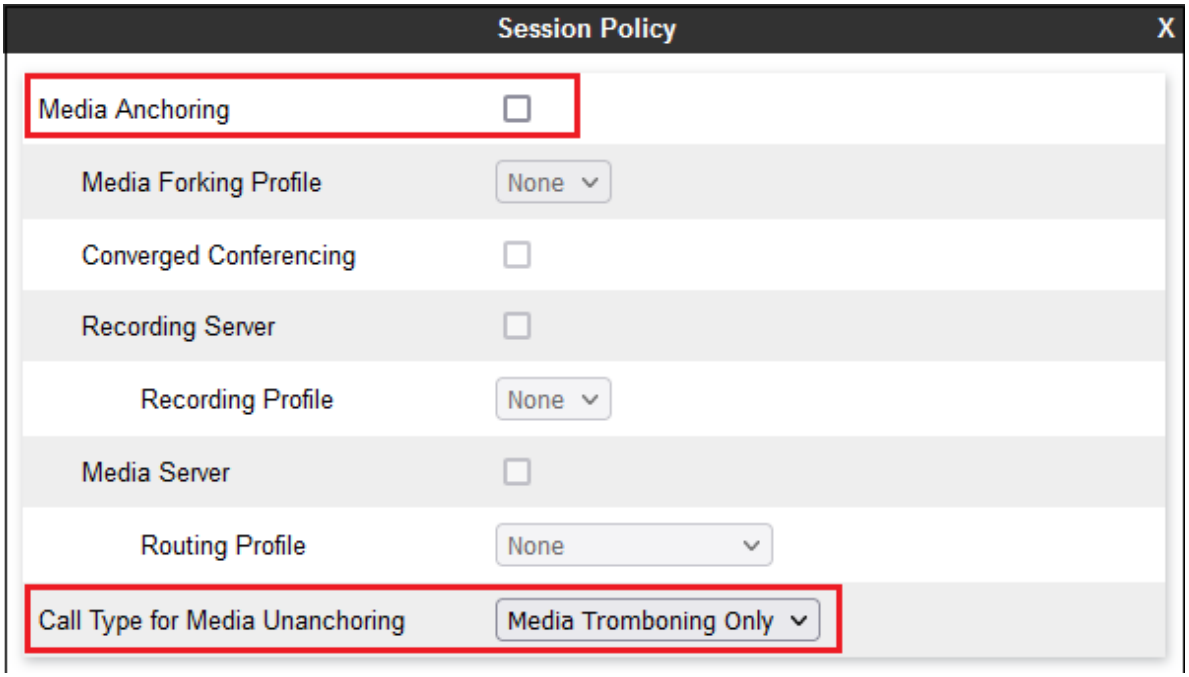
A session policy sets how the ASBCE should treat traffic between sites matched by any session flow that uses the policy. You can use the same policy for multiple session flows. That is, for multiple remotes sites.

Procedure

1. Select **Domain Policies** > **Session Policies**.
2. Click **Add**.
3. Enter a name. You can then use this to select the policy in other menus.



4. Click **Next**.



5. Deselect **Media Anchoring**.
6. Set the **Call type for Media Unanchoring** to **Media Tromboning Only**.
7. Click **Finish**.

Next steps

- Go to Creating a session flow for the remote site on page 66.

Related links

Unanchoring call media from the ASBCE on page 64

Creating a session flow for the remote site

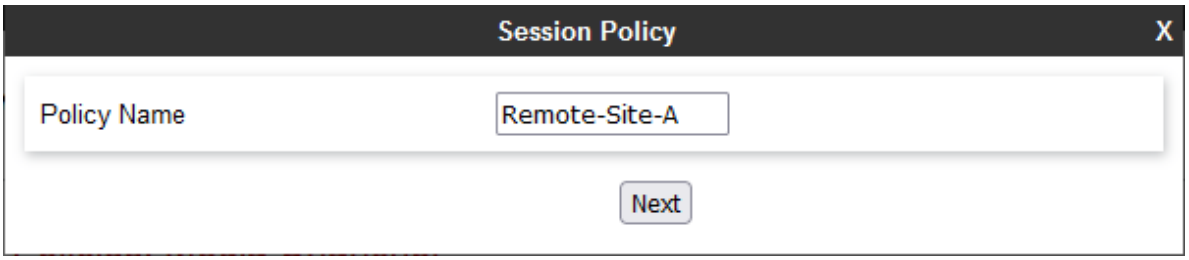
A session flow defines address ranges between which the ASBCE should apply a session policy. For a remote sub-net, the address ranges on both sides are the same.

Before you begin

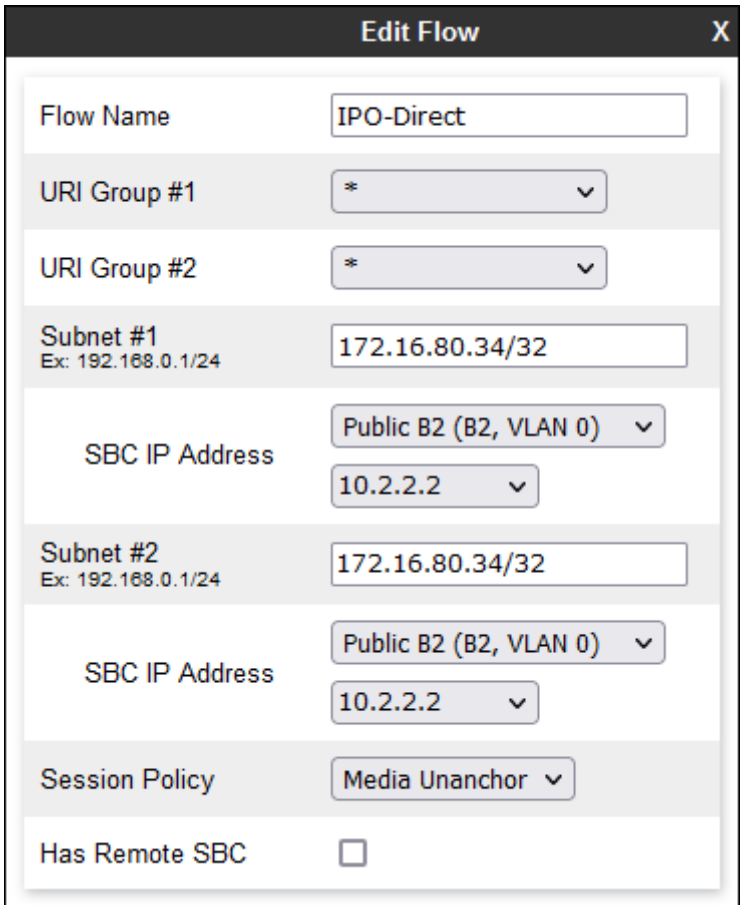
- Creating a session policy for a remote site on page 64.

Procedure

1. Select **Network & Flows** > **Session Flows**.
2. Click **Add**.
3. Enter a name. You can then use this to select the policy in other menus.



4. Click **Next**.



5. For **Subnet#1** set the IP address range used by remote extensions at the remote site. Set the **SBC IP Address** to the external interface of the ASBCE.
6. Set the same values for **Subnet#2**.
7. For the **Session Policy**, select the session policy that you created.
8. Click **Finish**.

Related links

Unanchoring call media from the ASBCE on page 64

Chapter 6: Supporting Avaya Workplace Client as a remote extension

This section provides notes regarding Avaya Workplace Client operation when used as a remote SIP extension for IP Office.

Related links

[Avaya Workplace Client SIP registration](#) on page 68
[Checking the remote settings](#) on page 69

Avaya Workplace Client SIP registration

1. Users can use the following methods to register their Avaya Workplace Client when it starts:
   - **Direct registration:**

     The user enters the IP Office address in the form `https://<IPOffice_FQDN>/46xxsettings.txt` when `://<IPOffice_FQDN>/` is the SIP registrar FQDN configured on the IP Office.

     - For remote extensions, public DNS resolves the FQDN to the public IP address of the customer's network firewall.
     - For IPv6, the user must use `https://<SBC_FQDN>/46xxsettings.txt` where <SBC_FQDN> is the FQDN of the ASBCE.
   - **Email-based address registration:**

     The user enters their email address. The client contacts Avaya cloud services where the profile configured for the customer's email domain provides the FQDN address of the IP Office system.

     - This method of registration is not supported for IPV6 remote extensions.
   - **SSO Login**

     This login method uses the same Avaya cloud services profile information as used by email-based registration above.

     - This method of registration is not supported for IPV6 remote extensions.

2. Having received a `46xxsettings.txt` file from the IP Office, the Avaya Workplace Client sends a DNS query for the IP address of the FQDN given to it in the **SIP_CONTROLLER_LIST** in the `46xxsettings.txt` file.
   - For remote extensions, the values used in the auto-generated `46xxsettings.txt` file are set by the **System** > **LAN1** > **Network Topology** > **SBC** settings in the IP Office configuration.
3. The client then attempts to register as a SIP extension using the IP address returned by the DNS server. For a remote extension, that is the customer's public IP address for their network firewall or ASBCE.

Related links

Supporting Avaya Workplace Client as a remote extension on page 68

Checking the remote settings

Using a remote PC, you can see and check the settings given to remote extensions.

Procedure

1. Use **nslookup** to verify that DNS resolves the FQDN for the IP Office to the correct IP addresses.

```
C:\ nslookup ipo.example.com
Server:  Unknown
Address: 203.0.113.30
```

2. Using a browser, request the `46xxsettings.txt` file from the IP Office. For example, enter `ipo.example.com/46xxsettings.txt`.
3. Check the port range shown. Avaya Workplace Client can use RTP/RTCP ports in the range `40750 to 50750`.

```
# SIPXAUTOGENERATEDSETTINGS
IF $SIG_IN_USE SEQ H323 GOTO 96X1AUTOGENERATEDSETTINGS
SET RTP_PORT_LOW 40750
SET RTP_PORT_RANGE 10002
SET TLSSRVRID 1
```

4. Other settings show the values used by the Avaya Workplace Client to connect to IP Office services:

```
# K1EXAUTOGENERATEDSETTINGS
SET ENABLE_AVAYA_CLOUD_ACCOUNTS 1
SET SIP_CONTROLLER_LIST ipo.example.com:5061;transport=tls
SET CONFERENCE_FACTORY_URI "ConfServer@ipo.example.com"
SET PSTN_VM_NUM "VM.user@ipo.example.com"
SET SETTINGS_FILE URL "https://ipo.example.com:411/46xxsettings.txt"
SET FQDN IP MAP "ipo.example.com=10.1.1.17"
```

5. For contacts and presence services, check if the `IPO_PRESENCE_ENABLED` and `IPO_CONTACTS_ENABLED` values are set to `1`.

```
# SETTINGSK1EX
SET SSOENABLED 0
SET EWSSSO 0
SET SIPREGPROXYPOLICY "alternate"
SET IPO_PRESENCE_ENABLED 1
SET IPO_CONTACTS_ENABLED 1
SET DND_SAC_LINK 1
SET POUND_KEY_AS_CALL_TRIGGER 0
```

Related links

Supporting Avaya Workplace Client as a remote extension on page 68

Chapter 7: Checking remote extension status in the ASBCE

The ASBCE provides a set of menus that display the status of connections and attempts to create connections.

Related links

Viewing ASBCE SIP statistics on page 71
Viewing ASBCE user statistics on page 72
Viewing ASBCE incidents on page 73

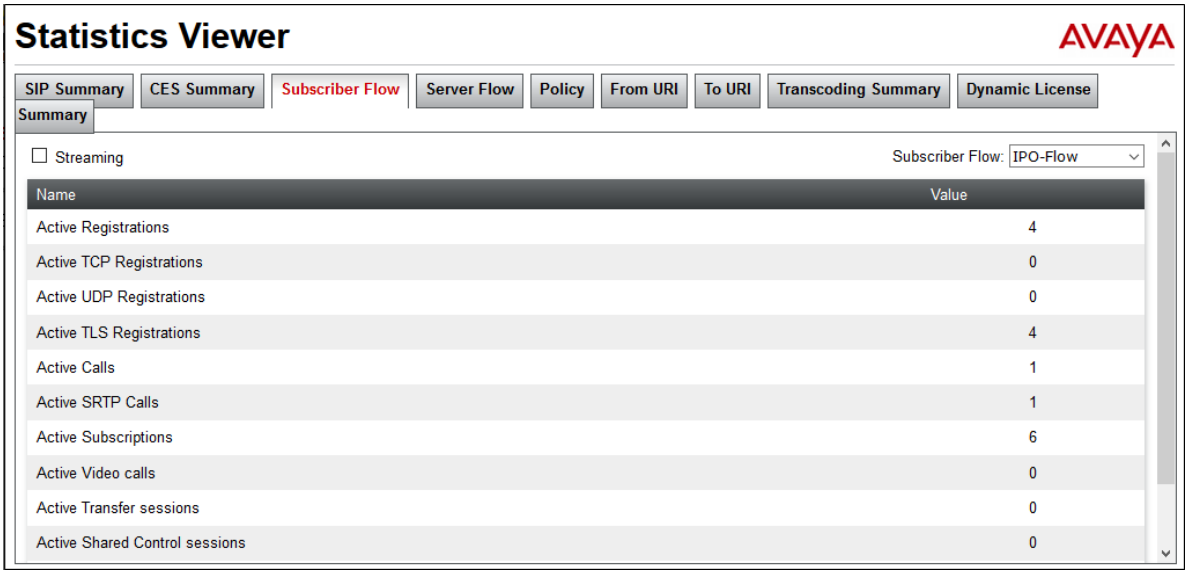
Viewing ASBCE SIP statistics

The **Statistics Viewer** can show details about the number of remote extension connections and calls.

Procedure

1. Select **Status** > **SIP Statistics**
2. Select **Subscriber Flow** and in the drop-down select the flow created for remote extensions.

3. The viewer displays details such as the number of registrations, number of calls, and so on.



Related links

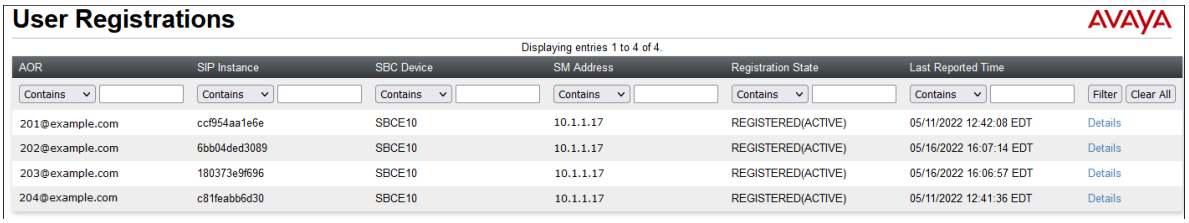
Checking remote extension status in the ASBCE on page 71

Viewing ASBCE user statistics

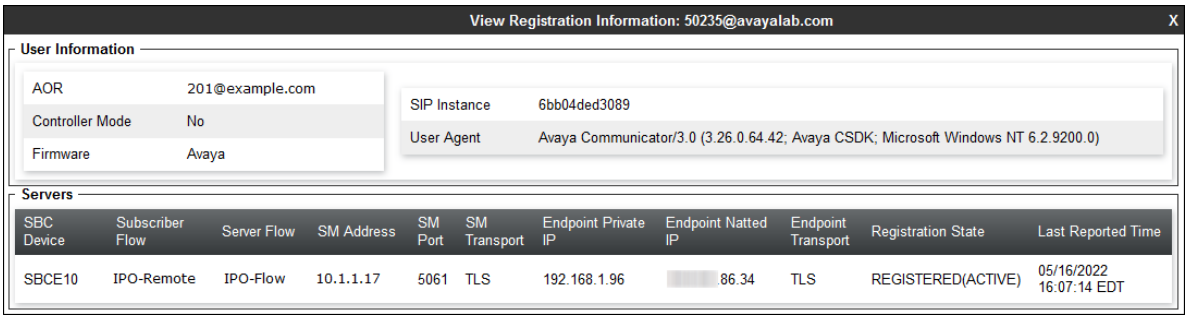
The **Statistics Viewer** can show details of individual remote extensions.

Procedure

1. Select **Status** > **User Registrations**
2. The viewer displays details of SIP clients registered through the ASBCE.



3. To display additional information for a particular user, click **Details**.



Related links

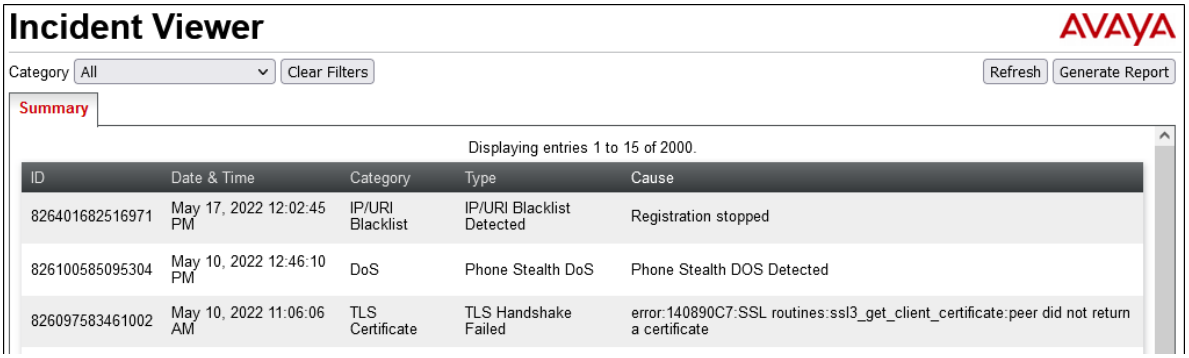
Checking remote extension status in the ASBCE on page 71

Viewing ASBCE incidents

The ASBCE can display details of issues such as such as certificate errors and registration problems. If remote extensions are experiencing issues in connecting to the IP Office, this may display the reason if the issue in on the ASBCE.

Procedure

1. Select **Incidents**.
2. The viewer displays details of incidents.



Related links

Checking remote extension status in the ASBCE on page 71

Part 2: Supporting IPv6

Chapter 8: Supporting IPv6 remote extensions

For IP Office R11.1.3.1 and higher, the IP Office supports Avaya Workplace Client remote extensions on iOS and Android using IPv6. This is done using a IPv4/IPv6 dual-stack ASBCE.

- Use of a dual-stack ASBCE is not supported with an IP Office that has been configured with its own IPv6 address.

Related links

Remote extension IPv6 support on page 75
IPv6 Remote extension schematic on page 76
IPv6 Remote extension limitations on page 77
DNS configuration for IPv6 remote extension support on page 77
Certificate configuration for IPv6 remote extension support on page 77
Avaya cloud services configuration for IPv6 remote extension support on page 78
Configuration checklist for IPv6 remote extensions on page 78
Configuration checklist for combined IPv4 and IPv6 remote extensions on page 79

Remote extension IPv6 support

For IP Office R11.1.3.1 and higher, remote mobile Avaya Workplace Client can use IPv6.

- You can configure the IP Office to provide the remote mobile Avaya Workplace Client with the ASBCE FQDN in the auto-generated `46xxsettings.txt` file.
- The connection requires an ASBCE R10.1.2 installed in a Dual-Stack installation. The ASBCE does the routing between the IPv6 clients and the IPv4 IP Office.
  - Use of a dual-stack ASBCE is not supported with an IP Office that has been configured with its own IPv6 address.
- Avaya Workplace Client:
  - iOS: Avaya Workplace Client R3.35 and higher.
  - Android: Avaya Workplace Client R3.35.1 and higher.
  - iPad and Vantage devices are not included in IPv6 support.

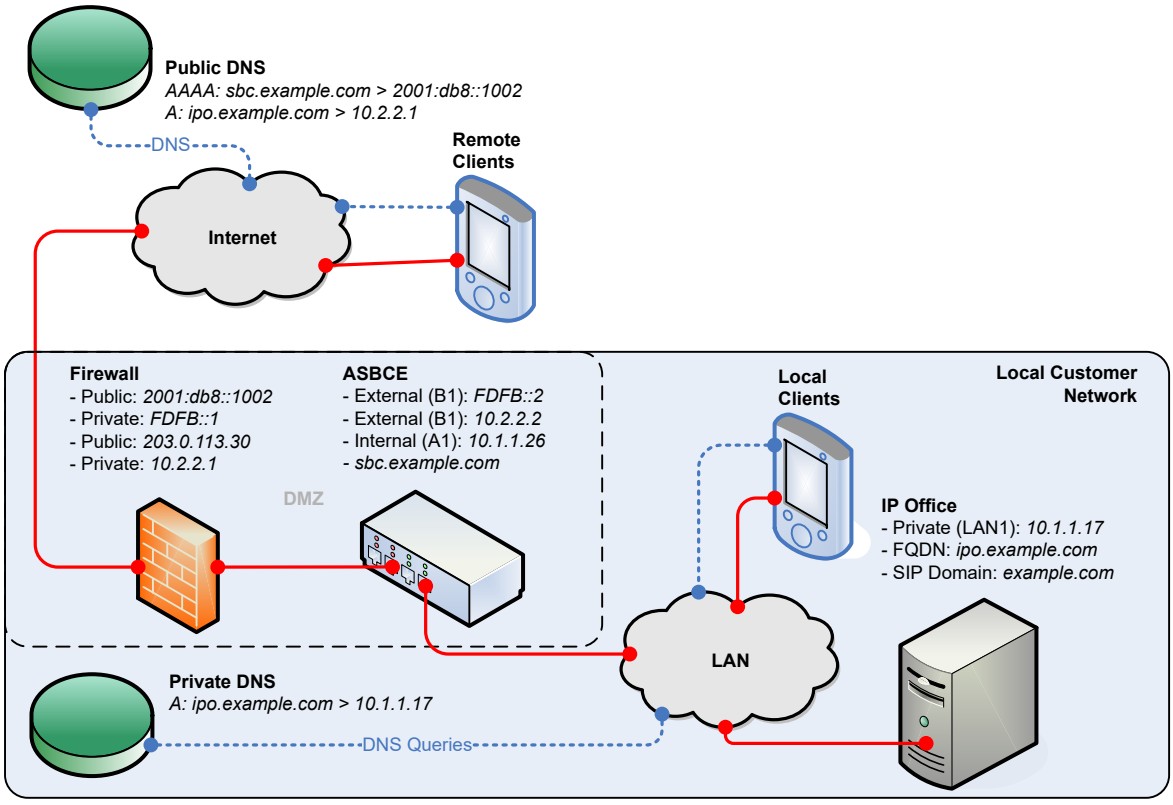
- SIP phones and clients on the customer's private network still use IPv4 to connect direct to the IP Office.
- If the network to which the Avaya Workplace Client is connected supports both IPv4 and IPv6, the Avaya Workplace Client defaults to IPv4.

Related links

Supporting IPv6 remote extensions on page 75

IPv6 Remote extension schematic

The following schematic is an example for supporting IPv6 remote extensions.



- The IP Office provides the remote extensions with the ASBCE FQDN.
- The public DNS resolves the ASBCE FQDN to the public IPv6 address of the customer firewall.
- The firewall forwards the ports used by the remote extensions to the external interface of the ASBCE.
- The dual-stack ASBCE handles routing between IPv6 and IPv4 addresses.
- For internal extensions, the private DNS resolves the IP Office FQDN to the IP Office system's IPv4 address.

Related links

Supporting IPv6 remote extensions on page 75

IPv6 Remote extension limitations

- Whilst firmware exists for J100 Series phone IPv6 operation, they must use IPv4 for remote extension connection to IP Office.
- Avaya cloud services does not support IPv6. Therefore, an Avaya Workplace Client using IPv6 does not support features provided by Avaya cloud services. For example:
  - No client registration using email or SSO login.
  - No instant messaging if the IP Office is configured to use Avaya cloud services as its messaging server.
- If the network to which the Avaya Workplace Client is connected supports both IPv4 and IPv6, the Avaya Workplace Client defaults to IPv4.

Related links

Supporting IPv6 remote extensions on page 75

DNS configuration for IPv6 remote extension support

To support IPv6, the DNS must resolve the ASBCE FQDN in addition to the IP Office FQDN:

- The public DNS for the IP Office FQDN must still resolve to an IPv4 address.
- The public DNS must also resolved the ASBCE FQDN to an IPv6 address. To do this, the customer must add `AAAA` records to their public DNS service.
- Local extensions continue to connect directly to the IP Office using IPv4 addresses. This is resolved by the customer's private DNS.

Related links

Supporting IPv6 remote extensions on page 75

Certificate configuration for IPv6 remote extension support

When supporting IPv6 remote extensions, in addition to the IP Office FQDN and IPv4 address, the ASBCE identity certificate must include the ASBCE FQDN and IPv6 address.

- The ASBCE FQDN can be added as part of the certificate common name (CN) or the subject alternative name (SAN).

- The IPv6 address must be added to the SAN.

Related links

Supporting IPv6 remote extensions on page 75

Avaya cloud services configuration for IPv6 remote extension support

Avaya cloud services does not support IPv6. Therefore, an Avaya Workplace Client using IPv6 does not support features provided by Avaya cloud services. For example:

- No client registration using email or SSO login.
- No instant messaging if the IP Office is configured to use Avaya cloud services as its messaging server.

Blank log in page

If you do not disable SSO support, when logging in IPv6 client users see a blank page. To log in, they must close the blank page and then log in directly using the IP Office `46xxsettings.txt` file address.

- If you want IPv4 client users to still be able to use SSO, you need to instruct the IPv6 remote extension users to close the blank page and login using the IP Office `46xxsettings.txt` file address.
- Otherwise, to prevent the blank page launching when user starts Avaya Workplace Client, you need to add a `46xxspecials.txt` file with the setting `SET SIPSSO 0` to the IP Office. Note, this will affect all Avaya Workplace Client users.

```
...
SETTINGSEQNX
SET SIPSSO 0
GOTO GENERALSPECIALS
```

Related links

Supporting IPv6 remote extensions on page 75

Configuration checklist for IPv6 remote extensions

If you are only supporting IPv6 remote extensions, follow the same configuration process as for IPv4, but replacing the external IPv4 addresses with IPv6 addresses where applicable. See ASBCE Configuration for remote SIP extensions on page 26.

#	Action	Link/Notes	✔
1.	Configure public DNS support for IPv6	DNS must resolve the ASBCE FQDN to the IPv6 address for traffic to the ASBCE. See DNS configuration for IPv6 remote extension support on page 77.	
2.	Include the ASBCE FQDN and IPv6 address in the ASBCE identity certificate.	See Certificate configuration for IPv6 remote extension support on page 77.	
3.	Disable Avaya cloud services support.	See Avaya cloud services configuration for IPv6 remote extension support on page 78.	
4.	Set the public IPv6 address for the IP Office	You need to give the remote extensions the IPv6 address to use for SIP registration and calls. See Setting the ASBCE details passed to remote extensions by the IP Office on page 14.	
5.	Configure the ASBCE call flow	Follow the same ASBCE configuration process used for IPv4 but using IPv6 addresses where appropriate. See ASBCE configuration checklist on page 29.	

Related links

Supporting IPv6 remote extensions on page 75

Configuration checklist for combined IPv4 and IPv6 remote extensions

This checklist assumes that you have completed ASBCE configuration to support IPv4 remote extensions. See ASBCE configuration checklist on page 29. The notes indicate where the ASBCE requires additional configuration to support both IPv4 and IPv6 remote extensions.

#	Action	Link/Notes	✔
1.	Configure public DNS support for IPv6	DNS must resolve the ASBCE FQDN to the IPv6 address for traffic to the ASBCE. See DNS configuration for IPv6 remote extension support on page 77.	
2.	Include the ASBCE FQDN and IPv6 address in the ASBCE identity certificate.	The ASBCE identity must include the IP Office FQDN and IPv4 address plus the ASBCE FQDN and IPv6 address. See Avaya cloud services configuration for IPv6 remote extension support on page 78.	

Table continues…

#	Action	Link/Notes	✔
3.	Disable Avaya Spaces support.	Avaya cloud services is not supported with IPv6. See Avaya cloud services configuration for IPv6 remote extension support on page 78.	
4.	Set the public IPv6 address for the IP Office	You need to give the remote extensions the IPv6 address to use for SIP registration and calls. See Setting the ASBCE details passed to remote extensions by the IP Office on page 14.	
5.	Configure firewall port forwarding	Add a new entry, like the IPv4 entry, but using the IPv6 addresses where applicable. See Firewall configuration on page 31.	
6.	Configure the external ASBCE network interface	Add a new entry for the external interface but using the IPv6 addresses. See Configure the external ASBCE interface on page 32.	
7.	Configure the internal ASBCE network interface	Use the existing IPv4 entry. See Configure the internal ASBCE interface on page 33.	
8.	Create a TLS client profile	Use the existing IPv4 entry. See Creating a TLS client profile on page 35.	
9.	Create a TLS server profile	Use the existing IPv4 entry. See Creating a TLS server profile on page 36.	
10.	Create an internal SIP media interface	Use the existing IPv4 entry. See Creating an internal media interface on page 38.	
11.	Create an external SIP media interface	Add a new entry, like the IPv4 entry, but using the IPv6 addresses where applicable. See Creating an external media interface on page 39.	
12.	Create an internal SIP call signaling interface	Use the existing IPv4 entry. See Creating an internal signaling interface on page 40.	
13.	Create an external SIP call signaling interface	Add a new entry, like the IPv4 entry, but using the IPv6 addresses where applicable. See Creating the external signaling interface on page 41.	
14.	Create a server profile	Use the existing IPv4 entry. See Creating a ASBCE server profile for the IP Office on page 42.	

Table continues…

#	Action	Link/Notes	✔
15.	Create server routing	Use the existing IPv4 entry. See Creating a server routing profile on page 44.	
16.	Setup topology hiding	Use the existing IPv4 entry. See Creating an ASBCE topology hiding policy on page 46.	
17.	Create an IP/URL blocklist.	Use the existing IPv4 entry. See Creating an IP/URI blocklist on page 47.	
18.	Create an application rule	Use the existing IPv4 entry. See Creating an application rule on page 48.	
19.	Create a media rule	Use the existing IPv4 entry. • Ensure the **Advanced Options** > **ANAT Enabled** is not selected. See Creating a media rule on page 49.	
20.	Create an endpoint policy	Use the existing IPv4 entry. See Creating an endpoint policy group on page 52.	
21.	Add a user agents profile	Use the existing IPv4 entry. See Configuring a user agents profile on page 53.	
22.	Create a subscriber flow	Add a new entry, like the IPv4 entry: • Set the media and signaling interfaces to use the external IPv6 interfaces. See Creating the subscriber flow on page 54.	
23.	Create a server flow	Add a new entry, like the IPv4 entry: • Set the IPv6 external signaling interface as the **Received Interface**. See Creating a server flow on page 57.	
24.	Add a reverse proxy for Avaya Workplace Client	Add new proxies using the external B1 interface configured for IPv6 addresses. See Adding reverse proxies for file requests on page 59.	

Related links

Supporting IPv6 remote extensions on page 75

Part 3: Resilience

Chapter 9: ASBCE and IP Office resilience

IP Office supports a range of resiliency options, including resilience for SIP phones and SIP softphone applications. For more information, see the IP Office Resilience Overview manual.

This section of this document gives an overview of the additional configuration required to add resilience support to an existing configuration. The main additional steps are:

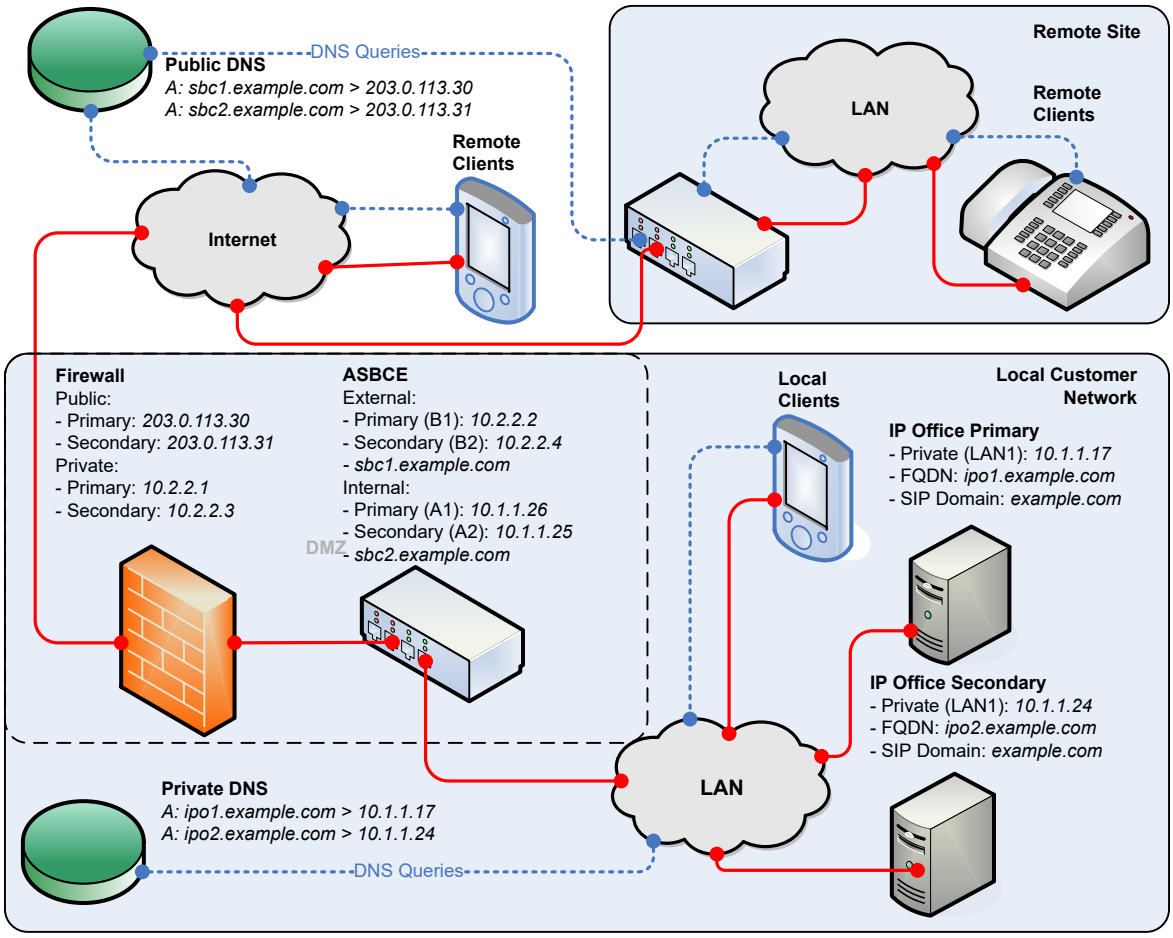
- The IP Office cannot use the remote extension IP address to match a location in the IP Office configuration. Therefore, to use location settings in resilience, you must configure the location in the extension configuration.

Related links

Example resilience schematic on page 83
Generating an identity certificate for the secondary IP Office on page 84
Installing the secondary IP Office identity certificate on page 85
Configuring the IP Office for remote extension resilience on page 86
Configuring the Avaya one-X Portal on page 86
Configuring the ASBCE for resilience on page 87
Configuring DNS for resilience on page 87

Example resilience schematic

The following is an example schematic for a resilient configuration.



For resilient support of remote extensions, the ASBCE uses 2 sets of public/private IP addresses:

- The ASBCE routes one set to the primary IP Office server and the other set to the secondary IP Office server.
- This logic is the same regardless of the ASBCE installation: Simplex, HA, two separate ASBCE servers or dual-stack.

Related links

ASBCE and IP Office resilience on page 83

Generating an identity certificate for the secondary IP Office

The secondary IP Office requires an identity certificate issued by the primary IP Office.

Procedure

1. Login to the IP Office Web Control menus by either:
   - From within IP Office Web Manager, select the primary server. Click on ☰ and select **Platform View**.
   - Browse to `https://<IP Office IP address>:7071` and log in.
2. Go to **Settings** tab and scroll down to **Certificates**.
3. Enter the following data:

Value	Description
Machine IP	Enter the IP address of the secondary server.
Password	Enter a password to encrypt the certificate and key.
Subject Name	Enter the FQDN of the secondary IP Office.
Subject Alternative Name(s)	List the FQDN of the secondary IP Office, the secondary XMPP domain, the SIP domain and the secondary IP Office internal and external IP addresses.

4. Click **Regenerate** and **Apply**.
5. In the pop-up window, click on the link to download the certificate.
6. Click **OK**.
7. Rename the downloaded file to `IPOSEC_ID.p12`.

Next steps

- Installing the secondary IP Office identity certificate on page 85.

Related links

ASBCE and IP Office resilience on page 83

Installing the secondary IP Office identity certificate

You need to add the identity certificate created for the secondary IP Office.

Before you begin

- Generating an identity certificate for the secondary IP Office on page 84.

Procedure

1. Log in to the system using IP Office Web Manager.
   - For an IP500 V2, enter the system address followed by `:8443/WebMgmtEE/WebManagerment.html`.
   - For a Linux-based server, enter the system address followed by `:7070/WebManagement/WebManagement.html`.

2. Go to **Security Manager** > **Certificates**.
3. Click on the icon next to the secondary server.
4. Click on **Set**.
5. Browse to and select the identity certificate file.
6. Enter the password.
7. Click **Upload**.

Related links

ASBCE and IP Office resilience on page 83

Configuring the IP Office for remote extension resilience

In addition to the standard configuration for resilience (see IP Office Resilience Overview), you must configure the secondary IP Office as follows:

- Set the SIP registrar settings, except **SIP Registrar FQDN**, to the same settings as used on the primary IP Office server. That includes matching the **SIP Domain Name**. See IP Office SIP VoIP Setup on page 12.
- Set the **SIP Registrar FQDN** to match the FQDN configured in DNS to route SIP traffic to the secondary IP Office server.
- Set the **SBC** settings to that the remote extensions must use to connect to the ASBCE configured to route SIP calls to the secondary ASBCE. See Setting the ASBCE details passed to remote extensions by the IP Office on page 14.

Related links

ASBCE and IP Office resilience on page 83

Configuring the Avaya one-X Portal

You must configure the Avaya one-X Portal service with the domain name of the secondary IP Office.

Procedure

1. Login to the Avaya one-X Portal administrator menus, either:
   - Within IP Office Manager, select **Applications** > **one-X Portal** > .
   - Browse to `https://<portal IP address>:9443/onexportal-admin.html` and login as the Administrator.

2. Select **Configuration** > **Host Domain Name**.
   a. Set the **Secondary Host Domain Name** to the FQDN of the secondary Avaya one-X Portal.
   b. Click **Save**.
3. Click on the icon at the top of the menus to restart the Avaya one-X Portal.

Related links

ASBCE and IP Office resilience on page 83

Configuring the ASBCE for resilience

The ASBCE configuration steps are like those for single server setup. The requirement is to create additional entries but using the public and private IP addresses of the secondary IP Office server.

Related links

ASBCE and IP Office resilience on page 83

Configuring DNS for resilience

The DNS server configuration is like that for a single IP Office server. DNS requires additional records the FQDN of the secondary IP Office and ASBCE servers.

Related links

ASBCE and IP Office resilience on page 83

Chapter 10: Checking the resilience configuration

You can use the following methods to check the resilience information that the IP Office provides to the remote extensions.

Related links

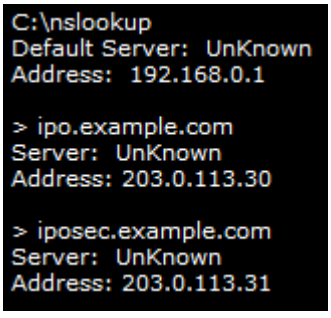
[Checking the resilience DNS routing](#) on page 88
[Viewing the ASBCE trace](#) on page 89
[Checking the Avaya one-X Portal responses](#) on page 90

Checking the resilience DNS routing

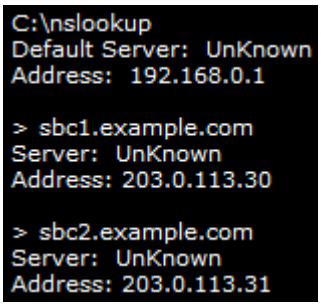
Using a remote PC, you can check that DNS is correctly resolving requests.

Procedure

1. Use the `nslookup` command to verify that DNS resolves the FQDNs of the primary IP Office and the secondary IP Office to the correct IP addresses. For example:



2. Use the `nslookup` command to verify that DNS resolves the FQDNs of the primary and secondary ASBCE.



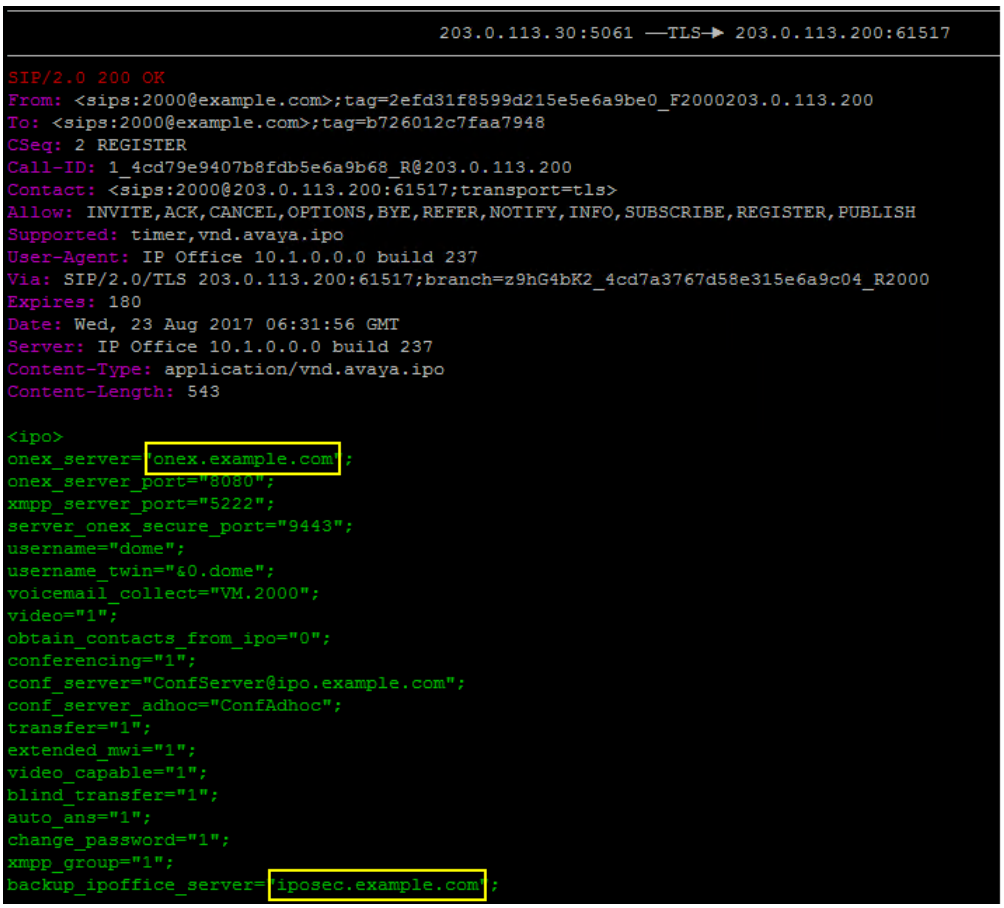
Related links

Checking the resilience configuration on page 88

Viewing the ASBCE trace

The following is an example traceSBC session for the registration of a client. It shows the SIP *200 OK* response sent to the client.

The response contains a number of configuration settings. For remote extensions, the response will include the SBC FQDN that you have configured on the secondary IP Office.



- **During normal operation:**

  The *200 OK* response shows the *onex_server* and *backup_ipoffice_server* values set with the primary and secondary servers respectively.

- **During resilience:**

  The *onex_server* contains the FQDN of secondary portal and *backup_ipoffice_server* is *0.0.0.0*.

Related links

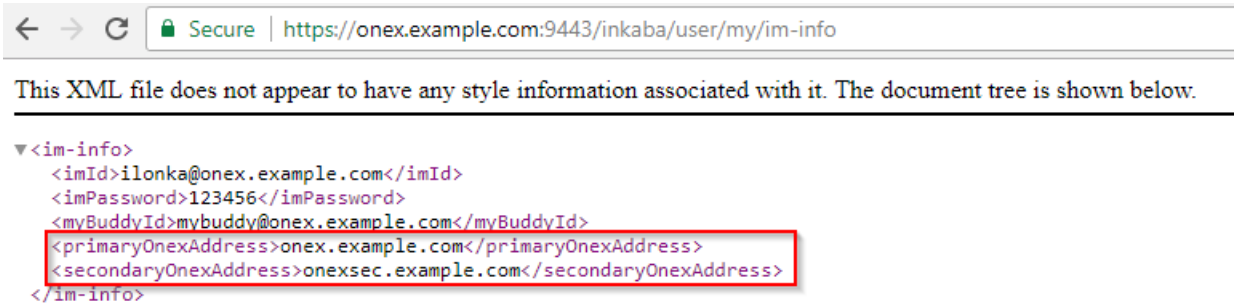
Checking the resilience configuration on page 88

Checking the Avaya one-X Portal responses

When a client requests XMPP information from the primary Avaya one-X Portal service, the response includes the primary and secondary XMPP server addresses.

Procedure

1. During normal operation, using a browser, enter `https://<FQDN>:9443/inkaba/user/my/im-info` where *<FQDN>* is the FQDN of the primary Avaya one-X Portal service.



2. Check that the response includes the FQDNs of both the primary and secondary Avaya one-X Portal services.

   a.

   b. The response should include the FQDN of the primary IP Office server.

3. Using a browser, enter `https://<FQDN>:9443/inkaba/user/my/sip-info` where *<FQDN>* is the FQDN of the primary Avaya one-X Portal service.

4. If you repeat the steps during resilience, use the FQDN of the secondary Avaya one-X Portal server.

   - The `im-info` information will be the same.
   - The `sip-info` information will show the FQDN of the secondary IP Office server.

Related links

[Checking the resilience configuration](#) on page 88

Part 4: Additional information

Chapter 11: Additional Help and Documentation

The following pages provide sources for additional help.

Related links

Additional Manuals and User Guides on page 93
Getting Help on page 93
Finding an Avaya Business Partner on page 94
Additional IP Office resources on page 94
Training on page 95

Additional Manuals and User Guides

The Avaya Documentation Center website contains user guides and manuals for Avaya products including IP Office.

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

For other types of documents and other resources, visit the various Avaya websites (see Additional IP Office resources on page 94).

Related links

Additional Help and Documentation on page 93

Getting Help

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

If your IP Office system currently does not have an Avaya business partner providing support and maintenance for it, you can use the Avaya Partner Locator tool to find a business partner. See Finding an Avaya Business Partner on page 94.

Related links

Additional Help and Documentation on page 93

Finding an Avaya Business Partner

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

Procedure

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

Related links

Additional Help and Documentation on page 93

Additional IP Office resources

In addition to the documentation website (see Additional Manuals and User Guides on page 93), there are a range of website that provide information about Avaya products and services including IP Office.

- Avaya Website (https://www.avaya.com)

  This is the official Avaya website. The front page also provides access to individual Avaya websites for different regions and countries.
- **Avaya Sales & Partner Portal** *(https://sales.avaya.com)*

  This is the official website for all Avaya business partners. The site requires registration for a username and password. Once accessed, you can customize the portal to show specific products and information type that you want to see.
- **Avaya Support** *(https://support.avaya.com)*

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

  - **Avaya Support Forums** *(https://support.avaya.com/forums/index.php)*

    This site provides forums for discussing product issues.

- **International Avaya User Group** *(*https://www.iuag.org*)*

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

- **Avaya Learning** *(*https://www.avaya-learning.com/*)*

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

Related links

Additional Help and Documentation on page 93

Training

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

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

Credential maps are available on the Avaya Learning website.

Related links

Additional Help and Documentation on page 93

Chapter 12: Glossary

The following are definitions for terms used within this document.

Related links

A record on page 96
AAAA record on page 96
ASBCE on page 97
DNS on page 97
Domain name on page 97
FQDN on page 97
Management IP on page 98
SBC on page 98
Split DNS on page 98
SRV record on page 98
XMPP on page 99

A record

"Address Record". A basic DNS record that maps a domain name or FQDN to an IPv4 address. For IPv6 addresses, DNS uses `AAAA` records.

Related links

Glossary on page 96

AAAA record

Also called a "Quad-A record". DNS services use `AAAA` records to map a domain name or FQDN to an IPv6 address. These are like the `A` records used for IPv4 addresses.

Related links

Glossary on page 96

ASBCE

"Avaya Session Border Controller for Enterprise". The Avaya platform for providing SBC services for a customer network.

Related links

Glossary on page 96

DNS

"Domain Name Server". A server or service that provides IP address information in response to a domain name or FQDN query. For example, when an application tries to connect to the `www.example.com`, it first contacts the DNS server on its network. The DNS server resolves the text address `www.example.com` to the required numeric IP address. The process involves the DNS server checking DNS records it holds, and if necessary, those held by other DNS servers in the network or on the internet.

Related links

Glossary on page 96

Domain name

The text address used to identify a network of devices. A DNS server translates the domain name and fully-qualified domain names to specific IP addresses.

Related links

Glossary on page 96

FQDN

"Fully Qualified Domain Name". The full text address assigned to a specific server, service or client within a domain.

Related links

Glossary on page 96

Management IP

The IP address used for administrator access to the ASBCE server. This is a different address from those used for the internal and external network traffic interfaces provided by the ASBCE.

Related links

Glossary on page 96

SBC

“Session Border Controller”. An SBC is a device that controls SIP call signaling and media between two networks.

Related links

Glossary on page 96

Split DNS

Using FQDNs and DNS servers to route traffic within and between networks simplifies network maintenance. However, issues can arise when you use FQDN routing for both internal and external network traffic. It can cause the network to route internal traffic to internal services externally. That exposes internal services and addresses that must remain hidden.

Split DNS uses a public DNS service for external traffic to the customer network and a private DNS service for internal traffic within the customer network.

Customers can configure split DNS using a single DNS server on the edge of the customer network or separate public and private DNS servers.

Related links

Glossary on page 96

SRV record

“Service Record”. For domains supporting multiple services, for example `www.example.com` or `sip.example.com`, DNS `A` records may not be sufficient for the routing required. DNS `SRV` records provide mapping for specific services running within a domain.

Related links

Glossary on page 96

XMPP

"Extensible Messaging and Presence Protocol". XMPP is an open standards protocol that allow devices to exchange instant message, presence and contacts information.

Related links

Glossary on page 96

Index

A

Administrator 93
alg 31
APIs 94
Application Notes 94
application rule 48
    endpoint policy 52
ASBCE
    identity certificate 21
audio 48
Avaya cloud services
    IPv6 78

B

blank page 78
block timer 47
blocklist 47, 54, 59
business partner locator 94

C

call server 42
certificate 35, 36
    IPv6 77
certificate authorities 35
ciphers 35, 36
clone 29
cloud services
    IPv6 78
codec 49
concurrent sessions 48
courses 94

D

default gateway 32, 33
direct media 64
DNS
    IPv6 77
domain name 12

E

endpoint
    sessions per 48
endpoint policy group 52

F

failed attempts 47
file proxy 59
file server 16
firewall 31
forums 94
fqdn 12
from 46

G

gateway 32, 33
glossary 96

H

headers 46
Help 93

I

identity certificate
    add to ASBCE 24
    generate 21, 22
    IPv6 77
interface
    external 32
    internal 33
ip address
    whitelist 17
IP address 32, 33
IP/URL blocklist 47, 54, 59
IPv6 75
    certificate 77
    cloud services 78
    DNS 77
    schematic 76

L

layer 3 nat 31
layer 4 protocol 12
licenses 12

M

Manuals 93
mask 32, 33
maximum sessions 48
media interface 39
media interfaces 38
media rule 49
    endpoint policy 52

N

nat 31
networks 32, 33
next hop 44
nouser 16

O

overwrite 46

P

password failed attempts 47
peer ca 35
peer verification 35, 36
policy group 52
port number range 12
preferred phone ports 59
priority 44
private key
    extract 23
proxy 59
public IP 32, 33
Public IP Address 77

Q

QOS 49
Quick Reference Guides 93

R

record-route 46
refer-to 46
referred-by 46
registration interval 16
regular expression 53
replace 46
request-line 46
Reseller 93
reverse proxy 59
    blocklist 47
root certificate
    download 19
    upload 20
rtp port range 12

S

sales 94
schematic
    IPv6 76
    sip extensions 8
SDKs 94
sdp 46
security 10
server flow 57
    endpoint policy 52
server profile 42
server routing 44
server type 42
session flow 66
session policy 64
sessions
    maximum 48
SET SIPSSO 78
signaling interface 40
    external 41
sip alg 31
sip extensions
    schematic 8
sip headers 46
sip registrar 12
SIPSSO 78
source numbers 16
SRTP 49
status 71
subnet mask 32, 33
subscriber flow 54
    blocklist 47
    endpoint policy 52
subscriptions 12
support 94
System Administrator 93

T

Technical Bulletins 94
tls client 35, 42
tls port 41
tls server 36
tls version 35, 36
to 46
topology hiding 46
training 94, 95

U

UA string 53
unanchor 64
use preferred phone ports 59
user agent 53, 54
User Guides 93
username failed attempts 47

V

verification depth 35
via 46
video 48

W

weblm 12
websites 94
weight 44
whitelist 17