Deploying MS Teams Direct Routing with IP Office

Release 11.1 FP2
Issue 4
April 2024

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO 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.

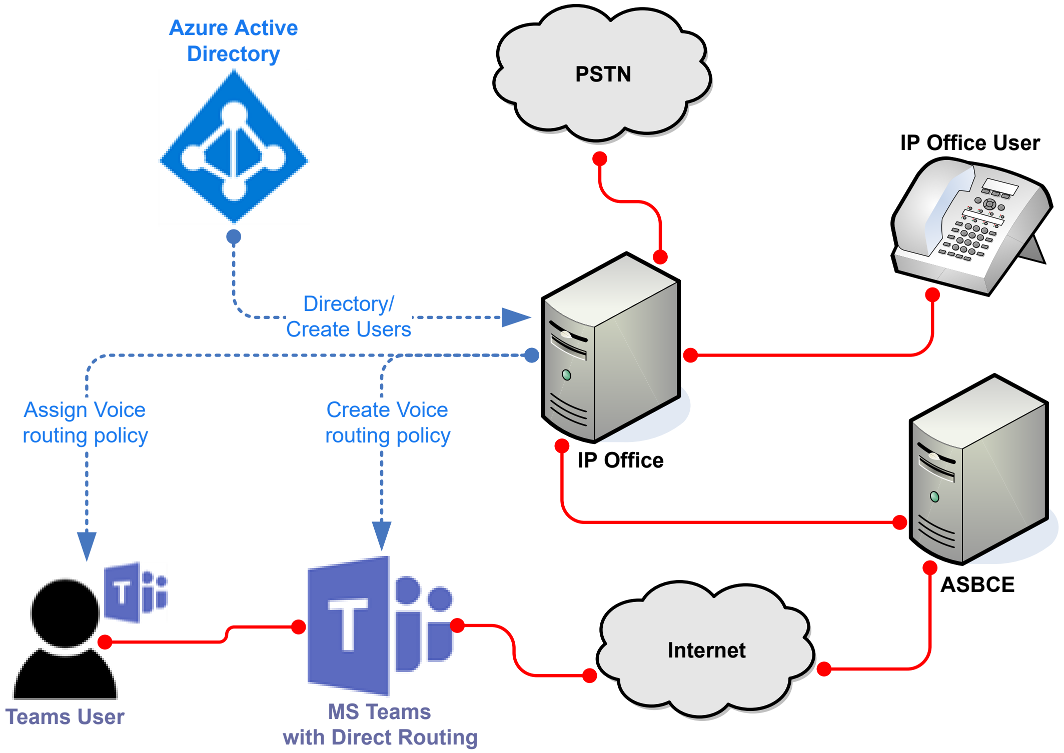
Contents

Part 1: MS Teams Direct Routing with IP Office

Chapter 1: IP Office and MS Teams

These notes cover the integration of MS Teams direct routing with IP Office systems.

IP Office supports this with IP Office R11.1 FP2 and higher.



Related links

- [IP Office and MS Teams Components] on page 9
- [MS Teams Call Routing Options] on page 10
- [User Types] on page 11
- [Requirements] on page 12
- [Known Call Limitations] on page 13

IP Office and MS Teams Components

Key components for MS Teams and IP Office integration are:

Component	Description
MS Teams	MS Teams licensed through Microsoft. IP Office does not support integration with the free version of MS Teams.
IP Office	IP Office R11.1 FP2 and higher.
Direct Routing	MS Teams Direct routing using an ASBCE R10.1 plus Hotfix 1. • Scenarios covered include calls by MS Teams only users, IP Office only users, and users who are simultaneous MS Teams+IP Office users. • Use these notes in conjunction with the Microsoft documentation. Refer to https://docs.microsoft.com/en-us/microsoftteams/direct-routing-landing-page.
Azure Active Directory Synchronization	MS Teams uses Azure Active Directory to store MS Teams user information. IP Office R11.1 FP2 supports integration with Azure Active Directory to perform a range of actions: • Automatically add Azure Active Directory user names and numbers to the IP Office system directory. • Automatically create, update and delete IP Office users matching users in the Azure Active Directory. • Automatically assign a voice routing policy to MS Teams users.
Direct Routing	Direct routing is an alternation method of integrating MS Teams and IP Office. For details, refer to the separate Deploying MS Teams Direct Routing with IP Office manual.

Related links

IP Office and MS Teams on page 9

MS Teams Call Routing Options

MS Teams users can make calls to normal PSTN telephone numbers using the following options. For more details, refer to https://docs.microsoft.com/en-us/microsoftteams/pstn-connectivity.

Method	Description
Microsoft Calling Plans	In this scenario, MS Teams routes PSTN calls over Microsoft's PSTN network. This uses Microsoft’s price plans for national and international calls.
Avaya Calling	In this scenario, the Avaya Calling plug-in links the MS Teams user's MS Teams and Avaya Workplace Client clients. This routes their PSTN calls through the IP Office. They can also call other IP Office users. For details, refer to the separate Deploying Avaya Calling for MS Teams with IP Office manual.
Direct Routing	In this scenario, MS Teams routes user PSTN calls through an ASBCE to the IP Office. They can also call other IP Office users.
Operator Connect	This option is like Direct Routing. However, all administration and services use the infrastructure of a PSTN provider who is part of the Microsoft Operator Connect program.

Related links

IP Office and MS Teams on page 9

User Types

This documentation refers to the following types of users:

User Type	Description
IP Office only user	This type of user: • Configured on the IP Office system with an IP Office extension number • Does not require any specific IP Office user profile to interact with MS Teams users. • Can see and call MS Teams users from the IP Office system directory.
MS Teams only user	This type of user: • Configured in MS Teams with a MS Teams telephone number and/or extension number. • Requires a MS Teams license (Microsoft 365 Business Voice without Calling Plan). • Does not need any IP Office license or subscription. • Can make and receive calls to and from IP Office extensions. • Cannot be part of IP Office features such as hunt groups, since they do not exist as a user/extension record in the IP Office configuration
MS Teams+IP Office user	This type of user: • Configured as a user in both MS Teams and IP Office. • Has the same extension number on MS Teams and IP Office. • Can also have a MS Teams telephone number. • Requires a MS Teams license (Microsoft 365 Business Voice without Calling Plan). • Requires an IP Office license or subscription for the following: - IP Office systems using PLDS licensing support MS Teams+IP Office users using the **Office Worker**, **Teleworker** and **Power User** profiles. - IP Office subscription mode systems support MS Teams+IP Office users using the **UC User** profile. • Incoming calls alert both their MS Teams client and IP Office extension. The user can use either for calls with other MS Teams or IP Office users. • You can include these users in other IP Office features such as hunt groups, park/page, and so on.

How are theses user types created?

In addition to manually creating the users, the creation of the different types of users can be partially automated using Azure Active Directory synchronization. This allows the IP Office to create and update users in its own configuration based on the Azure Active Directory user settings.

Within Azure Active Directory, you can define groups for different types of user. That allows you to configure IP Office synchronization rules for each group.

Related links

IP Office and MS Teams on page 9

Requirements

The following is a summary of the requirements for installation:

Area	Requirements
IP Office	• IP Office R11.1 FP2 running either subscription mode or IP Office Preferred edition. • System configured for Avaya Cloud synchronization.
ASBCE	• ASBCE R10.1 plus Hotfix 1 or higher. • `ipcs` and `root` passwords for administrator access. • Software for SSH and SFTP access.
Certificates	• Administrator rights to obtain the IP Office root certificate and to generate identity certificates for the same certificate authority (CA).
IP Office only users	• No special configuration requirements.
MS Teams only users	• MS Teams: MS Teams license including direct routing (Microsoft 365 Business Voice without Calling Plan).
MS Teams+IP Office users	• MS Teams: MS Teams license including direct routing (Microsoft 365 Business Voice without Calling Plan). • IP Office: IP Office User Profile/License: - Subscription mode systems: Supported by the UC User profile. - PLDS licensed systems: Supported by the Office Worker, Teleworker and Power User profiles.
MS Teams	• Single tenancy.
Domain	• Administrator rights to configure the customer's domain DNS or add files to the domains default website root.
Other requirements	• Administrator rights to the customer's tenancy through the Azure Active Directory and MS Teams admin portals.

Related links

IP Office and MS Teams on page 9

Known Call Limitations

The following are current known limitations for MS Teams integration with IP Office:

- **MS Teams does not propagate name updates:**

  In scenarios such as call transfers and forwards, the MS Teams user still sees the original call name. For example:

  - If MS Teams user Alice calls IP Office user Bob, and Bob then transfers the call to user Carol, Alice's display still shows the call as being with Bob.

- **MS Teams does not propagate hold indication:**

  With MS Teams, if MS Teams puts an IP Office user on hold, or vice versa, there is no indication that the call is on hold. However, the held user still hears hold music.

Related links

IP Office and MS Teams on page 9

Chapter 2: MS Teams Scenarios

The integration with MS Teams covered in this documentation covers the following scenarios:

Scenario	Description
Direct Routing	Direct routing allows MS Teams user to make and receive PSTN calls through an SBC connected to a SIP trunk provider. For IP Office, this uses an ASBCE R10.1 plus Hotfix 110.1 plus Hotfix 1.
Direct Routing with Azure Active Directory Synchronization	IP Office R11.1 FP2 and higher can connect to Azure Active Directory to obtain MS Teams user information. You can use this to update IP Office directory information and/or create IP Office users.

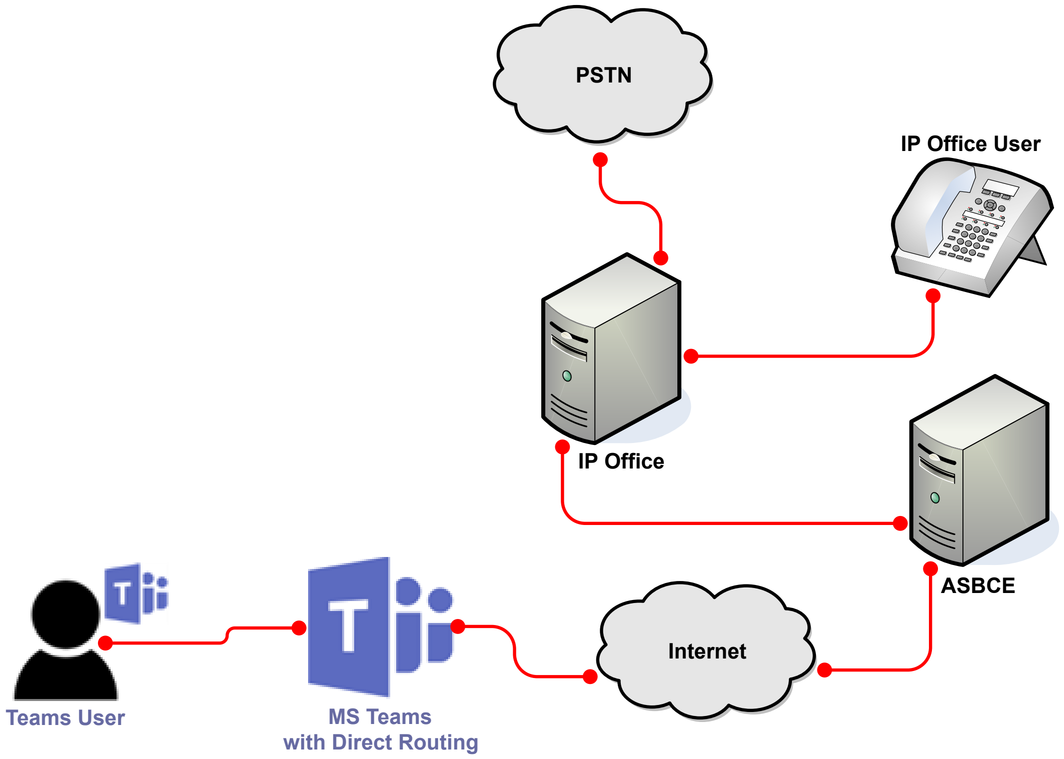
Related links

Integration with Direct Routing on page 14
Integration with Direct Routing and Azure Active Directory on page 15

Integration with Direct Routing

MS Teams direct routing uses a third-party SBC to route calls to and from MS Teams users. This replaces the need to use Microsoft calling plans.

For IP Office, direct routing requires ASBCE R10.1 plus Hotfix 1 or higher.

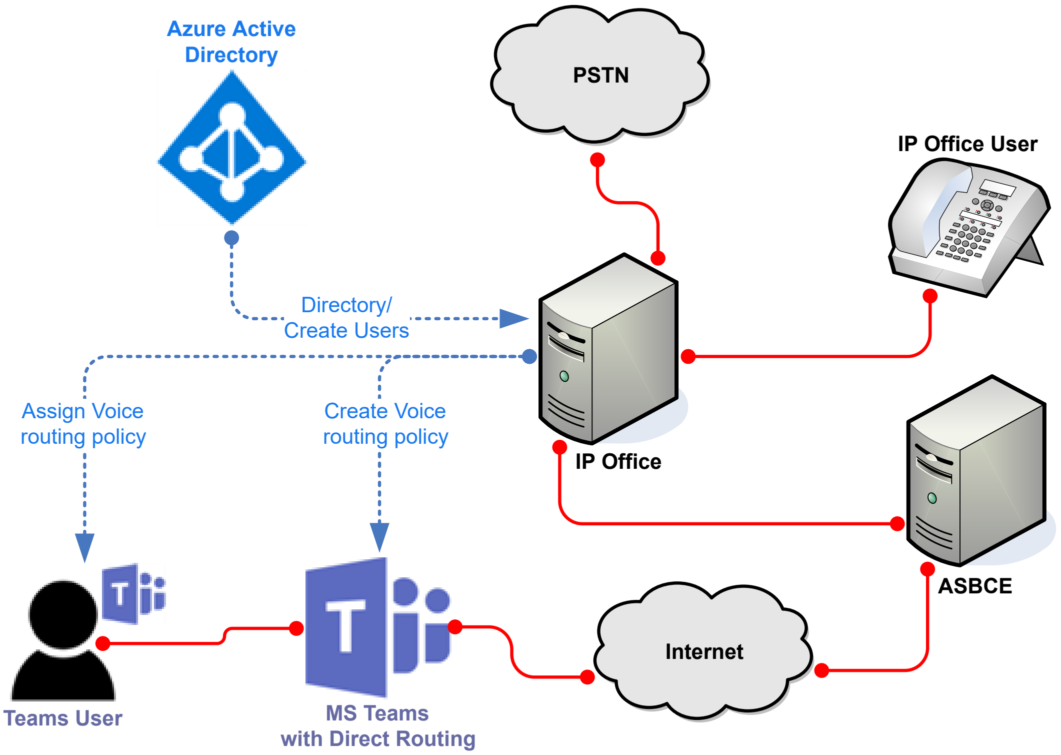


Related links

MS Teams Scenarios on page 14

Integration with Direct Routing and Azure Active Directory

This scenario builds on the previous direct routing integration by adding Azure Active Directory synchronization.



This allows the following:

- Automatically add MS Teams user contact details to the IP Office system directory.
- Create and maintain IP Office users from user records in Azure Active Directory. Those users can be ordinary IP Office users and/or MS Teams+IP Office users.
- Select and assign the voice routing policy to use to MS Teams users.

Related links

MS Teams Scenarios on page 14

Chapter 3: Telephone and Extension Numbers

Within MS Teams, a user can have a telephone number and/or extension number. MS Teams can use either to route calls to the user. For more information, refer to https://docs.microsoft.com/en-us/microsoftteams/manage-phone-numbers-landing-page.

Related links

Number Formats

It is important to look at the formats used to enter and display telephone numbers. MS Teams-IP Office integration involves different interfaces which differ in how they display the same number.

Interface		Telephone Number and Extension	Telephone Number Only	Extension Only
Azure AD Admin Portal		`+441632768402 x402`	`+441632768402`	`x402`
		`441632768402 x402`	`441632768402`	
Teams Admin Portal		`tel:441632768402;ext=402`	`tel:441632768402`	`402`
IP Office Admin Menu	**MS Teams URI**	`441632768000;ext=402`	`441632768402`	`+402`
	System Directory Number	`441632768402-402`	`441632768402`	`+402`
MS Teams Client		`(1632) 768 8402 extn 402`	`(1632) 768 8402`	`+402`

Table continues…

Interface	Telephone Number and Extension	Telephone Number Only	Extension Only
IP Office SIP URI[1]	`+441632768402;ext=402`	`+441632768402`	–

1. The IP Office also adds the required protocol prefix and domain/port suffix elements (for example `sip:+441632768402;ext=402@sip.pstnhub.microsoft.com:5061`).

Related links

Telephone and Extension Numbers on page 17

Telephone Numbers

This documentation assumes that incoming calls for all telephone numbers from the PSTN are route through the IP Office. It does not cover scenarios where the customer has telephone numbers routed directly to MS Teams through Microsoft calling plans.

- Note that the expected telephone number is a full number including international country code but no country specific international dialing prefix (except+ where indicated).
- If the customer has telephone numbers registered to Microsoft calling plans, those numbers must be migrated to one of the IP Office line providers.
- Microsoft recommend that customers configure phone numbers as full E.164 phone numbers with country code. MS Teams also supports phone numbers with extensions. MS Teams uses these match a user when the lookup against the telephone number returns more than one user.

Related links

Telephone and Extension Numbers on page 17

Extension Numbers

For scenarios that include MS Teams only users:

- The MS Teams only users' extension numbers must be unique from the IP Office extension numbers used by IP Office only and MS Teams+IP Office users.
- For ease of configuration and maintenance, use extension ranges for each that do not overlap.
- Due to the operation of MS Teams, the + indicator used for E.164 international numbers also appears on extension numbers in some interfaces.

Related links

Telephone and Extension Numbers on page 17

How MS Teams uses the telephone numbers

Where possible, Avaya recommends using the telephone number and extension number format. However, the values used depend on the scenario:

Common MS Teams Telephone Number	For scenarios where you need to use the same external PSTN number for all or several MS Teams users, you can combine the PSTN number and individual extension numbers. For example: • User A: *441632768000 x401* • User B: *441632768000 x402*
Individual MS Teams Telephone Numbers	For scenarios where you have an individual PSTN numbers for each user, you can configure the user with just that telephone number or with both their individual telephone number and an extension number. For example: • User A: *441632768401* or *441632768000 x401* • User B: *441632768402* or *441632768000 x402*
MS Teams Extension Number Only	For scenarios where you want uses to have just an extension number, you can omit the telephone number. For example: • User A: *x401* • User B: *x402*

Related links

Telephone and Extension Numbers on page 17

Routing IP Office Calls to the MS Teams Numbers

Once you have added the contact numbers for MS Teams users to the IP Office system directory, IP Office users can call MS Teams users using the directory. For incoming PSTN calls to the IP Office, you must add routing through incoming call routes.

You can add MS Teams numbers to the IP Office system directory either manually or using automatic directory synchronization.

Related links

Telephone and Extension Numbers on page 17

Chapter 4: Direct Routing Components

Direct routing configuration in MS Teams uses a range of components.

Related links

Dial Plans

Dial plans are sets of rules for how to translate any numbers dialed by MS Teams users. For more information, refer tohttps://docs.microsoft.com/en-us/microsoftteams/what-are-dial-plans.

- Each dial plan contains up to 50 dialing rules. MS Teams searches the rules for a match to the number dialed by the user.
- When a match occurs, the rule settings determine what changes MS Teams applies to the dialed number. MS Teams then uses the translated number for routing through the user's associated voice routing policy.

The following types of dial plan exist:

Dial Plan Type	Description
Country dial plans	Microsoft maintain dial plans for different countries. When the MS Teams user's location is set to a particular country, the appropriate country dial plan is automatically associated with the user's dialing.

Table continues…

Dial Plan Type	Description
Global dial plan	Each tenancy in MS Teams has a default global dial plan. MS Teams applies the global dial plan to all users who are not associated with a user plan (below). MS Teams searches the dialing rules in the global plan for a dialing match before searching against the country dial plan. • MS Teams uses the global dial plan as the template when you add a new user dial plan.
User dial plans	For each tenancy you can add up to a 1000 additional dial plans. You can associate each MS Teams users with a user plan. MS Teams searches the dialing rules in that user plan for a dialing match before searching the country dialing plan.

Planning a dial plan

Decide whether to use the Global dial plan or create a customer specific-plan or plans. Using a dial plan provides a method to override the default translations applied by the country plans.

- List all types of numbers for which you need custom dial rules.
- You must make this list as comprehensive as possible. MS Teams checks all numbers not matched by the global or user plan against the country dial plan. That can lead to MS Teams prefixing numbers with + or + and the country code for the user's location.
- List which users or groups of users need to dial which numbers. Use this to assess whether you need to add the dialing rules to the tenancy's global dial plan or into separate user dial plans.

Related links

Direct Routing Components on page 20

Regular Expressions

MS Teams menus use 'dial patterns' to match the dialed numbers. These patterns use regular expression (regex) strings to check for matches to the dialed digits. For example, the regex string `^2\d{2}$` matches any three-digit number beginning with a 2.

- In Dial plans, MS Teams uses these to match numbers dialed by a user and apply to number translations.
- In Voice routes, MS Teams uses these to match the number on outgoing calls to routes for the call.
- For more information, see Using Regular Expressions (regex) on page 128.

Related links

Direct Routing Components on page 20

Voice Routing Policies

For direct routing, each MS Teams user is associated with a Voice Routing Policy. For dialing that has matched an entry in the user's dial plan, MS Teams checks the resulting translation for matches against voice routes.

Each voice routing policy can list more than one PSTN usage. When matching outgoing calls to voice routes, MS Teams only considers routes that have a usage that matches a PSTN usage in the voice routing policy.

MS Teams checks the different usages for a matching voice route in the order that the voice routing policy lists the usages. MS Teams checks all the voice routes with the same usage for a match, using their dial pattern and priority settings.

The Global Policy

Each tenancy in MS Teams has a default global voice routing policy. MS Teams applies the policy to the dialing of all users who do not have an associated voice routing policy.

MS Teams uses the global policy as a template when you add a new policy.

Planning Voice Routing Policies

Decide whether you require separate policies. For example, using policies with different sets of PSTN usage records, you can configure policies for control of local/national/international calling.

- List the types of number for which you require different policies.
- List which users or groups of users need to dial which types of number. Use this to assess whether you should add the PSTN usages to the global dial plan or into separate user dial plans.
- For more details, refer to https://docs.microsoft.com/en-us/microsoftteams/manage-voice-routing-policies.

Related links

Direct Routing Components on page 20

Voice Routes

Once MS Teams has processed a user's dialing through their associated dial plan and voice routing policy, MS Teams checks the resulting number for matches in the MS Teams Voice Route entries. The match defines the SBC connection used for the call.

Each voice route has three settings MS Teams uses for matching: a usage label, a dial pattern, and a priority. Direct routing uses these as follows:

- MS Teams groups routes by usage. It checks them in the order that the usages appear in the user's assigned voice routing policy.
  - MS Teams checks the first set of usage voice routes for a dial pattern match.
  - If MS Teams does not find a match, it checks the next set of usage voice routes.

    - When MS Teams finds a dial pattern match, MS Teams attempts to connection to the SBC (or SBCs) listed in the matched usage route with the highest priority.
        - MS Teams first attempts to use an SBC which has recently had a successful handshake. It does this in random order. MS Teams refers to these as 'healthy' SBCs.
        - If connection to a 'healthy' SBC is not successful, MS Teams attempts to use any other SBC. Again, it does this in random order. MS Teams refers to these as 'demoted' SBCs.
        - After successful SBC connection, the call follows the SBCs routing settings.
        - If SBC connection fails, MS Teams checks the SBC settings of the next highest priority dial pattern match in the usage routes. Note, this means that after a dial pattern match has occurred in a set of usage routes, MS Teams will not use another set of usage routes if SBC connection fails.
- If MS Teams does not find a successfully route match, MS Teams re-routes the call to Microsoft calling plans if enabled for the user. Otherwise, MS Teams drops the call.

Related links

Direct Routing Components on page 20

Emergency Routing Policies

You can use emergency policies in MS Teams to set up emergency numbers and specify how MS Teams routes emergency calls.

- You can use the global policy or create and assign custom policies. Users automatically use the global policy unless you create and assign them a custom policy.
- For more information, refer to https://docs.microsoft.com/en-us/microsoftteams/manage-emergency-call-routing-policies.

Related links

Direct Routing Components on page 20

PSTN Usages

PSTN usage records are text labels. MS Teams uses them to link components in the call routing process that share the same label:

- Each emergency routing policy has a single PSTN usage. Calls routed by the policy can use voice routes with the same PSTN usage.
- Each voice routing policy has a list of PSTN usages. Calls routed by the policy can use voice routes set with one of those PSTN usages.
- Each voice route has a single PSTN usage.

Related links

Direct Routing Components on page 20

Session Border Controller (SBC)

When using direct routing, the final stage of outgoing call routing in MS Teams is to route the call to a Microsoft accredited SBC.

For IP Office support, use ASBCE R10.1 plus Hotfix 1 or higher. ASBCE R8.1.2 supports direct routing, however R10.1 plus Hotfix 1 contains updates required for IP Office.

Related links

Direct Routing Components on page 20

MS Teams Line

For direct routing, the connection between the ASBCE and IP Office uses an MS Teams line added to the IP Office configuration.

Related links

Direct Routing Components on page 20

Chapter 5: MS Teams Direct Routing

This section provides an overview of the components and routing involved. For more information on MS Teams direct routing, refer to https://docs.microsoft.com/en-us/microsoftteams/direct-routing-landing-page.

Related links

Direct Routing Call Flow on page 25

Emergency Call Direct Routing Call Flow on page 26

Direct Routing Flowchart on page 27

SBC Verification on page 27

Direct Routing Call Flow

The following is a summary of how MS Teams uses components for direct routing of normal calls.

- **Teams User** > **Dial plan** > **Voice routing policy** > **PSTN usage** > **Voice routes** > **SBCs**

1. The MS Teams user dials a number:
2. **Dial plan**

   MS Teams checks the number for a match in the user's associated dial plan. If a match occurs, the dial plan applies the number translation, otherwise MS Teams drops the call. The translation can include allowing the number dialed to remain as is.
3. **Voice routing policy**

   The user's associated voice routing policy indicates the PSTN usage records they can use.
4. **PSTN usage**

   MS Teams uses PSTN usage records to link a user's voice routing policy and the voice routes that the user's calls can use. The same PSTN usage must appear in each.
5. **Voice routes**

   MS Teams checks the translated number for a match in the available voice routes. MS Teams only checks voice routes with a PSTN usage that match a usage in the user's voice routing policy.
6. **SBC**

   The matched voice route specifies the SBC or SBCs to use. MS Teams uses the SBC if it is available. Otherwise, MS Teams attempts to match another route with the same usage.

Routing Failure

In the above call flow, if direct routing fails at any point, MS Teams redirects the call to Microsoft Calling Plans if configured for the user. Otherwise, MS Teams drops the call.

Related links

MS Teams Direct Routing on page 25

Emergency Call Direct Routing Call Flow

You must configure MS Teams to route emergency calls using emergency routing policies rather than the same voice routing policies MS Teams uses for normal calls.

The following is a summary of how MS Teams uses components for direct routing of emergency calls.

- **Teams User** > **Emergency routing policy** > **PSTN usage** > **Voice routes** > **SBCs**

1. The MS Teams user dials a number:
2. **Emergency routing policy**

   If the number matches one in the user's associated emergency routing policy, MS Teams uses that policy to route the call. If the number matches one in the policy's **Emergency dial mask**, MS Teams translated it to the **Emergency dial string** number. For example, if a user dials 911 or 999, MS Teams translates the number to 112.
3. **PSTN usage**

   MS Teams uses PSTN usage records to link a user's voice routing policy and the voice routes that the user's calls can use. The same PSTN usage must appear in each.
4. **Voice routes**

   MS Teams checks the translated number for a match in the available voice routes. MS Teams only checks voice routes with a PSTN usage that match a usage in the emergency routing policy.
5. **SBC**

   The matched voice route specifies the SBC or SBCs to use.

Routing Failure

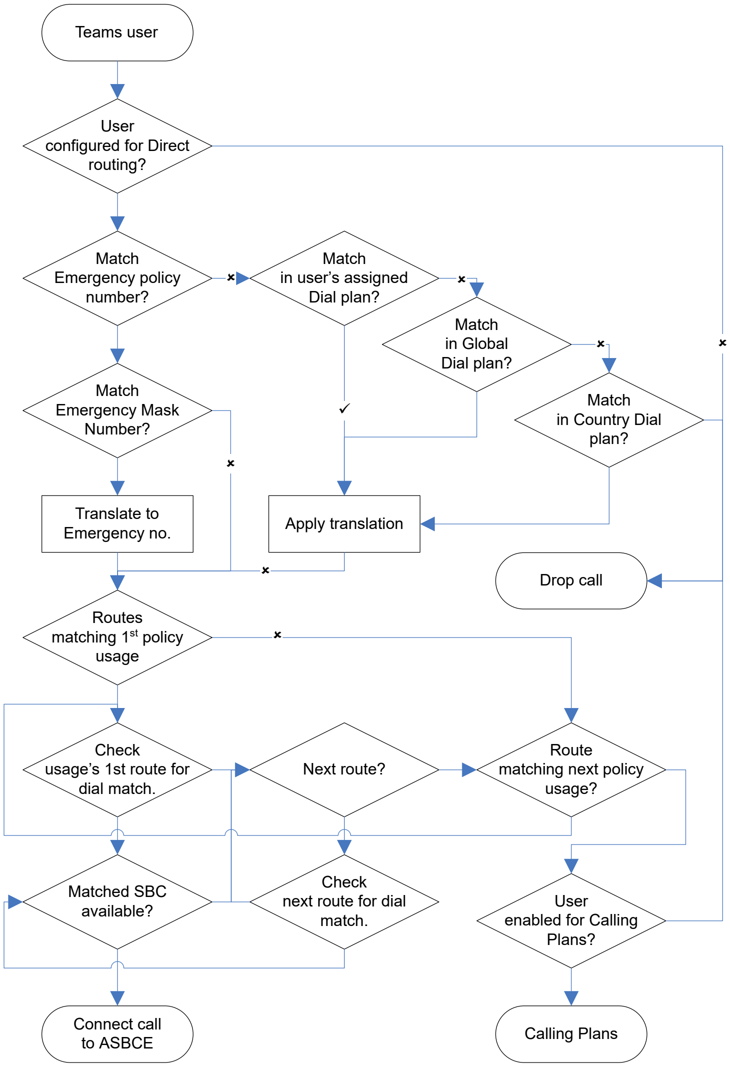
In the above call flow, if direct routing fails at any point, MS Teams redirects the call to Microsoft Calling Plans if configured for the user. Otherwise, MS Teams drops the call.

Related links

MS Teams Direct Routing on page 25

Direct Routing Flowchart

The following flowchart is a simplified summary of the call routing applied in MS Teams. Vertical results are positive, horizontal negative.


Teams user
User configured for Direct routing?
Match Emergency policy number?
Match in user's assigned Dial plan?
Match in Global Dial plan?
Match in Country Dial plan?
Match Emergency Mask Number?
Translate to Emergency no.
Apply translation
Drop call
Routes matching 1st policy usage
Check usage's 1st route for dial match.
Next route?
Route matching next policy usage?
Matched SBC available?
Check next route for dial match.
User enabled for Calling Plans?
Connect call to ASBCE
Calling Plans
×
✓

Related links

[MS Teams Direct Routing](#) on page 25

SBC Verification

When adding the ASBCE to MS Teams, you must verify the domain part of the ASBCE FQDN. For example, for the FQDN `sbc.example.com`, you must verify that you have administrator rights for the `example.com` domain.

Verification requires you to do one of the following:

- Add a TXT record to the domain's DNS records.
- Add an MX record to the domain's DNS records.
- Add a text file to the root of the domain's default web site.

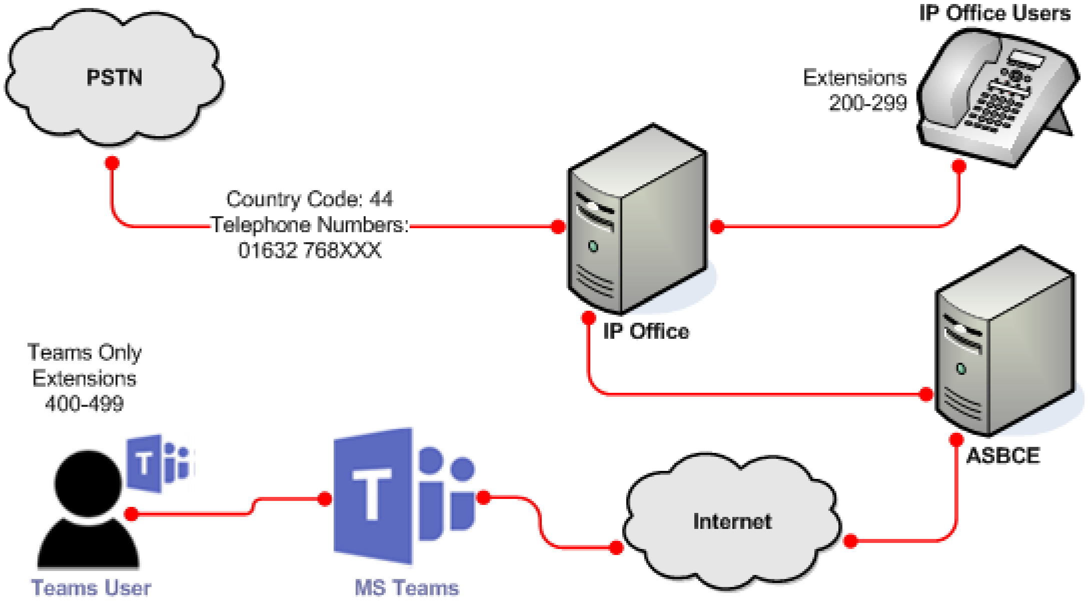
Related links

MS Teams Direct Routing on page 25

Part 2: Example Direct Routing Scenario

Chapter 6: Example Direct Routing Scenario

In this scenario, the customer has a single ASBCE and IP Office.



- IP Office extension numbers in the range 2XX. MS Teams only user extension numbers in the range 4XX.
    - For ease of implementation and maintenance, the extension number range used for MS Teams only users should not overlap with the range used for other users.
- Local area code 01632.
- Main telephone number 01632 768000
- The customer is based in the UK, international dialing prefix 44.
- The customer wants to be able to restrict which MS Teams users can make outgoing national and international PSTN through the IP Office.

Related links

Numbers to Consider on page 31
Proposed Dial Plan on page 31
Proposed Voice Routing Policies/PSTN Usages on page 32
Proposed Voice Routes on page 33

Proposed Emergency Routing Policy on page 33
Callflow on page 34
Simplified Callflow on page 34

Numbers to Consider

Begin planning by considering the different numbers used on or routed through the IP Office:

Dialed Numbers		Details
Extension Numbers	IP Office	These are 3-digit numbers in the range 200 to 299. The scenario uses these for IP Office only and MS Teams+IP Office users.
	MS Teams Only	These are 3-digit numbers in the range 400 to 499. The scenario uses these for MS Teams only users.
IP Office Short Codes		These are numbers of variable length but always beginning with *.
Incoming PSTN Calls		The customer's main number for calls to the IP Office is 01632 768000.
Emergency Calls		999 and 112.
PSTN	Local	Any 6-digit number.
	National	7 to 10-digit numbers with a leading 0.
	International	Numbers beginning 00.

There are special scenarios to consider for calls made by MS Teams users:

- We need to convert any calls from MS Teams prefixed with a +:
  - Change the + to the international dialing prefix for the customer's locale if the country code is not 44.
  - Remove the + or 00, and the country code, from calls that are national calls.
  - Remove the + from any other numbers.
- We want calls prefixed with the country code 44 changed back to being national numbers with just the national dialing prefix.

Related links

Example Direct Routing Scenario on page 30

Proposed Dial Plan

The example scenario will use a single dial plan for all users.

- The plan must convert all numbers to a format useable by the IP Office system. The translations also need to match the dial patterns used for the voice routes.

- The plan must contain the full range of required digit translations for all users. MS Teams uses the PSTN usages in the user's assigned voice routing policy to control numbers a particular user can call.
- The plan must cover the format used for numbers stored within Azure Active Directory (typically full E.164 format) and numbers dialed from the MS Teams client.
- The order of the dial patterns is important. MS Teams checks the entries in the dial plan for a match from the top-down.
- The matching of calls already dialed in the format expected by the IP Office appears superfluous. However, doing this in the dial plan, prevents the country dial plan matching and altering the numbers.

In this case, the plan matches expected dialing in the customer's UK location.

Pattern	Translation	Description
`^\+?(2\d{2})$`	`$1`	Match any 3-digit numbers beginning with a 2. That is, IP Office extension numbers. Translate the full number as is. The \+? part matches numbers prefixed with or without a +.
`^(\*.+)$`	`$1`	Match any numbers prefixed with a *. That is, IP Office short codes. Translate the full number as is.
`^(\+44|0044|0)?(1632)?768([24]\d{2})$`	`$3`	Match any DID/DDI number dialed as a local, nation or international number. Translate to the extension number.
`^(\d{6})$`	`$1`	Match any 6-digit numbers. That is local phone numbers without the local area code. Translate the full number as is.
`^(0\d{6,10})$`	`$1`	Match any 7 to 10-digit numbers prefixed with a 0. That is national numbers. Translate the full number as is.
`^(\+|00)44(.+)$`	`0$2`	Match any number prefixed with 0044 or +44. That is, UK numbers dialed as full international numbers. Translate back to national numbers prefixed with just 0.
`^(\+|00)(.+)$`	`00$2`	Match any number prefixed with 00 or +. Translate the number to the international dialing prefix for the customer's location, for this scenario 00.

Related links

Example Direct Routing Scenario on page 30

Proposed Voice Routing Policies/PSTN Usages

The customer wants to be able to configure MS Teams users with internal only, national only and all dialing rights. We can configure that using the following set of three PSTN usages and three voice routing policies:

PSTN usage	Voice routing policy		
	IPO	**PSTN**	**All**
IPOffice	Yes	Yes	Yes
National	–	Yes	Yes
International	–	–	Yes

Related links

Example Direct Routing Scenario on page 30

Proposed Voice Routes

For the voice routes, we need digit pattern matches for numbers resulting from the translations applied by the dial plan.

Voice Route	Priority	Dial Pattern	PSTN Usage	SBC
Extn2xx	1	`^2\d{2}$`	`IPOffice`	`sbc1.example.com`
Shortcodes	1	`^*.+$`	`IPOffice`	`sbc1.example.com`
PSTN_Local	1	`^\d{6}$`	`National`	`sbc1.example.com`
PSTN_National	1	`^0\d{10}$`	`National`	`sbc1.example.com`
PSTN_Global	1	`^00.+$`	`International`	`sbc1.example.com`
Emergency	1	`^\+?999`	`National`	`sbc1.example.com`

The dial patterns do not need the ( ) brackets as in the dial plan since we are do not need to refer to them in any translation.

Related links

Example Direct Routing Scenario on page 30

Proposed Emergency Routing Policy

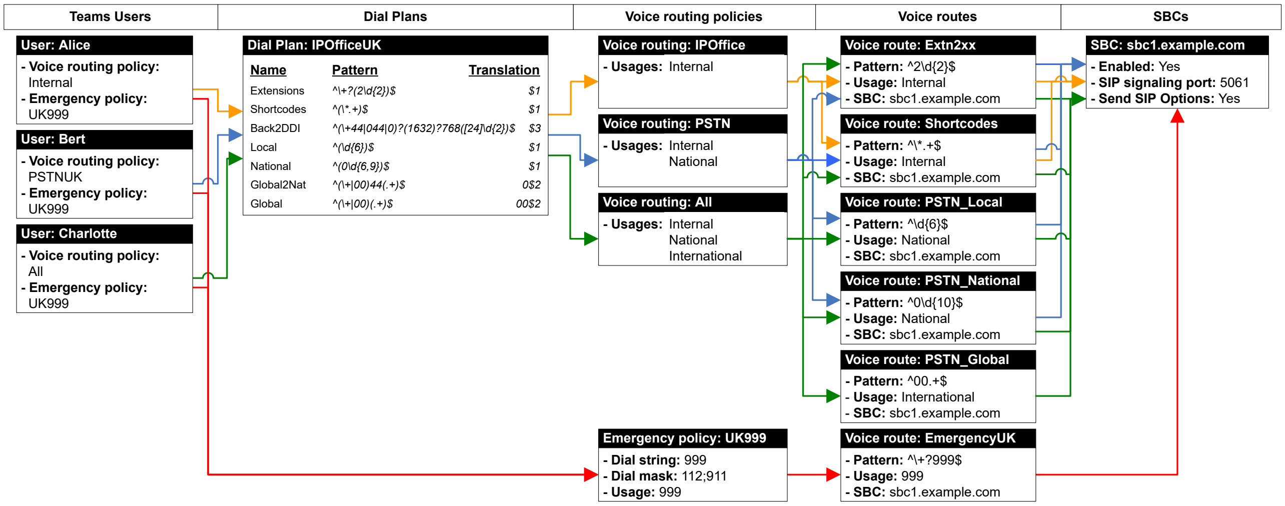
Setting	Value
Emergency Dial Number	`999`
Emergency Dial Mask	`112;911`
PSTN Usage	`National`

Related links

Example Direct Routing Scenario on page 30

Callflow

The following is a view of the call routing within MS Teams for our example:



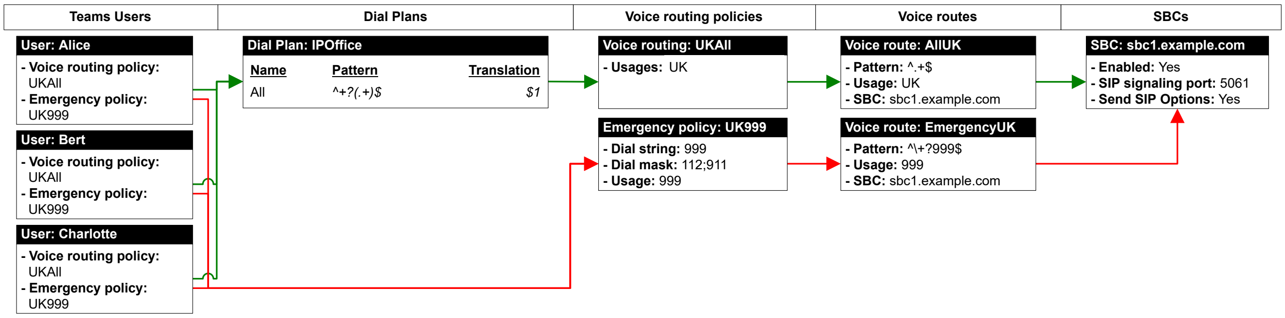
- In theory, the emergency calls could use the same voice route and PSTN usage. However, using separate entries just for emergency calls means you can make future changes to the normal call routing without affecting emergency call routing.

Related links

Example Direct Routing Scenario on page 30

Simplified Callflow

This simplified version of the example callflow allows all users to dial any numbers. The dial plan and the voice route match any dialing.



In this case:

- The callflow still needs the dial plan to perform number translations between numbers used in MS Teams and number formats supported by the IP Office. In this case, the dial plan strips the + from any numbers.

- The callflow only requires a single voice route and PSTN usage for normal calls.
    - In theory, the emergency calls could use the same voice route and PSTN usage. However, using separate entries just for emergency calls means you can make future changes to the normal call routing without affecting emergency call routing.
- In theory, you can configure this using the global dial plan, global voice routing policy and global emergency routing policy.

Related links

Example Direct Routing Scenario on page 30

Part 3: Configuring Direct Routing

Chapter 7: Configuring the Users in MS Teams

This section covers the general configuration of users within MS Teams.

Related links

User Configuration in MS Teams on page 37
Checking MS Teams User Numbers on page 38

User Configuration in MS Teams

You configure the user telephone numbers for MS Teams users in Azure Active Directory.

Procedure

1. Using a user account with full administrator rights, login to Azure Active Directory at https://portal.azure.com.
2. Select **Azure AD** and then **Users**.
3. Select the required user.
4. Select **Contact Info**.
5. Set the user's **Office phone number** as required. Azure Active Directory stores this as the `businessPhone` value. The format varies depending on the type of number being set, see Telephone and Extension Numbers on page 17.

Number	Example Azure Active Directory Phone Number Format
Telephone Number and Extension	`+441632768000;ext=402`
Telephone Number Only	`+441632768402`
Extension Number Only	`x402`

6. For all users allowed to make PSTN calls using direct routing, you also need to check that they have a suitable MS Teams license.
    a. You must populate the user's **Location** field. MS Teams uses this to determine the country dial plan for any dialing by the user.

b. Select **Licenses**.

c. Click **Assignments** and add a license that includes support for Direct Routing.

7. Repeat this process for all other users.

Related links

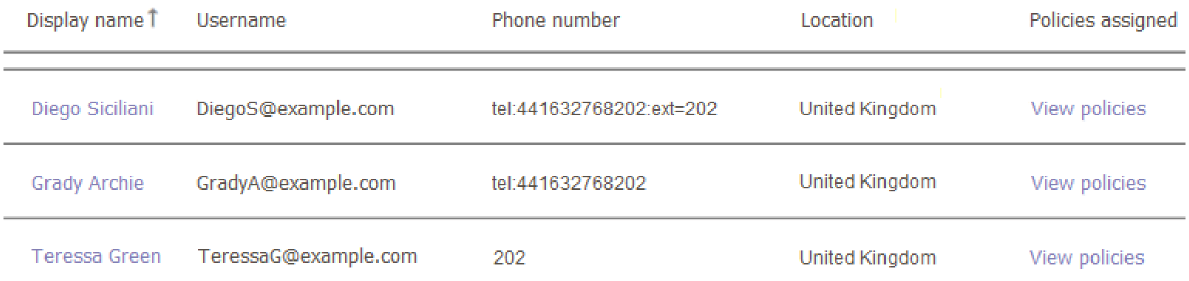
Configuring the Users in MS Teams on page 37

Checking MS Teams User Numbers

Use the following process to check that the *Office* phone numbers set for users in Azure Active Directory. MS Teams uses this number as the user's *Phone number*.

Procedure

1. Login to the MS Teams admin portal at https://admin.teams.microsoft.com/user.
2. If necessary, select **User**.
3. MS Teams displays the list of users, including their MS Teams telephone numbers.



Display name ↑	Username	Phone number	Location	Policies assigned
Diego Siciliani	DiegoS@example.com	tel:441632768202:ext=202	United Kingdom	View policies
Grady Archie	GradyA@example.com	tel:441632768202	United Kingdom	View policies
Teressa Green	TeressaG@example.com	202	United Kingdom	View policies

4. Verify that the **Phone number** is correct. For more information, see Telephone and Extension Numbers on page 17.

Number	Example MS Teams Format
Telephone Number and Extension	`tel:441632768202;ext=202`
Telephone Number only	`tel:441632768202`
Extension Number only	`202`

Related links

Configuring the Users in MS Teams on page 37

Chapter 8: Configuring the IP Office for MS Teams

This section covers the basic steps for configuring the IP Office system to support MS Teams.

Related links

Manually Adding MS Teams+IP Office Users on page 39
Manually Adding Directory Entries for MS Teams Only Users on page 40

Manually Adding MS Teams+IP Office Users

The process below describes the steps for adding a MS Teams+IP Office user manually.

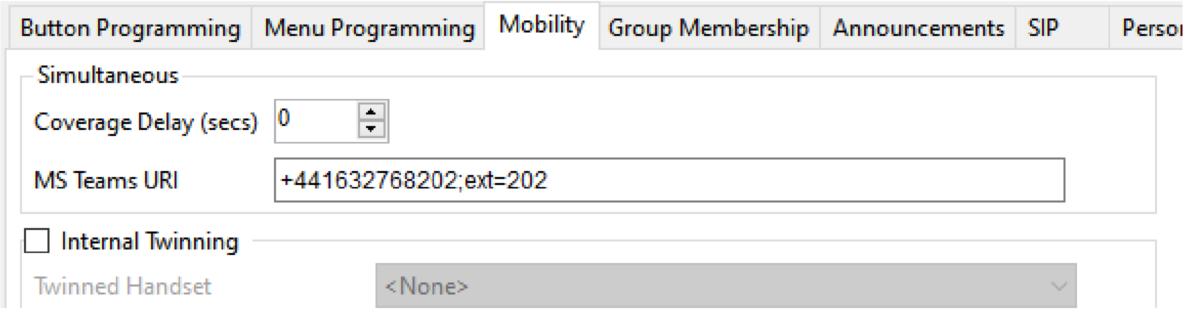
- If configured to only allow automatic updates through Azure Active Directory synchronization, IP Office grays out the **MS Teams URI** field.

Procedure

1. Using IP Office Manager or IP Office Web Manager, access the IP Office system configuration.
2. Configure the user as required for their IP Office operation. This process only covers the changes required for MS Teams.
3. Select **User** or **Call Management | Users**.
4. Add a new user or select the existing user you want to edit.
5. Select the **User** tab:
    a. Select a **Profile** that supports MS Teams user integration:
        - **On subscription mode systems:** The IP Office supports MS Teams+IP Office users using the **UC User** profile.
        - **On PLDS licensed systems:** The IP Office supports MS Teams+IP Office users using the **Office Worker**, **Teleworker** and **Power User** profiles.

    b. Select **Enable MS Teams Client**.

6. Select the **Mobility** tab:



Simultaneous

Coverage Delay (secs): 0

MS Teams URI: +441632768202;ext=202

□ Internal Twinning

Twinned Handset: <None>

   a. The **Coverage Delay** sets a pause, if required, between calls alerting on the user's IP Office extension devices and then also altering on their MS Teams client.

   b. The user's **MS Teams URI** should match their Office phone setting as specified in Azure Active Directory (for more information, see Telephone and Extension Numbers on page 17):

Number	Example MS Teams URI Format
Telephone Number and Extension	`+441632768202;ext=202`
Telephone Number Only	`+441632768202`
Extension Only	`+202`

7. Click **OK** or **Save**.

8. If prompted to allow the system to automatically create a matching extension entry, allow the system to create one matching the type of IP Office extension the user uses.

9. If using IP Office Manager, save the configuration back to the IP Office system.

Related links

Configuring the IP Office for MS Teams on page 39

Manually Adding Directory Entries for MS Teams Only Users

MS Teams only users do not exist in the IP Office configuration. However, you can add their details to the IP Office system directory. This allows IP Office users to select and call MS Teams only users from the directory.

Procedure

1. Using IP Office Web Manager, access the IP Office system configuration.

2. Select **System Settings** > **Directory**.

3. Select **Add Directory Entry**.

4. For the **Name**, enter the user's name followed by a space and `MST`. For example: `Diego Siciliani MST`
5. For the **Number**, use one of the following formats (for more information, see Telephone and Extension Numbers on page 17):

Number	IP Office Format
Extension and DDI Number	`441632768402-402` [a], [b]
Telephone Number Only	`441632768402`
Extension Number Only	`+402`

   a. A dash is a delimiter signifying that the following number is an extension number.
   b. Dialing either number matches the directory entry.

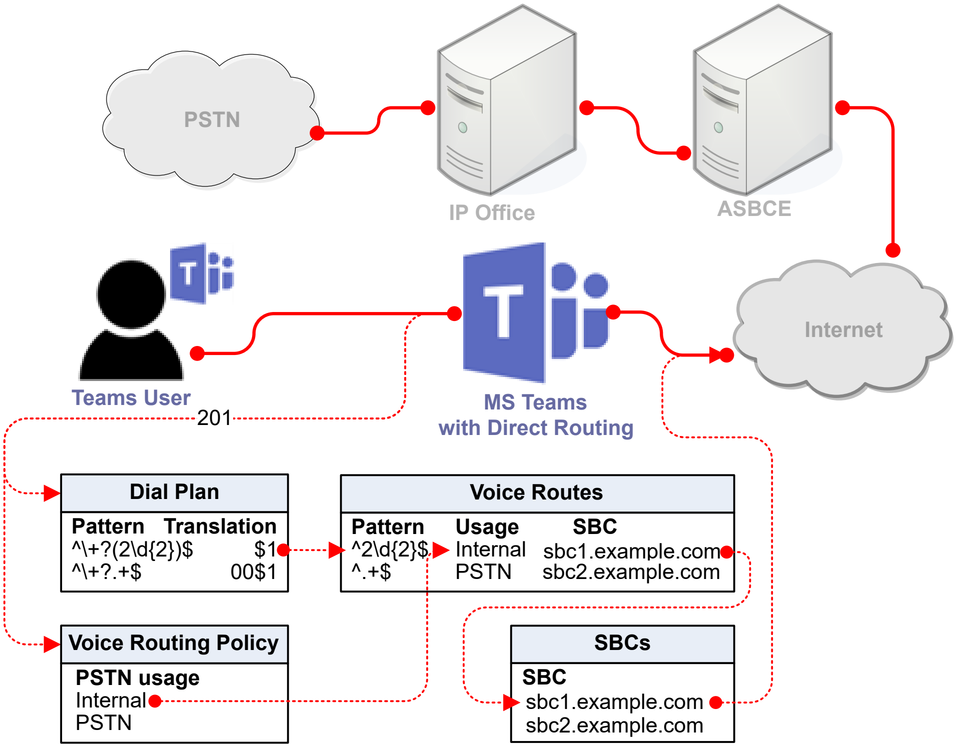
6. Click **Save**.

Related links

Configuring the IP Office for MS Teams on page 39

Chapter 9: Configuring MS Teams Direct Routing

This section of the document contains a summary of the configuration done within MS Teams to support direct routing to the IP Office through the ASBCE.



Dial Plan	
Pattern	**Translation**
^\+?(2\d{2})$	$1
^\+?.+$	00$1

Voice Routes		
Pattern	**Usage**	**SBC**
^2\d{2}$	Internal	sbc1.example.com
^.+$	PSTN	sbc2.example.com

Voice Routing Policy
PSTN usage
Internal
PSTN

SBCs
SBC
sbc1.example.com
sbc2.example.com

- The processes in this document are just examples. For example:
  - You can perform processes such as assigning policies to users, for a whole tenancy, for a group of users or for individual users.
  - You can use PowerShell scripts for most processes rather than using the MS Teams menus.
- A policy assigned to an individual user overrides any assigned to a group, which itself overrides any assigned globally. Bear this is mind for ease of maintenance when planning the customer's policies and how to assign those policies. For more information, see https://docs.microsoft.com/en-us/microsoftteams/assign-policies-users-and-groups.
- In mixed scenarios, the setting applied directly to a user typically overrides any applied to their group, which themselves override any applied to the whole tenancy. Keep this in mind when planning the implementation as it will also affect maintenance.

Related links

[Adding an MS Teams Line](#) on page 43
[Verify the SBC Domain](#) on page 44
[Adding the ASBCE to MS Teams](#) on page 45

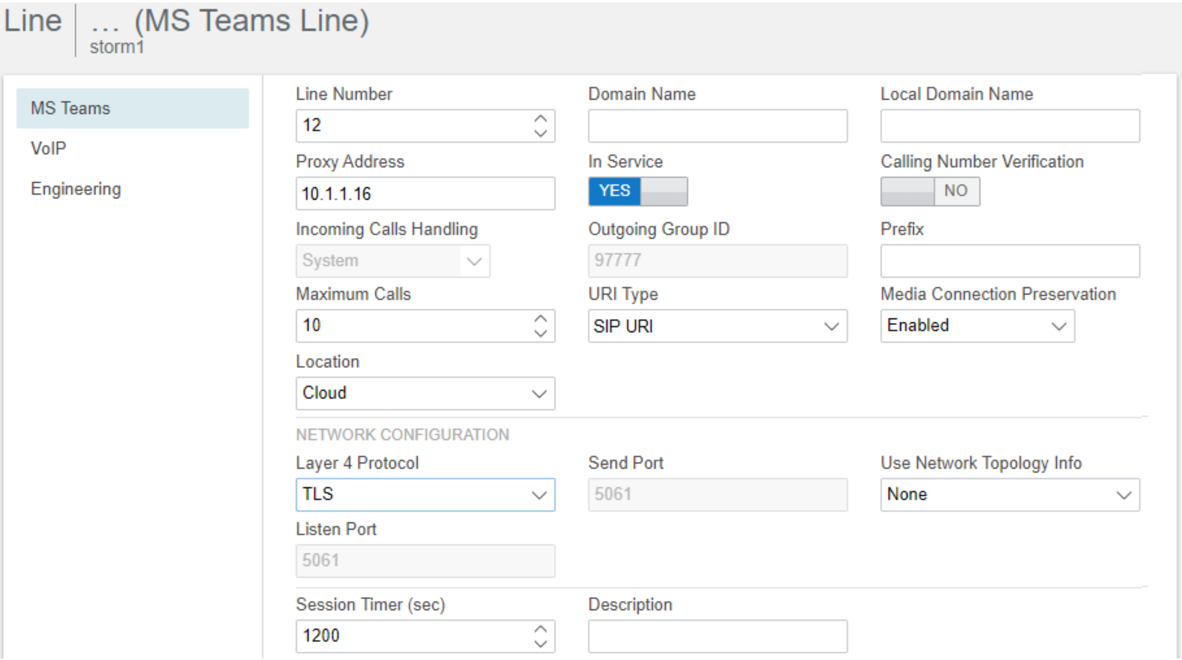
Adding an MS Teams Line

The MS Teams line links the IP Office to the ASBCE required for direct routing.

This document assumes that you have already configured the IP Office system to support SIP trunks.

Procedure

1. Using IP Office Manager or IP Office Web Manager, access the IP Office system configuration.
2. Select **Line** or **System Settings** > **Lines**.
3. Click **Add** and select **MS Teams Line**. If using IP Office Web Manager in a Server Edition network, also select the server to which you want to add the line. Click **OK**.
4. On the **MS Teams** tab, configure the number of calls:



Line | … (MS Teams Line)
storm1

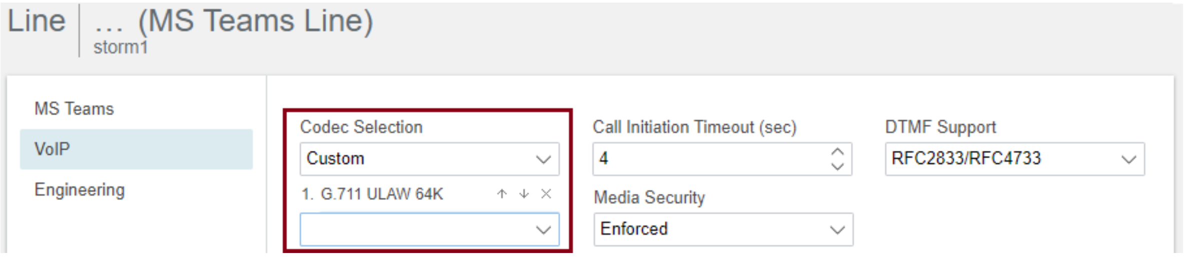
Line Number: 12
Domain Name:
Local Domain Name:
Proxy Address: 10.1.1.16
In Service: YES
Calling Number Verification: NO
Incoming Calls Handling: System
Outgoing Group ID: 97777
Prefix:
Maximum Calls: 10
URI Type: SIP URI
Media Connection Preservation: Enabled
Location: Cloud

NETWORK CONFIGURATION
Layer 4 Protocol: TLS
Send Port: 5061
Use Network Topology Info: None
Listen Port: 5061

Session Timer (sec): 1200
Description:

   a. Set the **Proxy Address** to the IP Address of the ASBCE interface (A1 or A2).
   b. Ensure that the **Max Calls** value matches the **Concurrent call capacity** of the ASBCE entry in MS Teams.

5. On the **VoIP** tab, ensure you have selected a single codec.



Line | … (MS Teams Line)
storm1

Codec Selection: Custom
1. G.711 ULAW 64K
Call Initiation Timeout (sec): 4
Media Security: Enforced
DTMF Support: RFC2833/RFC4733

6. Click **Save** or **OK**.
7. If using IP Office Manager, save the configuration back to the IP Office system.

Next steps

- Proceed to Verify the SBC Domain on page 44.

Related links

Configuring MS Teams Direct Routing on page 42

Verify the SBC Domain

To add an SBC (ASBCE), MS Teams must verify that you manage the domain. This requires you to do one of the following:

- Add a TXT record to the domain's DNS records.
- Add an MX record to the domain's DNS records.
- Add a text file to the root of the domain's default web site.

Procedure

1. Login to the admin portal at https://admin.microsoft.com/Adminportal.
2. Select **Settings** > **Domain**.
3. Select **Add Domain**.
4. Enter the domain name and click **Use this domain**.
5. Select the method you want to use to verify the domain and click **Continue**.
6. Follow the instructions to add details to the domain's DNS server or root website.
7. When you have prepared the DNS server records or web site files as requested, click **Verify**.
8. Skip any other actions and click **Continue**.
9. Click **Done**.

Next steps

- Proceed to Adding the ASBCE to MS Teams on page 45.

Related links

Configuring MS Teams Direct Routing on page 42

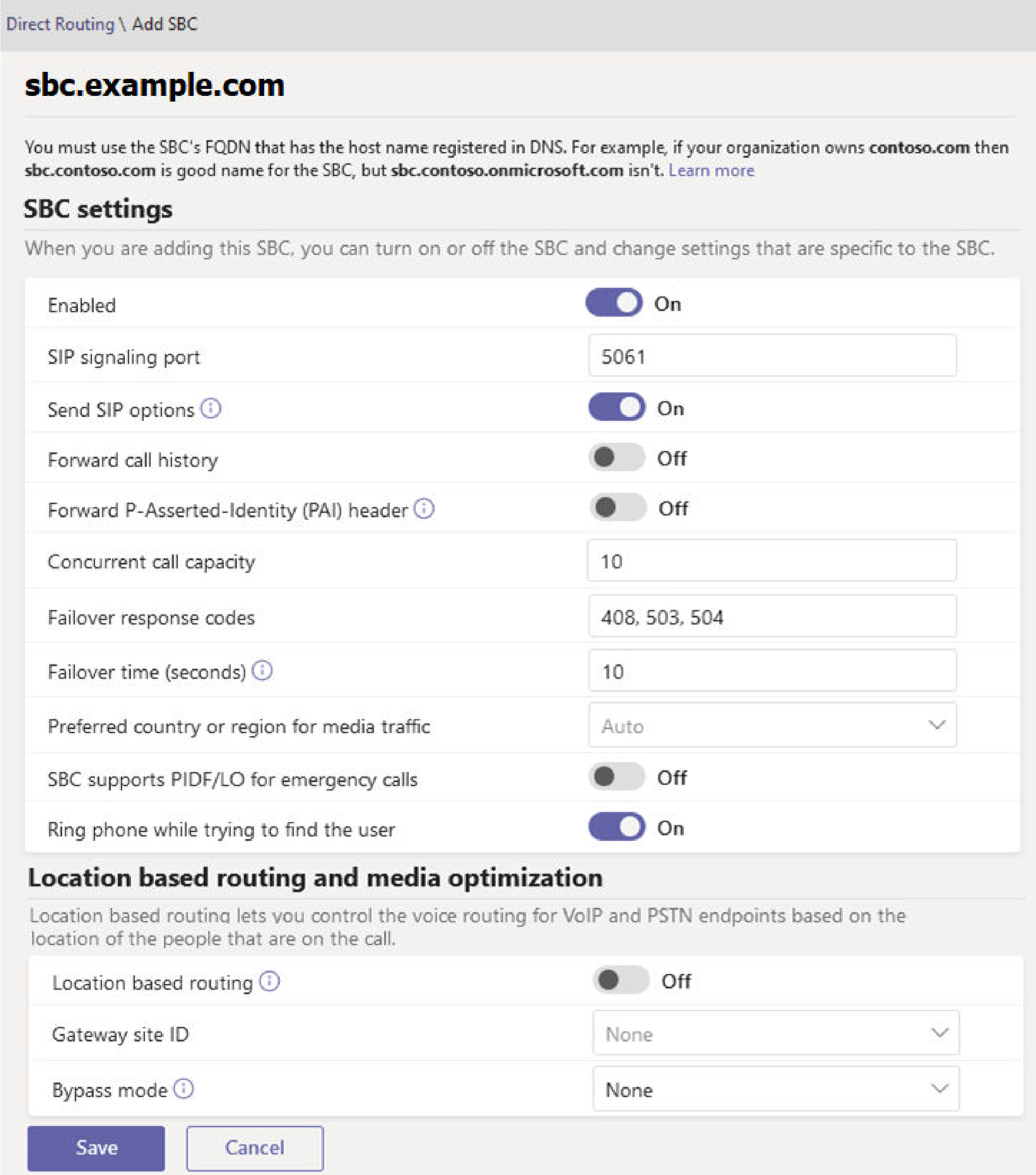
Adding the ASBCE to MS Teams

This process configures the SIP connection from MS Teams to the Avaya ASBCE used by the IP Office.

Procedure

1. Login to the MS Teams admin portal at https://admin.teams.microsoft.com/direct-routing/v2
2. Select **Voice** and then **Direct Routing**.

3. Select the **SBCs** tab and select **Add**.



Direct Routing \ Add SBC

sbc.example.com

You must use the SBC's FQDN that has the host name registered in DNS. For example, if your organization owns **contoso.com** then **sbc.contoso.com** is good name for the SBC, but **sbc.contoso.onmicrosoft.com** isn't. Learn more

SBC settings

When you are adding this SBC, you can turn on or off the SBC and change settings that are specific to the SBC.

Enabled	On
SIP signaling port	5061
Send SIP options	On
Forward call history	Off
Forward P-Asserted-Identity (PAI) header	Off
Concurrent call capacity	10
Failover response codes	408, 503, 504
Failover time (seconds)	10
Preferred country or region for media traffic	Auto
SBC supports PIDF/LO for emergency calls	Off
Ring phone while trying to find the user	On

Location based routing and media optimization

Location based routing lets you control the voice routing for VoIP and PSTN endpoints based on the location of the people that are on the call.

Location based routing	Off
Gateway site ID	None
Bypass mode	None

4. Enter the FQDN of the ASBCE. If the domain used in the FQDN is not already one verified by Microsoft (see Verify the SBC Domain on page 44), follow the instructions displayed by MS Teams after adding the SBC entry.

5. Enable the SBC and set the **SIP signaling port** to 5061.

6. Ensure that the **Concurrent call capacity** matches the **Max Calls** setting of the IP Office MS Teams line. See Adding an MS Teams Line on page 43.
7. Click **Save**.

Next steps

- Proceed to Creating Dial Plans on page 48.

Related links

Configuring MS Teams Direct Routing on page 42

Chapter 10: Creating Dial Plans

Dial plans are sets of rules for how to translate any numbers dialed by MS Teams users. For more information, refer tohttps://docs.microsoft.com/en-us/microsoftteams/what-are-dial-plans.

- Each dial plan contains up to 50 dialing rules. MS Teams searches the rules for a match to the number dialed by the user.
- When a match occurs, the rule settings determine what changes MS Teams applies to the dialed number. MS Teams then uses the translated number for routing through the user's associated voice routing policy.

The following types of dial plan exist:

Dial Plan Type	Description
Country dial plans	Microsoft maintain dial plans for different countries. When the MS Teams user's location is set to a particular country, the appropriate country dial plan is automatically associated with the user's dialing.
Global dial plan	Each tenancy in MS Teams has a default global dial plan. MS Teams applies the global dial plan to all users who are not associated with a user plan (below). MS Teams searches the dialing rules in the global plan for a dialing match before searching against the country dial plan. • MS Teams uses the global dial plan as the template when you add a new user dial plan.
User dial plans	For each tenancy you can add up to a 1000 additional dial plans. You can associate each MS Teams users with a user plan. MS Teams searches the dialing rules in that user plan for a dialing match before searching the country dialing plan.

Planning a dial plan

Decide whether to use the Global dial plan or create a customer specific-plan or plans. Using a dial plan provides a method to override the default translations applied by the country plans.

- List all types of numbers for which you need custom dial rules.
- You must make this list as comprehensive as possible. MS Teams checks all numbers not matched by the global or user plan against the country dial plan. That can lead to MS Teams prefixing numbers with + or + and the country code for the user's location.
- List which users or groups of users need to dial which numbers. Use this to assess whether you need to add the dialing rules to the tenancy's global dial plan or into separate user dial plans.

Related links

Creating a Dial Plan on page 49

Assigning a Dial Plan to Users on page 51

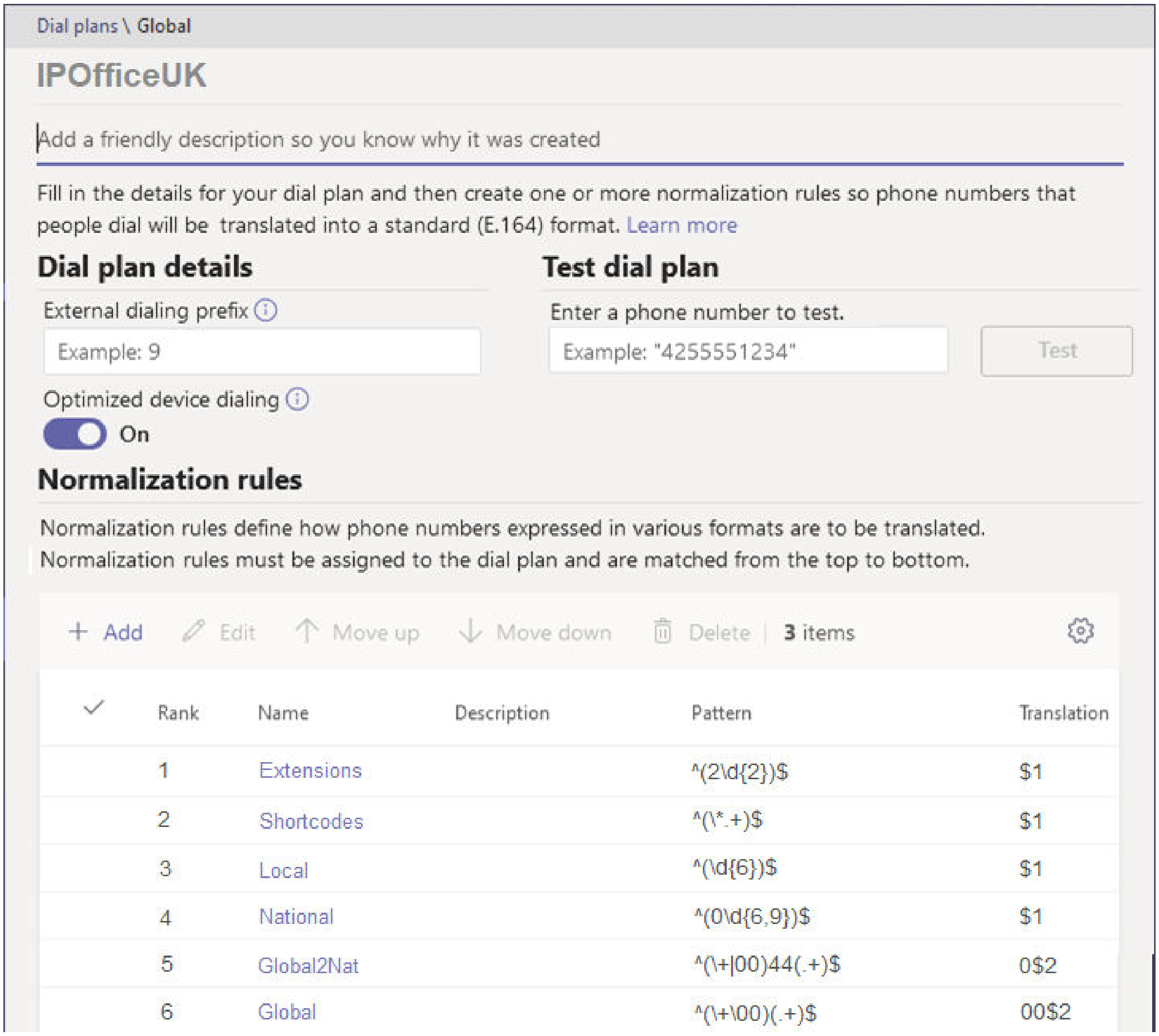
Creating a Dial Plan

Dial plans are sets of rules for how to translate any numbers dialed by MS Teams users into the format required by the IP Office.

Procedure

1. Login to the MS Teams admin portal at https://admin.teams.microsoft.com/policies/teamsdialplan
2. If necessary, select **Voice** and then select **Dial plans**.
3. Either select the **Global dial plan** or click **Add to add a new plan**.
   - MS Teams applies the global plan to the dialing of any users who do not have an associated user dial plan.
   - Adding a new plan creates a copy of the existing global plan including its existing translations.
4. Edit the plan details as required.
5. For a new plan, replace the label at the top of the menu with a unique descriptive name for the dial plan.
6. Edit the dialed digits matches and their translations as required:
   a. To add a new match, click **Add**.
   b. Enter a name for the dialing rule and, if needed, a description.
   c. Either select **Basic** or **Advanced** mode to define the actions of the dialing rule. Basic mode uses the menu options to create the required regex expressions. Advanced mode allows direct entry of the regex strings used for the match and translation.
   d. Enter the regex string needed to match the number and the string for the resulting translation. For details of regex, see Using Regular Expressions (regex) on page 128.
   e. To edit an existing match, click to the left of the rule translation name and then click **Edit**.
   f. Sort the matches by selecting the match that needs moving and then clicking **Move up** or **Move down**. In use, MS Teams checks entries from the top-down and uses the first match.

7. The final plan should for our example scenario looks like the following.



Dial plans \ Global

IPOfficeUK

Add a friendly description so you know why it was created

Fill in the details for your dial plan and then create one or more normalization rules so phone numbers that people dial will be translated into a standard (E.164) format. Learn more

Dial plan details

External dialing prefix ⓘ

Example: 9

Optimized device dialing ⓘ

● On

Test dial plan

Enter a phone number to test.

Example: "4255551234"

Test

Normalization rules

Normalization rules define how phone numbers expressed in various formats are to be translated. Normalization rules must be assigned to the dial plan and are matched from the top to bottom.

<table>
<tr><th>✓</th><th>Rank</th><th>Name</th><th>Description</th><th>Pattern</th><th>Translation</th></tr>
<tr><td></td><td>1</td><td>Extensions</td><td></td><td>^(2\d{2})$</td><td>$1</td></tr>
<tr><td></td><td>2</td><td>Shortcodes</td><td></td><td>^(*.+)$</td><td>$1</td></tr>
<tr><td></td><td>3</td><td>Local</td><td></td><td>^(\d{6})$</td><td>$1</td></tr>
<tr><td></td><td>4</td><td>National</td><td></td><td>^(0\d{6,9})$</td><td>$1</td></tr>
<tr><td></td><td>5</td><td>Global2Nat</td><td></td><td>^(\+|00)44(.+)$</td><td>0$2</td></tr>
<tr><td></td><td>6</td><td>Global</td><td></td><td>^(\+\00)(.+)$</td><td>00$2</td></tr>
</table>

8. Click **Save**.

Next steps

- Proceed to Assigning a Dial Plan to Users on page 51.

Related links

Creating Dial Plans on page 48

Assigning a Dial Plan to Users

Use the following process to associate the user with the dial plan.

- This process assigns a policy to individual users and is an example. You can also assign policies to groups of users or globally. For more information, see https://docs.microsoft.com/en-us/microsoftteams/assign-policies-users-and-groups.

Procedure

1. Login to the MS Teams admin portal at https://admin.teams.microsoft.com
2. Select **Users**.
3. Select the required user or users.
4. Click **Edit settings**.
5. Select the dial plan you want assigned and click **Apply**.

Next steps

- Proceed to Creating Voice Routing Policies on page 52.

Related links

Creating Dial Plans on page 48

Chapter 11: Creating Voice Routing Policies

For direct routing, each MS Teams user is associated with a Voice Routing Policy. For dialing that has matched an entry in the user's dial plan, MS Teams checks the resulting translation for matches against voice routes.

Each voice routing policy can list more than one PSTN usage. When matching outgoing calls to voice routes, MS Teams only considers routes that have a usage that matches a PSTN usage in the voice routing policy.

MS Teams checks the different usages for a matching voice route in the order that the voice routing policy lists the usages. MS Teams checks all the voice routes with the same usage for a match, using their dial pattern and priority settings.

The Global Policy

Each tenancy in MS Teams has a default global voice routing policy. MS Teams applies the policy to the dialing of all users who do not have an associated voice routing policy.

MS Teams uses the global policy as a template when you add a new policy.

Planning Voice Routing Policies

Decide whether you require separate policies. For example, using policies with different sets of PSTN usage records, you can configure policies for control of local/national/international calling.

- List the types of number for which you require different policies.
- List which users or groups of users need to dial which types of number. Use this to assess whether you should add the PSTN usages to the global dial plan or into separate user dial plans.
- For more details, refer to https://docs.microsoft.com/en-us/microsoftteams/manage-voice-routing-policies.

Related links

Creating a Voice Routing Policy on page 52

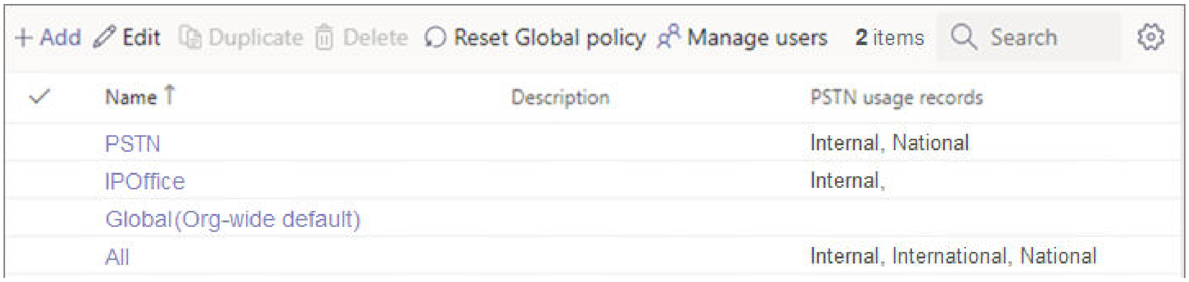
Assigning a Voice Routing Policy to a User on page 54

Creating a Voice Routing Policy

For direct routing, each MS Teams user is associated with a Voice Routing Policy. That policy contains PSTN usage records. Each of these usage records defines a number pattern that MS Teams checks for a match to the user dialing.

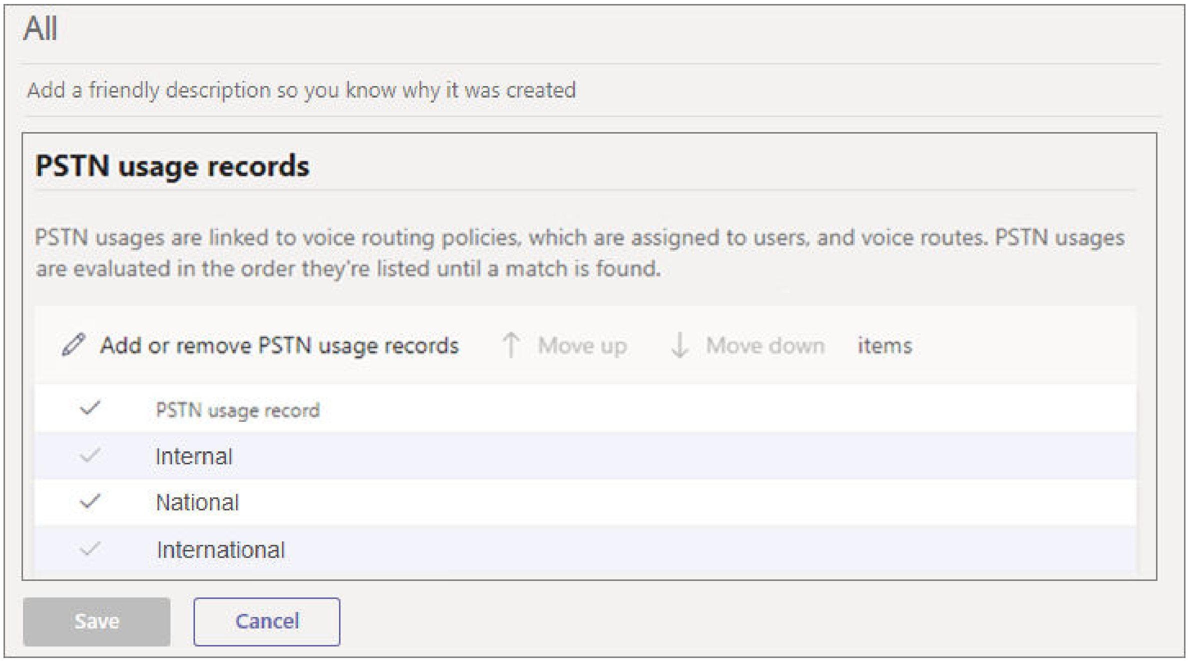
Procedure

1. Log in to the MS Teams admin portal at https://admin.teams.microsoft.com/policies/teamsonlinevoicerouting.
2. If necessary, select **Voice** and then **Voice routing policies**.



✓	Name ↑	Description	PSTN usage records
	PSTN		Internal, National
	IPOffice		Internal,
	Global(Org-wide default)		
	All		Internal, International, National

3. Select **Add** to add a new policy. Otherwise, select an existing policy and click **Edit**.


All

Add a friendly description so you know why it was created

PSTN usage records

PSTN usages are linked to voice routing policies, which are assigned to users, and voice routes. PSTN usages are evaluated in the order they're listed until a match is found.

✓	PSTN usage record
✓	Internal
✓	National
✓	International

4. For a new policy, add a unique descriptive name and, if necessary, a description.
5. To add PSTN usage records:
   a. Click **Add or remove PSTN usage records**.
   b. Select an existing PSTN usage from the list of those available and click **Save and apply**. Alternatively, to create a new PSTN usage, click **Add** and when completed, select it and click **Save and apply**.
6. The order of the usages sets the order in which MS Teams checks matching voice routes for dial pattern matches. If necessary, select a record and click **Move up** or **Move down**.
7. Click **Save**.

8. Create any other voice policies required.

Next steps

- Proceed to Assigning a Voice Routing Policy to a User on page 54.

Related links

Creating Voice Routing Policies on page 52

Assigning a Voice Routing Policy to a User

Each MS Teams users uses either the default global voice routing policy or the policy specifically assigned to them. You can assign a policy:

- Automatically using IP Office synchronization. See Azure Active Directory Synchronization on page 61.
- Manually using the process below.
- This process assigns a policy to individual users and is an example. You can also assign policies to groups of users or globally. For more information, see https://docs.microsoft.com/en-us/microsoftteams/assign-policies-users-and-groups.

Procedure

1. Login to the MS Teams admin portal at https://admin.teams.microsoft.com.
2. Select **Users**.
3. Select the required user or users.
4. Click **Edit** settings.
5. Select the **Policies** tab and click **Edit**.
6. In the **Voice routing policy** drop-down, select the policy you want assigned to the user or users, and click **Apply**.

Next steps

- Proceed to Creating Voice Routes on page 55.

Related links

Creating Voice Routing Policies on page 52

Chapter 12: Creating Voice Routes

Once MS Teams has processed a user's dialing through their associated dial plan and voice routing policy, MS Teams checks the resulting number for matches in the MS Teams Voice Route entries. The match defines the SBC connection used for the call.

Each voice route has three settings MS Teams uses for matching: a usage label, a dial pattern, and a priority. Direct routing uses these as follows:

- MS Teams groups routes by usage. It checks them in the order that the usages appear in the user's assigned voice routing policy.
  - MS Teams checks the first set of usage voice routes for a dial pattern match.
  - If MS Teams does not find a match, it checks the next set of usage voice routes.
  - When MS Teams finds a dial pattern match, MS Teams attempts to connection to the SBC (or SBCs) listed in the matched usage route with the highest priority.
    - MS Teams first attempts to use an SBC which has recently had a successful handshake. It does this in random order. MS Teams refers to these as 'healthy' SBCs.
    - If connection to a 'healthy' SBC is not successful, MS Teams attempts to use any other SBC. Again, it does this in random order. MS Teams refers to these as 'demoted' SBCs.
    - After successful SBC connection, the call follows the SBCs routing settings.
    - If SBC connection fails, MS Teams checks the SBC settings of the next highest priority dial pattern match in the usage routes. Note, this means that after a dial pattern match has occurred in a set of usage routes, MS Teams will not use another set of usage routes if SBC connection fails.
- If MS Teams does not find a successfully route match, MS Teams re-routes the call to Microsoft calling plans if enabled for the user. Otherwise, MS Teams drops the call.

Emergency Call Route

If you want to also include a route for emergency calls (see Configure Emergency Calling on page 58), add a route with a dial pattern that will match the primary emergency number (the Emergency Dial String) with and without a proceeding +. For example, ^\+?112. Set the voice route's usage to match that specified in the emergency routing profile.

Related links

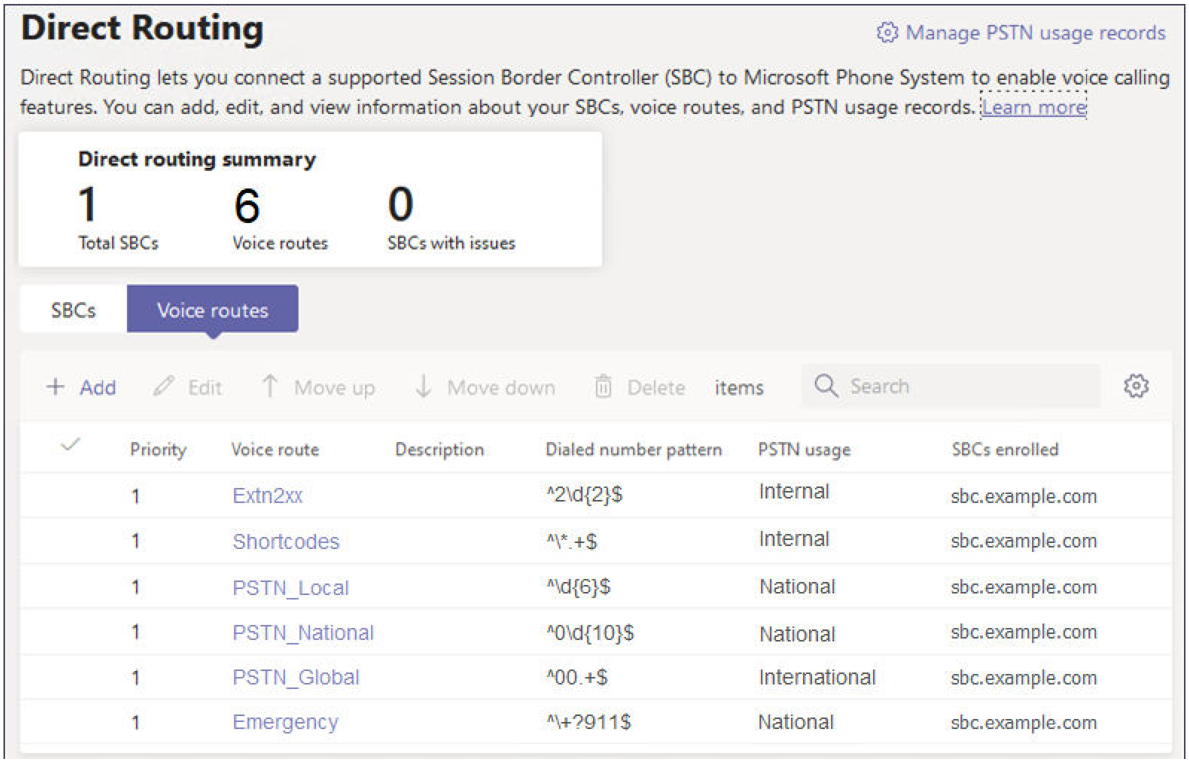
Creating a Voice Route on page 56

Creating a Voice Route

Use the following process to create voice routes.

Procedure

1. Log in to the MS Teams admin portal at https://admin.teams.microsoft.com/direct-routing/v2/voice-routes.
2. Select **Voice** and then **Direct Routing**.
3. Select the **Voice Routes** tab.



Direct Routing

Direct Routing lets you connect a supported Session Border Controller (SBC) to Microsoft Phone System to enable voice calling features. You can add, edit, and view information about your SBCs, voice routes, and PSTN usage records. Learn more

Direct routing summary

1 Total SBCs

6 Voice routes

0 SBCs with issues

✓	Priority	Voice route	Description	Dialed number pattern	PSTN usage	SBCs enrolled
	1	Extn2xx		^2\d{2}$	Internal	sbc.example.com
	1	Shortcodes		^*.+$	Internal	sbc.example.com
	1	PSTN_Local		^\d{6}$	National	sbc.example.com
	1	PSTN_National		^0\d{10}$	National	sbc.example.com
	1	PSTN_Global		^00.+$	International	sbc.example.com
	1	Emergency		^\+?911$	National	sbc.example.com

- In this example from the simple single server scenario (see [Example Direct Routing Scenario](#) on page 30), the **Dial number pattern** matches any dialed number following their processing through the user voice routing policies. The single ASBCE is set as the destination for calls.

4. To add a new route, click **Add**. To edit an existing route, select it and then click **Edit**.
   a. Enter a unique descriptive name for the voice route and, if necessary, a description.
   b. Set the **Priority**. When multiple voice route matches occur, MS Teams checks the one with the highest priority first.
   c. Enter the **Dialed number match**. MS Teams uses this dial pattern to match numbers that it will route using the voice route. The dial pattern uses regex format syntax. For example, `^2\d{2})$` matches 3-digit extension numbers being with a 2. See [Regular Expressions](#) on page 21.

   d. To add an SBC to the list of SBCs used by this voice route:

      a. Click **Add SBCs**.

      b. Select the ASBCE from the list of enrolled SBCs and click **Apply**.

   e. Add a PSTN usage for the voice route. Only calls by users who have the same usage in their associated voice routing policy can use the voice route.

      a. Click **Add PSTN usage** or from the list of those already shown, click **Add**.

      b. Select an existing PSTN usage from the list of those available and click **Save and apply**. Alternatively, to create a new PSTN usage, click **Add** and when completed, select it and click **Save and apply**.

   f. Click **Save**.

5. Repeat the process to define any additional voice routes required.

6. Once you have added the voice routes required, check they are in the required order. If necessary, select a record and click **Move up** or **Move down**.

Next steps

- Proceed to Configure Emergency Calling on page 58.

Related links

Creating Voice Routes on page 55

Chapter 13: Configure Emergency Calling

You can use emergency policies in MS Teams to set up emergency numbers and specify how MS Teams routes emergency calls.

- You can use the global policy or create and assign custom policies. Users automatically use the global policy unless you create and assign them a custom policy.
- For more information, refer to https://docs.microsoft.com/en-us/microsoftteams/manage-emergency-call-routing-policies.

Related links

Configuring an Emergency Policy on page 58

Assigning an Emergency Policy to Users on page 59

Configuring an Emergency Policy

Use the following process to configure an emergency policy.

Procedure

1. Login to the MS Teams admin portal at https://admin.teams.microsoft.com/direct-routing/v2.
2. Select **Voice** and then **Emergency policies**.
3. Either click **Add** to add a new policy or select an existing policy and click **Edit**.
   - MS Teams uses the Global policy for all users without an assign an emergency policy.
4. If adding a new policy, enter a unique descriptive name for the policy and, if necessary, add a description.
5. If **Dynamic emergency calling** is enabled, Teams retrieves policy and location information from the service and includes that information as part of the emergency call.
6. Define the emergency numbers required:
   a. Click **Add**.
   b. In the **Emergency dial string**, enter the main emergency number that users will dial. For example: *112*.
   c. You can define an optional **Emergency dial mask**. This can contain any other numbers that MS Teams should automatically translated to the **Emergency dial**

string. To add multiple additional numbers to the mask, separate each number with a semi-colon. For example: *999;911*.

- For locales where all emergency calls go to the same emergency service operator, using an Emergency dial mask simplifies configuration.
- Use of a mask also allows you to include numbers that visitors from locales might dial for emergency calls.
- For locales where emergency calls go to different operators based on the number dialed, repeat this step to add a separate Emergency dial string for each different operator service rather than using masks.

d. Select a **PSTN usage record**. MS Teams uses the record to determine which voice route to use for emergency calls.

7. Click **Save**.
8. If using an emergency policy other than the global one, assign the policy to the required users. See Assigning an Emergency Policy to Users on page 59.

Next steps

- Proceed to Assigning an Emergency Policy to Users on page 59.

Related links

Configure Emergency Calling on page 58

Assigning an Emergency Policy to Users

Use the following process to assign an emergency call routing policy to a user. This is necessary if you have configured your emergency settings in a policy other than the global emergency routing policy.

- This process assigns a policy to individual users and is an example. You can also assign policies to groups of users or globally. For more information, see https://docs.microsoft.com/en-us/microsoftteams/assign-policies-users-and-groups.

Procedure

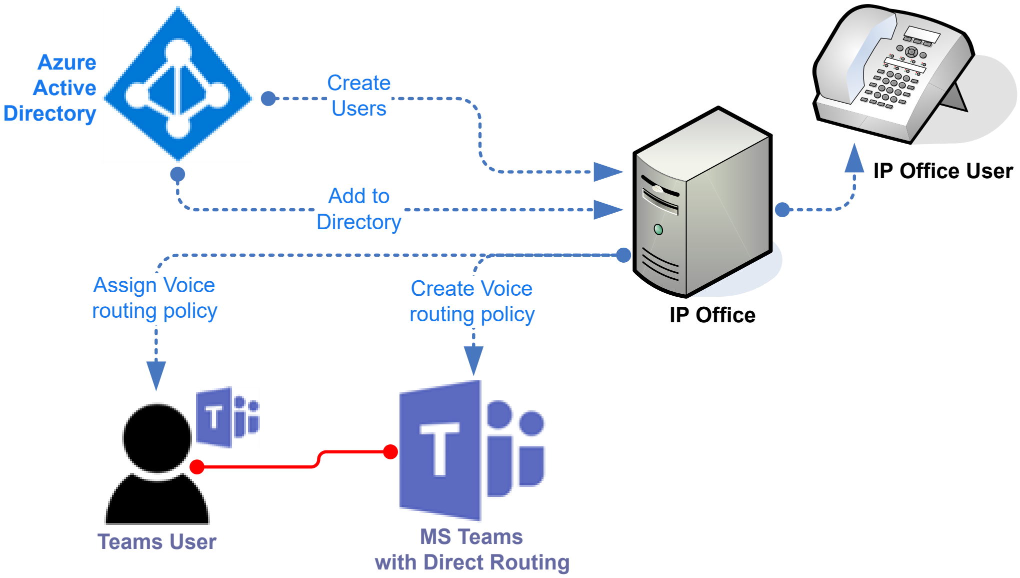
1. Login to the MS Teams admin portal at https://admin.teams.microsoft.com.
2. Select **Users**.
3. Select the required user or users.
4. Click **Edit settings**.
5. Select the **Policies** tab and click **Edit**.
6. In the **Emergency call routing policy** drop-down, select the policy to assigned to the user or users and click **Apply**.

Related links

Configure Emergency Calling on page 58

Chapter 14: Azure Active Directory Synchronization

This section provides notes for Azure Active Directory synchronization to support systems using direct routing. This synchronization can perform a range of actions, using multiple separate synchronization entries if necessary.



- **Directory Synchronization -** Add the name and telephone number details of MS Teams only users to the IP Office system directory. Also add the contact details of other contacts that the customer stores in Azure Active Directory. Note: Avaya one-X Portal does not display MS Teams only users in its directories.
- **MS Teams Voice Routing Policy Synchronization -** For MS Teams users, assign which voice routing policy the user uses.
- **IP Office User Creation and Maintenance -** The IP Office can use user details from Azure Active Directory to create and update users and extensions entries in its configuration. The This IP Office can use this to create IP Office only and MS Teams+IP Office users.

User Type	Directory Sync	Routing Policy Sync	Create/Maintain IP Office Users
MS Teams Only Users	✔	✔	–

Table continues…

User Type	Directory Sync	Routing Policy Sync	Create/Maintain IP Office Users
IP Office Only Users	–	–	✔
MS Teams+IP Office Users	–	✔	✔

Related links

Preventing Manual URI Editing on page 62
Enabling Directory Synchronization on page 63
Configuring Azure Active Directory App Registration on page 63
Configuring a Teams Administrator on page 64
Creating User and Extension Templates on page 65
Creating User Provisioning Rules on page 66
Setting Up a Direct Routing Synchronization Process on page 67

Preventing Manual URI Editing

If the IP Office is using automatic Azure Active Directory synchronization to create and update MS Teams+IP Office users, you must prevent the manual editing of the user **MS Team URI** settings.

Procedure

1. Using IP Office Manager or IP Office Web Manager, load the IP Office system configuration.
2. Select **System** or **System Settings** > **System**.
3. Select the **Telephony** settings and then select the **MS Teams** tab.
4. To prevent manual editing of **MS Teams URI** settings, select **Auto Populate MS Teams Data**.
5. Click **Update** or **OK**.
6. If using IP Office Manager, save the configuration changes back to the IP Office system.

Next steps

- Proceed to Enabling Directory Synchronization on page 63.

Related links

Azure Active Directory Synchronization on page 61

Enabling Directory Synchronization

Directory synchronization with Azure Active Directory uses a service called Collaboration Service running on the IP Office server. For IP500 V2 systems, an IP Office Application Server or Unified Communications Module provides the service.

Before you begin

- Preventing Manual URI Editing on page 62.

Procedure

1. Using IP Office Manager or IP Office Web Manager, load the IP Office configuration.
2. Select **System** or **System Settings** > **System**. If necessary, select the required server in the network.
3. Select **Directory Services**.
4. Select **HTTP**.
5. Set the **Directory Type** to **Collaboration Services**.
6. The default **Resync Interval** is set to 3600 seconds (1 hour). Adjust the value if required.
7. Click **OK** or **Update** to save the changes.
8. If using IP Office Manager, save the configuration back to the IP Office system.

Next steps

- Proceed to Configuring Azure Active Directory App Registration on page 63.

Related links

Azure Active Directory Synchronization on page 61

Configuring Azure Active Directory App Registration

To connect the IP Office to Azure Active Directory, you must register an application ('app') in Azure Active Directory. During that process, Azure Active Directory assigns the app a *Client ID* and *Client Secret*. The IP Office uses those values to connect to Azure Active Directory.

In addition, IP Office connections require the customer's *Tenant ID* and, if setting up a connection for a specific group of users, that group's *Group ID*.

Before you begin

- Configuring Azure Active Directory App Registration on page 63.

Procedure

1. Using a user account with full administrator rights, login to Azure Active Directory at https://portal.azure.com.
2. Search for and select **Azure Active Directory**.

3. Select **Overview**.
4. The **Basic Information** section includes the *Tenant ID* required for IP Office connections. Copy the value to a text file.
5. If planning to create a connection for a particular group of users:
   a. Select **Groups** and locate the required group.
   b. Select the group. Select **Properties**.
   c. The **Object ID** shown next to the group name is the **Group ID** needed for the connection. Copy the value to the text file.
6. Select **App registrations**.
   a. Click **New registration**.
   b. For the **Display name**, enter a unique descriptive name such as `IPOSync`.
   c. Note the displayed **Application (client) ID**. This is the **Client ID** value required by the IP Office. Copy the value to the text file.
   d. Click the link next to **Client credentials**.
   e. Click **New client secret**.
   f. Copy the **Value** shown (not the **Secret ID**) to the text file.
7. Select **API Permissions**.

   Using the **Add a permission** option, add read permission for calendars and contacts. Add read all permission for the directory and groups.
8. You now have the information required to create connections between the IP Office and Azure Active Directory.

Next steps

- Proceed to Configuring a Teams Administrator on page 64.

Related links

Azure Active Directory Synchronization on page 61

Configuring a Teams Administrator

MS Teams only user synchronization uses the username and password of a user you have configured as the Teams Administrator in Azure Active Directory.

Before you begin

- Configuring Azure Active Directory App Registration on page 63.

Procedure

1. Create a new user whose name and password:
    a. Using a user account with administrator rights, login to Azure Active Directory at https://portal.azure.com.
    b. Search for and select **Azure Active Directory**.
    c. Select **Users** and add a new user and set a unique descriptive name for their function. For example, `IPOLink`. This user does not require any user licenses.
    d. Select **Assigned Roles**.
    e. Select **Add Assignment**.
    f. Select **Teams Administrator** and click **Add**.
2. After creating the user:
    a. Login at https://admin.teams.microsoft.com using the user details and set a password when prompted. Do not enable multi-factor authentication.
    b. If a password expiry policy is in place for users, you must disable it for this user. Note the user's **UserID**. Then, using PowerShell, connect to Azure Active Directory and use the following command:

    ```
    Get -AzureADUser -ObjectId <user ID> -PasswordPolicies
    DisablePasswordExpiration
    ```

Next steps

- Proceed to Creating User and Extension Templates on page 65.

Related links

Azure Active Directory Synchronization on page 61

Creating User and Extension Templates

When creating new IP Office users, the synchronization process uses a 'user provisioning rule' to define element such as the starting extension number and extension type. The user provisioning rule can also use extension and user templates to automatically configure settings not taken from Azure Active Directory details. If you do not use templates, then those settings use the IP Office system default values.

- The process below uses the template management menus to create or upload new templates. You can also create templates from existing users or extensions by selecting them and then clicking **Save As Template**.
- For MS Teams+IP Office users, the user template used must configure the user's **Profile** setting to one of the following and enable the **Enable MS Teams Client** setting.
    - **On subscription mode IP Office systems:**

      The IP Office supports MS Teams+IP Office users using the **UC User** profile.

- **On PLDS licensed IP Officesystems:**

  The IP Office supports MS Teams+IP Office users using the **Office Worker**, **Teleworker** and **Power User** profiles.

- This process is not needed for MS Teams only user synchronization.

Before you begin

- Configuring a Teams Administrator on page 64.

Procedure

1. Using IP Office Web Manager, access the IP Office configuration.
2. Select **Call Management** and then either **Users** or **Extensions**.
3. Click **Actions** and select **Template Management**.
   1. To create a new template, click **+Add**. For extension templates, you also need to select the type of extension.
   2. You can use the menu to edit, rename and delete existing templates.
   3. You can also download the templates as `.xml` files.
   4. You can upload `.xml` template files that you have downloaded from another IP Office.

Next steps

- Proceed to Creating User Provisioning Rules on page 66.

Related links

Azure Active Directory Synchronization on page 61

Creating User Provisioning Rules

When using a connection to Azure Active Directory to create new IP Office users, the connection settings specify which IP Office 'user provisioning rule' to use. That rule:

- Sets the starting extension number for new users.
- Sets the extension type for the new users using either a specified extension template or specified extension type.
- Sets user settings, other than those taken from Azure Active Directory, for the new users using a user template. The IP Office applies default user settings if you do not specify a user template.
- Optionally configure on which IP Office in a network the IP Office creates each new user.

Before you begin

- Creating User and Extension Templates on page 65.

Procedure

1. Using IP Office Web Manager, access the IP Office system configuration.
2. Select **Solution**.
3. Select **Solution Settings** and then **User Synchronization**.
4. Click **+ADD** and select **User Synchronization using Microsoft Teams**.
5. Click **Manage User Provisioning Rules**.
6. Click **+Add User Provisioning Rule**.
7. Enter a name for the rule.
8. For an IP Office network, set how the synchronization process determines on which IP Office to create new users. The process can:
    - Use the **IP Office** field to select the IP Office system on which to create the users.
    - Use a field in the users Azure Active Directory settings to set the system name, FQDN or LAN1/LAN2 IP address of the required system.
    - Otherwise, the process creates all the new users on the primary server.
9. If not setting the extension numbers using a value received from Azure Active Directory, set the **Starting Extension** number. Otherwise, leave this field blank.
10. Select the required extension template or select an extension type.
    - If you select an extension type, the IP Office applies the default extension settings to the new users' extensions.
11. Select the required user template. If you do not select a user template, the IP Office applies default settings to the new users.
12. Click **Save**.

Next steps

- Proceed to Setting Up a Direct Routing Synchronization Process on page 67.

Related links

Azure Active Directory Synchronization on page 61

Setting Up a Direct Routing Synchronization Process

After configuring any templates and/or user provisioning rules required, you can use the following process to configure synchronization. You can configure multiple synchronization settings if necessary.

Before you begin

- Creating User Provisioning Rules on page 66.

Procedure

1. Using IP Office Web Manager, access the IP Office system configuration.
2. Select **Solution**.
3. Select **Solution Settings** and then **User Synchronization**.
4. Click **+ADD** and select **User Synchronization using Microsoft Teams**.
5. Using IP Office Web Manager, access the IP Office system configuration.
6. Select **Solution**.
7. Select **Solution Settings** and then **User Synchronization**.
8. Click **+ADD** and select **User Synchronization using Microsoft Teams**.
9. Select the **Connect to Directory Service** tab.
    a. Enter a **Configuration Name** to identify the purpose for this connection. For example, `DirectRoutingSync`.

    b. For **Collaboration Client**, select **Direct Call Routing**.

    c. Use **User Synchronization** type to select the roles that the synchronization should perform. The selection affects the additional fields and tabs available:

Setting	Description
IP Office Users Only	Support the creation, updating and deletion of IP Office users to match the users in Azure Active Directory.
Microsoft Teams Users Only	Add details of the MS Teams only users to the IP Office user directory. • Also update their settings in MS Teams with any Office telephone number configured for them in Azure Active Directory. • Optionally, also assign a specific voice routing policy to the MS Teams user settings.
Both	Perform a combination of the above actions. • You must configure the template to use a **Profile** that support MS Teams+IP Office users (**Office Worker**, **Teleworker**, **Power User** or **UC User**) and have **Enable MS Teams Client** enabled.

    d. Select the type of **Directory**:

    - Use **Tenant Directory** to manage IP Office entries for all the customer's Azure Active Directory users.
    - Use **Group Directory** to manage IP Office entries for just those users who are members of a specific Azure Active Directory group.

    e. Enter the details obtained from Azure Active Directory into the matching fields.

    f. Click **Test Connection** and wait a couple of minutes.

    g. If successful, continue with the configuration. Otherwise, check and adjust the settings.

10. **If using MS Teams Users Only:** You must set the Azure Active Directory fields from which to take the user's name and number information. For other modes, the values are set through the **Synchronize User Fields** settings below.

    a. In the **Name Attribute** field, enter the Azure Active Directory user field that synchronization should use to populate the name in the IP Office system directory. The default is to use the `displayName` from Azure Active Directory.

    b. The synchronization process uses the Azure Active Directory `businessPhones` field for the user telephone number.

11. **If using MS Teams Users Only or Both:** You need to enter the details of the MS Teams admin user for the IP Office connection to Azure Active Directory. In addition, you can set the direct routing settings that MS Teams applies to the users.

    a. In the **Microsoft Teams PowerShell Username** and **Microsoft Teams PowerShell Password** fields, enter the username and password of the Azure Active Directory user configured as a MS Teams administrator.

    b. You can use the **Voice Routing Policy Name** and **Voice Routing Policy Usage** fields to specify the voice routing policy assigned to the users.

       - The usage must already exist in MS Teams admin.
       - If the policy does not already exist, MS Teams creates it and adds the usage to it. MS Teams assigned the policy to the users.
       - If the policy already exists, MS Teams assigns it to the users with no changes to the usages it contains. MS Teams ignores the **Voice Routing Policy Usage** value in the IP Office sync settings.

12. **If using IP Office Users Only or Both:** Specify which fields in Azure Active Directory map onto IP Office user settings, and how the synchronization process uses the new values. Select the **Synchronize User Fields** tab:

    a. Use the drop-down menus in the **Microsoft Teams Fields** column to select which Azure Active Directory field the synchronization process will use to set the value for the matching IP Office configuration settings.

       - Selecting fields for the **User Identification** and **Name** fields is mandatory. All other fields are optional and will use the values defined by the user/extension templates or default IP Office values.
       - The **User Identification** must be unique. The IP Office uses this to ensure that it applies future synchronization update/delete actions to the correct users.
       - You can use the final pair of drop-downs to set on which IP Office system in a network the synchronization process creates new users. If not set, you can specify the required IP Office system in the user provisioning rule. Otherwise, the synchronization process creates new users on the primary system.

    b. Select which functions the synchronization process performs. You can select more than one function:

       - **New** - Create new IP Office user and extension records for any user whose user identification is not already present.

- **Update** - Update the settings, if required, of the user with the same user identification.
- **Delete** - Delete the user and extension records for any users whose user identification is not present in the latest synchronization.

c. If you want the IP Office to regularly perform synchronization, click **Use Schedule** and define the required schedule.

d. Click **Preview Results**. The menu shows a summary of the changes that would occur. If necessary, amend the settings.

e. When complete, click **Synchronize**.

13. Click **Save**.

Related links

Azure Active Directory Synchronization on page 61

Part 4: ABSCE Configuration

Chapter 15: Creating SIGMA Scripts

The ASBCE uses SIGMA (Signal Manipulation) scripts to modify the content of SIP signaling headers.

Related links

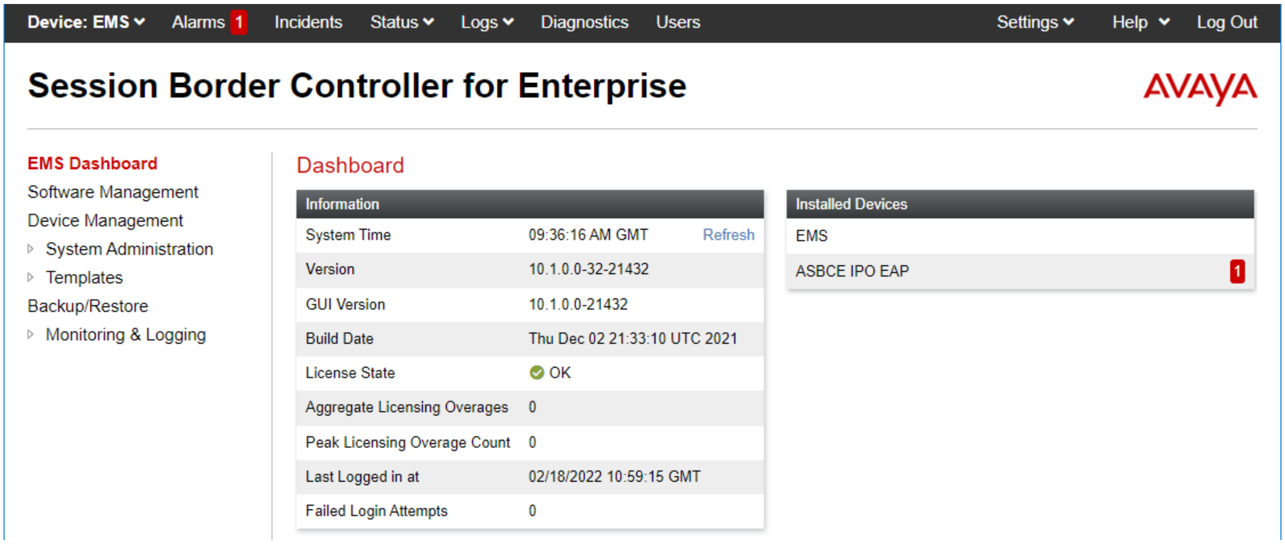
- Get the ASBCE Version on page 72
- Create the SIGMA Script Files on page 73
- The IP Office SIGMA Script on page 73
- The MS Teams SIGMA Script on page 74
- Upload the SIGMA Scripts on page 75

Get the ASBCE Version

You need the ASBCE version for customizing the SIGMA scripts. You should also check it to ensure that the ASBCE is running 10.1 plus Hotfix 1 or higher.

Procedure

After logging in to the ASBCE, note its version number in full. This must be 10.1 plus Hotfix 1 or higher.



Information	
System Time	09:36:16 AM GMT
Version	10.1.0.0-32-21432
GUI Version	10.1.0.0-21432
Build Date	Thu Dec 02 21:33:10 UTC 2021
License State	✓ OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	02/18/2022 10:59:15 GMT
Failed Login Attempts	0

Installed Devices	
EMS	
ASBCE IPO EAP	1

Next steps

- Proceed to Create the SIGMA Script Files on page 73.

Related links

Creating SIGMA Scripts on page 72

Create the SIGMA Script Files

The ASBCE uses SIGMA (Signal Manipulation) scripts to modify the content of SIP signaling headers.

Before you begin

- Get the ASBCE Version on page 72.

Procedure

1. On your PC, a text file containing the script for the IP Office
2. Then create a text file containing the SIGMA scription for MS Teams.

Next steps

- Proceed to Upload the SIGMA Scripts on page 75.

Related links

Creating SIGMA Scripts on page 72

The IP Office SIGMA Script

The following is a template for the SIGMA script used for the connection between the ASBCE and the IP Office. Use this template to create a text file on your PC.

```
within session "INVITE"
{
act on request where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK"
  {
    %ContactValue = %HEADERS["Contact"][1];
    %HEADERS["Record-Route"][1] = %ContactValue;
   }
}
```

Related links

Creating SIGMA Scripts on page 72

The MS Teams SIGMA Script

The following is a template for the SIGMA script used for the connection between the ASBCE and MS Teams. Use this template to create a text file on your PC.

In the sample script:

- Replace each instance of `<ASBCE_FQDN>` with the public FQDN of the ASBCE.
- Replace each instance of `<ASBCE_IP_ADDRESS>` with the public IP address to which DNS resolves the ASBCE FQDN above.
- Replace `<ASBCE_VERSION>` with `AVAYA SBCE-<version` where `<version>` is the **Version** value shown on the ASBCE's initial menu after logging in. See Get the ASBCE Version on page 72.

```
within session "all"
{
act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
  {
       %SDP[1].regex_replace("a=sendonly","a=inactive");
       %SDP[1].regex_replace("a=recvonly","a=inactive");
  }
}
within session "all"
{
act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
  {
        %HEADERS["Contact"][1].URI.HOST = "<ASBCE_FQDN>";
        %HEADERS["Record-Route"][1].URI.HOST = "<ASBCE_FQDN>";
  }
}
within session "all"
{
act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
  {
    %HEADERS["X-MS-SBC"][1] = "<ASBCE_VERSION>";
   }
}
within session "all"
{
act on message where %DIRECTION="INBOUND" and %ENTRY_POINT="PRE_ROUTING"
  {
    %HEADERS["Request_Line"][1].URI.HOST = "<ASBCE_IP_ADDRESS>";
        if (%HEADERS["Record-Route"][1].regex_match("<ASBCE_FQDN>")) then
        {
                %HEADERS["Record-Route"]
[1].regex_replace("<ASBCE_FQDN>","<ASBCE_IP_ADDRESS>");
        }
         if (%HEADERS["Record-Route"][2]. regex_match("<ASBCE_FQDN>")) then
        {
                %HEADERS["Record-Route"]
[1].regex_replace("<ASBCE_FQDN>","<ASBCE_IP_ADDRESS>");
        }
         if (%HEADERS["Route"][1].regex_match("<ASBCE_FQDN>")) then
        {
                %HEADERS["Route"][1].regex_replace("<ASBCE_FQDN>","<ASBCE_IP_ADDRESS>");
        }
         if (%HEADERS["Route"][2].regex_match("<ASBCE_FQDN>")) then
        {
                %HEADERS["Route"][2].regex_replace("<ASBCE_FQDN>","<ASBCE_IP_ADDRESS>");
        }
    }
}
within session "INVITE"
{
 act on response where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
    {
        if (%SDP[1].regex_match("c=IN IP4 0.0.0.0")) then
  {
       %SDP[1].regex_replace("c=IN IP4 0.0.0.0","c=IN IP4 <ASBCE_IP_ADDRESS>");
     }
  }
}
```

MS Teams SIGMA Script Additional values

You can use the MS Teams SIGMA script to perform optional number transformations. In the example below, the additional lines for the `From`, `To` and `Request Line` headers prefix matching numbers with +1.

```
act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
  {
        %HEADERS["Contact"][1].URI.HOST = "<ASBCE_FQDN>";
        %HEADERS["Record-Route"][1].URI.HOST = "<ASBCE_FQDN>";
        %HEADERS["From"][1].URI.USER.regex_replace("^214","+1214");
        %HEADERS["To"][1].URI.USER.regex_replace("^719","+1719");
        %HEADERS["Request_Line"][1].URI.USER.regex_replace("719","+1719");
  }
```

Related links

Creating SIGMA Scripts on page 72

Upload the SIGMA Scripts

Upload the two SIGMA script files to the ASBCE.

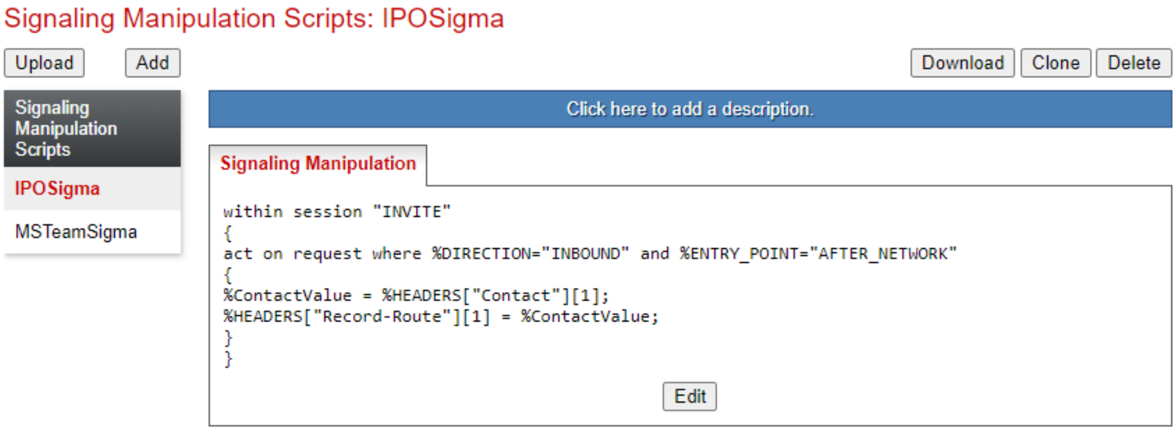
Before you begin

- Create the SIGMA Script Files on page 73.

Procedure

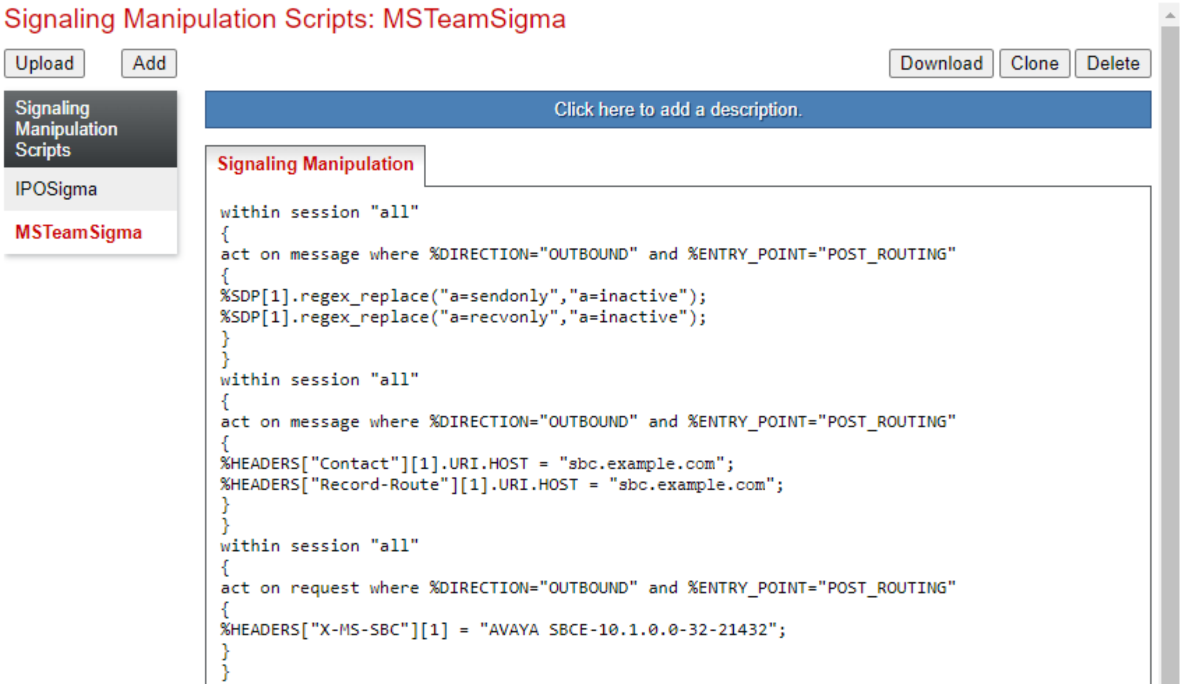
1. Select **Configuration Profiles** and then **Signaling Manipulation**.
2. Click **Upload**.
3. Enter a name and select the SIGMA file created for the IP Office.

4. Click **Upload**.


Signaling Manipulation Scripts: IPOSigma
Upload
Add
Download
Clone
Delete
Signaling Manipulation Scripts
IPOSigma
MSTeamSigma
Click here to add a description.
Signaling Manipulation
Edit

```
within session "INVITE"
{
act on request where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK"
{
%ContactValue = %HEADERS["Contact"][1];
%HEADERS["Record-Route"][1] = %ContactValue;
}
}
```

5. Click **Upload** again and select the SIGMA file created for MS Teams.


Signaling Manipulation Scripts: MSTeamSigma
Upload
Add
Download
Clone
Delete
Signaling Manipulation Scripts
IPOSigma
MSTeamSigma
Click here to add a description.
Signaling Manipulation

```
within session "all"
{
act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
{
%SDP[1].regex_replace("a=sendonly","a=inactive");
%SDP[1].regex_replace("a=recvonly","a=inactive");
}
}
within session "all"
{
act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
{
%HEADERS["Contact"][1].URI.HOST = "sbc.example.com";
%HEADERS["Record-Route"][1].URI.HOST = "sbc.example.com";
}
}
within session "all"
{
act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
{
%HEADERS["X-MS-SBC"][1] = "AVAYA SBCE-10.1.0.0-32-21432";
}
}
```

Next steps

- Proceed to Obtain the ASBCE Certificates on page 77.

Related links

Creating SIGMA Scripts on page 72

Chapter 16: Obtain the ASBCE Certificates

The ASBCE requires certificates from both MS Teams and the IP Office to validate the connections with each. These certificates, and their private key, must be in base-64 format

Related links

MS Teams Certificates on page 77
Downloading the IP Office Root Certificate on page 78
Generating an Identity Certificate for the ASBCE on page 80
Extracting the ASBCE Private Key and Identity Certificate on page 83
Adding the Root Certificates to the ASBCE on page 85
Adding the Identity Certificates to the ASBCE on page 86

MS Teams Certificates

To support MS Teams, the ASBCE requires the following certificates.

Microsoft Certificates

From Microsoft, the ASBCE requires the following certificates:

Certificate	Description
MS Teams Root Certificate	This is the root certificate used by Microsoft for MS Teams. • The certificate and details of the certificate can be obtained from https://cacerts.digicert.com/DigiCertGlobalRootG2.crt. • The examples in this document use the certificate name `DigiCertGlobalRootG2.crt`
ASBCE MS Teams Certificate	The ASBCE uses this certificate for its connection to MS Teams. • For details of how to request the certificate, refer to https://docs.microsoft.com/en-us/microsoftteams/direct-routing-plan#public-trusted-certificate-for-the-sbc. • The examples in this document use the certificate name `MSTeamsSBC.crt`.

IP Office Certificates

From the IP Office, the ASBCE requires the following certificates.

- If IP Office certificates are already present, for example if the ASBCE is supporting remote IP Office extensions, you can use the existing certificates.

Certificate	Description
IP Office Root Certificate	The IP Office uses this certificate for SIP TLS. • If the IP Office root certificate is self-signed, set the **Verification depth** to 1. If the certificate is from an external verification authority, set the **Verification Depth** to 2 (the length of certificate chain). • The examples in this document use the certificate is name `IPO_RootCA.pem`.
IP Office Identity Certificate for the ASBCE	The ASBCE uses this certificate to connect to the IP Office. It can either be an identity certificate for another server generated by the IP Office, or one provided by the same external CA as imported as a trusted certificate. • The examples in this document use the certificate name `IPO_SBCID.pem`.

Related links

Obtain the ASBCE Certificates on page 77

Downloading the IP Office Root Certificate

If the IP Office system is using a self-signed certificate, use one of the following processes to download the system's root certificate.

Related links

Obtain the ASBCE Certificates on page 77
Downloading the IP Office Root Certificate in IP Office Web Manager on page 78
Downloading the IP Office Root Certificate in IP Office Web Control/Platform View on page 79

Downloading the IP Office Root Certificate in IP Office Web Manager

If the IP Office system is using a self-signed certificates, use the following process to download the IP Office root certificate using IP Office Web Manager.

Procedure

1. Login to the system using IP Office Web Manager.
2. Select **Security** > **Security Settings**.
3. Select **Certificates**.
4. In the **Trusted Certificate Store**, locate the IP Office root CA certificate.
5. Click on the ⤓ download icon next to the certificate details and select **Yes**.

Next steps

Proceed to generating an ID certificate for the ASBCE:

- For IP Office subscription mode systems with Automatic Certificate Management enabled, see Generating an Identity Certificate using IP Office Web Manager on page 82.
- For other IP Office systems, see Generating an Identity Certificate using IP Office Web Control/Platform View on page 80.

Related links

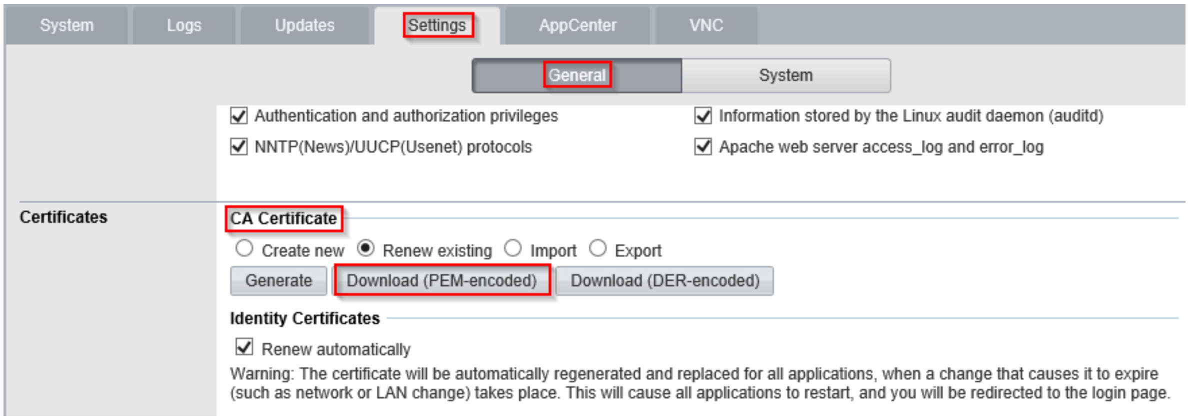
Downloading the IP Office Root Certificate on page 78

Downloading the IP Office Root Certificate in IP Office Web Control/Platform View

If the IP Office system is using a self-signed certificates, use the following process to download the IP Office root certificate using IP Office Web Control/Platform View.

Procedure

1. Login to the IP Office Web Control/Platform View by either:
   - In IP Office Web Manager, select the primary server. Click on ≡ and select **Platform View**.
   - Browse to `https://<IP Office IP address>:7071` and login as the `Administrator`.
2. Select the **Settings** tab and scroll down to **Certificates**.



☑ Authentication and authorization privileges
☑ Information stored by the Linux audit daemon (auditd)
☑ NNTP(News)/UUCP(Usenet) protocols
☑ Apache web server access_log and error_log

Certificates

CA Certificate

○ Create new ● Renew existing ○ Import ○ Export

Identity Certificates

☑ Renew automatically

Warning: The certificate will be automatically regenerated and replaced for all applications, when a change that causes it to expire (such as network or LAN change) takes place. This will cause all applications to restart, and you will be redirected to the login page.

3. Under **CA Certificate**, click on **Download (PEM-encoded)** and save the `root_ca.pem` file to your PC.

Next steps

Proceed to generating an ID certificate for the ASBCE:

- For IP Office subscription mode systems with Automatic Certificate Management enabled, see Generating an Identity Certificate using IP Office Web Manager on page 82.
- For other IP Office systems, see Generating an Identity Certificate using IP Office Web Control/Platform View on page 80.

Related links

Downloading the IP Office Root Certificate on page 78

Generating an Identity Certificate for the ASBCE

When the IP Office is using self-signed certificates, it can also generate an identity certificate for the ASBCE to use for its connections to the IP Office.

Related links

Obtain the ASBCE Certificates on page 77

Generating an Identity Certificate using IP Office Web Control/Platform View on page 80

Generating an Identity Certificate using IP Office Web Manager on page 82

Generating an Identity Certificate using IP Office Web Control/Platform View

When the IP Office is using self-signed certificates, it can also generate an identity certificate for the ASBCE to use for its connections to the IP Office.

- For IP Office subscription mode systems using **Automatic Certificate Management**, see Generating an Identity Certificate using IP Office Web Manager on page 82.

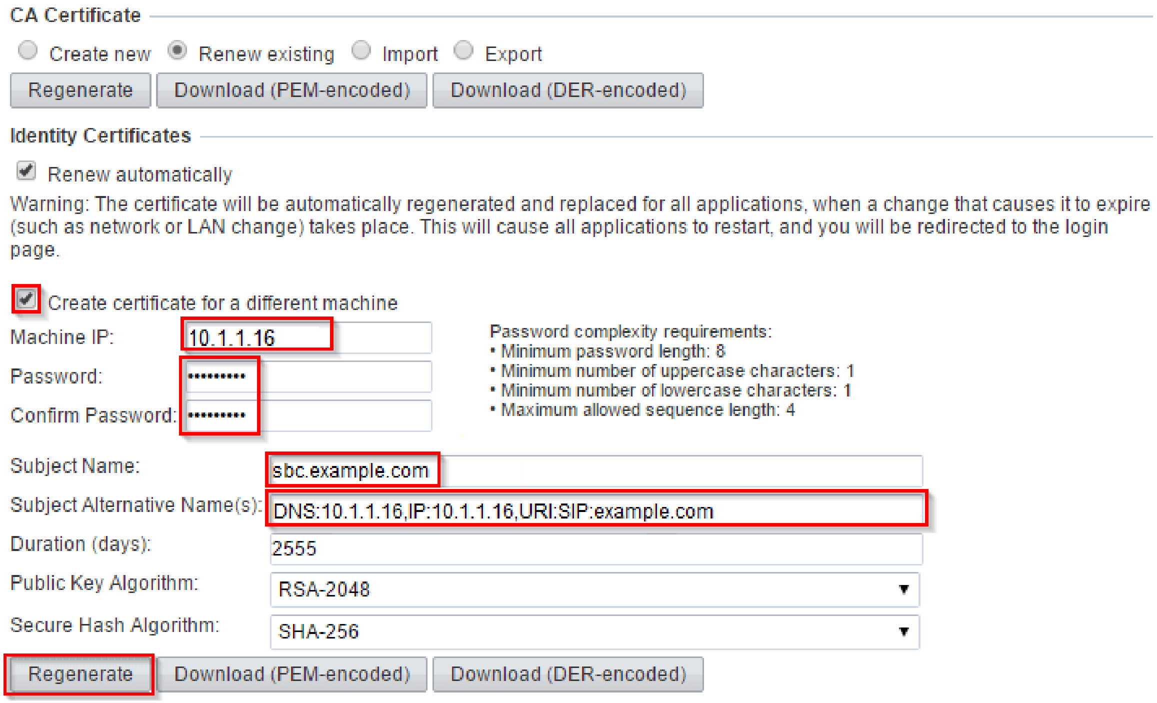
Before you begin

- Downloading the IP Office Root Certificate in IP Office Web Control/Platform View on page 79.

Procedure

1. Login to the IP Office Web Control/Platform View by either:
   - In IP Office Web Manager, select the primary server. Click on ≡ and select **Platform View**.
   - Browse to `https://<IP Office IP address>:7071` and login as the `Administrator`.
2. Go to **Settings** tab and scroll down to **Certificates**.

3. Check **Create certificate for a different machine**.



CA Certificate

○ Create new ● Renew existing ○ Import ○ Export

Identity Certificates

☑ Renew automatically

Warning: The certificate will be automatically regenerated and replaced for all applications, when a change that causes it to expire (such as network or LAN change) takes place. This will cause all applications to restart, and you will be redirected to the login page.

☑ Create certificate for a different machine

Machine IP: 10.1.1.16

Password: •••••••••

Confirm Password: •••••••••

Password complexity requirements:
• Minimum password length: 8
• Minimum number of uppercase characters: 1
• Minimum number of lowercase characters: 1
• Maximum allowed sequence length: 4

Subject Name: sbc.example.com

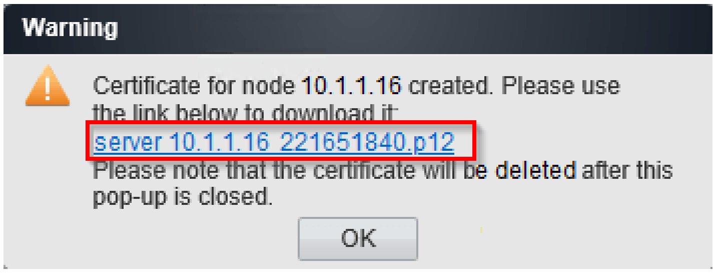
Subject Alternative Name(s): DNS:10.1.1.16,IP:10.1.1.16,URI:SIP:example.com

Duration (days): 2555

Public Key Algorithm: RSA-2048

Secure Hash Algorithm: SHA-256

4. Enter the following data:
   a. **Machine IP** - Enter the internal IP address of the ASBCE. That is, either the A1 or A2 interface of the ASBCE to which the IP Office connects.
   b. **Password** - Enter a password to encrypt the certificate and key.
   c. **Subject Name** - Enter the FQDN of the ASBCE.
   d. **Subject Alternative Name(s)** - Enter comma separate values for the `DNS:<FQDN>` and `IP:<IP address>`.
5. Click **Regenerate**.
6. Click on the link in the popup window and save the file.



Warning

Certificate for node 10.1.1.16 created. Please use the link below to download it:
server 10.1.1.16 221651840.p12
Please note that the certificate will be deleted after this pop-up is closed.

Next steps

- Proceed to Extracting the ASBCE Private Key and Identity Certificate on page 83.

Related links

Generating an Identity Certificate for the ASBCE on page 80

Generating an Identity Certificate using IP Office Web Manager

When the IP Office is using self-signed certificates, it can also generate an identity certificate for the ASBCE to use for its connections to the IP Office.

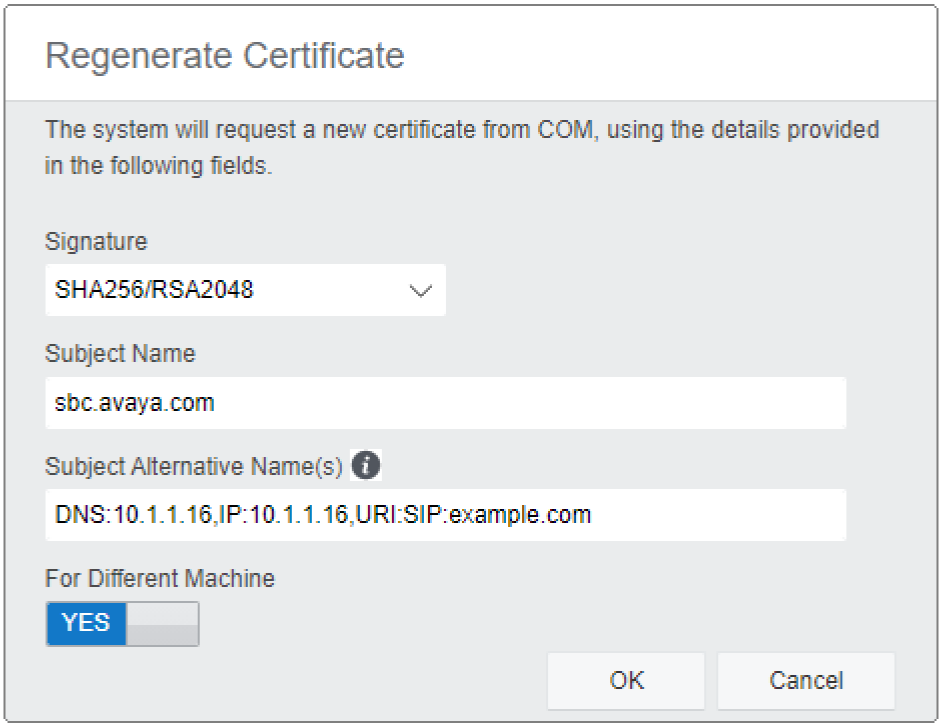
- This process is only for subscription mode IP Office systems using **Automatic Certificate Management**. For other systems, see Generating an Identity Certificate using IP Office Web Manager on page 82.

Before you begin

- Downloading the IP Office Root Certificate in IP Office Web Control/Platform View on page 79.

Procedure

1. Login to IP Office Web Manager for the subscription mode IP Office system.
2. Select **Security** > **Security Settings**.
3. If the system is in a Server Edition network, click on the ✎ next to the primary server.
4. Select **Certificates**.
5. Click **Regenerate**.
6. Enable **For Different Machine**.



Regenerate Certificate

The system will request a new certificate from COM, using the details provided in the following fields.

Signature: SHA256/RSA2048

Subject Name: sbc.avaya.com

Subject Alternative Name(s): DNS:10.1.1.16,IP:10.1.1.16,URI:SIP:example.com

For Different Machine: YES

7. In **Subject Name** enter the FQDN of the ASBCE.
8. In **Subject Alternative Name(s)**, enter any additional values for other IP Office servers and services to which the ASBCE may also need to connect.

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.

Next steps

- Proceed to Extracting the ASBCE Private Key and Identity Certificate on page 83.

Related links

Generating an Identity Certificate for the ASBCE on page 80

Extracting the ASBCE Private Key and Identity Certificate

The identity certificate created for the ASBCE from the IP Office is a single file. For ASBCE configuration, you must split it into two files; a certificate file and a private key for the certificate.

Before you begin

- Downloading the IP Office Root Certificate in IP Office Web Control/Platform View on page 79.

Procedure

1. Using SFTP, 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 `/home/ipcs` directory.
3. Using SSH, login to the ASBCE management IP using port 222 and `ipcs` login.
4. Enter the command `su root` or `su -root` and enter the ASBCE root password.
5. Enter the following commands:
   - When prompted for a password or PEM pass phrase, enter the password specified when generating the certificate file.
   - To enter special characters in the password, you must prefix the character with a `\`. For example, to enter a `@` you must type `\@` in the command line.
   - **IP Office Web Control/Platform View Certificate:** Use the following steps for a certificate generated using IP Office Web Control/Platform View:
     a. `openssl pkcs12 -in SBCE_ID.p12 -out SBCE_ID.crt -nokeys -clcerts`
     b. `openssl pkcs12 -in SBCE_ID.p12 -out SBCE_ID.key -nocerts`

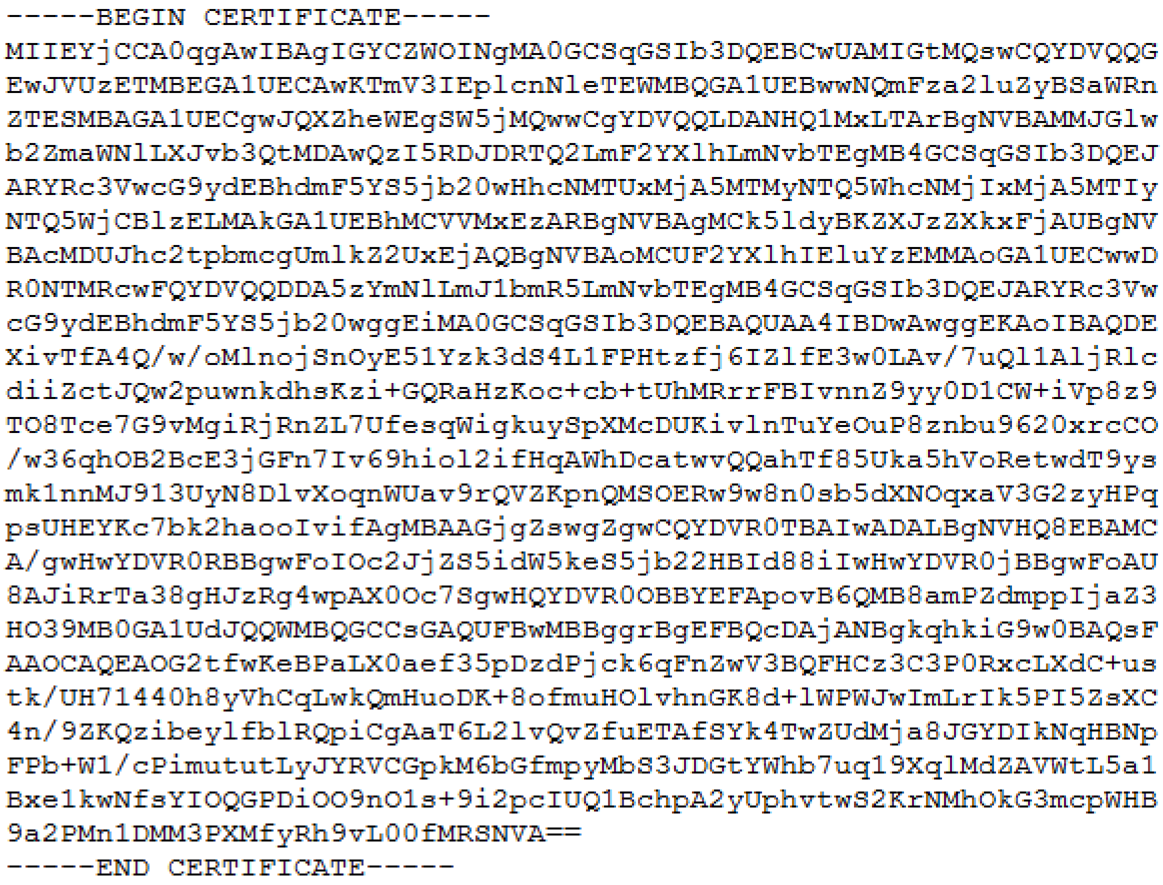
- **IP Office Web Manager Certificate:** Use the following steps for a certificate generated using IP Office Web Manager.

    a. `openssl enc -base64 -d -in SBCE_ID.p12 -out SBCE_ID_BIN.p12 -A`

    b. `openssl pkcs12 -in SBCE_ID_BIN.p12 -out SBCE_ID.crt -nokeys -clcerts`

    c. `openssl pkcs12 -in SBCE_ID_BIN.p12 -out SBCE_ID.key -nocerts`

6. Copy the `SBCE_ID.crt` and `SBCE_ID.key` files from the ASBCE to your PC.
7. Open `SBCE_ID.crt` in WordPad on your PC.
8. Remove all lines except those which are between and including the first `BEGIN CERTIFICATE` and `END CERTIFICATE` lines. The resulting file will look like the following:



```
-----BEGIN CERTIFICATE-----
MIIEYjCCA0qgAwIBAgIGYCZWOINgMA0GCSqGSIb3DQEBCwUAMIGtMQswCQYDVQQG
EwJVUzETMBEGA1UECAwKTmV3IEplcnNleTEWMBQGA1UEBwwNQmFza2luZyBSaWRn
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/UH7144Oh8yVhCqLwkQmHuoDK+8ofmuHOlvhnGK8d+lWPWJwImLrIk5PI5ZsXC
4n/9ZKQzibeylfblRQpiCgAaT6L2lvQvZfuETAfSYk4TwZUdMja8JGYDIkNqHBNp
FPb+W1/cPimututLyJYRVCGpkM6bGfmpyMbS3JDGtYWhb7uq19XqlMdZAVWtL5a1
Bxe1kwNfsYIOQGPDiOO9nO1s+9i2pcIUQ1BchpA2yUphvtwS2KrNMhOkG3mcpWHB
9a2PMn1DMM3PXMfyRh9vL00fMRSNVA==
-----END CERTIFICATE-----
```

Next steps

- Proceed to Adding the Root Certificates to the ASBCE on page 85.

Related links

Obtain the ASBCE Certificates on page 77

Adding the Root Certificates to the ASBCE

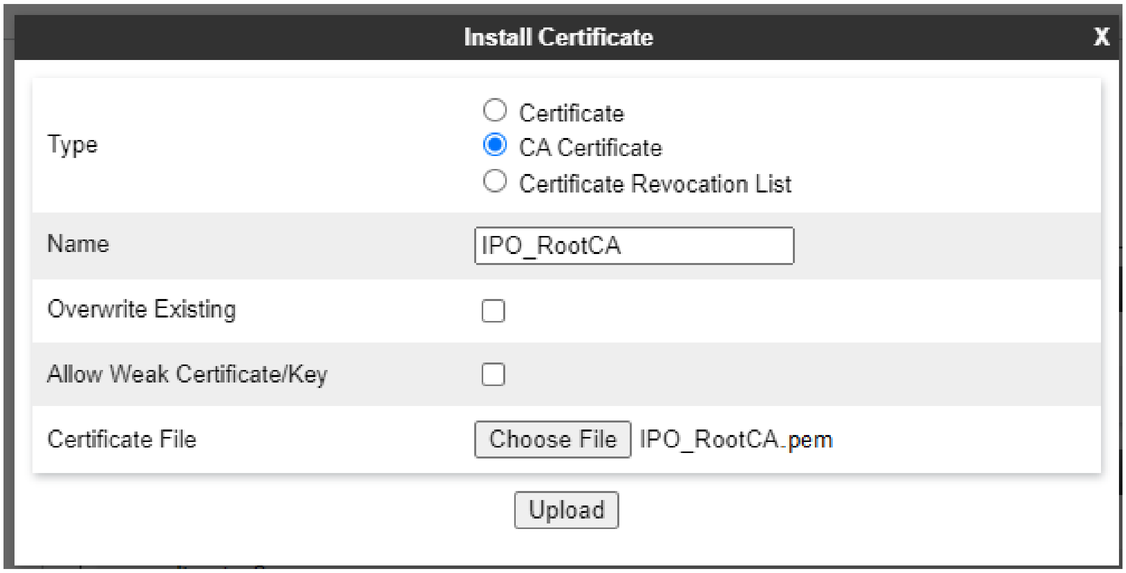
The following process adds the MS Teams and IP Office root certificates to the ASBCE.

Before you begin

- Extracting the ASBCE Private Key and Identity Certificate on page 83.

Procedure

1. Login to ASBCE web interface.
2. Go to **TLS Management** > **Certificates**.
3. For the IP Office root certificate:
    a. Click **Install**.

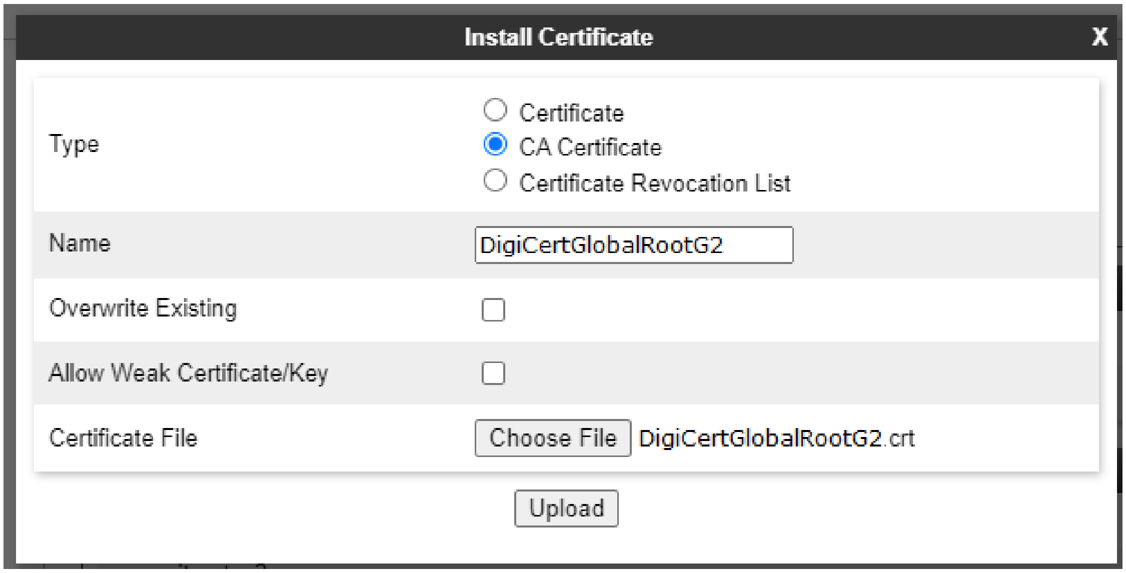


Type	○ Certificate ● CA Certificate ○ Certificate Revocation List
Name	IPO_RootCA
Overwrite Existing	□
Allow Weak Certificate/Key	□
Certificate File	Choose File IPO_RootCA.pem

    b. **Type** - Select **CA Certificate**.
    c. **Name** - Enter a unique descriptive name for the root CA certificate.
    d. **Allow Weak Certificate/Key** - Enable this option.
    e. **Certificate File** - Click **Choose File** and select the IP Office certificate file. For our example, this is the `IPO_RootCA.pem` certificate file.
    f. Click **Upload**. If the ASBCE displays a warning that this is a self-signed certificate, click **Proceed**.
    g. The ASBCE displays the certificate. Click **Install** and then **Finish**.

4. For the MS Teams root certificate:

   Repeat the process for the MS Teams root certificate. For our example, this is the `DigiCertGlobalRootG2.crt` certificate file.

   Install Certificate

Type	○ Certificate ● CA Certificate ○ Certificate Revocation List
Name	DigiCertGlobalRootG2
Overwrite Existing	□
Allow Weak Certificate/Key	□
Certificate File	Choose File DigiCertGlobalRootG2.crt

5. Click **Install** and then **Finish**.

Next steps

- Proceed to Adding the Identity Certificates to the ASBCE on page 86.

Related links

Obtain the ASBCE Certificates on page 77

Adding the Identity Certificates to the ASBCE

You need to add the MS Teams and IP Office identity certificates to the ASBCE.

Before you begin

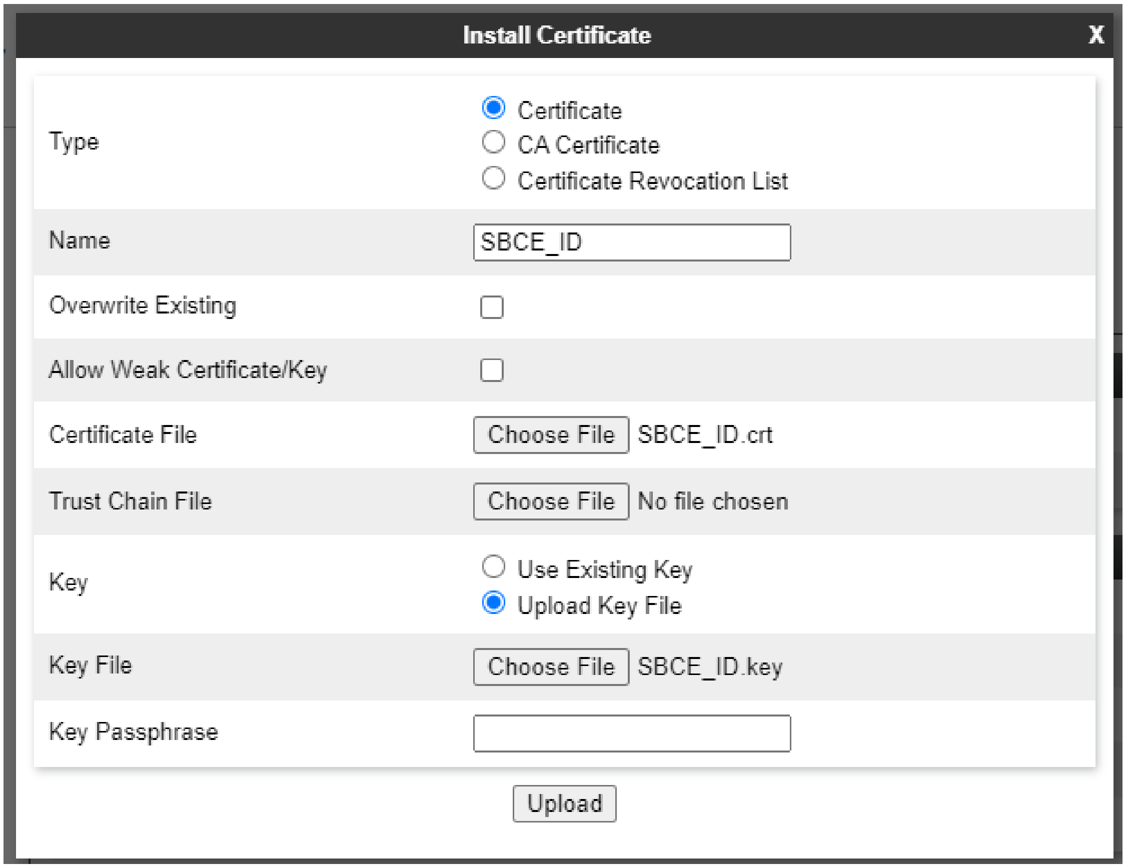
- Adding the Root Certificates to the ASBCE on page 85.

Procedure

1. Login to ASBCE web interface.
2. Go to **TLS Management** > **Certificates**.

3. Add the IP Office identity certificate:

   a. Click **Install**.



Install Certificate X

Type	● Certificate ○ CA Certificate ○ Certificate Revocation List
Name	SBCE_ID
Overwrite Existing	□
Allow Weak Certificate/Key	□
Certificate File	Choose File SBCE_ID.crt
Trust Chain File	Choose File No file chosen
Key	○ Use Existing Key ● Upload Key File
Key File	Choose File SBCE_ID.key
Key Passphrase	

   b. **Type** - Select **Certificate**.

   c. **Name** - Enter a unique descriptive name for the certificate.

   d. **Certificate File** - Click **Choose File** and select the IP Office identity certificate.

   e. **Trust Chain File** - Leave this field empty.

   f. **Key** - Select **Upload Key File**.

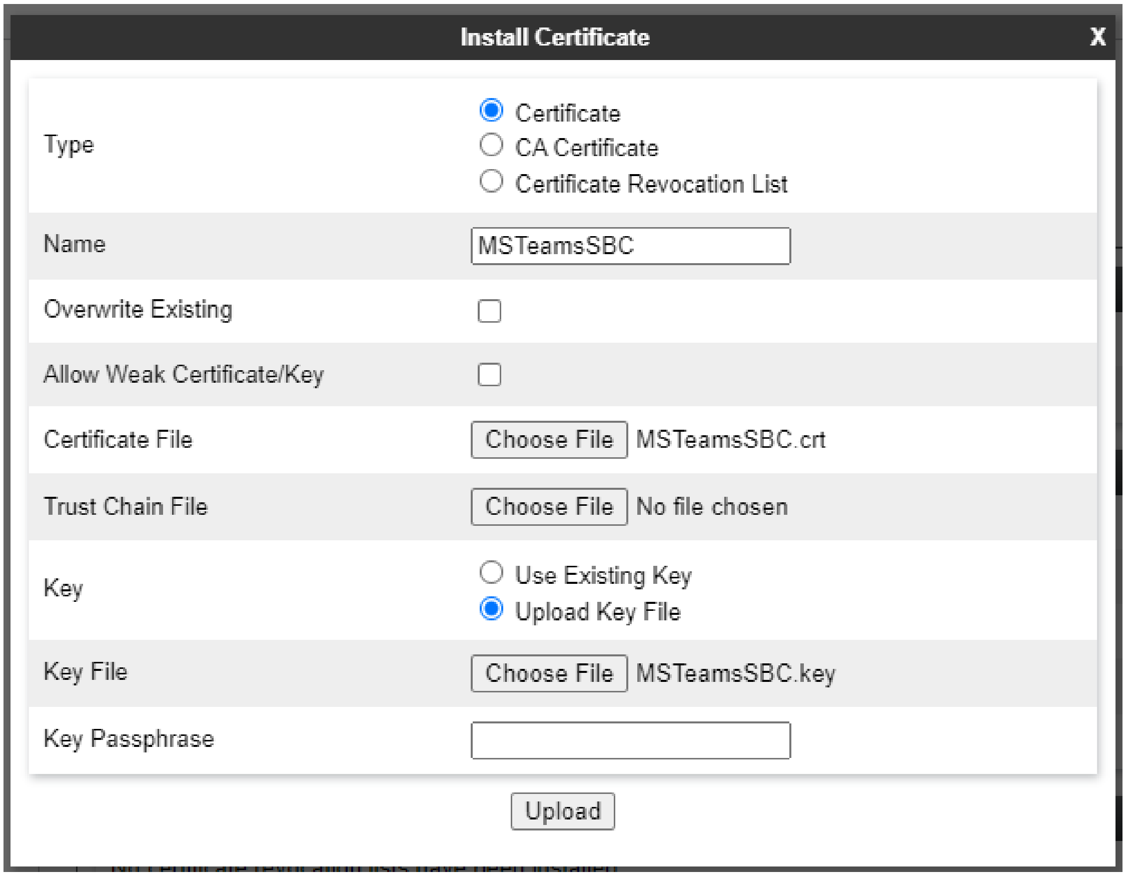
   g. **Key File** - Click **Choose File** and select the private key file for the IP Office identity certificate.

   h. Click **Upload**.

   i. Click **Install** and then **Finish**.

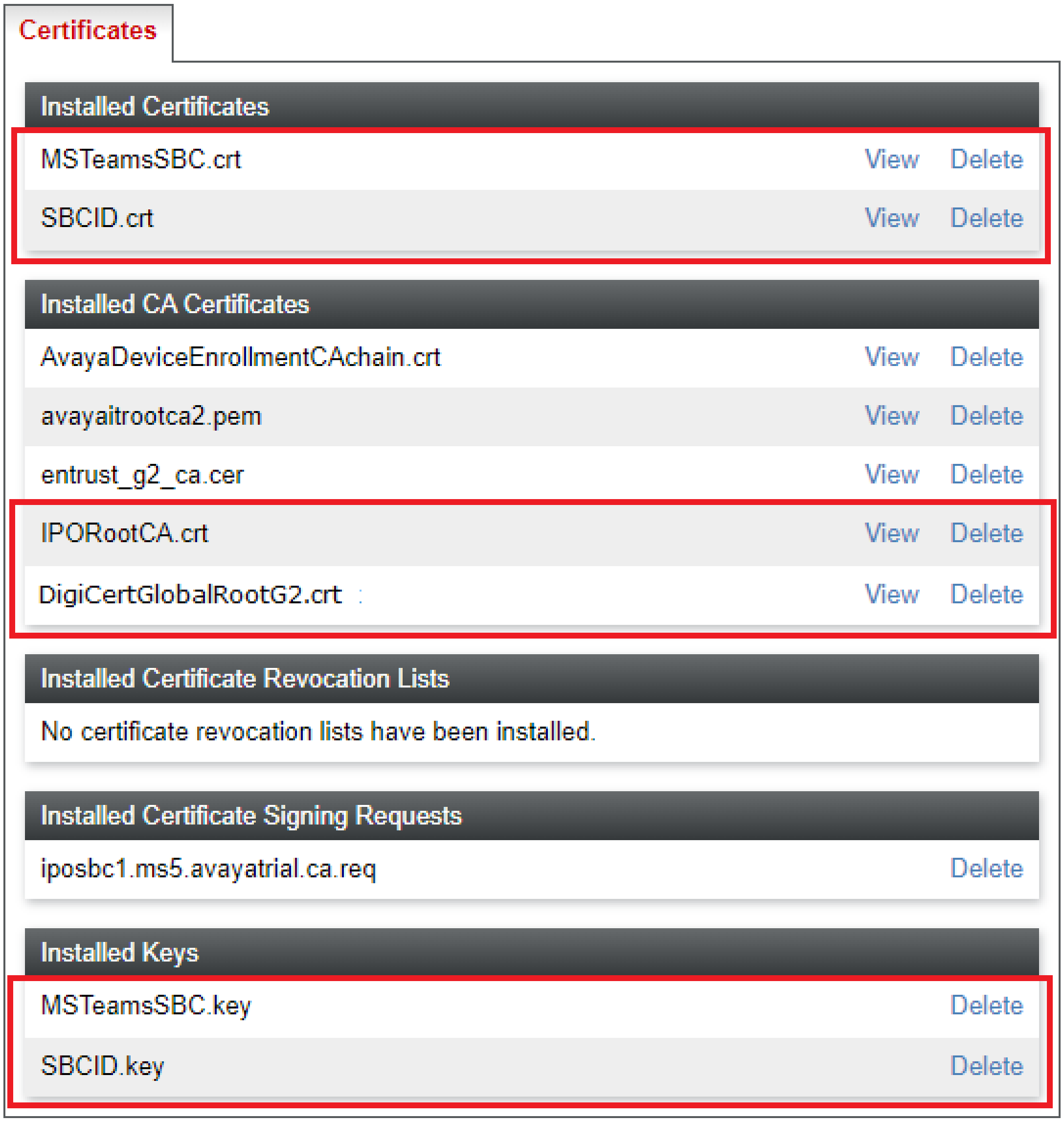
4. Add the MS Teams identity certificate:

   Repeat the process for the MS Teams root certificate.



Type	● Certificate ○ CA Certificate ○ Certificate Revocation List
Name	MSTeamsSBC
Overwrite Existing	□
Allow Weak Certificate/Key	□
Certificate File	Choose File MSTeamsSBC.crt
Trust Chain File	Choose File No file chosen
Key	○ Use Existing Key ● Upload Key File
Key File	Choose File MSTeamsSBC.key
Key Passphrase	

5. Check that the certificates display now lists the 2 root certificates, 2 identity certificates and 2 certificate keys.



Certificates

Installed Certificates

MSTeamsSBC.crt View Delete

SBCID.crt View Delete

Installed CA Certificates

AvayaDeviceEnrollmentCAchain.crt View Delete

avayaitrootca2.pem View Delete

entrust_g2_ca.cer View Delete

IPORootCA.crt View Delete

DigiCertGlobalRootG2.crt View Delete

Installed Certificate Revocation Lists

No certificate revocation lists have been installed.

Installed Certificate Signing Requests

iposbc1.ms5.avayatrial.ca.req Delete

Installed Keys

MSTeamsSBC.key Delete

SBCID.key Delete

Next steps

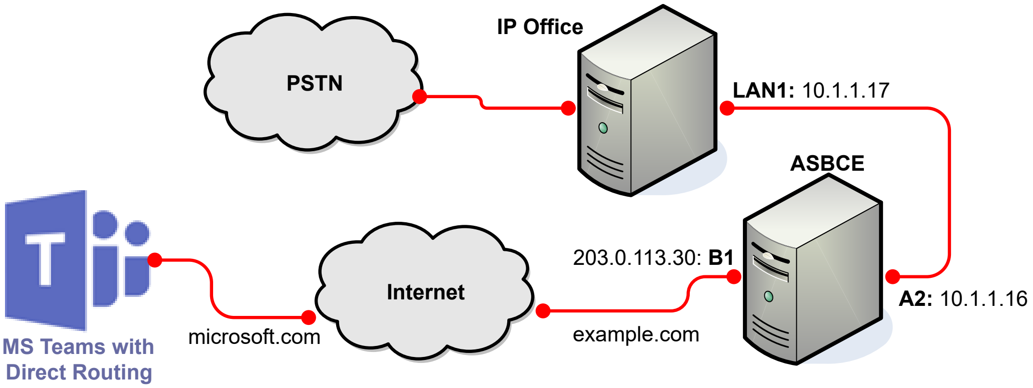
- Proceed to Configuring the ASBCE Callflow on page 90.

Related links

Obtain the ASBCE Certificates on page 77

Chapter 17: Configuring the ASBCE Callflow

The Avaya ASBCE provides SIP connectivity between MS Teams and IP Office. These steps assume that you have completed the installation and basic configuration of the ASBCE internal and external IP addresses.



- **Use Unique Names** - ASBCE setup requires configuration of multiple components, linked to each other by name. Using unique and descriptive names for each component simplifies this process and future maintenance. For example: do not name all the components relating to the IP Office connection as "IPOffice".

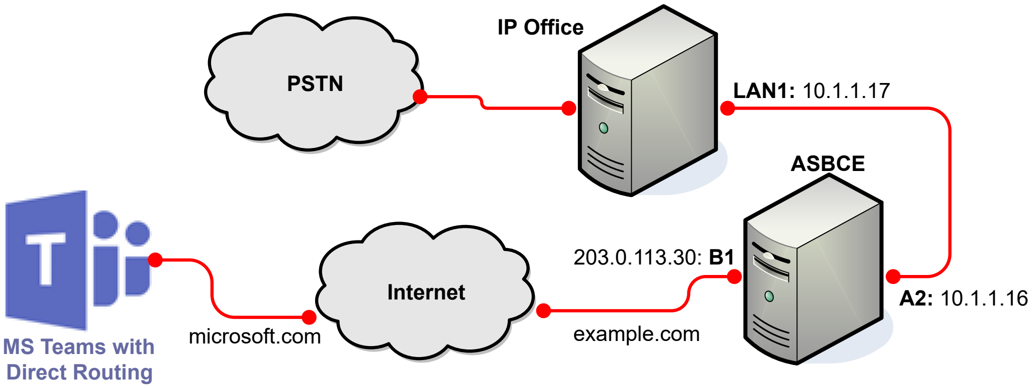
Related links

Example Schematic on page 91
Information Required on page 91
Define the IP Office Server Interworking Profile on page 92
Define the MS Teams Server Interworking Profile on page 94
Create a TLS Client Profile for the IP Office on page 97
Create a TLS Client Profile for MS Teams on page 99
Create the TLS Server Profiles on page 100
Create a SIP Server for the IP Office on page 102
Create a SIP Server for MS Teams on page 104
Define a SIP Call Routing Profile for the IP Office on page 107
Create a URI Group for IP Office Extensions on page 108
Define a SIP Call Routing Profile for MS Teams on page 109
Configure Topology Hiding for the IP Office on page 112

Configure Topology Hiding for MS Teams on page 113
Define the Media Rules for the IP Office on page 114
Define the Media Rules for MS Teams on page 115
Create the Endpoint Policy Groups on page 116
Create the SIP Signaling Interfaces on page 118
Create the SIP Media Interfaces on page 119
Configure the Server Flow for IP Office on page 121
Configure the Server Flow for MS Teams on page 124
ASBCE Flowchart on page 126

Example Schematic

This documentation uses the following example addresses and FQDNs:



- This document does not include the configuration of the private and public DNS to ensure correct resolution of the FQDNs.

Related links

Configuring the ASBCE Callflow on page 90

Information Required

Before proceeding, ensure that you have the following information available:

1. The IP address of the ASBCE external port (B1 or B2) to use for the connection to MS Teams.
2. The IP address of the ASBCE internal port (A1 or A2) to use for the connection to the IP Office.
3. The FQDN of the ASBCE.

4. The IP address of the IP Office LAN interface to use.
5. Software for SSH access to the ASBCE.
6. Details for administrator access to the ASBCE using a browser. That is, the management IP address, user name and password.
7. The ASBCE server's root password.

Related links

Configuring the ASBCE Callflow on page 90

Define the IP Office Server Interworking Profile

The ASBCE uses this interworking profile to support the SIP connection from the IP Office (the MS Teams Line).

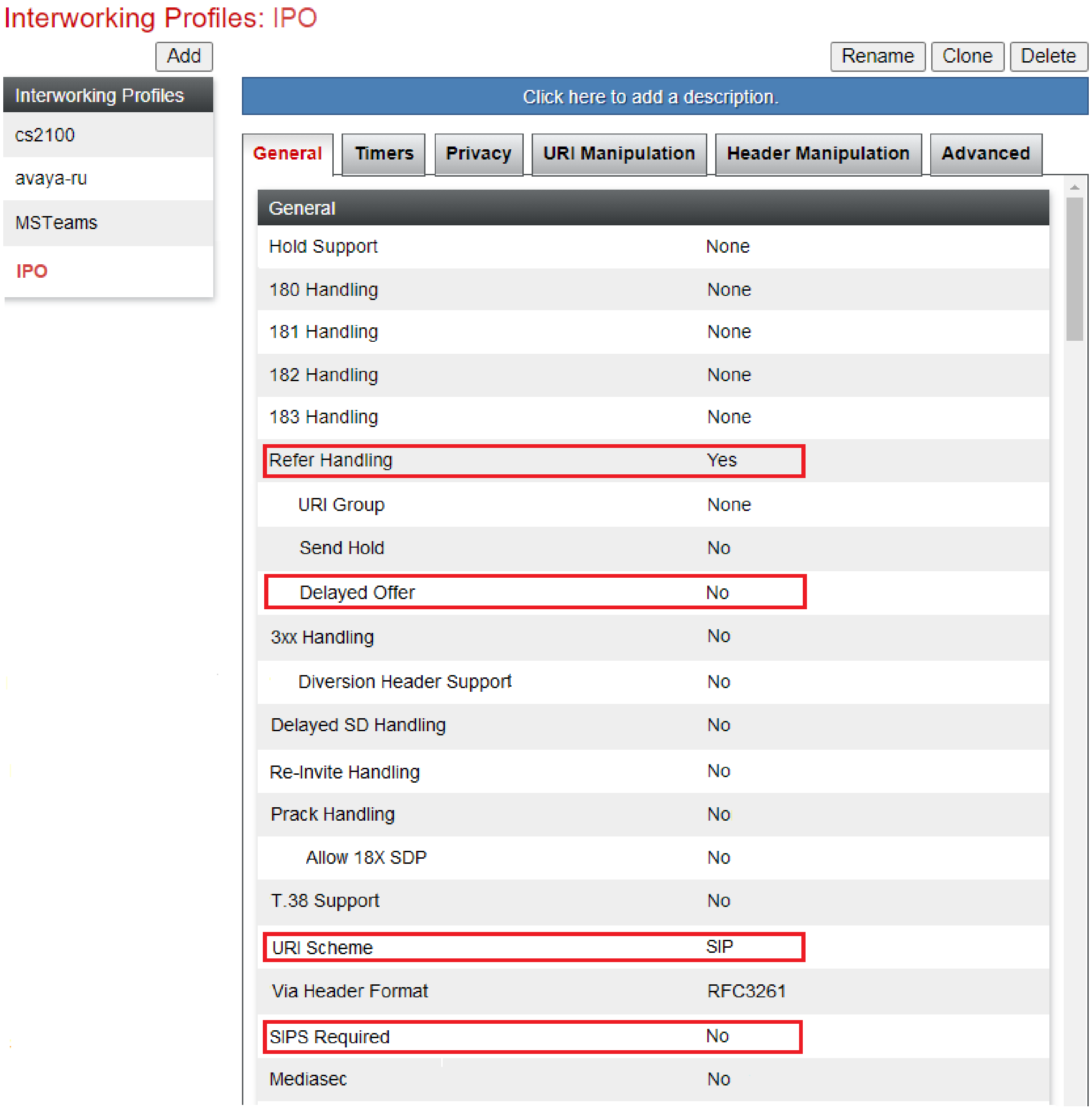
Before you begin

- Obtain the ASBCE Certificates on page 77.

Procedure

1. Select **Configuration Profiles** and then **Server Interworking**.
2. Click **Add**.
3. For the **Profile Name**, enter a unique descriptive name and click **Next**.
4. From the **General** settings tab, change the following
   a. Enable **Refer Handling**.
   b. Disable **Delayed Offer**.
   c. Set the **URI Scheme** to **SIP**.
   d. Disable **SIPS Required**.
5. Click **Next**. Leave the **SIP Timers** unchanged. Click **Next**.
6. Leave the **Privacy** settings unchanged. Click **Next**.
7. On the **Advanced** settings tab, change the following:
   a. Set **Record Routes** to **Both Sides**.
   b. Set **Extensions** to **Avaya**.
   c. Set **DTMF Support** to **None**.
8. Click **Finish**.

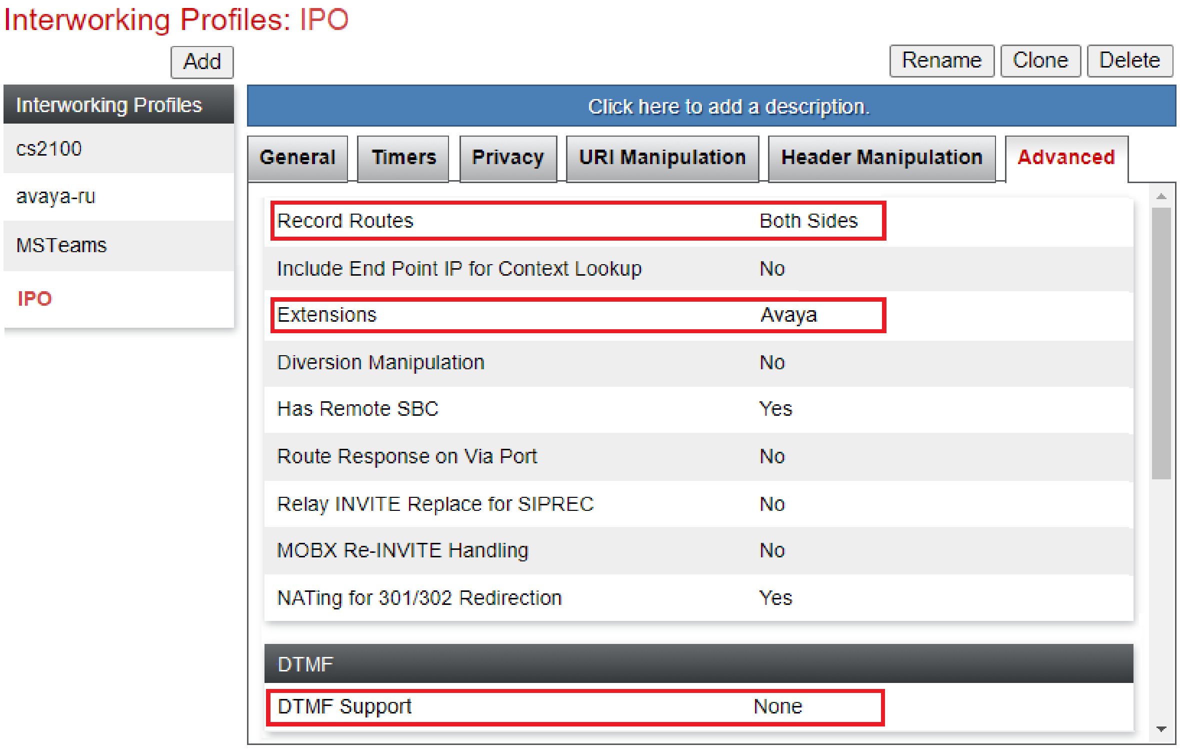
9. The IP Office interworking profile will look like the following example:



Interworking Profiles: IPO

Interworking Profiles
- cs2100
- avaya-ru
- MSTeams
- IPO

General	
Hold Support	None
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	Yes
URI Group	None
Send Hold	No
Delayed Offer	No
3xx Handling	No
Diversion Header Support	No
Delayed SD Handling	No
Re-Invite Handling	No
Prack Handling	No
Allow 18X SDP	No
T.38 Support	No
URI Scheme	SIP
Via Header Format	RFC3261
SIPS Required	No
Mediasec	No



Record Routes	Both Sides
Include End Point IP for Context Lookup	No
Extensions	Avaya
Diversion Manipulation	No
Has Remote SBC	Yes
Route Response on Via Port	No
Relay INVITE Replace for SIPREC	No
MOBX Re-INVITE Handling	No
NATing for 301/302 Redirection	Yes
DTMF Support	None

Next steps

- Proceed to Define the MS Teams Server Interworking Profile on page 94.

Related links

Configuring the ASBCE Callflow on page 90

Define the MS Teams Server Interworking Profile

The ASBCE uses this interworking profile to support the SIP connection from MS Teams.

Before you begin

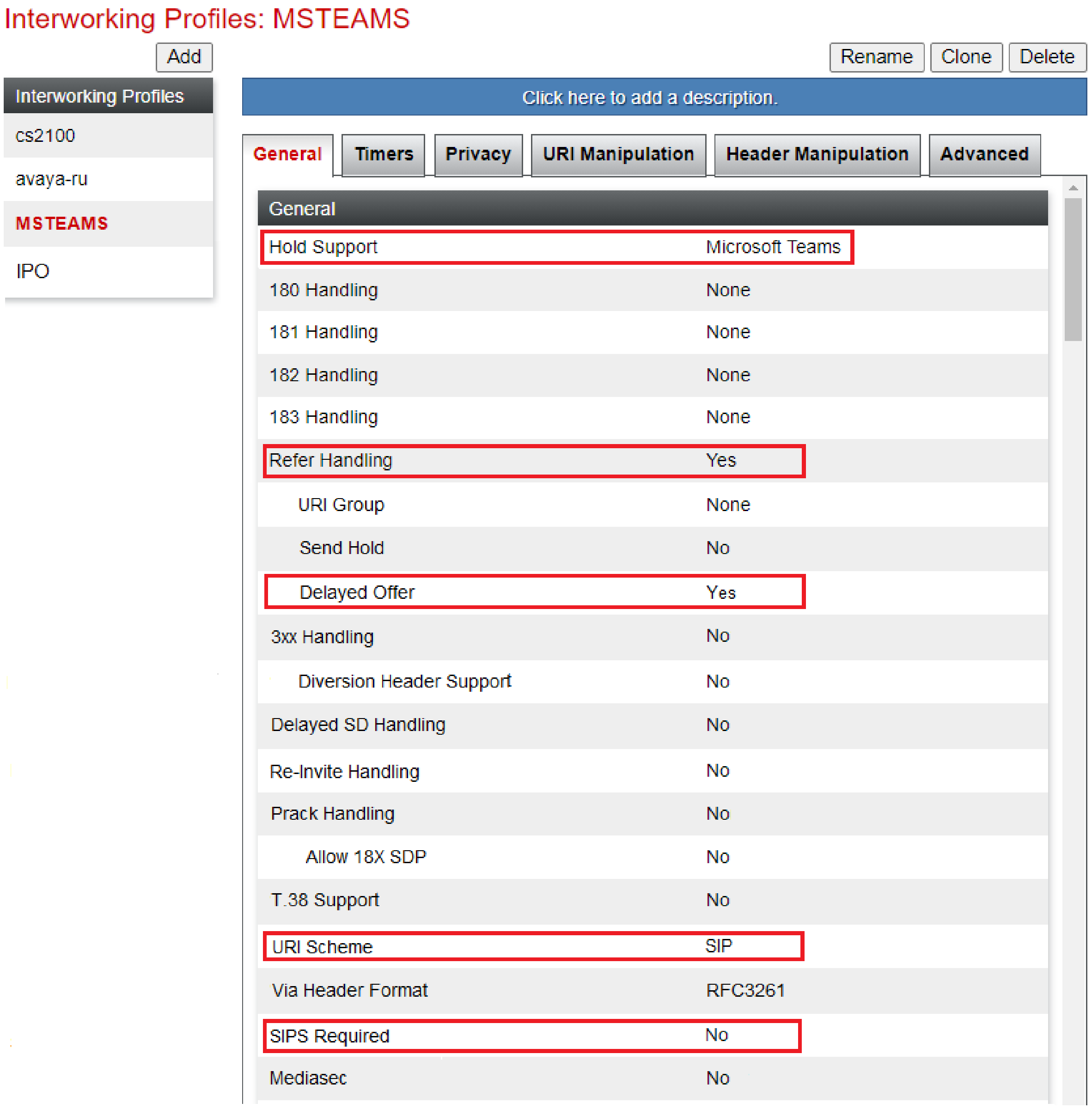
- Define the IP Office Server Interworking Profile on page 92.

Procedure

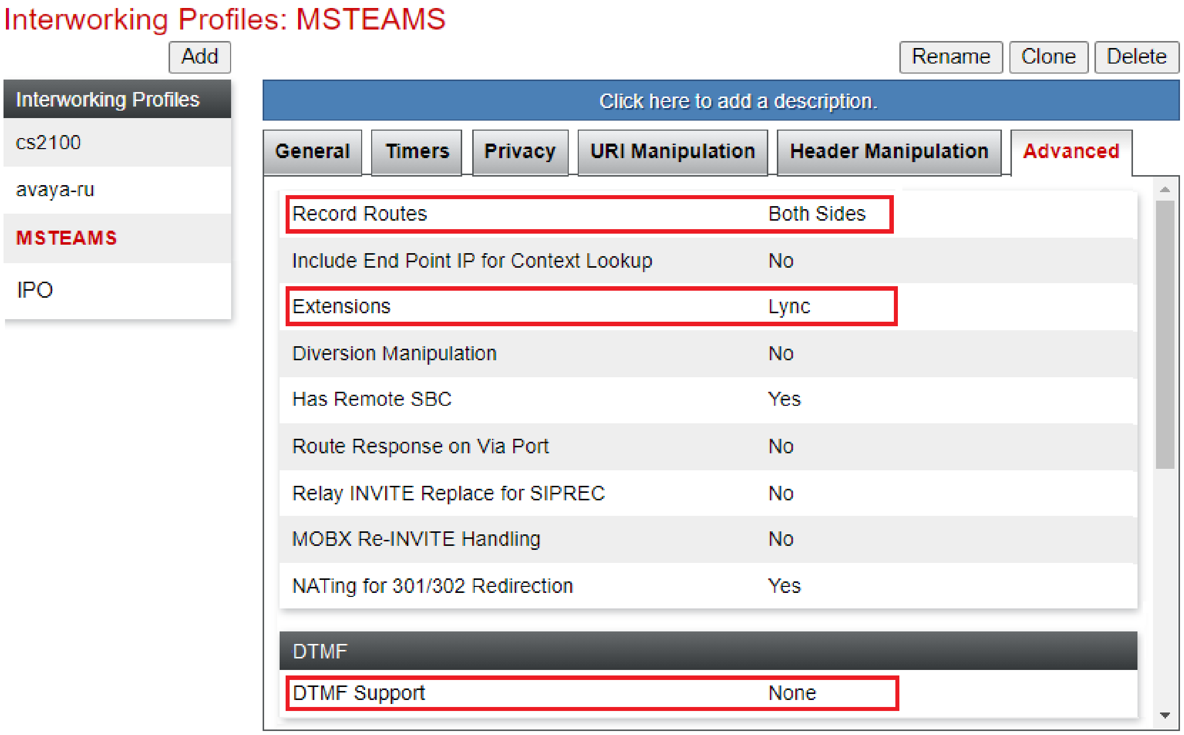
1. Select **Configuration Profiles** and then **Server Interworking**.
2. Click **Add**.
3. For the **Profile Name**, enter a unique descriptive name and click **Next**.
4. On the **General** settings tab, change the following settings:
    a. Set the **Hold Support** to **Microsoft Teams**.
    b. Set the **Refer Handling** to **Yes**.

   c. Set the **Delayed Offer** to **Yes**.
   d. Set the **URI Scheme** to **SIP**.
   e. Set **SIP Required** to **No**.
5. Click **Next**. Leave the **SIP Timers** unchanged. Click **Next**.
6. Leave the **Privacy** settings unchanged. Click **Next**.
7. On the **Advanced** settings tab, change the following:
   a. Set **Record Routes** to **Both Sides**.
   b. Set **Extensions** to **Lync**.
   c. Set **DTMF Support** to **None**.

8. Leave all other tabs at their default values. Click **Finish**. The MS Teams interworking profile will look like to the following example:



General	
Hold Support	Microsoft Teams
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	Yes
URI Group	None
Send Hold	No
Delayed Offer	Yes
3xx Handling	No
Diversion Header Support	No
Delayed SD Handling	No
Re-Invite Handling	No
Prack Handling	No
Allow 18X SDP	No
T.38 Support	No
URI Scheme	SIP
Via Header Format	RFC3261
SIPS Required	No
Mediasec	No



Record Routes	Both Sides
Include End Point IP for Context Lookup	No
Extensions	Lync
Diversion Manipulation	No
Has Remote SBC	Yes
Route Response on Via Port	No
Relay INVITE Replace for SIPREC	No
MOBX Re-INVITE Handling	No
NATing for 301/302 Redirection	Yes

DTMF

DTMF Support	None

Next steps

- Proceed to Create a TLS Client Profile for the IP Office on page 97.

Related links

Configuring the ASBCE Callflow on page 90

Create a TLS Client Profile for the IP Office

Each connection to the ASBCE requires a TLS client and TLS server entry in the ASBCE configuration. This process creates a TLS client profile for the IP Office connection.

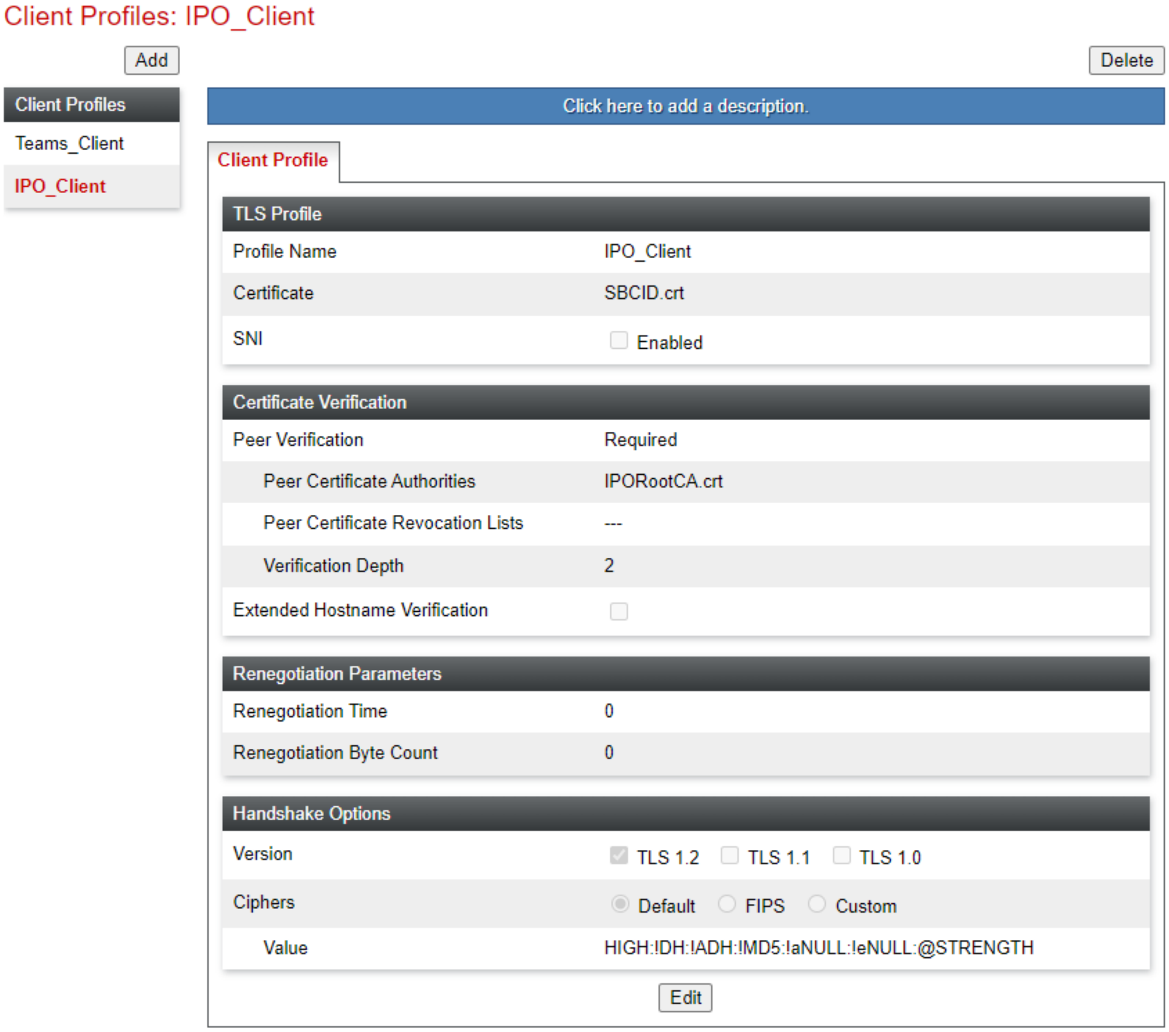
Before you begin

- Define the MS Teams Server Interworking Profile on page 94.

Procedure

1. Select **TLS Management** and then **Client Profiles**.
2. Click **Add**.
3. For the **Profile Name**, enter a unique descriptive name to help select this profile later in other menus. For example, `IPO_Client`.
4. For the **Certificate**, select the IP Office identity certificate created for the ASBCE. For this example, `IPO_SBCID.pem`.

5. For **Peer Certificate Authorities**, select the IP Office system's root certificate. For this example,`IPO_RootCA.pem`.
6. For the **Verification Depth**:
   - If the IP Office root certificate is self-signed, set this to 1. That includes subscription systems using Automatic Certificate Management.
   - If the certificate is coming from external verification authority, set this to 2 (length of certificate chain).
7. Click **Next** and then **Finish**.
8. The TLS client profile for the IP Office system will look like the following example:



Client Profiles: IPO_Client

TLS Profile	
Profile Name	IPO_Client
Certificate	SBCID.crt
SNI	□ Enabled

Certificate Verification	
Peer Verification	Required
Peer Certificate Authorities	IPORootCA.crt
Peer Certificate Revocation Lists	---
Verification Depth	2
Extended Hostname Verification	□

Renegotiation Parameters	
Renegotiation Time	0
Renegotiation Byte Count	0

Handshake Options	
Version	☑ TLS 1.2 □ TLS 1.1 □ TLS 1.0
Ciphers	● Default ○ FIPS ○ Custom
Value	HIGH:!DH:!ADH:!MD5:!aNULL:!eNULL:@STRENGTH

Next steps

- Proceed to Create a TLS Client Profile for MS Teams on page 99.

Related links

Configuring the ASBCE Callflow on page 90

Create a TLS Client Profile for MS Teams

Each connection to the ASBCE requires a TLS client and TLS server entry in the ASBCE configuration. This process creates a TLS client profile for the MS Teams connection.

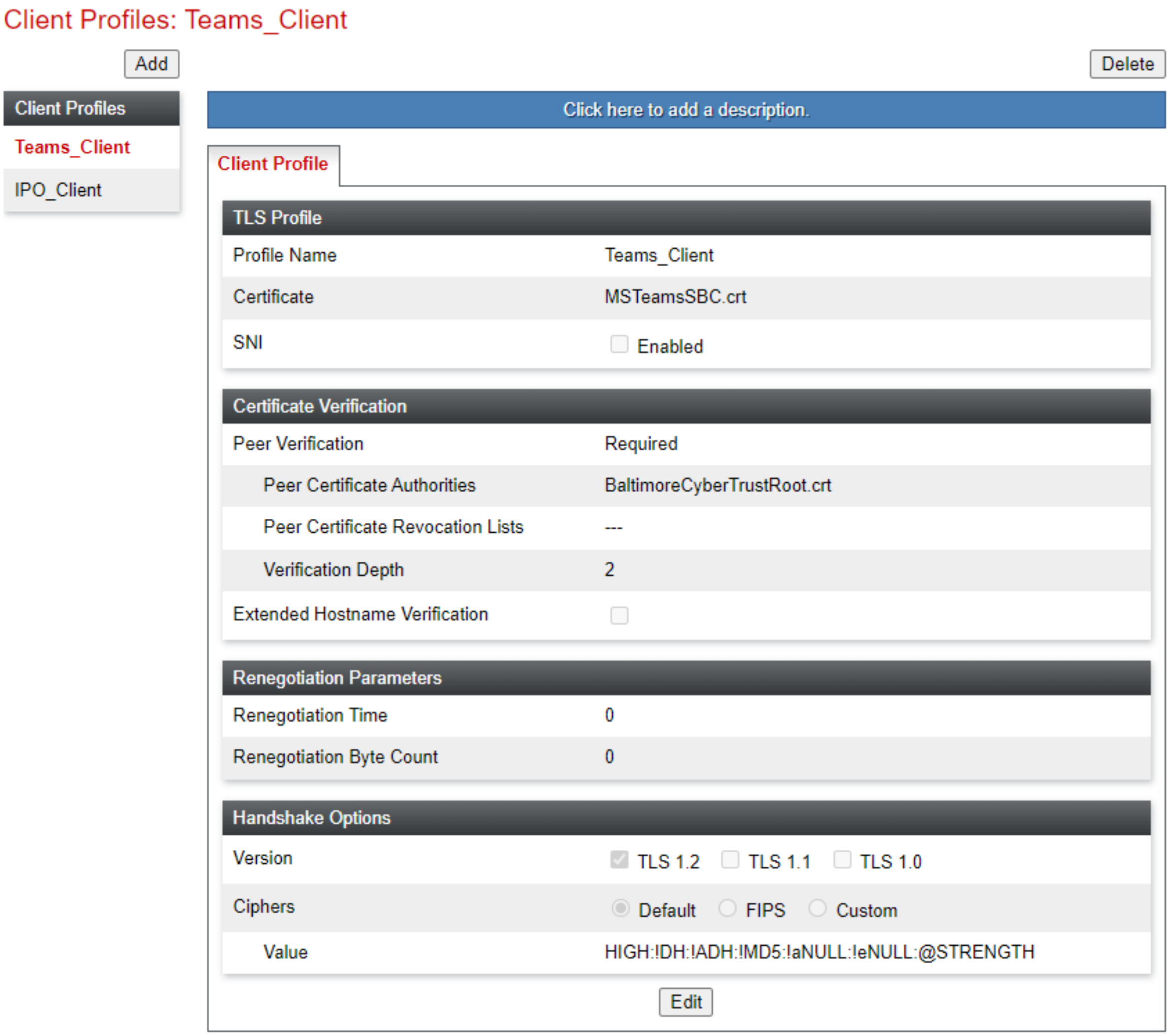
Before you begin

- Create a TLS Client Profile for the IP Office on page 97.

Procedure

1. Select **TLS Management** and then **Client Profiles**.
2. Click **Add**.
3. For the **Profile Name**, enter a unique descriptive name to help select this profile later in other menus.
4. For the **Certificate**, select the certificate requested from MS Teams for the ASBCE. For this example, `MSTeamsSBC.crt`.
5. For **Peer Certificate Authorities**, select the MS Teams root certificate. That is the `DigiCertGlobalRootG2.crt`.
6. For the **Verification Depth**, set this to 2.
7. Click **Next** and then **Finish**.

8. The TLS client profile for MS Teams will look like the following example:



TLS Profile	
Profile Name	Teams_Client
Certificate	MSTeamsSBC.crt
SNI	□ Enabled

Certificate Verification	
Peer Verification	Required
Peer Certificate Authorities	BaltimoreCyberTrustRoot.crt
Peer Certificate Revocation Lists	---
Verification Depth	2
Extended Hostname Verification	□

Renegotiation Parameters	
Renegotiation Time	0
Renegotiation Byte Count	0

Handshake Options	
Version	☑ TLS 1.2 □ TLS 1.1 □ TLS 1.0
Ciphers	● Default ○ FIPS ○ Custom
Value	HIGH:!DH:!ADH:!MD5:!aNULL:!eNULL:@STRENGTH

Next steps

- Proceed to Create the TLS Server Profiles on page 100.

Related links

Configuring the ASBCE Callflow on page 90

Create the TLS Server Profiles

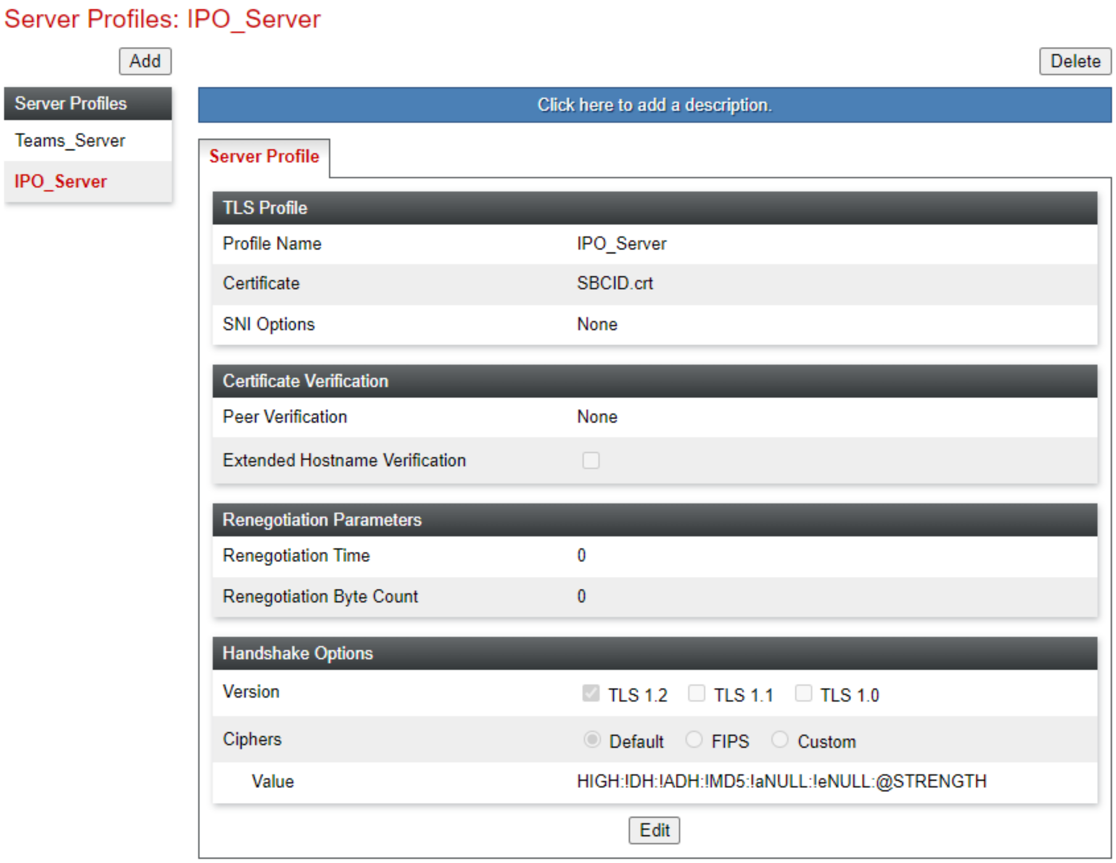
Define the TLS server profiles for the IP Office and MS Teams connections.

Before you begin

- Create a TLS Client Profile for MS Teams on page 99.

Procedure

1. Select **TLS Management** > **Server Profiles**.
2. Click **Add** and create a TLS server profile for the IP Office.
    a. **Profile Name** - Enter a unique descriptive name to help select this profile later in other menus.
    b. **Certificate** - Select the IP Office identity certificate created for the ASBCE.
    c. **Peer Verification** - Select **None**.
    d. Click **Next** and then **Finish**.
    e. The TLS server profile setting for the IP Office system will look like the following example:



Server Profiles: IPO_Server

TLS Profile	
Profile Name	IPO_Server
Certificate	SBCID.crt
SNI Options	None

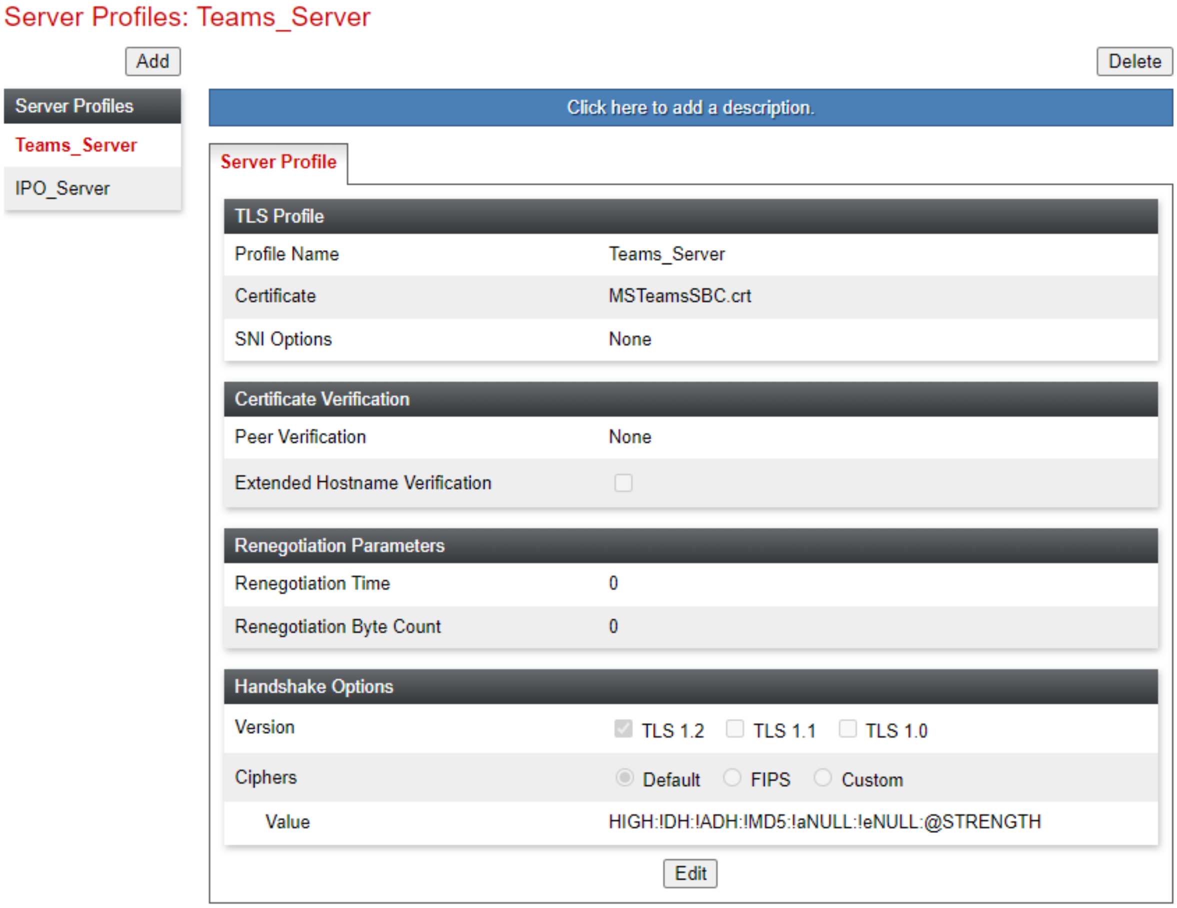
Certificate Verification	
Peer Verification	None
Extended Hostname Verification	□

Renegotiation Parameters	
Renegotiation Time	0
Renegotiation Byte Count	0

Handshake Options	
Version	☑ TLS 1.2 □ TLS 1.1 □ TLS 1.0
Ciphers	● Default ○ FIPS ○ Custom
Value	HIGH:!DH:!ADH:!MD5:!aNULL:!eNULL:@STRENGTH

3. Click **Add** and create a TLS server profile for MS Teams.
    a. **Profile Name** - Enter a unique descriptive name to help select this profile later in other menus.
    b. **Certificate** - Select the certificate requested from MS Teams for the ASBCE.
    c. **Peer Verification** - Select **None**.
    d. Click **Next** and then **Finish**.

4. The TLS server profile setting for MS Teams will look like the following example:



TLS Profile	
Profile Name	Teams_Server
Certificate	MSTeamsSBC.crt
SNI Options	None

Certificate Verification	
Peer Verification	None
Extended Hostname Verification	□

Renegotiation Parameters	
Renegotiation Time	0
Renegotiation Byte Count	0

Handshake Options	
Version	☑ TLS 1.2 □ TLS 1.1 □ TLS 1.0
Ciphers	● Default ○ FIPS ○ Custom
Value	HIGH:!DH:!ADH:!MD5:!aNULL:!eNULL:@STRENGTH

Next steps

- Proceed to Create a SIP Server for the IP Office on page 102.

Related links

Configuring the ASBCE Callflow on page 90

Create a SIP Server for the IP Office

The ASBCE needs a SIP server for each server to which it connects.

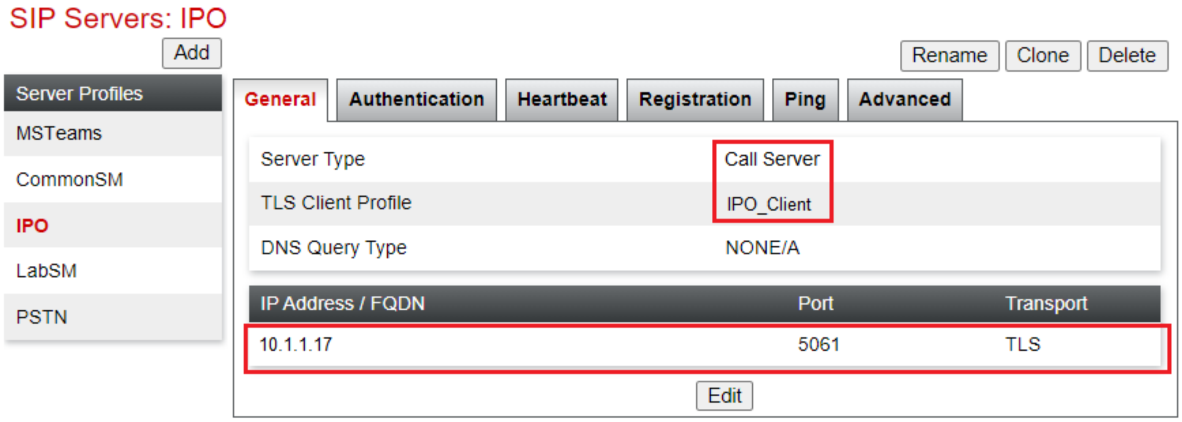
Before you begin

- Create the TLS Server Profiles on page 100.

Procedure

1. Select **Services** and then **SIP Server**.
2. Click **Add** and add a SIP server profile for the IP Office.

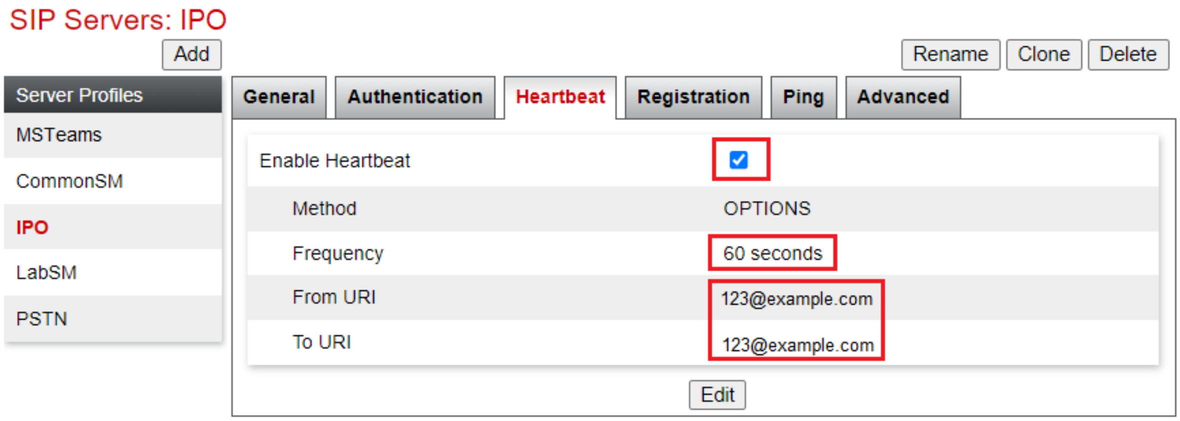
3. Enter a **Profile Name**. Click **Next**.
4. In the **General Settings** menu:
    a. Set the **Server Type** to **Call Server**.
    b. Set the **TLS Client Profile** to the one previously created for the IP Office connection.
    c. Set the address, port and transport details to match the IP Office setting.
    d. Click **Next**.
5. There are no changes to the default **Authentication** settings. Click **Next**.
6. In the **Heartbeat** settings:
    a. Select **Enable heartbeat**.
    b. Set the **Frequency** to 60.
    c. For the **From URI** and **To URI** values, enter a dummy value.
    d. Click **Next**.
7. There are no changes to the default **Registration** and **Ping** settings. Click **Next** to skip each.
8. In the **Advance** settings:
    a. **Enable Grooming** - Enable this setting.
        - Note: This SIP Server connection with the IP Office has grooming enabled. For a SIP Server for endpoints such as remote extension, any similar connection to the IP Office should have grooming disabled because the IP Office does not support TCP connection sharing between endpoints.
    b. **Interworking Profile** - Select the interworking profile previously created for the IP Office.
    c. **Signaling Manipulation Script** - Select the SIGMA script uploaded for the IP Office.
    d. Click **Finish**.
9. The settings will look like the following example:



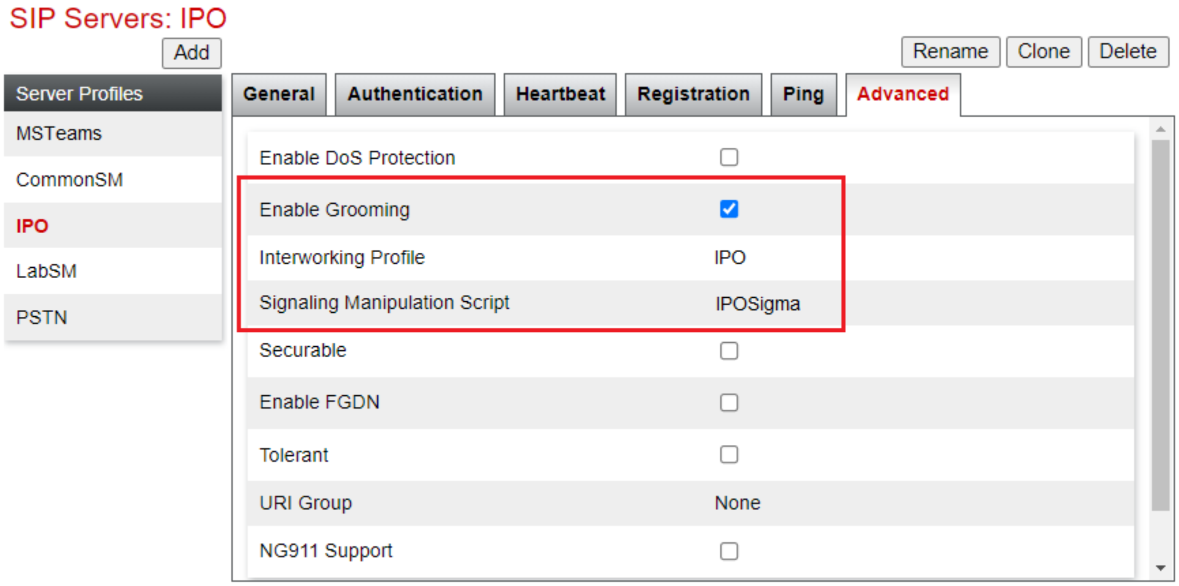
SIP Servers: IPO

Server Type	Call Server
TLS Client Profile	IPO_Client
DNS Query Type	NONE/A

IP Address / FQDN	Port	Transport
10.1.1.17	5061	TLS



Enable Heartbeat	☑
Method	OPTIONS
Frequency	60 seconds
From URI	123@example.com
To URI	123@example.com



Enable DoS Protection	☐
Enable Grooming	☑
Interworking Profile	IPO
Signaling Manipulation Script	IPOSigma
Securable	☐
Enable FGDN	☐
Tolerant	☐
URI Group	None
NG911 Support	☐

Next steps

- Proceed to Create a SIP Server for MS Teams on page 104.

Related links

Configuring the ASBCE Callflow on page 90

Create a SIP Server for MS Teams

Create a SIP Server record for MS Teams as below.

- Note: The use of CIDR IP address ranges requires the ASBCE to be running 10.1 plus Hotfix 1 (ASBCE R10.1.0.0 plus sbce-10.1.0.0-34-21958-hotfix-05192022).

Before you begin

- Create a SIP Server for the IP Office on page 102.

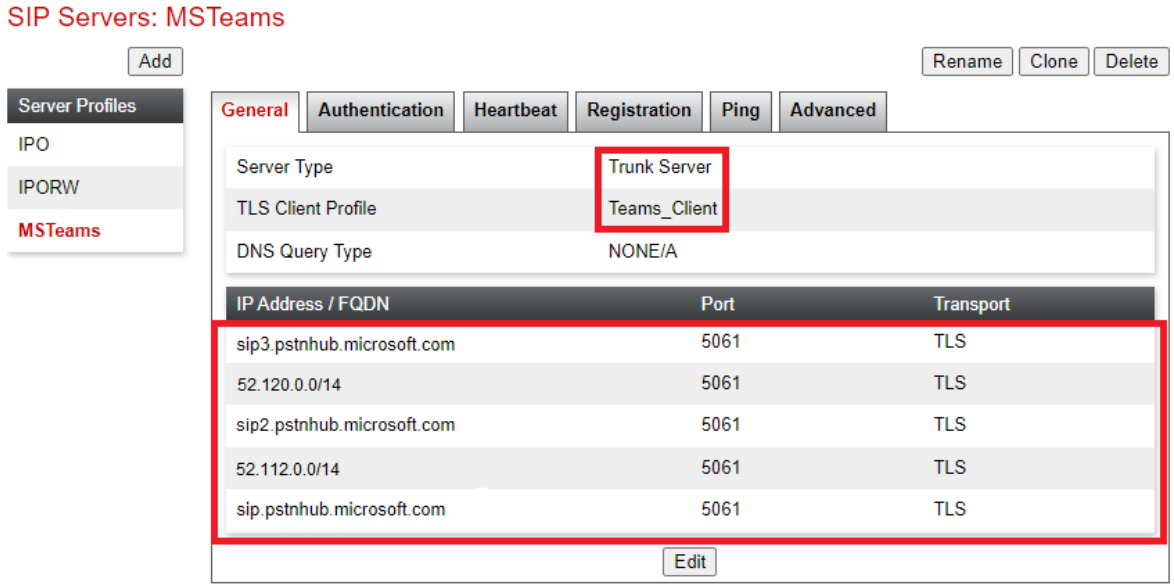
Procedure

1. Select **Services** and then **SIP Servers**.
2. Click **Add** and add a SIP server profile for MS Teams.
3. Enter a **Profile Name**. Click **Next**.
4. In the **General Settings** menu:
    a. Set the **Server Type** to **Trunk Server**.
    b. Set the **TLS Client Profile** to the one previously created for the MS Teams connection.
    c. Add the following entries for the address/port/transport settings:

IP Address/FQDN/CIDR Range	Port	Transport
`sip.pstnhub.microsoft.com`	5061	TLS
`52.112.0.0/14`	5061	TLS
`sip2.pstnhub.microsoft.com`	5061	TLS
`52.120.0.0/14`	5061	TLS
`sip3.pstnhub.microsoft.com`	5061	TLS

    d. Click **Next**.
5. There are no changes to the default **Authentication** settings. Click **Next**.
6. In the **Heartbeat** settings:
    a. Select **Enable heartbeat**.
    b. Set the **Frequency** to 60.
    c. For the **From URI** and **To URI**, add dummy addresses using the ASBCE and MS Teams FQDN's respectively.
    d. Click **Next**.
7. There are no changes to the default **Registration** and **Ping** settings. Click **Next** to skip each.
8. In the **Advanced** settings:
    a. **Enable Grooming** - Enable this setting.
    b. **Interworking Profile -** Select the interworking profile previously created for MS Teams.
    c. **Signaling Manipulation Script** - Select the SIGMA script uploaded for MS Teams.
    d. Click **Finish**.

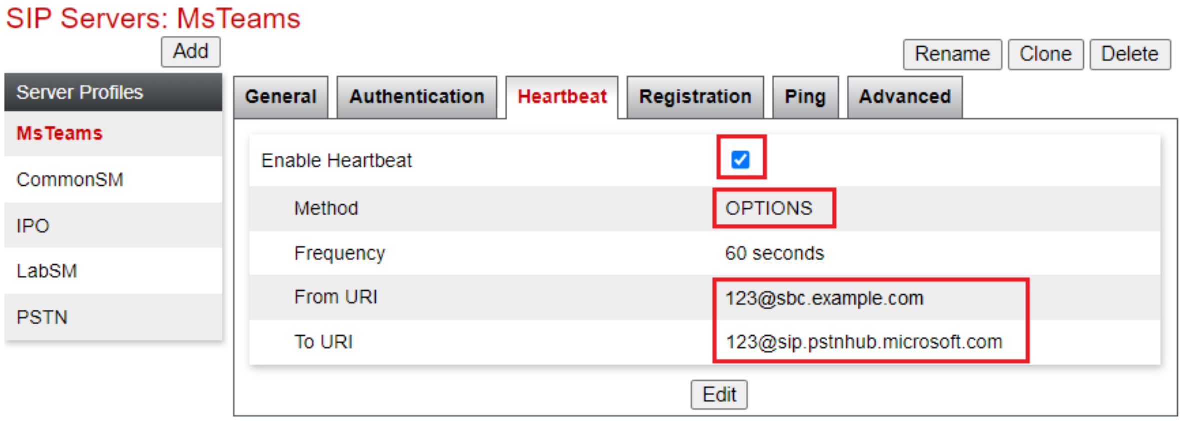
9. The settings will look like the following example:



SIP Servers: MSTeams

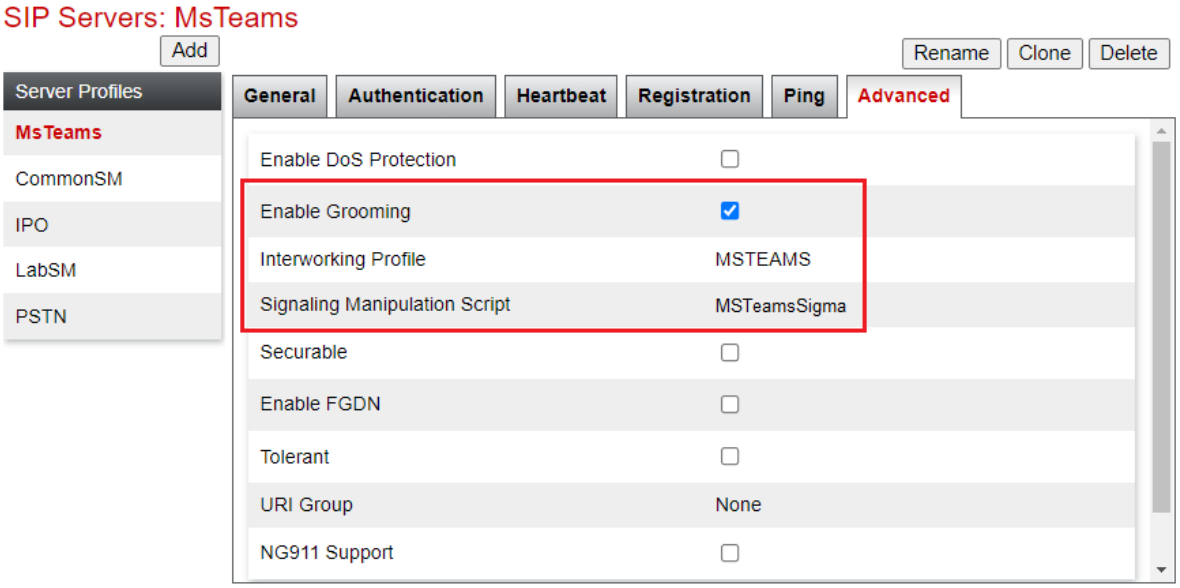
Server Type	Trunk Server
TLS Client Profile	Teams_Client
DNS Query Type	NONE/A

IP Address / FQDN	Port	Transport
sip3.pstnhub.microsoft.com	5061	TLS
52.120.0.0/14	5061	TLS
sip2.pstnhub.microsoft.com	5061	TLS
52.112.0.0/14	5061	TLS
sip.pstnhub.microsoft.com	5061	TLS



SIP Servers: MsTeams

Enable Heartbeat	☑
Method	OPTIONS
Frequency	60 seconds
From URI	123@sbc.example.com
To URI	123@sip.pstnhub.microsoft.com



Enable DoS Protection	□
Enable Grooming	☑
Interworking Profile	MSTEAMS
Signaling Manipulation Script	MSTeamsSigma
Securable	□
Enable FGDN	□
Tolerant	□
URI Group	None
NG911 Support	□

Next steps

- Proceed to Define a SIP Call Routing Profile for the IP Office on page 107.

Related links

Configuring the ASBCE Callflow on page 90

Define a SIP Call Routing Profile for the IP Office

The ASBCE requires routing information to route calls to the configured SIP Servers. The ASBCE uses the information as the destination addresses for SIP signaling messages.

This process creates a routing profile for the connection to the IP Office.

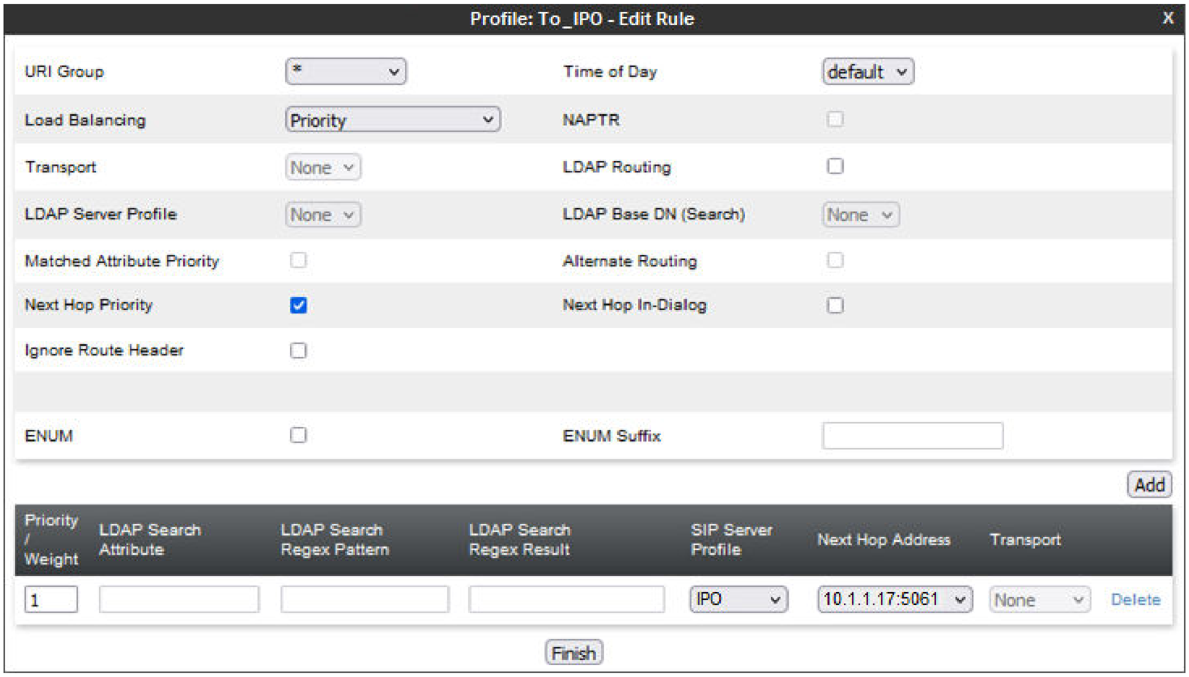
Before you begin

- Create a SIP Server for MS Teams on page 104.

Procedure

1. Select **Configuration Profiles** and then **Routing**.
2. Click **Add**.
3. Enter a **Profile Name** and click **Next**.

4. In the routing profile settings, click **Add** to specify the IP route details:



Profile: To_IPO - Edit Rule

URI Group	*	Time of Day	default
Load Balancing	Priority	NAPTR	□
Transport	None	LDAP Routing	□
LDAP Server Profile	None	LDAP Base DN (Search)	None
Matched Attribute Priority	□	Alternate Routing	□
Next Hop Priority	☑	Next Hop In-Dialog	□
Ignore Route Header	□		
ENUM	□	ENUM Suffix	

Add

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport	
1				IPO	10.1.1.17:5061	None	Delete

Finish

   a. Set the **Priority/Weight** to 1.

   b. For the **Server Configuration**, select the SIP server entry created for the IP Office.

   c. In the **Next Hop Address**, select the IP Office address/port to use.

5. Click **Finish**.

Next steps

- Proceed to Create a URI Group for IP Office Extensions on page 108.

Related links

Configuring the ASBCE Callflow on page 90

Create a URI Group for IP Office Extensions

In scenarios such as call transfers, MS Teams can send a *REFER* with an IP Office extension number and the MS Teams domain. You need a URI group to match that traffic. The ASBCE uses the URI group to redirect those calls back to the IP Office.

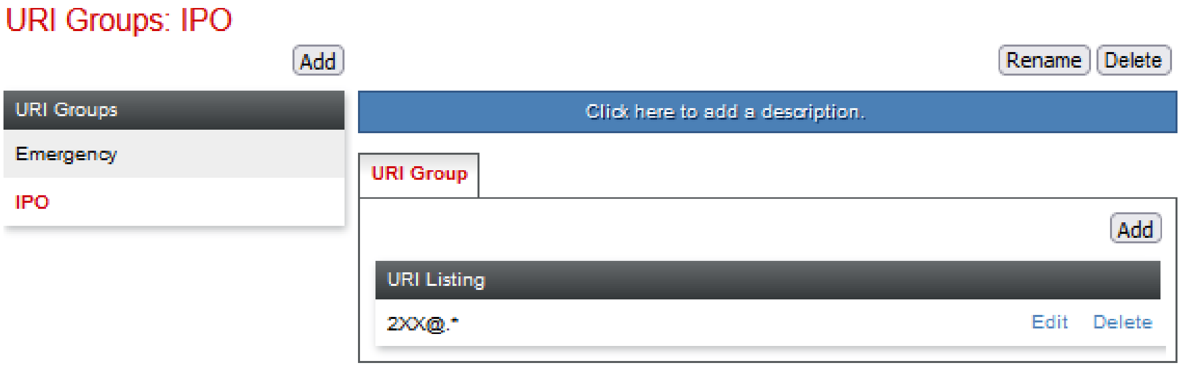
Before you begin

- Define a SIP Call Routing Profile for the IP Office on page 107.

Procedure

1. Select **Configuration Profiles** and then **URI Groups**.

2. Click **Add** and set a unique descriptive name for the URI group.
3. Click **Add** and define the string that should trigger a match.
4. Repeat the steps above for any other extension number patterns required.
5. Click **Finish**.
6. The URI group details will look like the following example:



URI Groups: IPO

URI Groups
Emergency
IPO

Click here to add a description.

URI Group

URI Listing		
2XX@.*	Edit	Delete

   - For the example scenario, IP Office extensions use the range 200 to 299. MS Teams only extensions use the range 400 to 499. Therefore, the URI Group only needs an entry for the IP Office range.

Next steps

- Proceed to Define a SIP Call Routing Profile for MS Teams on page 109.

Related links

Configuring the ASBCE Callflow on page 90

Define a SIP Call Routing Profile for MS Teams

The ASBCE requires routing information to route calls to the SIP Servers. The routing profile defines the IP addresses, ports and transport used as the destination addresses for signaling to the servers.

This process creates a routing profile for the connection to MS Teams.

Before you begin

- Create a URI Group for IP Office Extensions on page 108.

Procedure

1. Select **Configuration Profiles** and then **Routing**.
2. Enter a **Profile Name** and click **Next**.
3. Create a route for IP Office extension numbers:
   a. Click **Add**.

b. For the **URI Group**, select the group created to match IP Office extension numbers.

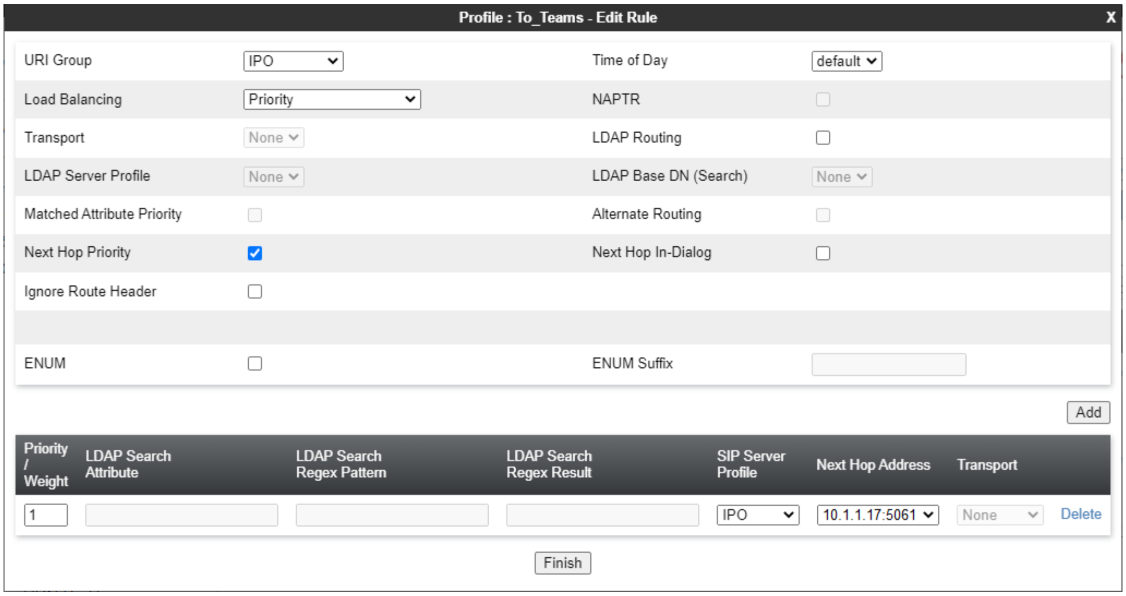
c. In the routing profile settings, click **Add** and add a call route with the following setting:

d. Set the **Priority/Weight** to 1.

e. For the **Server Configuration**, select the SIP server profile entry created for the IP Office.

f. For the **Next Hop Address**, enter the address for the IP Office and the port to use. For example: 10.1.1.17:5061.

g. The settings will look like the following example:



Profile : To_Teams - Edit Rule

URI Group	IPO	Time of Day	default
Load Balancing	Priority	NAPTR	□
Transport	None	LDAP Routing	□
LDAP Server Profile	None	LDAP Base DN (Search)	None
Matched Attribute Priority	□	Alternate Routing	□
Next Hop Priority	☑	Next Hop In-Dialog	□
Ignore Route Header	□		
ENUM	□	ENUM Suffix	

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport	
1				IPO	10.1.1.17:5061	None	Delete

4. Create a route for all other numbers addressed to MS Teams:

   a. Click **Add**.

   b. Enter a **Profile Name** and click **Next**.

   c. In the routing profile settings, click **Add** and add a call route with the following setting:

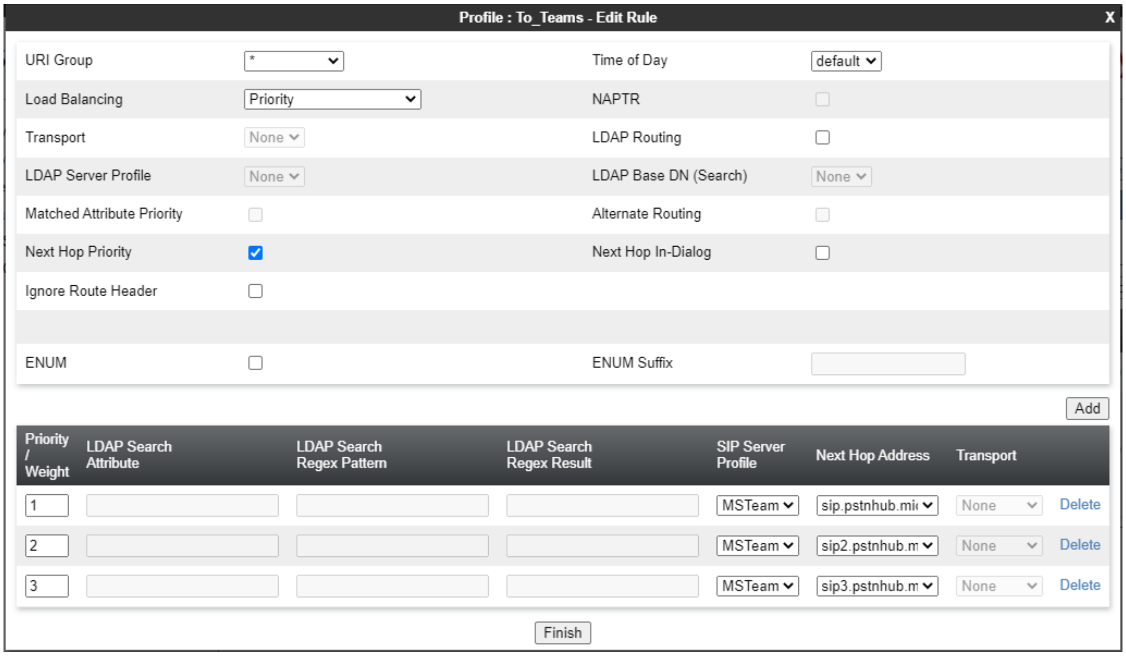
   d. Set the **Priority/Weight** to 2.

   e. For the **Server Configuration**, select the SIP server entry created for MS Teams.

   f. For the **Next Hop Address**, enter `sip.pstnhub.microsoft.com:5061`.

   g. Repeat the above to add `sip2.pstnhub.microsoft.com:5061` with priority 2, `sip3.pstnhub.microsoft.com:5061` with priority 3.

h. The settings will look like the following example:



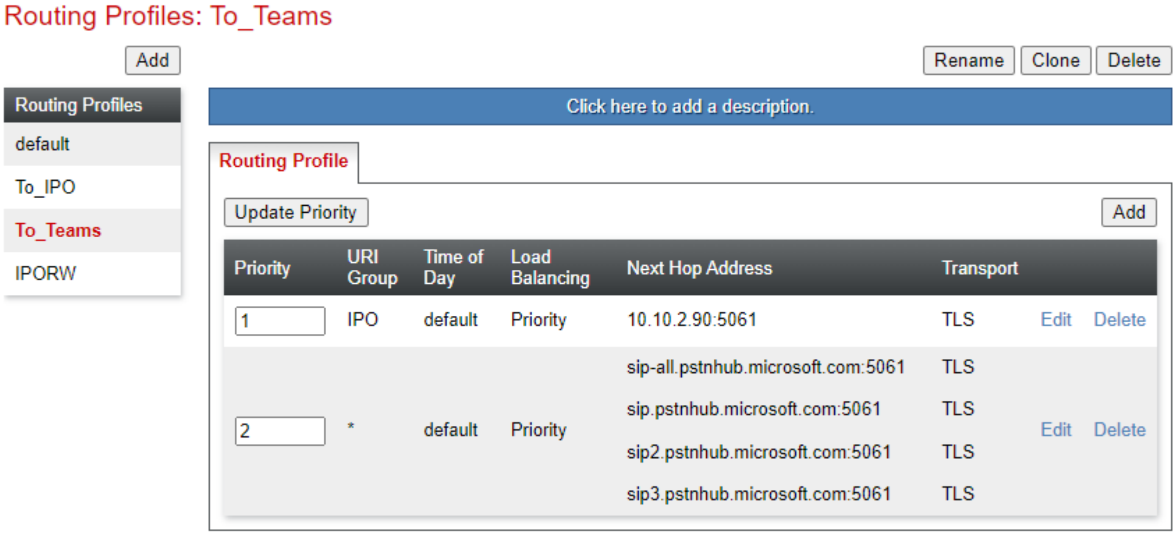
Profile : To_Teams - Edit Rule

URI Group	*	Time of Day	default
Load Balancing	Priority	NAPTR	☐
Transport	None	LDAP Routing	☐
LDAP Server Profile	None	LDAP Base DN (Search)	None
Matched Attribute Priority	☐	Alternate Routing	☐
Next Hop Priority	☑	Next Hop In-Dialog	☐
Ignore Route Header	☐		
ENUM	☐	ENUM Suffix	

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport	
1				MSTeam	sip.pstnhub.mi	None	Delete
2				MSTeam	sip2.pstnhub.m	None	Delete
3				MSTeam	sip3.pstnhub.m	None	Delete

i. Click **Finish**.

5. The final routing profile will look like the following example:



Routing Profiles: To_Teams

Routing Profiles: default, To_IPO, To_Teams, IPORW

Click here to add a description.

Routing Profile

Priority	URI Group	Time of Day	Load Balancing	Next Hop Address	Transport		
1	IPO	default	Priority	10.10.2.90:5061	TLS	Edit	Delete
2	*	default	Priority	sip-all.pstnhub.microsoft.com:5061 sip.pstnhub.microsoft.com:5061 sip2.pstnhub.microsoft.com:5061 sip3.pstnhub.microsoft.com:5061	TLS TLS TLS TLS	Edit	Delete

Next steps

- Proceed to Configure Topology Hiding for the IP Office on page 112.

Related links

Configuring the ASBCE Callflow on page 90

Configure Topology Hiding for the IP Office

The ASBCE uses topology hiding to modify the content of SIP headers. It uses this for two main roles:

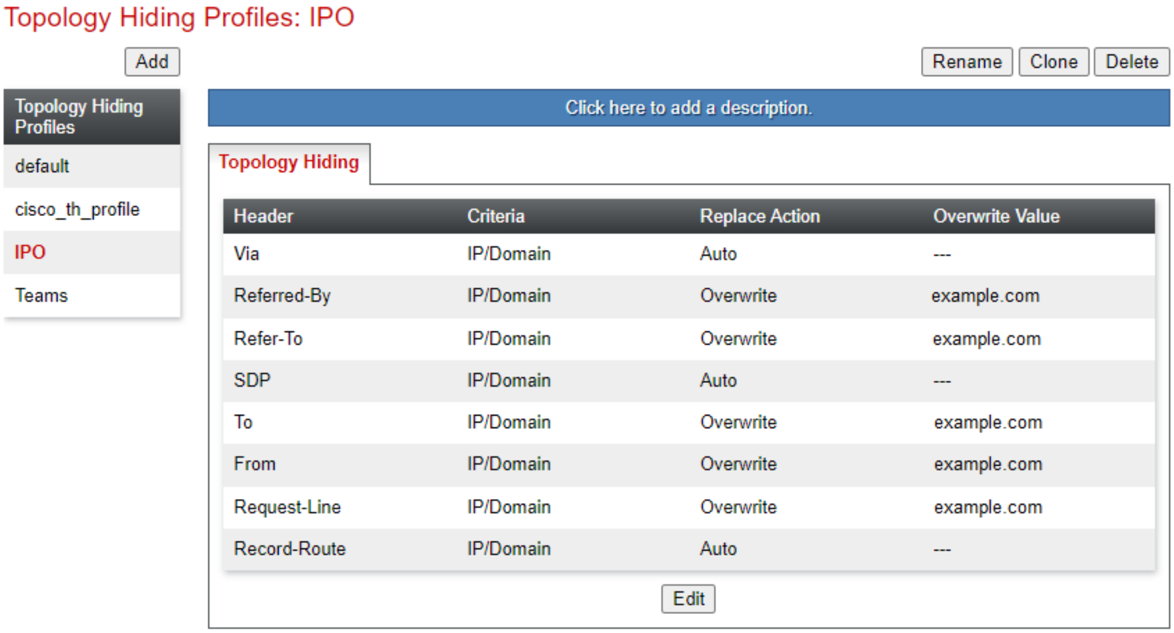
- As a security feature to preventing sending private enterprise network information to the public network.
- As an interoperability tool to adapt the headers to the IP addresses or domains expected by the remote the service provider or enterprise networks.

Before you begin

- Define a SIP Call Routing Profile for MS Teams on page 109.

Procedure

1. Select **Configuration Profiles** and then **Topology Hiding**.
2. Select the default profile and click **Clone**.
3. Enter a unique descriptive name for the profile for connections to the IP Office and click **Next**.
4. Using the **Add Header** option, add the following settings. For those headers set to **Overwrite**, use the IP Office system's SIP domain.



Header	Criteria	Replace Action	Overwrite Value
Via	IP/Domain	Auto	---
Referred-By	IP/Domain	Overwrite	example.com
Refer-To	IP/Domain	Overwrite	example.com
SDP	IP/Domain	Auto	---
To	IP/Domain	Overwrite	example.com
From	IP/Domain	Overwrite	example.com
Request-Line	IP/Domain	Overwrite	example.com
Record-Route	IP/Domain	Auto	---

5. Click **Finish**.

Next steps

- Proceed to Configure Topology Hiding for MS Teams on page 113.

Related links

Configuring the ASBCE Callflow on page 90

Configure Topology Hiding for MS Teams

The ASBCE uses topology hiding to modify the content of SIP headers. It uses this for two main roles:

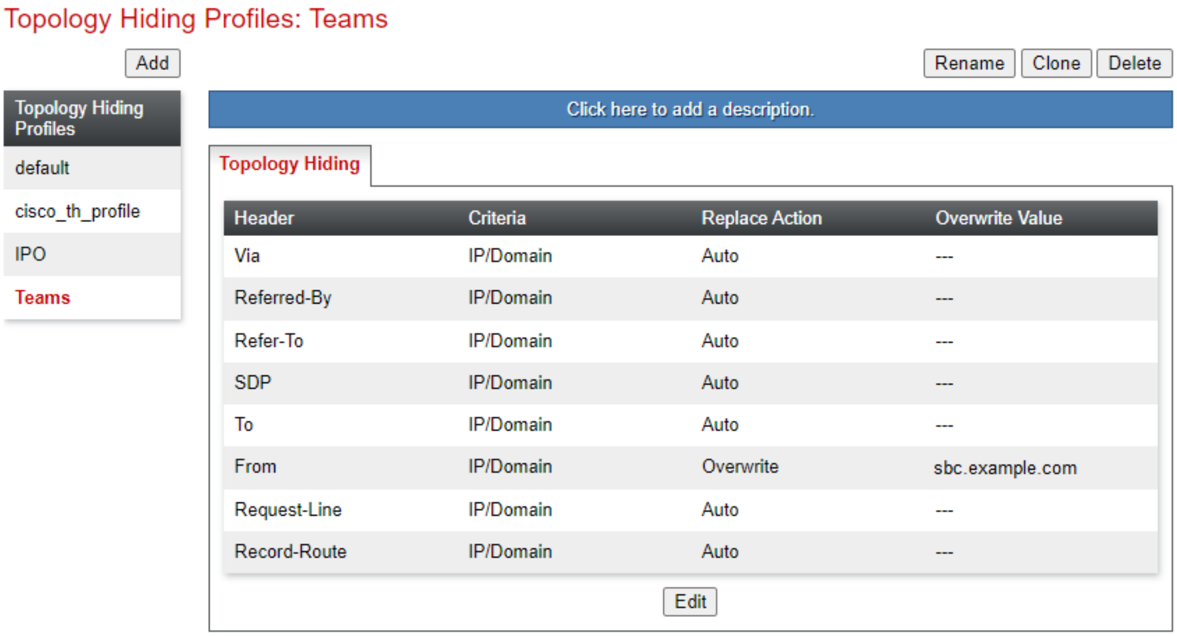
- As a security feature to preventing sending private enterprise network information to the public network.
- As an interoperability tool to adapt the headers to the IP addresses or domains expected by the remote the service provider or enterprise networks.

Before you begin

- Configure Topology Hiding for the IP Office on page 112.

Procedure

1. Select **Configuration Profiles** and then **Topology Hiding**.
2. Select the default profile and click **Clone**.
3. Enter a unique descriptive name for the profile for connections to the MS Teams and click **Next**.
4. Using the **Add Header** option, add the following settings. For those headers set to **Overwrite**, use the ASBCE system's FQDN.



Topology Hiding Profiles: Teams

Header	Criteria	Replace Action	Overwrite Value
Via	IP/Domain	Auto	---
Referred-By	IP/Domain	Auto	---
Refer-To	IP/Domain	Auto	---
SDP	IP/Domain	Auto	---
To	IP/Domain	Auto	---
From	IP/Domain	Overwrite	sbc.example.com
Request-Line	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---

5. Click **Finish**.

Next steps

- Proceed to Define the Media Rules for the IP Office on page 114.

Related links

Configuring the ASBCE Callflow on page 90

Define the Media Rules for the IP Office

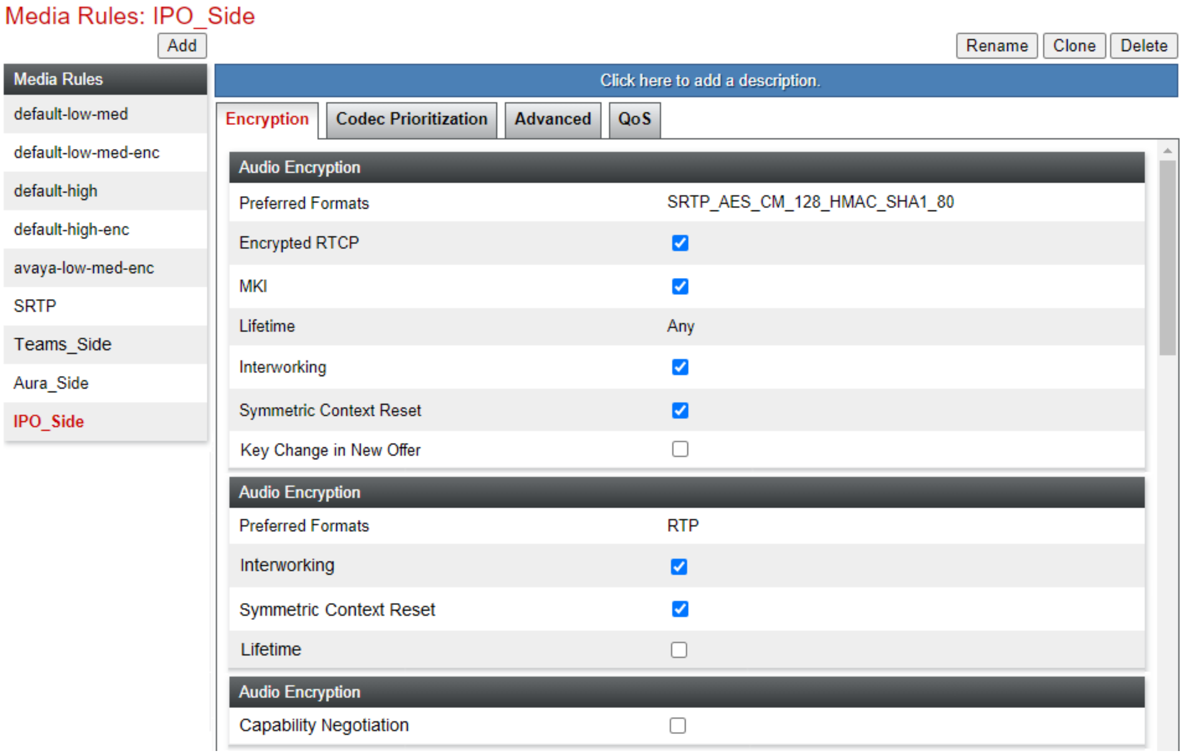
The ASBCE uses media rules to define RTP media packet parameters, such as prioritizing encryption techniques and packet encryption techniques. This process creates the media rules used for the MS Teams connection.

Before you begin

- Configure Topology Hiding for MS Teams on page 113.

Procedure

1. Select **Domain Policies** and then **Media Rules**.
2. Select the existing `default-low-med` rule and click **Clone**.
3. Enter a unique descriptive name for the new media rule and click **Finish**.
4. Select the new media rule and click **Edit**.
5. On the **Encryption** settings tab, set the settings as shown below:



Audio Encryption	
Preferred Formats	SRTP_AES_CM_128_HMAC_SHA1_80
Encrypted RTCP	☑
MKI	☑
Lifetime	Any
Interworking	☑
Symmetric Context Reset	☑
Key Change in New Offer	☐

Audio Encryption	
Preferred Formats	RTP
Interworking	☑
Symmetric Context Reset	☑
Lifetime	☐

Audio Encryption	
Capability Negotiation	☐

6. Click **Finish**.

Next steps

- Proceed to Define the Media Rules for MS Teams on page 115.

Related links

Configuring the ASBCE Callflow on page 90

Define the Media Rules for MS Teams

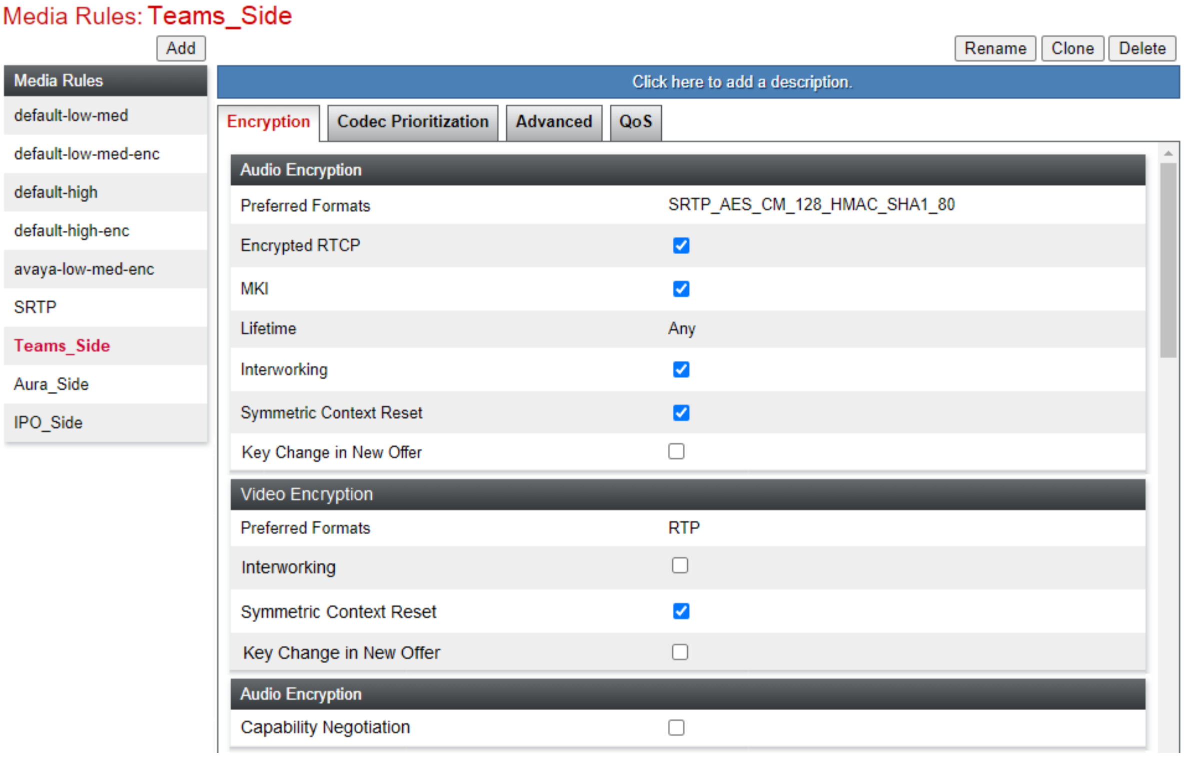
The ASBCE uses media rules to define RTP media packet parameters, such as prioritizing encryption techniques and packet encryption techniques. This process creates the media rules used for the MS Teams connection.

Before you begin

- Define a SIP Call Routing Profile for the IP Office on page 107.

Procedure

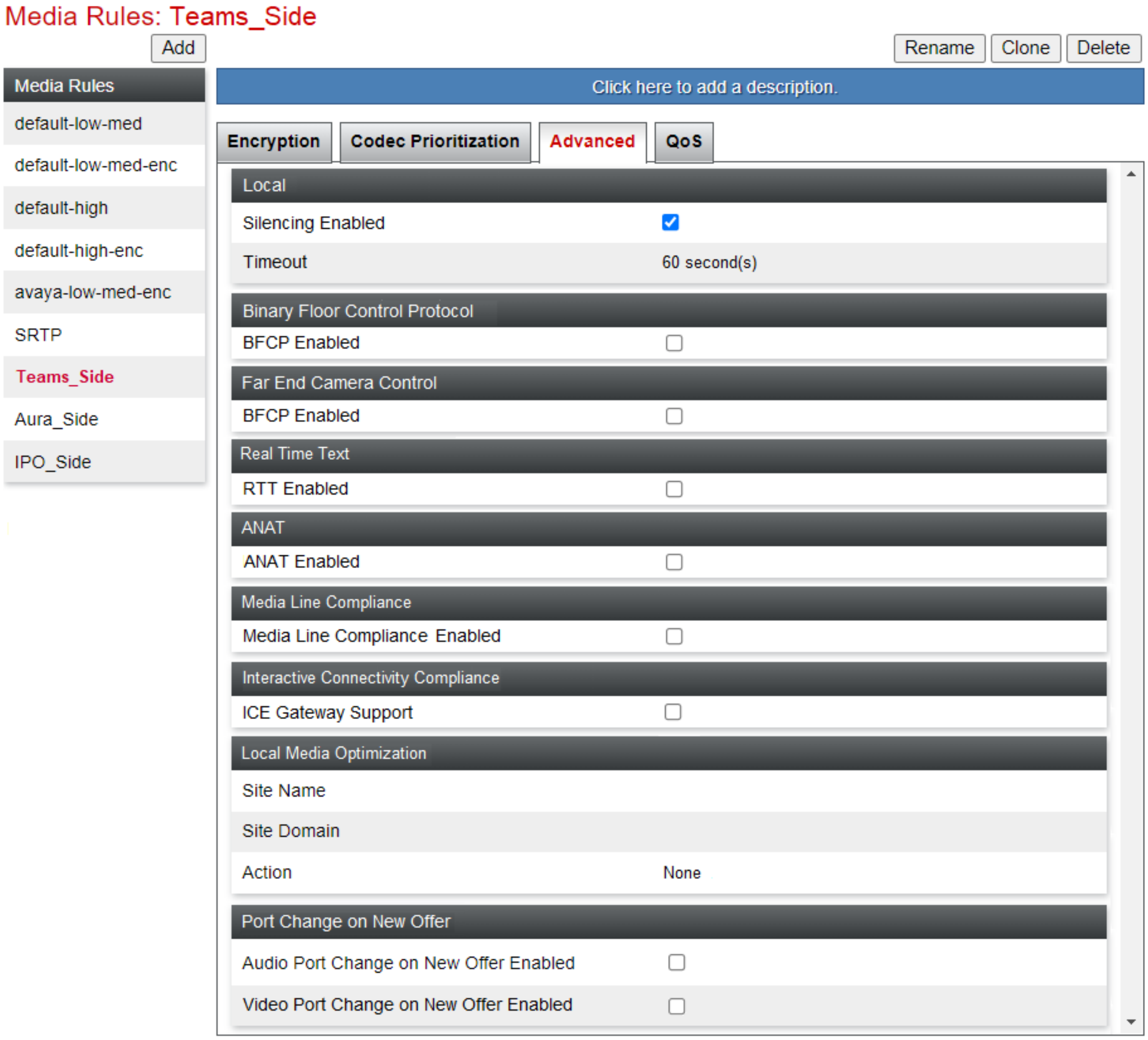
1. Select **Domain Policies** and then **Media Rules**.
2. Select the existing `default-low-med` rule and click **Clone**.
3. Enter a unique descriptive name for the new media rule and click **Finish**.
4. Select the new media rule and click **Edit**.
5. On the **Encryption** settings tab, set the settings as shown below:



Media Rules: Teams_Side

Audio Encryption	
Preferred Formats	SRTP_AES_CM_128_HMAC_SHA1_80
Encrypted RTCP	☑
MKI	☑
Lifetime	Any
Interworking	☑
Symmetric Context Reset	☑
Key Change in New Offer	□
Video Encryption	
Preferred Formats	RTP
Interworking	□
Symmetric Context Reset	☑
Key Change in New Offer	□
Audio Encryption	
Capability Negotiation	□

6. On the **Advanced** settings tab, set the settings as shown below:



Local	
Silencing Enabled	☑
Timeout	60 second(s)
Binary Floor Control Protocol	
BFCP Enabled	☐
Far End Camera Control	
BFCP Enabled	☐
Real Time Text	
RTT Enabled	☐
ANAT	
ANAT Enabled	☐
Media Line Compliance	
Media Line Compliance Enabled	☐
Interactive Connectivity Compliance	
ICE Gateway Support	☐
Local Media Optimization	
Site Name	
Site Domain	
Action	None
Port Change on New Offer	
Audio Port Change on New Offer Enabled	☐
Video Port Change on New Offer Enabled	☐

7. Click **Finish**.

Next steps

- Proceed to Create the Endpoint Policy Groups on page 116.

Related links

Configuring the ASBCE Callflow on page 90

Create the Endpoint Policy Groups

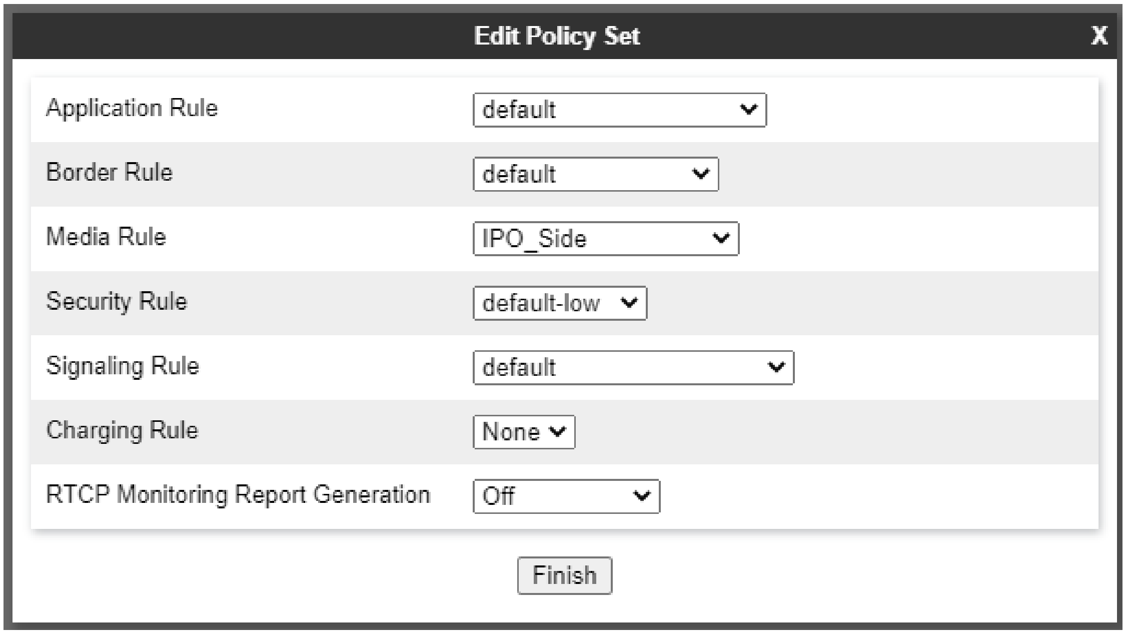
The ASBCE uses endpoint policy groups to group endpoint policy sets.

Before you begin

- Define the Media Rules for MS Teams on page 115.

Procedure

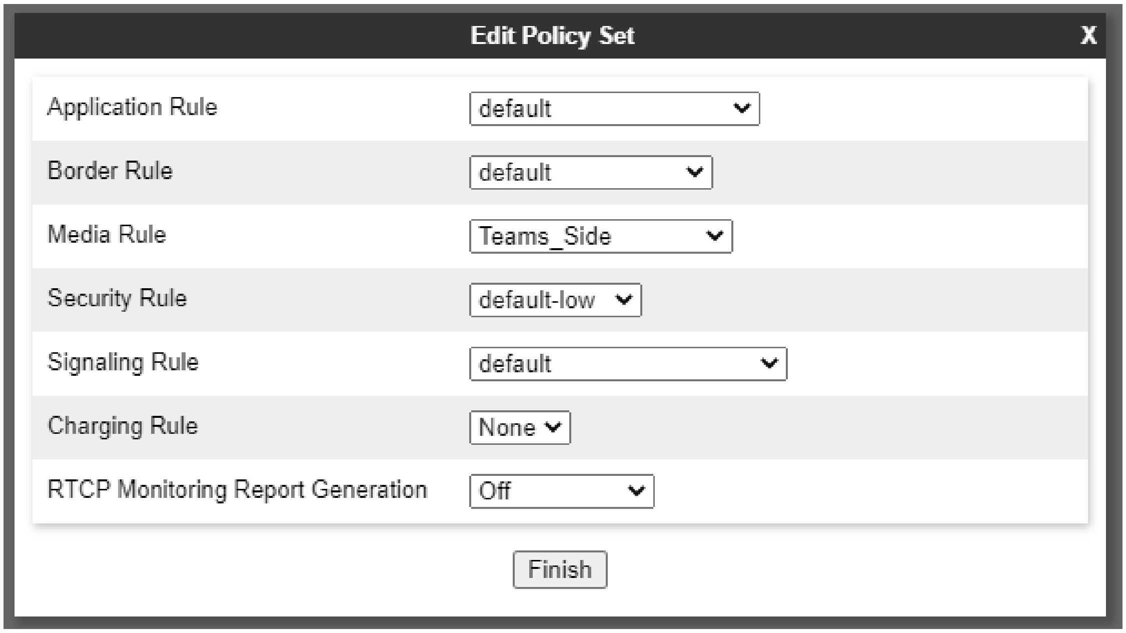
1. Select **Domain Policies** and then **Endpoint Policy Groups**.
2. Create an endpoint policy for the IP Office:
    a. Select the existing default-low policy and click **Clone**.
    b. Enter a unique descriptive name for the new policy and click **Finish**.
    c. Select the new policy and click **Edit**.
    d. Set the **Media Rule** to the media rule previously created for the IP Office connection.



Application Rule	default
Border Rule	default
Media Rule	IPO_Side
Security Rule	default-low
Signaling Rule	default
Charging Rule	None
RTCP Monitoring Report Generation	Off

    e. Click **Finish**.
3. Create an endpoint policy for MS Teams:
    a. Select the existing default-low policy and click **Clone**.
    b. Enter a unique descriptive name for the new policy and click **Finish**.
    c. Select the new policy and click **Edit**.

d. Set the **Media Rule** to the media rule previously created for the MS Teams connection.



Edit Policy Set

Application Rule	default
Border Rule	default
Media Rule	Teams_Side
Security Rule	default-low
Signaling Rule	default
Charging Rule	None
RTCP Monitoring Report Generation	Off

e. Click **Finish**.

Next steps

- Proceed to Create the SIP Signaling Interfaces on page 118.

Related links

Configuring the ASBCE Callflow on page 90

Create the SIP Signaling Interfaces

You need to define a SIP signaling interface for each SIP Server.

Before you begin

- Create the Endpoint Policy Groups on page 116.

Procedure

1. Select **Network & Flows** and then **Signaling Interface**.
2. Add a signaling interface for the IP Office:
   a. Click **Add**.
   b. In the **Name** field, enter a description name for the interface.
   c. In the **IP Address** field, select the ASBCE's internal network interface.
   d. Set the **TCP Port** and **UDP Port** values to blank. Set the **TLS Port** value to the port required.

e. In the **TLS Profile**, select the TLS server profile previously created for the IP Office.

f. Click **Finish**.

3. Add a signaling interface for MS Teams:

   a. Click **Add**.

   b. In the **Name** field, enter a description name for the interface.

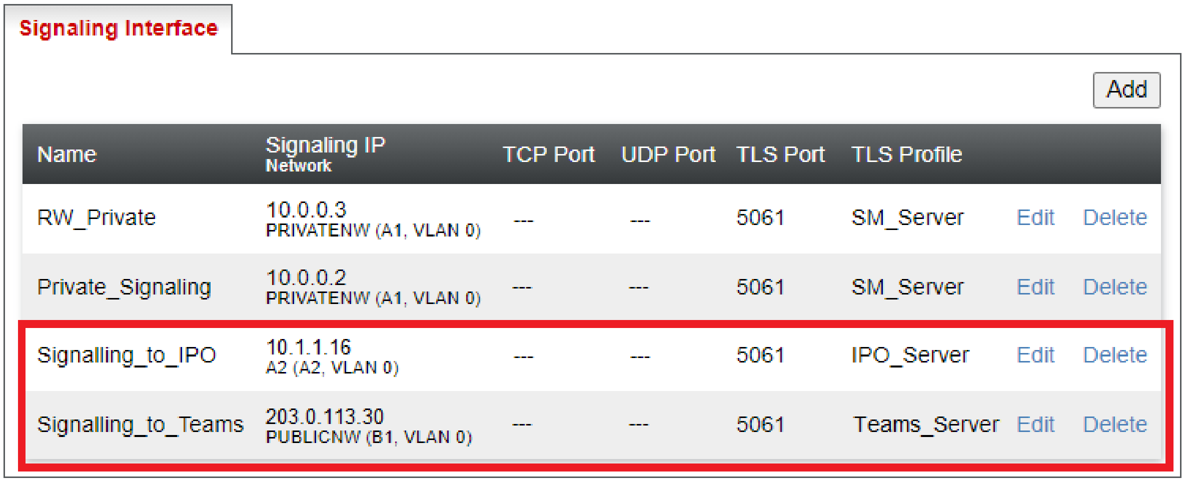
   c. In the **IP Address** field, select the ASBCE's external network interface.

   d. Set the **TCP Port** and **UDP Port** values to blank. Set the **TLS Port** to the port required.

   e. In the **TLS Profile**, select the TLS server profile previously created for MS Teams.

   f. Click **Finish**.

4. The final settings will look like the following example:



Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile		
RW_Private	10.0.0.3 PRIVATENW (A1, VLAN 0)	---	---	5061	SM_Server	Edit	Delete
Private_Signaling	10.0.0.2 PRIVATENW (A1, VLAN 0)	---	---	5061	SM_Server	Edit	Delete
Signalling_to_IPO	10.1.1.16 A2 (A2, VLAN 0)	---	---	5061	IPO_Server	Edit	Delete
Signalling_to_Teams	203.0.113.30 PUBLICNW (B1, VLAN 0)	---	---	5061	Teams_Server	Edit	Delete

Next steps

- Proceed to Create the SIP Media Interfaces on page 119.

Related links

Configuring the ASBCE Callflow on page 90

Create the SIP Media Interfaces

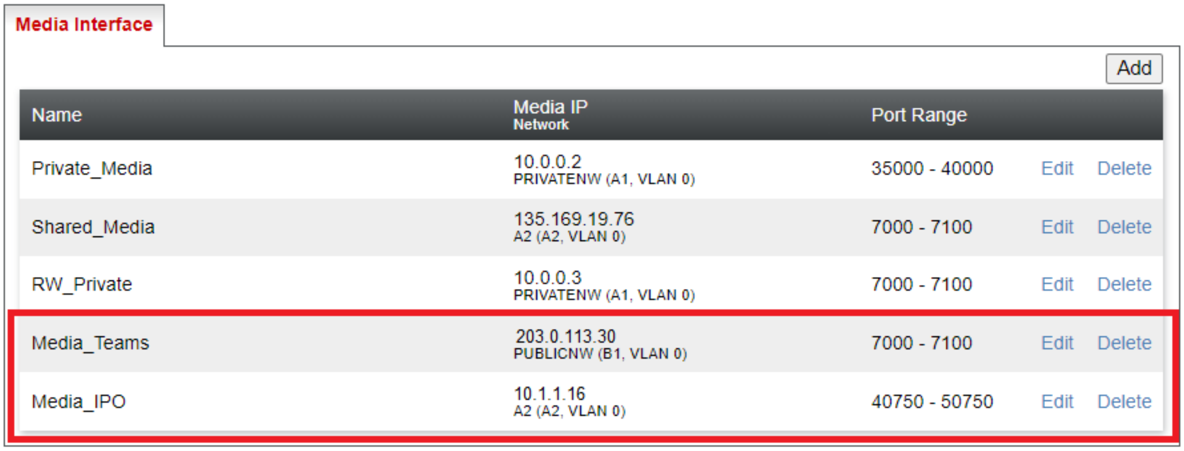
You need to define a media interface for each SIP Server to send and receive media (RTP or SRTP).

Before you begin

- Create the SIP Signaling Interfaces on page 118.

Procedure

1. Select **Network & Flows** and then **Media Interface**.
2. Add a media interface for the IP Office:
    a. Click **Add**.
    b. In the **Name** field, enter a description name for the interface.
    c. In the **IP Address** field, select the ASBCE's internal network interface.
    d. Set the ports range to match the RTP port range configured on the IP Office system. The default range is 46750 to 50750.
    e. Click **Finish**.
3. Add a media interface for MS Teams:
    a. Click **Add**.
    b. In the **Name** field, enter a description name for the interface.
    c. In the **IP Address** field, select the ASBCE's external network interface.
    d. Set the ports to match those used for SIP media with MS Teams.
    e. Click **Finish**.
4. The final settings will look like the following example:



Name	Media IP Network	Port Range		
Private_Media	10.0.0.2 PRIVATENW (A1, VLAN 0)	35000 - 40000	Edit	Delete
Shared_Media	135.169.19.76 A2 (A2, VLAN 0)	7000 - 7100	Edit	Delete
RW_Private	10.0.0.3 PRIVATENW (A1, VLAN 0)	7000 - 7100	Edit	Delete
Media_Teams	203.0.113.30 PUBLICNW (B1, VLAN 0)	7000 - 7100	Edit	Delete
Media_IPO	10.1.1.16 A2 (A2, VLAN 0)	40750 - 50750	Edit	Delete

Next steps

- Proceed to Configure the Server Flow for IP Office on page 121.

Related links

Configuring the ASBCE Callflow on page 90

Configure the Server Flow for IP Office

When the ASBCE receives a packet, it uses the (IP addresses, URIs, and so on) to determine which server flow it matches. After determining the server flow, the ASBCE applies the policies for the destination endpoint.

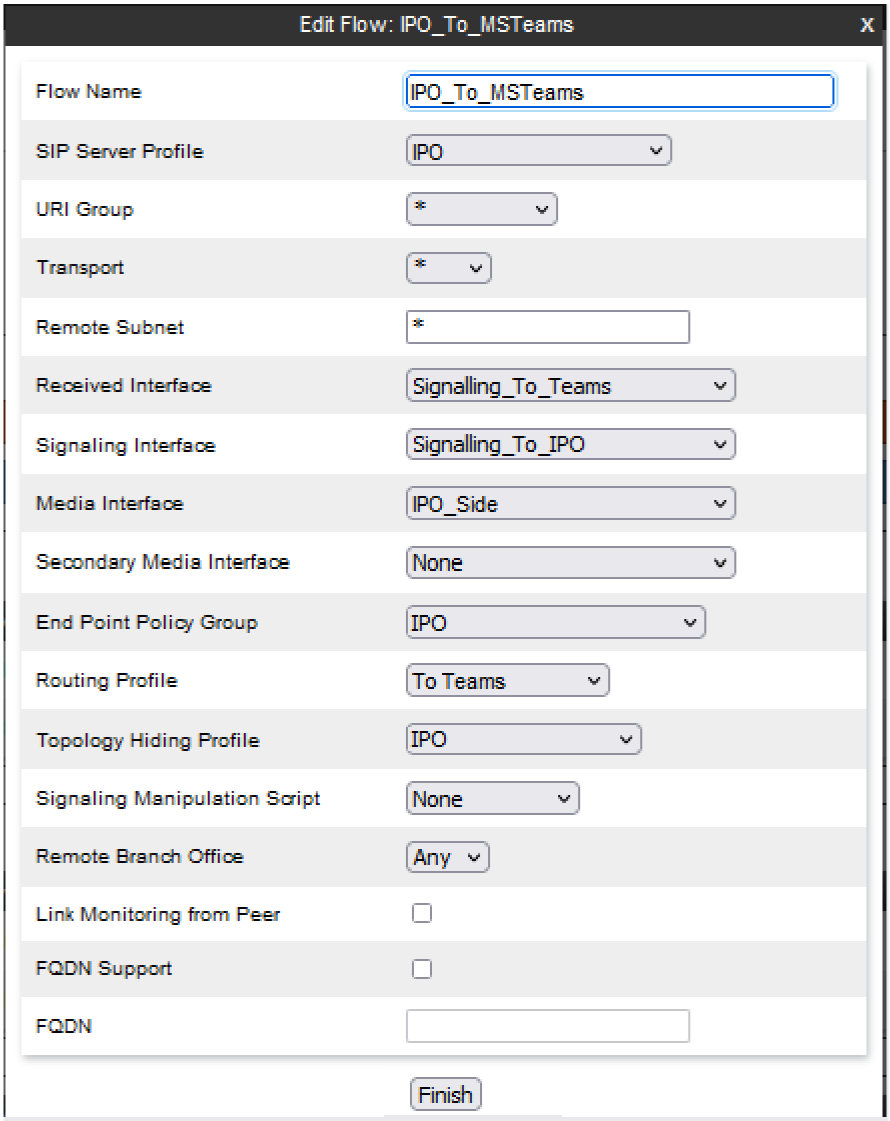
Before you begin

- Create the SIP Media Interfaces on page 119.

Procedure

1. Select **Network & Flows** and then **End Point Flows**.
2. Select the **Server Flows** tab.
3. Create a flow for calls from the IP Office to MS Teams:
    a. Click **Add**.
    b. For the **Flow Nam**e, enter a unique descriptive name.
    c. In the **SIP Server Profile**, **Signaling Interface**, **Media Interface**, **End Point Policy Group** and **Topology Hiding** fields, select entries created for the IP Office.
    d. For the **Received Interface** and **Routing Profiles**, select the signaling interface and routing profiles created for the MS Teams.

e. The final settings will look like the following example. Click **Finish**.



Edit Flow: IPO_To_MSTeams

Flow Name	IPO_To_MSTeams
SIP Server Profile	IPO
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Signalling_To_Teams
Signaling Interface	Signalling_To_IPO
Media Interface	IPO_Side
Secondary Media Interface	None
End Point Policy Group	IPO
Routing Profile	To Teams
Topology Hiding Profile	IPO
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	□
FQDN Support	□
FQDN	

4. Create a server flow for calls returning to the IP Office:

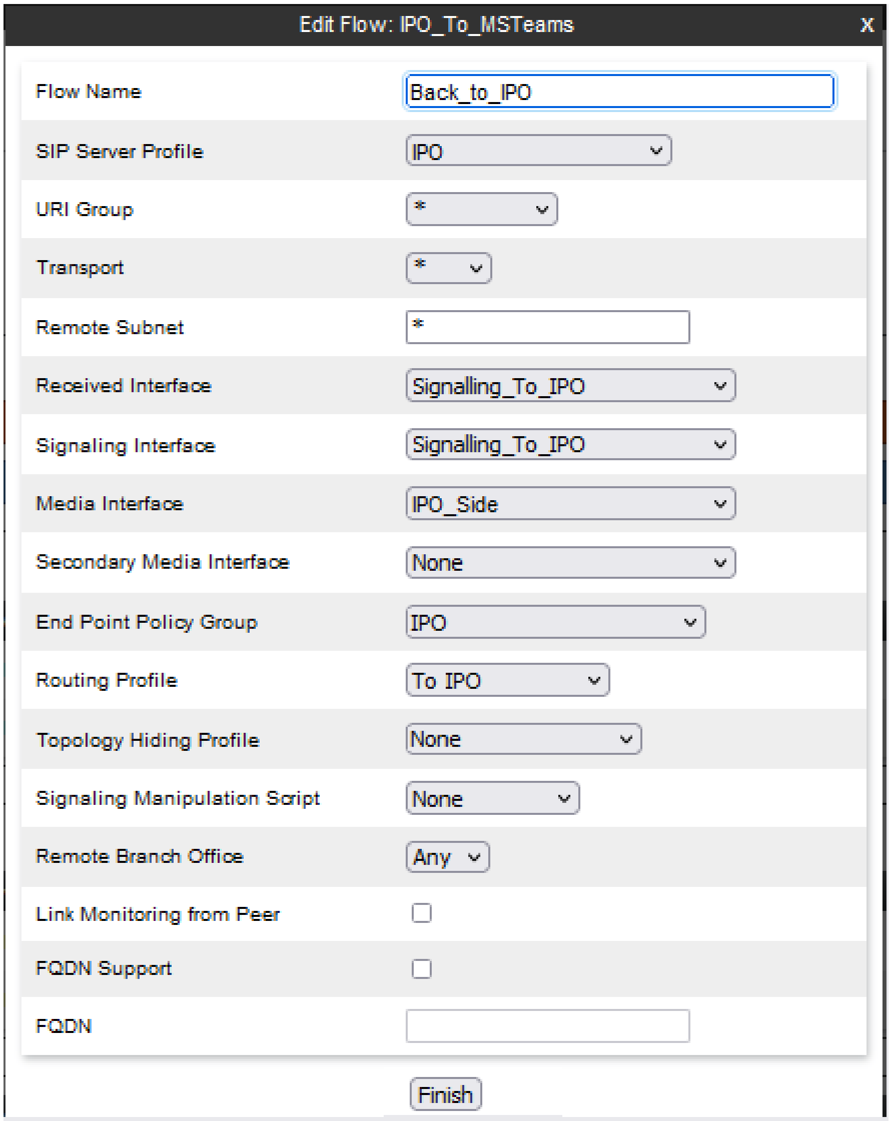
   a. Click **Add**.

   b. For the **Flow Name**, enter a unique descriptive name.

   c. In the **SIP Server Profile**, **Signaling Interface**, **Media Interface** and **End Point Policy Group** fields, select entries created for the IP Office.

   d. For the **Received Interface** and **Routing Profiles**, select the profiles created for IP Office.

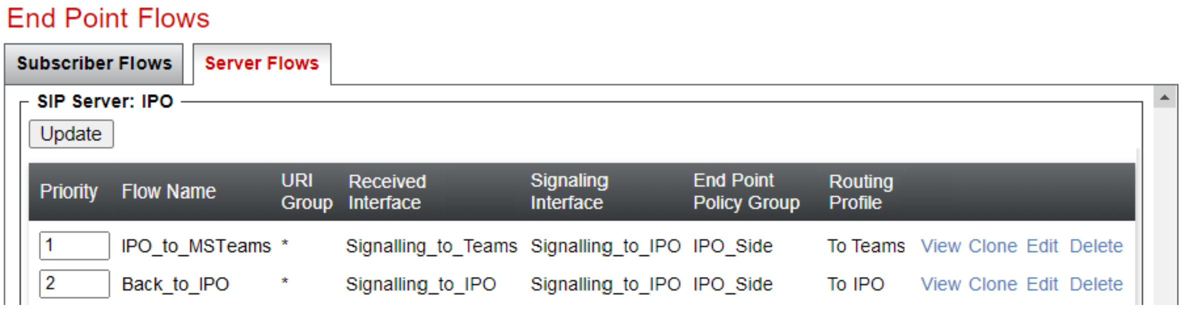
e. The final settings will look like the following example. Click **Finish**.



Edit Flow: IPO_To_MSTeams

Flow Name	Back_to_IPO
SIP Server Profile	IPO
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Signalling_To_IPO
Signaling Interface	Signalling_To_IPO
Media Interface	IPO_Side
Secondary Media Interface	None
End Point Policy Group	IPO
Routing Profile	To IPO
Topology Hiding Profile	None
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	□
FQDN Support	□
FQDN	

5. The server flow details will look like the following example:



End Point Flows

SIP Server: IPO

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	IPO_to_MSTeams	*	Signalling_to_Teams	Signalling_to_IPO	IPO_Side	To Teams	View Clone Edit Delete
2	Back_to_IPO	*	Signalling_to_IPO	Signalling_to_IPO	IPO_Side	To IPO	View Clone Edit Delete

Next steps

- Proceed to Configure the Server Flow for MS Teams on page 124.

Related links

Configuring the ASBCE Callflow on page 90

Configure the Server Flow for MS Teams

When the ASBCE receives a packet, it uses the (IP addresses, URIs, and so on) to determine which server flow it matches. After determining the server flow, the ASBCE applies the policies for the destination endpoint.

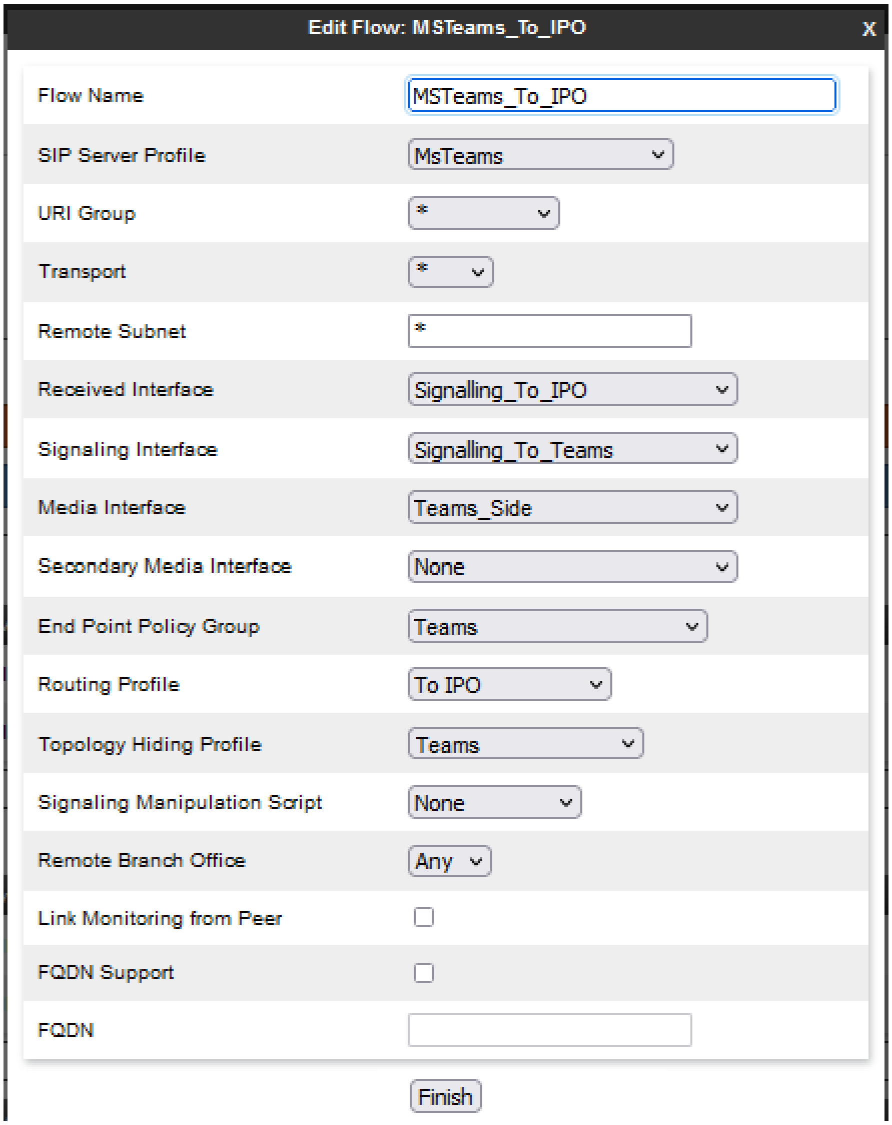
Before you begin

- Configure the Server Flow for IP Office on page 121.

Procedure

1. Select **Network & Flows** and then **End Point Flows**.
2. Select the **Server Flows** tab.
3. Click **Add**.
    a. For the **Flow Name**, enter a unique descriptive name.
    b. In the **SIP Server Profile**, **Signaling Interface**, **Media Interface**, **End Point Policy Group** and **Topology Hiding** fields, select entries created for the MS Teams.
    c. For the **Received Interface** and **Routing Profiles**, select the signaling interface and routing profiles created for the IP Office.

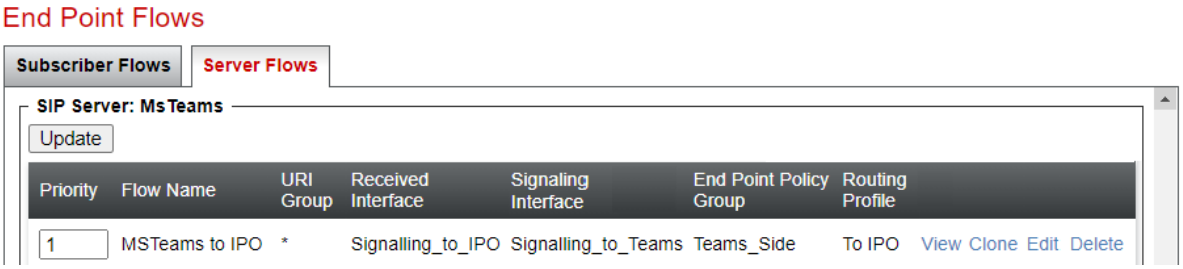
d. The final settings will look like the following example. Click **Finish**.



Edit Flow: MSTeams_To_IPO

Flow Name	MSTeams_To_IPO
SIP Server Profile	MsTeams
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Signalling_To_IPO
Signaling Interface	Signalling_To_Teams
Media Interface	Teams_Side
Secondary Media Interface	None
End Point Policy Group	Teams
Routing Profile	To IPO
Topology Hiding Profile	Teams
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	□
FQDN Support	□
FQDN	

4. Click **Finish**. The server flow details will look like the following example:



End Point Flows

SIP Server: MsTeams

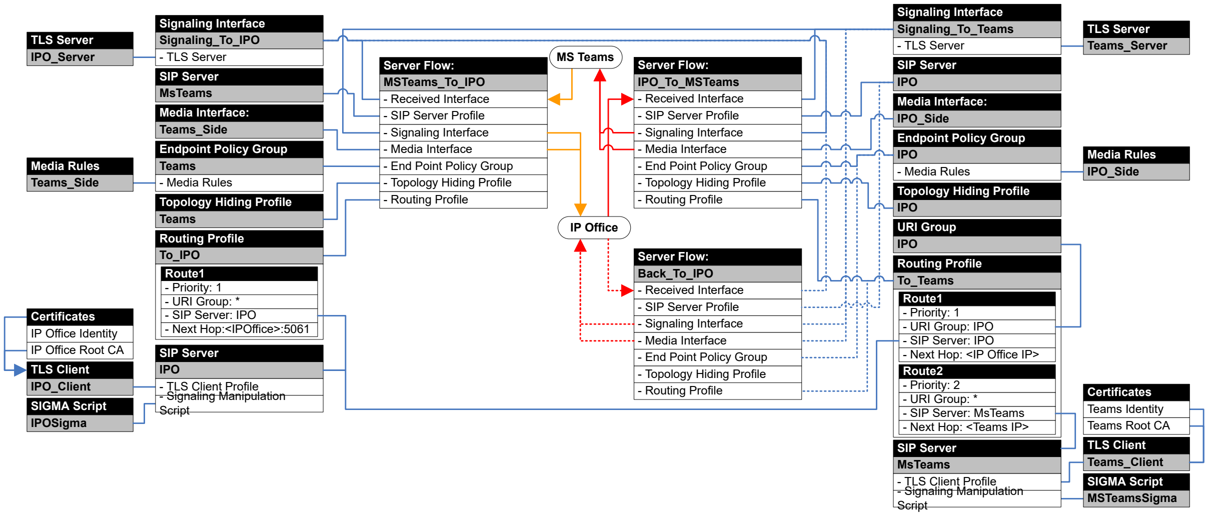
Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	MSTeams to IPO	*	Signalling_to_IPO	Signalling_to_Teams	Teams_Side	To IPO	View Clone Edit Delete

Related links

Configuring the ASBCE Callflow on page 90

ASBCE Flowchart

The following diagram is a summary of the elements configured on the ASBCE for our example scenario.



Related links

[Configuring the ASBCE Callflow](#) on page 90

Part 5: Additional Information

Chapter 18: Using Regular Expressions (regex)

MS Teams menus use 'dial patterns' to match numbers dialed. These patterns use regular expression (regex) strings. For example, the regex string `^2\d{2}$` matches any three-digit number beginning with a 2.

- MS Teams uses dial patterns in dial plans to match numbers dialed by a user and apply a number translation.
- MS Teams uses dial patterns in voice routes to match the number on outgoing calls to the routes for the call.

For additional information, refer to:

- https://docs.microsoft.com/en-us/dotnet/standard/base-types/regular-expression-language-quick-reference
- https://support.microsoft.com/en-us/topic/6ea76427-0892-4237-b024-10b418dcb05e
- https://regex101.com/ - This site provides a useful tool for testing the operation of your own regex strings.

Related links

Regex Example: Extension Number Matching on page 128
Regex Example: International Number Matching on page 129
Regex Syntax on page 130
Regex Telephone Number Examples on page 131
Digit Translations on page 132

Regex Example: Extension Number Matching

The example scenario uses a regex string to match any 3-digit number that begins with a 2. It does that to match any internal extension numbers on the IP Office system.

The regex string used was: `^\+?(2\d{2})$`

The string works as follows:

1. The `^` matches the start of the string.

2. The `\+?` is an optional match:
    a. The `\+` matches a literal `+` character (the E.164 international prefix indicator). The string needs a `\` as a `+` on its own is a regex command.
    b. The `?` modifies the preceding `\+` to mean match if the `+` is present or not.
3. The `( )` brackets group elements.
4. The brackets contain `2\d{2}`:
    a. The `2` matches a 2 at the start of the number.
    b. The `\d` matches any digit. The string needs a `\` as a `d` is the regex to match an alphabetic d.
    c. The `{2}` modifies the preceding `\d` to match 2 instances of that element.
    d. Therefore, `\d{2}` matches any two digits.
5. The `$` matches the end of the string. Including this means the pattern will not match longer numbers that begin with a 2.

Related links

Using Regular Expressions (regex) on page 128

Regex Example: International Number Matching

The example scenario uses a regex string to match the dialing of international calls. The string matches calls prefixed with either + or 00 (the UK dialing prefix for international calls).

The regex string used was: `^(\+|00)(.+)$`

The string works as follows:

1. The `^` matches the start of the string.
2. The `( )` brackets group elements for processing and, potentially for future digit translations.
3. The first pair of brackets contain `\+|00`:
    a. The `\+` matches a literal `+` character (the E.164 international prefix indicator). The string needs a `\` as a `+` on its own is a regex command.
    b. The `|` separates different possible matches.
    c. Therefore, the first pair of brackets matches any numbers beginning with a `+` or `00`.
4. The second pair of brackets contains `.+`:
    a. The `.` matches any digit or character.
    b. The `+` modifies the preceding . to match any number of matches.
    c. Therefore, the `.+` operate together to match any number of digits and characters.

5. The second pair of brackets enclose the match for any number of characters. In this example, a translation can use the value `$2` to refer to the matched characters, without their + or 00 prefix.
6. The `$` matches the end of the string.

Related links

Using Regular Expressions (regex) on page 128

Regex Syntax

This is a partial that considers regex items useful in the matching of telephone numbers.

String Position

Enclose a pattern with these to ensure matching to the full number.

Syntax	Description
`^`	**Start of String:** A ^ matches the start of the string.
`$`	**End of String:** A $ matches the end of the string.

Character Types

Syntax	Description
`.`	**Any Character:** Match any character.
`\d`	**Any Digit:** Match any digit. This just matches 0 to 9, not the dialing characters *, + and #.
`\`	**Escape:** Use `\` to escape characters that otherwise are regex commands. For example, `\*` matches a * digit, `\+` matches a +. • Note: You do not need the escape character when the character to match is in `[]` brackets.

Group

Syntax	Description
`|`	**Or:** Separate alternate possible matches. For example: `569|669` matches either 569 or 669. You can specify multiple alternates, for example: `569|669|779`.
`( )`	**Group:** Use `( )` brackets to group syntax. When performing digit translations, the element `$1` in a translation represents the digits matched by the syntax in the first pair of `( )` brackets in the original pattern, `$2` the second pair of brackets, and so on.

Table continues…

Syntax	Description
[ ]	**Range of Characters:** Use [ ] square brackets to group specific characters or a character range to match. For example: [569] matches a 5, 6 or 9; [5-7] matches a 5, 6 or 7; [0-9*#+] matches any telephone number character. • When used in [ ] brackets, characters such as + and * do not need a preceding \ escape. • Use a ^ character inside the [] brackets to perform a non-match. For example: [^569] matches any digit other than a 5, 6 or 9.

Number of Matches

Syntax	Description
?	**Match zero or one:** Use a ? question mark to match zero or one occurrences of the preceding element. For example: ^\+? matches numbers beginning with or without a + prefix.
*	**Match zero or more:** Use an * to match zero or more occurrences of the preceding element. For example: ^1.*$ matches 1 and numbers beginning with a 1. To match an actual *, use *.
+	**Match one or more:** Use a + plus sign to match one or more occurrences of the preceding element. For example: ^1.+$ matches number beginning with a 1 but not just 1. To match an actual +, use \+.
{n}	**Match N times:** Match the preceding item exactly n times. For example: ^.{3} matches 3-digit numbers.
{n,}	**Match N or more times:** Match the preceding item n or more times. For example: ^. {3,}$ matches 3-digit or longer numbers.
{,m}	**Match up to M times:** Match the preceding item up to m times. For example: ^.{,4}$ matches numbers up to 4-digits long.
{n,m}	**Match between N to M times:** Match the preceding item at least m times, but no more than n times. For example: ^.{3,4}$ matches 3 and 4-digit numbers.

Related links

Using Regular Expressions (regex) on page 128

Regex Telephone Number Examples

The following are example regex strings for telephone number matching.

Purpose	Pattern	Description
Match any numeric telephone number	^\d+$	–
Match any dialing	^.+$	This differs from the above match for any numbers as it also includes +, * and # elements that may occur in telephone number.
	^[0-9*#]$	This differs from the above match in that is only matches telephone numbers using the numeric digits, * and #.
Match any 7-digit number	^(\d{7})$	This would for example, match the dialing of a local number in the US. The number requires a transform to add the digits for national dialing with the local area code.
Match any 11-digit number beginning with a +1	^\+1(\d{10})$	This would for example, match the dialing of a national number within the US.
Match any 11-digit number beginning with 1555 or 1666	^\+1(555|666)(\d{7})$	This example would match the dialing of national numbers in the US with the area code 555 or 565.

Related links

Using Regular Expressions (regex) on page 128

Digit Translations

The MS Teams Dial plan forms use regex strings to perform digit translations (see Creating a Dial Plan on page 49). For these, it is important to understand the role of ( ) brackets in the original digit pattern and the $ elements in the translations.

The strings use ( ) brackets to group elements in the original match. The translations refer to each pair of brackets using the format $n in the translation. That is, $1 represents the characters matched by the regex pattern in the first pair of brackets, $2 the second pair of brackets, and so on.

Regex numbers the brackets in order of the opening (bracket symbols from left-to-right in the original patterns. That includes patterns with nested bracket pairs, for example ((\+44)|(044)|(0)) contains $1 [((\+44)|(044)|(0))], $2 [(\+44)], $3 [(044)], and $4 [(0)].

- Note: In these examples, spaces in the numbers are just present for readability and do not represent actual spaces in the number strings.

Name	Original Number	Pattern	Translation	Translated Number
Add UK 01632 area code to any 6-digit numbers	`309348`	`^(\d{6})$`	`01632$1`	`01632 309348`
Add US 416 area code to 7-digit numbers	`555 0134`	`^(\d{7})$`	`416$1`	`416 555 0134`
Change 00 prefix numbers to E.164 format	`0044 1632 309348`	`^00(.+)$`	`+1$1`	`+44 1632 309348`
	`001 416 555 0134`			`+1 416 555 0134`
Change E.164 format numbers to non-E.164 format	`+44 1632 309348`	`^\+(.*)$`	`00$1`	`0044 1632 309348`
	`+1 416 555 0134`			`001 416 555 0134`
Convert an international number back to a national number	`0044 1632 309348`	`^(00|\+)44(.+)$`	`0$2`	`01632 309348`
	`+44 1632 309348`			`01632 309348`

Related links

Using Regular Expressions (regex) on page 128

Chapter 19: Troubleshooting

This section provides notes for obtaining information on direct routing operation.

Related links

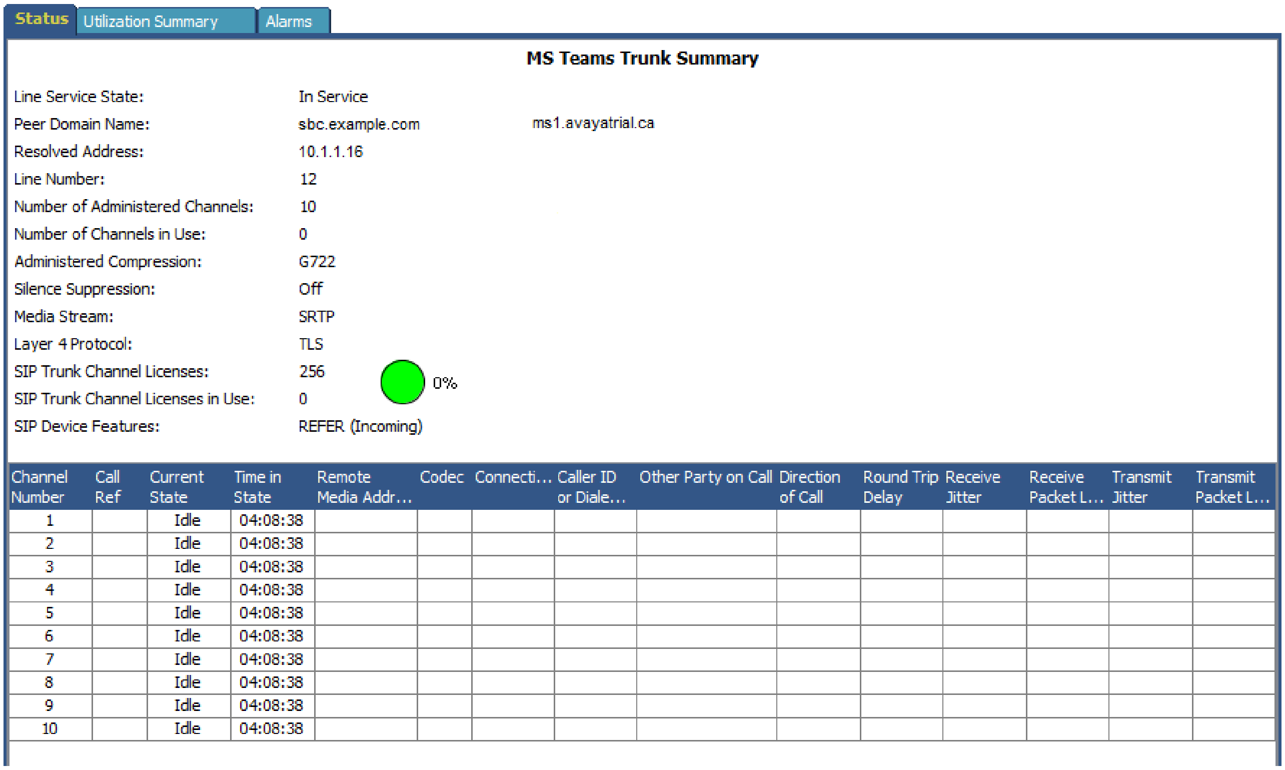
System Status Application on page 134
SysMonitor on page 135
Monitoring Direct Routing on page 137

System Status Application

You can use the System Status Application to check the status of the MS Teams Line and the users.

Line Status

System Status Application displays the MS Teams Line in the same way as other types of SIP trunks.



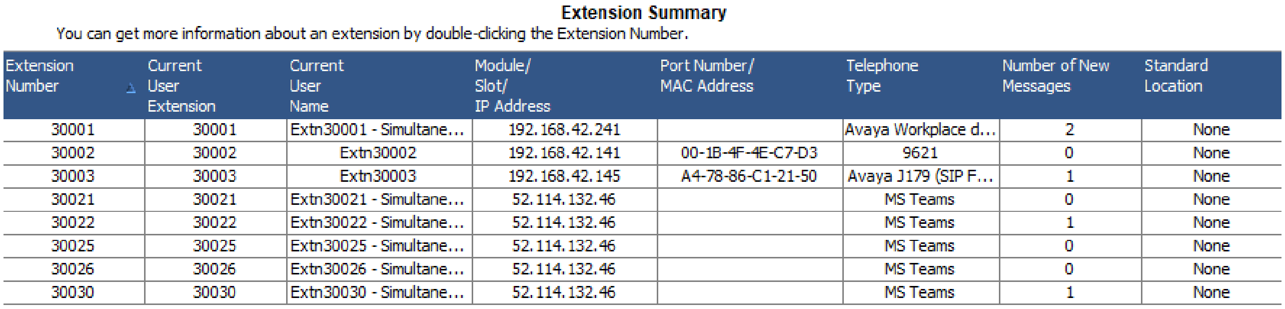
MS Teams Trunk Summary

Line Service State:	In Service	
Peer Domain Name:	sbc.example.com	ms1.avayatrial.ca
Resolved Address:	10.1.1.16	
Line Number:	12	
Number of Administered Channels:	10	
Number of Channels in Use:	0	
Administered Compression:	G722	
Silence Suppression:	Off	
Media Stream:	SRTP	
Layer 4 Protocol:	TLS	
SIP Trunk Channel Licenses:	256	● 0%
SIP Trunk Channel Licenses in Use:	0	
SIP Device Features:	REFER (Incoming)	

Channel Number	Call Ref	Current State	Time in State	Remote Media Addr…	Codec	Connecti…	Caller ID or Diale…	Other Party on Call	Direction of Call	Round Trip Delay	Receive Jitter	Receive Packet L…	Transmit Jitter	Transmit Packet L…
1		Idle	04:08:38											
2		Idle	04:08:38											
3		Idle	04:08:38											
4		Idle	04:08:38											
5		Idle	04:08:38											
6		Idle	04:08:38											
7		Idle	04:08:38											
8		Idle	04:08:38											
9		Idle	04:08:38											
10		Idle	04:08:38											

User Status

System Status Application displays MS Teams IP Office users in the same way as simultaneous users.



Extension Summary

You can get more information about an extension by double-clicking the Extension Number.

Extension Number	Current User Extension	Current User Name	Module/ Slot/ IP Address	Port Number/ MAC Address	Telephone Type	Number of New Messages	Standard Location
30001	30001	Extn30001 - Simultane…	192.168.42.241		Avaya Workplace d…	2	None
30002	30002	Extn30002	192.168.42.141	00-1B-4F-4E-C7-D3	9621	0	None
30003	30003	Extn30003	192.168.42.145	A4-78-86-C1-21-50	Avaya J179 (SIP F…	1	None
30021	30021	Extn30021 - Simultane…	52.114.132.46		MS Teams	0	None
30022	30022	Extn30022 - Simultane…	52.114.132.46		MS Teams	1	None
30025	30025	Extn30025 - Simultane…	52.114.132.46		MS Teams	0	None
30026	30026	Extn30026 - Simultane…	52.114.132.46		MS Teams	0	None
30030	30030	Extn30030 - Simultane…	52.114.132.46		MS Teams	1	None

Related links

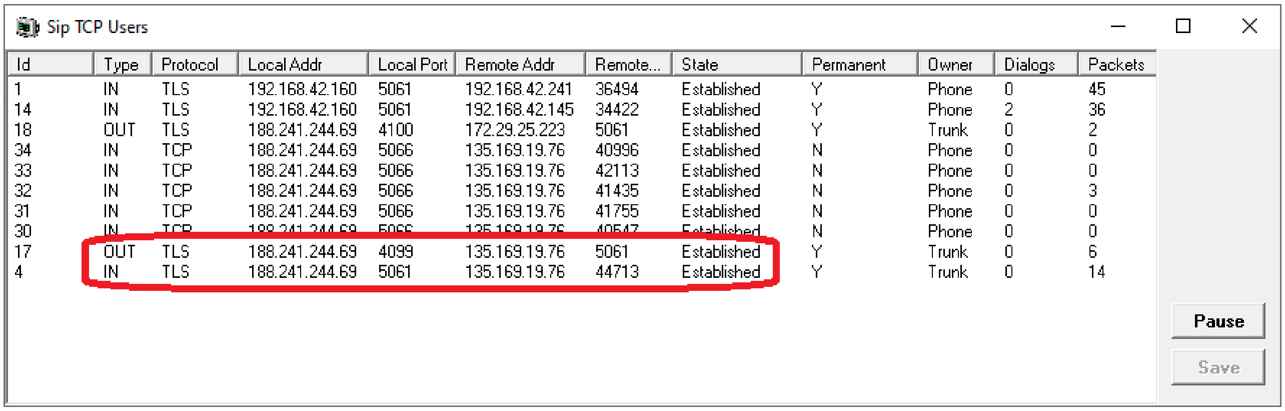
Troubleshooting on page 134

SysMonitor

You can use SysMonitor for troubleshooting.

Connection Status

Supporting MS Teams uses 2 TLS sockets between ASBCE and IP Office. You can check these in the SIP TCP Users status menu (**Status** > **SIP Tcp User Data...**).

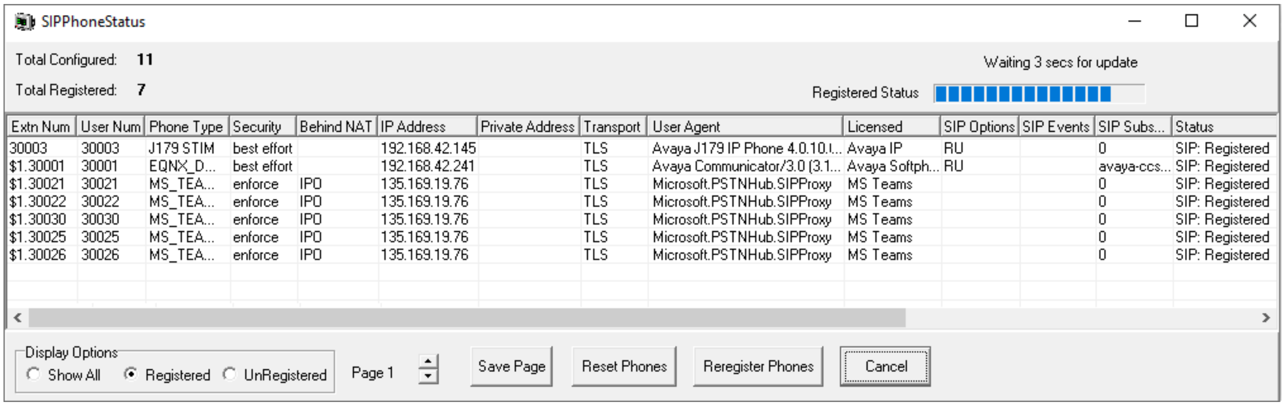


Id	Type	Protocol	Local Addr	Local Port	Remote Addr	Remote...	State	Permanent	Owner	Dialogs	Packets
1	IN	TLS	192.168.42.160	5061	192.168.42.241	36494	Established	Y	Phone	0	45
14	IN	TLS	192.168.42.160	5061	192.168.42.145	34422	Established	Y	Phone	2	36
18	OUT	TLS	188.241.244.69	4100	172.29.25.223	5061	Established	Y	Trunk	0	2
34	IN	TCP	188.241.244.69	5066	135.169.19.76	40996	Established	N	Phone	0	0
33	IN	TCP	188.241.244.69	5066	135.169.19.76	42113	Established	N	Phone	0	0
32	IN	TCP	188.241.244.69	5066	135.169.19.76	41435	Established	N	Phone	0	3
31	IN	TCP	188.241.244.69	5066	135.169.19.76	41755	Established	N	Phone	0	0
30	IN	TCP	188.241.244.69	5066	135.169.19.76	40547	Established	N	Phone	0	0
17	OUT	TLS	188.241.244.69	4099	135.169.19.76	5061	Established	Y	Trunk	0	6
4	IN	TLS	188.241.244.69	5061	135.169.19.76	44713	Established	Y	Trunk	0	14

If there are not 2 TCP sockets to the ASBCE IP address, the most likely cause is a certificate issue between ASBCE and IP Office.

User Status

You can check the configuration of individual users using **SIP Phone Status** menu (**Status** > **SIP Phone Status**).



Total Configured: **11**

Total Registered: **7**

Waiting 3 secs for update

Extn Num	User Num	Phone Type	Security	Behind NAT	IP Address	Private Address	Transport	User Agent	Licensed	SIP Options	SIP Events	SIP Subs...	Status
30003	30003	J179 STIM	best effort		192.168.42.145		TLS	Avaya J179 IP Phone 4.0.10.l...	Avaya IP	RU		0	SIP: Registered
$1.30001	30001	EQNX_D...	best effort		192.168.42.241		TLS	Avaya Communicator/3.0 (3.1...	Avaya Softph...	RU		avaya-ccs...	SIP: Registered
$1.30021	30021	MS_TEA...	enforce	IPO	135.169.19.76		TLS	Microsoft.PSTNHub.SIPProxy	MS Teams			0	SIP: Registered
$1.30022	30022	MS_TEA...	enforce	IPO	135.169.19.76		TLS	Microsoft.PSTNHub.SIPProxy	MS Teams			0	SIP: Registered
$1.30030	30030	MS_TEA...	enforce	IPO	135.169.19.76		TLS	Microsoft.PSTNHub.SIPProxy	MS Teams			0	SIP: Registered
$1.30025	30025	MS_TEA...	enforce	IPO	135.169.19.76		TLS	Microsoft.PSTNHub.SIPProxy	MS Teams			0	SIP: Registered
$1.30026	30026	MS_TEA...	enforce	IPO	135.169.19.76		TLS	Microsoft.PSTNHub.SIPProxy	MS Teams			0	SIP: Registered

Tracing Calls

To escalate issues to Avaya, you will require SysMonitor traces. You should generate these using the default filters plus, enable **SIP** and **Verbose** for the **Filters** > **Trace Options** > **SIP** tab. For call related issues, ASBCE traces for the same event/time period are also required, see ASBCE SIP Tracing on page 138.

Related links

Troubleshooting on page 134

Monitoring Direct Routing

The MS Teams admin portal displays a summary of the status of all SBC connections including the ASBCE. To display these details, after logging in select **Voice** > **Direct Routing**. The dashboard shown lists various details for the SBC connections and indicates if there are any issues such as certificate errors.

For details, refer to https://docs.microsoft.com/en-us/microsoftteams/direct-routing-health-dashboard.

Related links

Troubleshooting on page 134

Chapter 20: ASBCE SIP Tracing

This section provides a summary of generating and downloading SIP call traces from the ASBCE.

- The processes require you to know the `ipcs` and `root` passwords for ASBCE.
- You need to use SSH to access the ASBCE command line.
- You need to use SFTP/SSH file transfer to download the trace files.

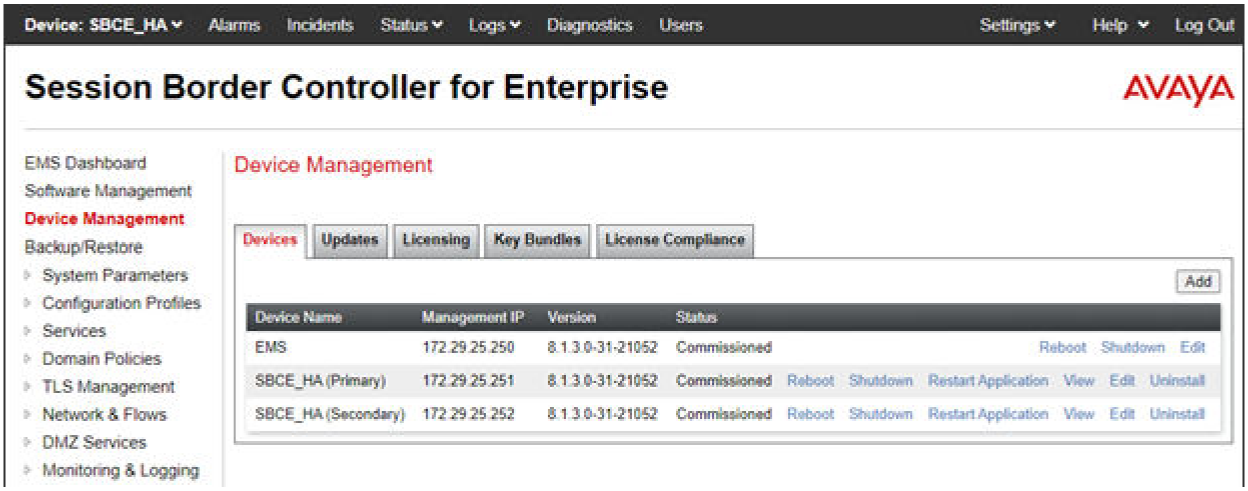
Related links

Tracing Address on page 138
Tracing SIP Calls on the ASBCE on page 139
Downloading Traces from the ASBCE on page 140

Tracing Address

First login into EMS web page of the ASBCE to check the IP address of the *SBCE_HA (Primary)*. You need that address for SSH access to the session to it. If the ASBCE is not a setup with High Availability, then SSH uses the ASBCE IP address.

In the upper left corner of the web page, choose **Device: SBCE** and click on **Device Management**. Note the IP address of the *SBCE_HA(Primary)*. In the example below, `172.29.25.251`.



Device Name	Management IP	Version	Status	
EMS	172.29.25.250	8.1.3.0-31-21052	Commissioned	Reboot Shutdown Edit
SBCE_HA (Primary)	172.29.25.251	8.1.3.0-31-21052	Commissioned	Reboot Shutdown Restart Application View Edit Uninstall
SBCE_HA (Secondary)	172.29.25.252	8.1.3.0-31-21052	Commissioned	Reboot Shutdown Restart Application View Edit Uninstall

Related links

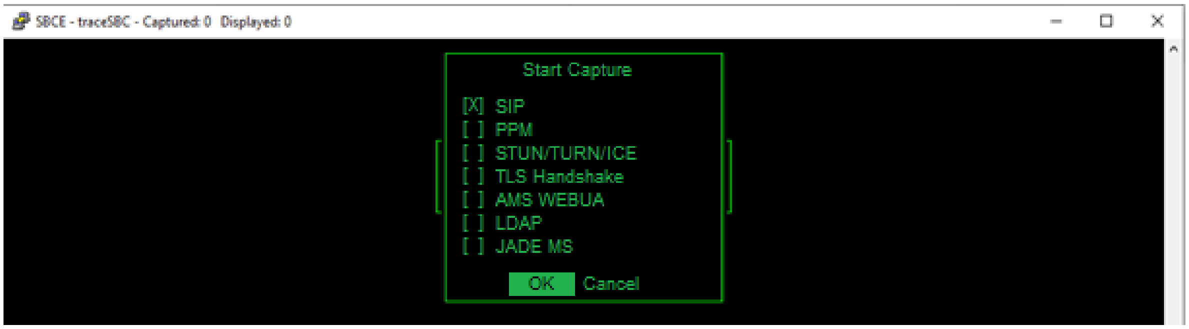
ASBCE SIP Tracing on page 138

Tracing SIP Calls on the ASBCE

Use the following process to obtain SIP traces from the ASBCE.

Procedure

1. Open an SSH command line session to the SBCE_HA(Primary) IP address.
2. Enter the command login as `ipcs` and enter the ipcs user password when requested.
3. Enter the command `[ipcs@SBCE ~]$ su –` and enter the root password when requested.
4. Check that the cursor is now prefixed with `[root@SBCE ~]`.
5. Enter the command `traceSBC`.
6. Press **S** to start setting up the trace capture.

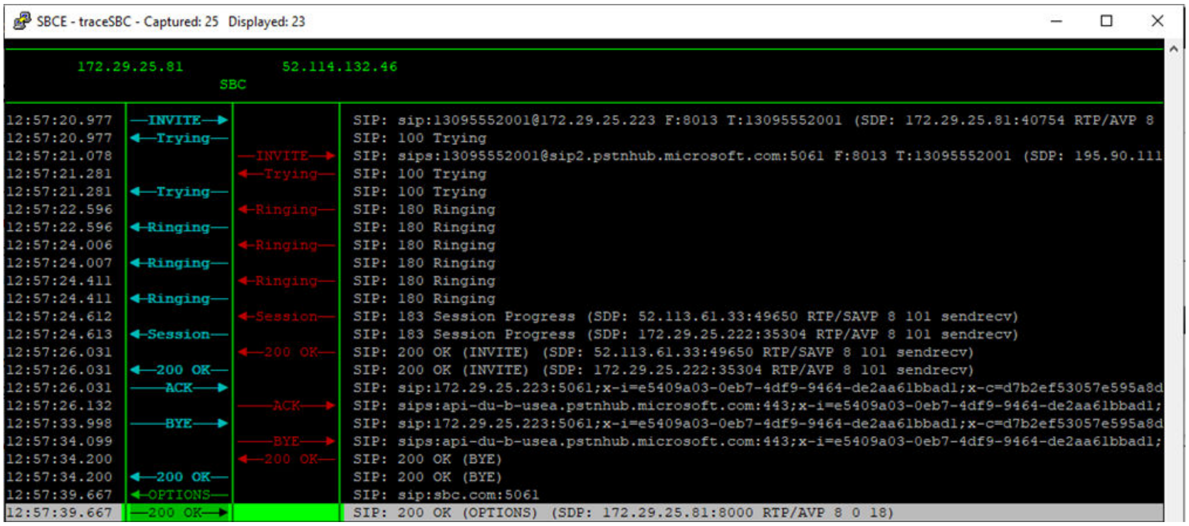


```
Start Capture

[X] SIP
[ ] PPM
[ ] STUN/TURN/ICE
[ ] TLS Handshake
[ ] AMS WEBUA
[ ] LDAP
[ ] JADE MS

OK   Cancel
```

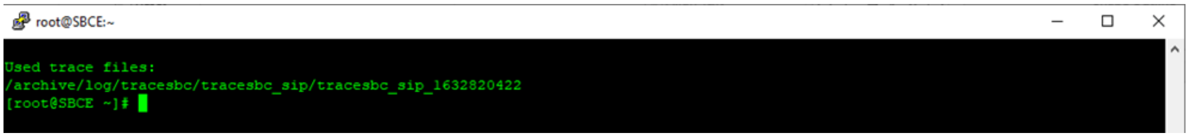
7. Using the space and cursor keys, select **SIP**.
8. Select **OK** and press enter. The trace shows the current SIP activities.



```
        172.29.25.81          52.114.132.46
                    SBC
12:57:20.977 ──INVITE──►              SIP: sip:13095552001@172.29.25.223 F:8013 T:13095552001 (SDP: 172.29.25.81:40754 RTP/AVP 8
12:57:20.977 ◄──Trying──              SIP: 100 Trying
12:57:21.078              ──INVITE──► SIP: sips:13095552001@sip2.pstnhub.microsoft.com:5061 F:8013 T:13095552001 (SDP: 195.90.111
12:57:21.281              ◄──Trying── SIP: 100 Trying
12:57:21.281 ◄──Trying──              SIP: 100 Trying
12:57:22.596              ◄─Ringing── SIP: 180 Ringing
12:57:22.596 ◄─Ringing──              SIP: 180 Ringing
12:57:24.006              ◄─Ringing── SIP: 180 Ringing
12:57:24.007 ◄─Ringing──              SIP: 180 Ringing
12:57:24.411              ◄─Ringing── SIP: 180 Ringing
12:57:24.411 ◄─Ringing──              SIP: 180 Ringing
12:57:24.612              ◄─Session── SIP: 183 Session Progress (SDP: 52.113.61.33:49650 RTP/SAVP 8 101 sendrecv)
12:57:24.613 ◄─Session──              SIP: 183 Session Progress (SDP: 172.29.25.222:35304 RTP/AVP 8 101 sendrecv)
12:57:26.031              ◄──200 OK── SIP: 200 OK (INVITE) (SDP: 52.113.61.33:49650 RTP/SAVP 8 101 sendrecv)
12:57:26.031 ◄──200 OK──              SIP: 200 OK (INVITE) (SDP: 172.29.25.222:35304 RTP/AVP 8 101 sendrecv)
12:57:26.031 ─────ACK───►             SIP: sip:172.29.25.223:5061;x-i=e5409a03-0eb7-4df9-9464-de2aa61bbad1;x-c=d7b2ef53057e595a8d
12:57:26.132              ─────ACK───► SIP: sips:api-du-b-usea.pstnhub.microsoft.com:443;x-i=e5409a03-0eb7-4df9-9464-de2aa61bbad1;
12:57:33.998 ─────BYE───►             SIP: sip:172.29.25.223:5061;x-i=e5409a03-0eb7-4df9-9464-de2aa61bbad1;x-c=d7b2ef53057e595a8d
12:57:34.099              ─────BYE───► SIP: sips:api-du-b-usea.pstnhub.microsoft.com:443;x-i=e5409a03-0eb7-4df9-9464-de2aa61bbad1;
12:57:34.200              ◄──200 OK── SIP: 200 OK (BYE)
12:57:34.200 ◄──200 OK──              SIP: 200 OK (BYE)
12:57:39.667 ◄─OPTIONS──              SIP: sip:sbc.com:5061
12:57:39.667 ──200 OK──►              SIP: 200 OK (OPTIONS) (SDP: 172.29.25.81:8000 RTP/AVP 8 0 18)
```

9. Run the call scenarios which you want traced.
10. When completed, press **Q** to quit tracing.

11. The screen displays the details of the saved trace log file. Note the details.



```
Used trace files:
/archive/log/tracesbc/tracesbc_sip/tracesbc_sip_1632820422
[root@SBCE ~]# 
```

Next steps

- See Downloading Traces from the ASBCE on page 140.

Related links

ASBCE SIP Tracing on page 138

Downloading Traces from the ASBCE

The ASBCE stores trace logs in the directory `/archive/log/tracesbc/tracesbc_sip`.

You can download the files using the `ipcs` user name and password and an SFTP client.

Related links

ASBCE SIP Tracing on page 138

Chapter 21: Additional Help and Documentation

The following pages provide sources for additional help.

Related links

Additional Manuals and User Guides on page 141
Getting Help on page 141
Finding an Avaya Business Partner on page 142
Additional IP Office resources on page 142
Training on page 143

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 142).

Related links

Additional Help and Documentation on page 141

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 142.

Related links

Additional Help and Documentation on page 141

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 141

Additional IP Office resources

In addition to the documentation website (see Additional Manuals and User Guides on page 141), there are a range of website that provide information about Avaya products and services including IP Office.

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

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

- **Avaya Sales & Partner Portal** *(*https://sales.avaya.com*)*

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

- **Avaya IP Office Knowledgebase** *(*https://ipofficekb.avaya.com*)*

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

- **Avaya Support** *(*https://support.avaya.com*)*

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

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

    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 DevConnect** (https://www.devconnectprogram.com/)

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

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

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

Related links

Additional Help and Documentation on page 141

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 141

Index