



ORACLE

Oracle SBC with Microsoft Survivable Branch Appliance

Technical Application Note

ORACLE
COMMUNICATIONS

Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Revision History

As a best practice always follow the latest Application note found on the Oracle TechNet Website.

<https://www.oracle.com/technical-resources/documentation/acme-packet.html>

Version	Description of Changes	Date Revision Completed
1.0 GA	Initial Publication	8/12/2020
2.0 GA	Changes to Network Design and Architecture Changes to Oracle SBC Configuration	8/11/2021



Contents

1. INTENDED AUDIENCE.....	5
2. PREREQUISITES.....	5
3 RELATED DOCUMENTATION	5
3.1 ORACLE DOCUMENTATION –	5
3.2 MICROSOFT DOCUMENTATION –	5
4. ABOUT MICROSOFT SURVIVABLE BRANCH APPLIANCE	6
4.1 SUPPORTED MICROSOFT TEAMS CLIENTS.....	7
4.2 AVAILABLE CALLING FUNCTIONALITY IN OFFLINE MODE.....	7
5. SET UP REQUIREMENTS	7
5.1 ORACLE SBC	7
5.2 MICROSOFT SBA.....	8
5.3 DR-SBA SERVER DIMENSIONS	8
5.4 FIREWALL AND PORT REQUIREMENTS	8
5.5 DNS RESOLUTION	9
5.6 TLS CERTIFICATES	10
6. DEPLOYING THE MICROSOFT SBA	12
6.1 INSTALL THE MICROSOFT SBA APPLICATION.....	12
6.2 CREATE AZURE ACTIVE DIRECTORY SBA APPLICATION	16
6.2.1 SBA CONNECTOR REGISTRATION ON MICROSOFT AZURE.....	16
6.2.2 SETTING IMPLICIT GRANT TOKEN.....	18
6.2.3 REQUEST API PERMISSIONS	18
6.2.4 CREATE CLIENT SECRET	20
6.3 CONFIGURE DIRECT ROUTING SURVIVABLE BRANCH APPLIANCE (SBA) IN OFFICE 365	22
6.3.1 TEAMS SURVIVABLE BRANCH APPLIANCE	23
6.3.2 TEAMS BRANCH SURVIVABILITY POLICY.....	23
6.3.3 ASSIGNING TEAMS BRANCH SURVIVABILITY POLICY TO USERS	24
6.4 SBA API CONFIGURATION.....	25
6.4.1 BASIC CONFIGURATION	26
6.4.2 GENERAL CONFIGURATION	27
6.4.3 SECURE CONFIGURATION.....	28

7. CONFIGURING THE ORACLE SBC	29
7.1 CONFIGURE PHYSICAL INTERFACE FOR DR-SBA	30
7.2 CONFIGURE NETWORK INTERFACE FOR DR-SBA	30
7.3 CONFIGURE REALM FOR DR-SBA	31
7.4 CREATE MICROSOFT SBA CERTIFICATE-RECORD	32
7.5 CREATE DR-SBA TLS PROFILE.	34
7.6 MEDIA SECURITY	35
7.6.1 SDES PROFILE	36
7.6.2 MEDIA-SEC-POLICY	37
7.7 CONFIGURE THE SBA SESSION-AGENT	37
7.8 CONFIGURE THE SIP-INTERFACE	39
7.9 CONFIGURE STEERING-POOL	40
7.10 MODIFICATION TO LOCAL-POLICY	41
7.10.1 OUTBOUND CALLS TO MICROSOFT	41
7.10.2 INBOUND CALLS FROM MICROSOFT	41



1. Intended Audience

This document describes how to connect the **Oracle SBC to Microsoft Survivable Branch Appliance**. The document is intended for use by Oracle Systems Engineers, third party Systems Integrators, Oracle Enterprise customers and partners and end users of the Oracle Session Border Controller (SBC). It is assumed that the reader is familiar with basic operations of the Oracle Session Border Controller.

2. Prerequisites

This Document assumes users have an existing environment with the **Oracle SBC connected to Microsoft Teams Direct Routing Interface with Media Bypass Enabled**. All the Tenant and Licensing requirements are in place and operational. In addition, the information used below is for example only, and specific to Oracle's Test environment. All IP addresses, FQDN's and other information used in the example below cannot be used outside of this Oracle Communications test environment.

The initial implementation of the Oracle SBC with Microsoft Teams is outside the scope of this document. If users do not have an existing, operational setup and require information regarding the initial setup and configuration, please refer to the documentation at the link below or reach out to your Oracle Account Team.

Oracle highly recommends referring **Oracle ESBC with Microsoft Teams Media Bypass - Enterprise Model** Application Note before configuring the Microsoft SBA with the Oracle SBC. To interwork Microsoft SBA with Oracle SBC several configuration elements for the existing Microsoft Teams Direct Routing configuration will be reused.

Please visit the Section 4 of the document "Planning Direct Routing" to understand the requirements related to Tenant Licensing and FQDN requirements.

<https://www.oracle.com/a/otn/docs/OracleSBCwithMSFTTeamsMediaBypassEnabled.pdf>

3 Related Documentation

3.1 Oracle Documentation –

<https://www.oracle.com/a/otn/docs/OracleSBCwithMSFTTeamsMediaBypassEnabled.pdf>

https://docs.oracle.com/en/industries/communications/enterprise-session-bordercontroller/8.4.0/configuration/esbc_scz840_configuration.pdf

https://docs.oracle.com/en/industries/communications/session-bordercontroller/8.4.0/security/sbc_scz840_security.pdf

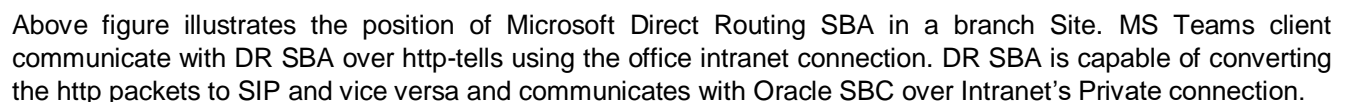
3.2 Microsoft Documentation –

<https://docs.microsoft.com/en-us/microsoftteams/direct-routing-survivable-branch-appliance>


<https://docs.microsoft.com/en-us/microsoftteams/direct-routing-configure>

PSTN voice is considered as a business-critical application with high expectation to availability. Microsoft **Survivable Branch Appliance** allows customers to place and receive calls via **Microsoft Teams Direct Routing** utilizing the **Oracle SBC** if the internet/Office 365 connectivity is broken.

Note: Local Media Optimization (LMO) is not supported through DR SBA.



Microsoft SBA communicates with Office 365 over REST API connection and Oracle SBC over the Session initiation Protocol SIP protocol. The communication is secured via TLS and SRTP where the signaling is encrypted with TLS 1.2 and media packets are encrypted with SRTP Protocol for security.



During an internet outage when client is unable to communicate with O365 it automatically switches to DR SBA which is assigned to the User Survivable Business Appliance Policy. The client in offline mode can make receive PSTN Calls via DR SBA. Once the internet connectivity is restored, calls automatically switch to O365 SIP proxy and are completed over internet using the normal direct routing path using the Microsoft SIP Proxy and Oracle SBC Public connection. CDRs are pushed to O365 once the internet connectivity is restored.

DR SBA requires media bypass enabled on the Tenant so in both modes the media traverses directly from MS Teams Client to Oracle SBC and vice versa.

4.1 Supported Microsoft Teams clients

The SBA feature is supported on the following Microsoft Teams clients:

- Microsoft Teams Windows desktop
- Microsoft Teams MacOS desktop

4.2 Available calling functionality in offline mode

When the Microsoft Teams client is in offline mode, the following calling related functionality is available:

- Making PSTN calls via local SBA/SBC with media flowing via the SBC
- Receiving PSTN calls via local SBA/SBC with media flowing via the SBC
- Hold & Resume of PSTN calls

5. Set Up Requirements

5.1 Oracle SBC

Microsoft SBA has been successfully tested and validated with the Oracle SBC running the Software release **SCZ900**. This software release with the configuration listed below can run on any of the following products: -

- AP 1100
- AP 3900
- AP 4600
- AP 6350
- AP 6300
- AP 3950
- AP 4900
- VME

5.2 Microsoft SBA

Windows Server - Microsoft SBA application is a software Application that runs on **Microsoft Windows Server**. This can be a standalone server, or a Virtual Machine on VMware Esxi / Windows Hyper-V. Recommended Microsoft Windows Server version are Windows Server 2012, 2016 and 2019.

The Direct Routing SBA utilizes the Azure AD to sync the Subscriber information and Data, so an internet connection is **must** requirement on the SBA Server. A Public IP address is not necessary on SBA Server.

Microsoft SBA Package requires **.net Framework 4.8 and C++ redistributable v14** to be installed as prerequisites on the Windows Server. TLS1.2 should be enabled on the Server to support DR-SBA TLS requirements.

Please contact your Microsoft Representative for the Latest DR SBA Package.

5.3 DR-SBA Server Dimensions

As per Microsoft Load Testing Standards an Azure Standard B2ms Machine i.e. - Windows Server with 2 Vcpus and 8 GiB or RAM can handle up to 5000 Users. This can be scaled in or out as per your specific requirement. Oracle has performed the Microsoft SBA validation testing on Windows Server 2016 Datacenter Edition with 128 GB SSD and 2 cups, 8 GiB memory configurations.

5.4 Firewall and Port Requirements

Below Table illustrates the firewall Port requirements for the Communication of DR-SBA with MS Teams Client, O365 and Oracle SBC.

Microsoft Teams Client to Direct Routing SBA

Traffic Type	From	To	Source Port	Destination Port
TCP	MS Teams Client	DR-SBA	Any	3443
TCP	MS Teams Client	DR-SBA	Any	4444
TCP	MS Teams Client	DR-SBA	Any	8443

Direct Routing SBA to Office 365 and Oracle SBC

Traffic Type	From	To	Source Port	Destination Port
Https	SBA	Azure IPs	Any	443
TCP	SBA	Oracle SBC	Any	5061 (may vary based on the port configured on SBC)
Https	Oracle SBC	DR SBA	Any	5061

For the purpose of this document It is assumed that the Windows server has been properly deployed, configured and is setup with the necessary rules to allow **ICMP,TCP,UDP,HTTP,HTTPS** communication methods.

5.5 DNS Resolution

A DNS-Name (FQDN) must be assigned to the DR SBA Server. The DR-SBA-FQDN resolves to the IP address of the DR SBA. A Public IP is not required on DR SBA, but SBA Server must have an internet connection to access Azure AD. The DR-SBA-FQDN can be Public or a Private. Optionally you can join the Windows Server to a Domain as well.

Oracle SBC communicates with DR-SBA over the Oracle-SBC-FQDN which is registered on the O365 Tenant.(New-CsOnlinePSTNGateway).Normally Oracle-SBC-FQDN resolves to a Public IP Address. If there is no internet SBA Server will not be able to resolve the Oracle-SBC-FQDN, also since the communication happens over the Private Subnet a Local DNS can be used to resolve the SBC FQDN to the Private IP of the sip-interface communicating with the DR-SBA. In case a DNS Server is not available/required you can edit the host file entry on the Windows Server to resolve the Oracle SBC FQDN to the Private IP.

The Hosts file can be found under **C:\Windows\System32\drivers\etc**.Enter the Oracle SBC Direct Routing FQDN and the Ip address used to communicate the Oracle SBC with DR-SBA

Below is an example of a host file taken from the SBA Server which resolves the Oracle SBC FQDN to the Private IP Address of the sip-interface used to communicate with DR-SBA.

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com           # source server
#       38.25.63.10       x.acme.com               # x client host
192.168.3.62             telechat.o-test06161977.com
#
# localhost name resolution is handled within DNS itself.
#   127.0.0.1             localhost
#   ::1                   localhost
```

Similarly, the workstations running MS Teams Client should be able to resolve the DR-SBA FQDN and establish a connectivity with the SBA. Update the hosts file if required on the Windows Machines or update the

corresponding file on MAC-OS. If the SBA Application is not reachable by Teams Client, the SBA will be marked OOS and calls won't switch to DR-SBA in Survivability mode.

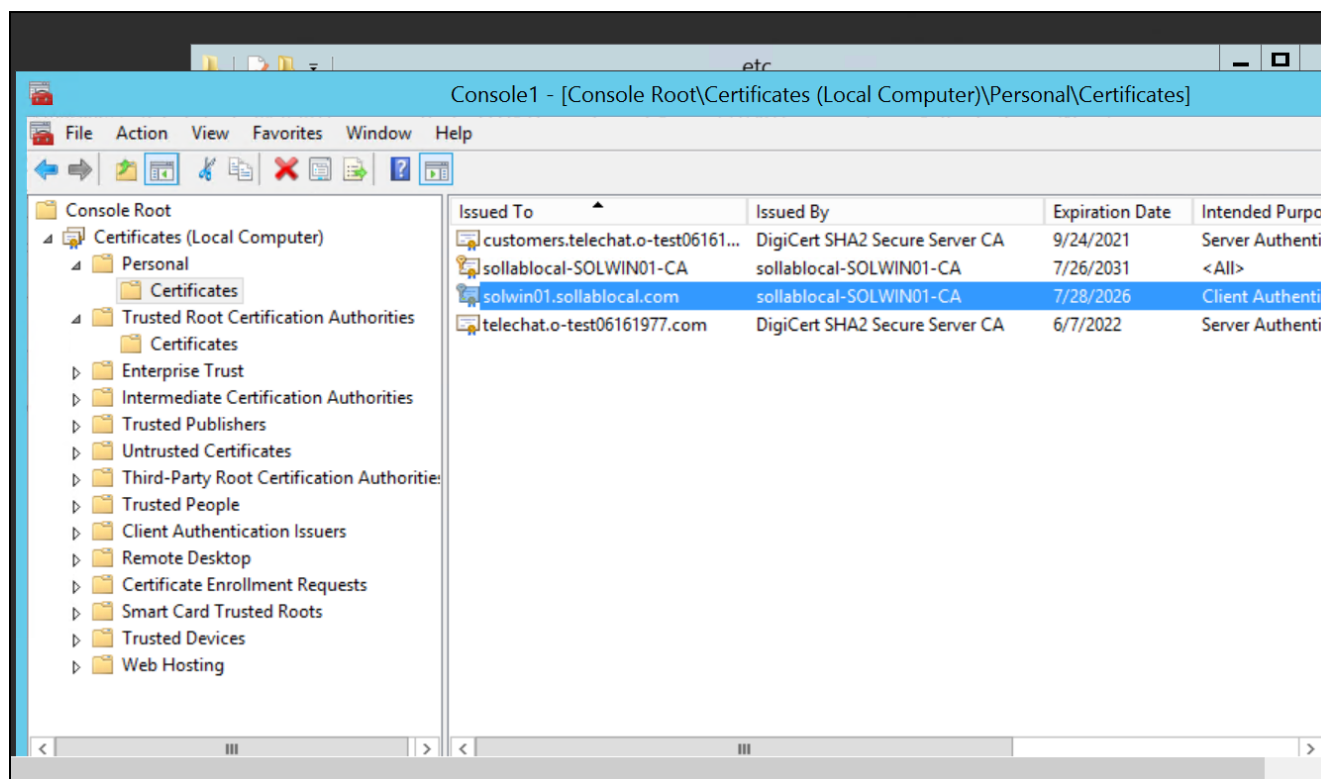
5.6 TLS Certificates

SBA communicates with Oracle SBC and Teams Client over TLS 1.2 Transport Protocol. This requires certificates exchange between the entities. Microsoft requires a SHA-256 Certificate to be assigned on the SBA Server.

DR-SBA can be assigned a Public or a Private Certificate. Create and assign a TLS Certificate (Public or Private to the DR-SBA).

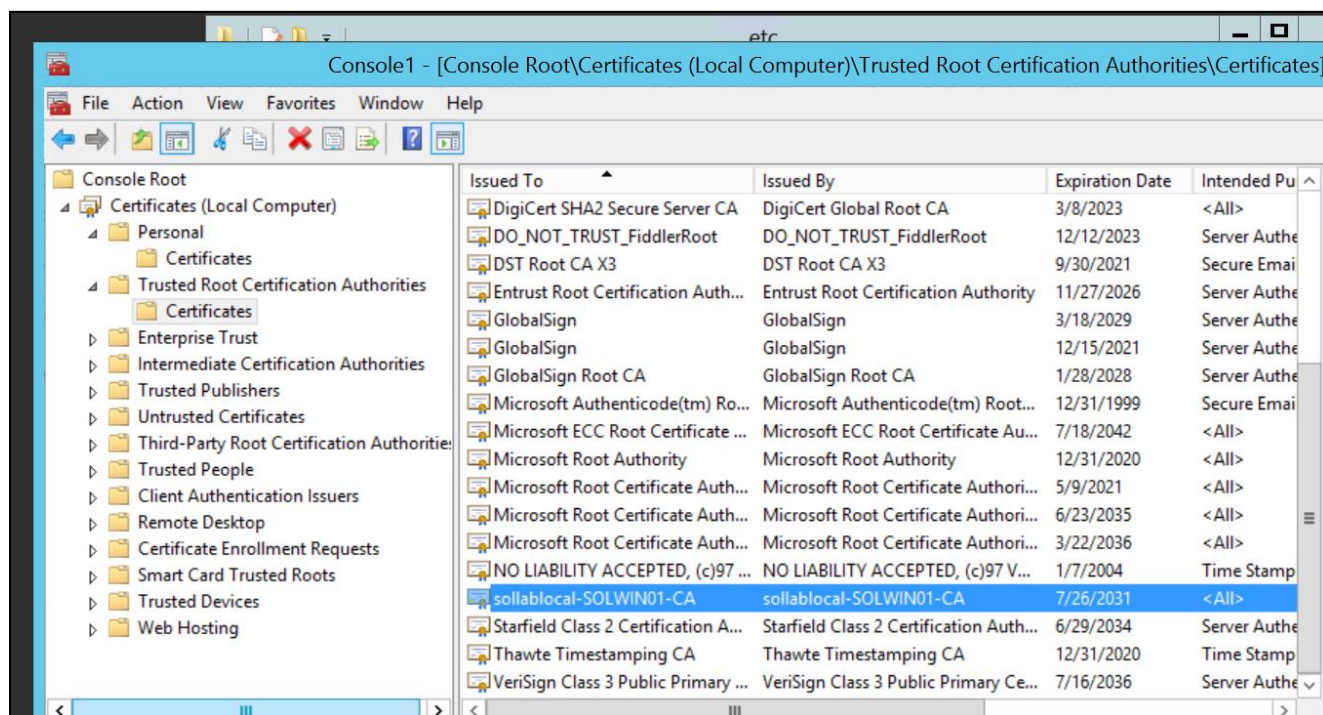
DR-SBA-FQDN should be present in the common-name or in the SAN on the TLS Certificate. Wildcard Certificates are also supported.

The SBA Server Certificate must be present in the Personal>Certificates Location on the Certificate Store on the SBA Server.



The Root CA Certificate of the Certificate Signaling Authority that signed the SBA Certificate as well as the Oracle SBC Certificate must be present in the Trusted root Certificate Authorities Location on the Certificate Store on the DR-SBA Server. Any Intermediate Certificate must also be imported to Intermediate Certificate Authorities location.

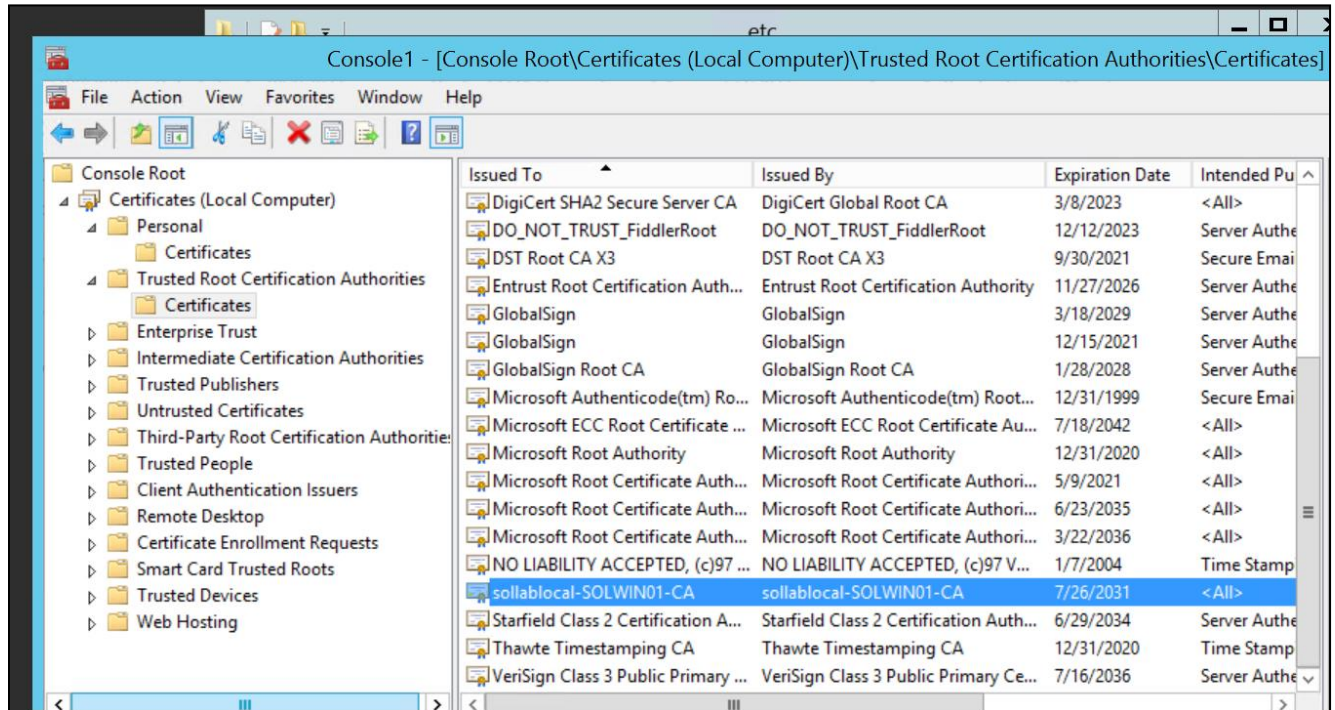
Below Figure is an example from the Certificate Store on the DR-SBA Server.



All the Teams Client Workstations that require DR-SBA Support **must also trust the DR-SBA's Certificate Authority Certificate**. The Root CA of the Certificate Signaling Authority that signed the SBA Certificate must be present in the Trusted root Certificate Authorities Location on the Certificate Store. Any Intermediate Certificate must also be imported to Intermediate Certificate Authorities location.

Upload the Certificate at the equivalent location on MAC-OS Workstations.

Below Figure is an example from the Certificate Store on a Windows Machine that runs the MS Teams Client. DR-SBA CAs Certificate is present in the Trusted Root Certificates Section as show below.



6. Deploying the Microsoft SBA

The Deployment of Microsoft SBA is divided to Four Sections -

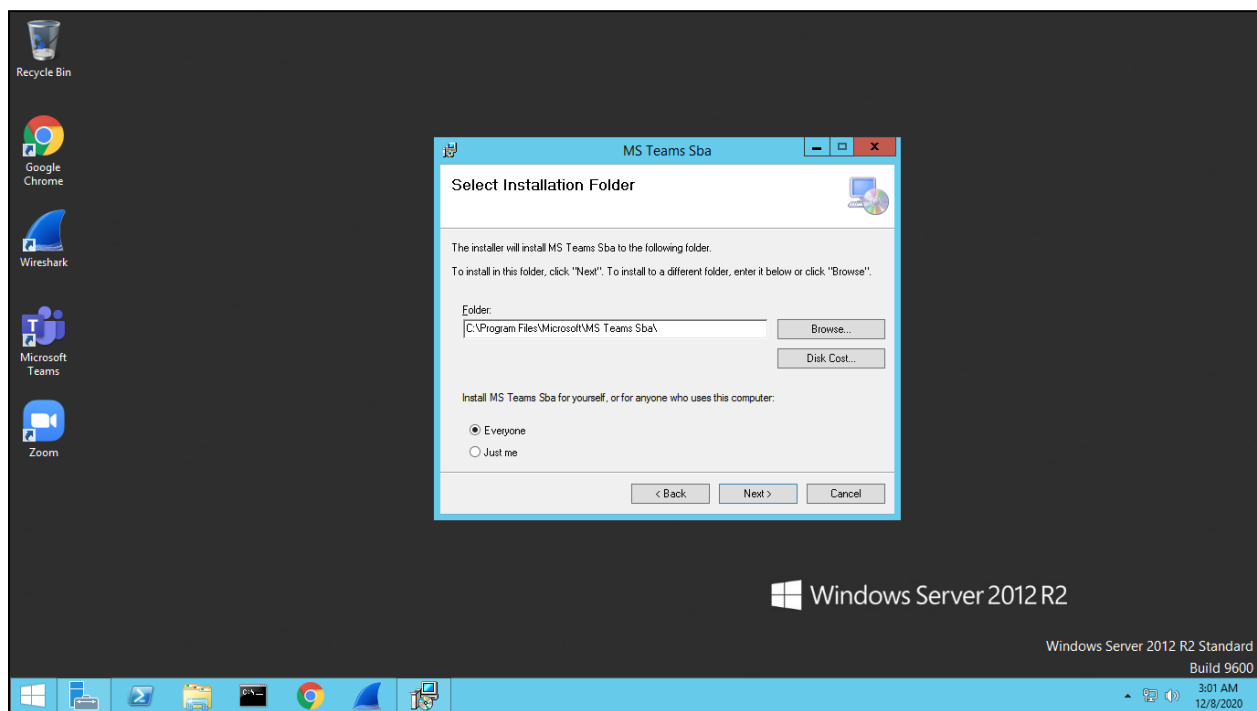
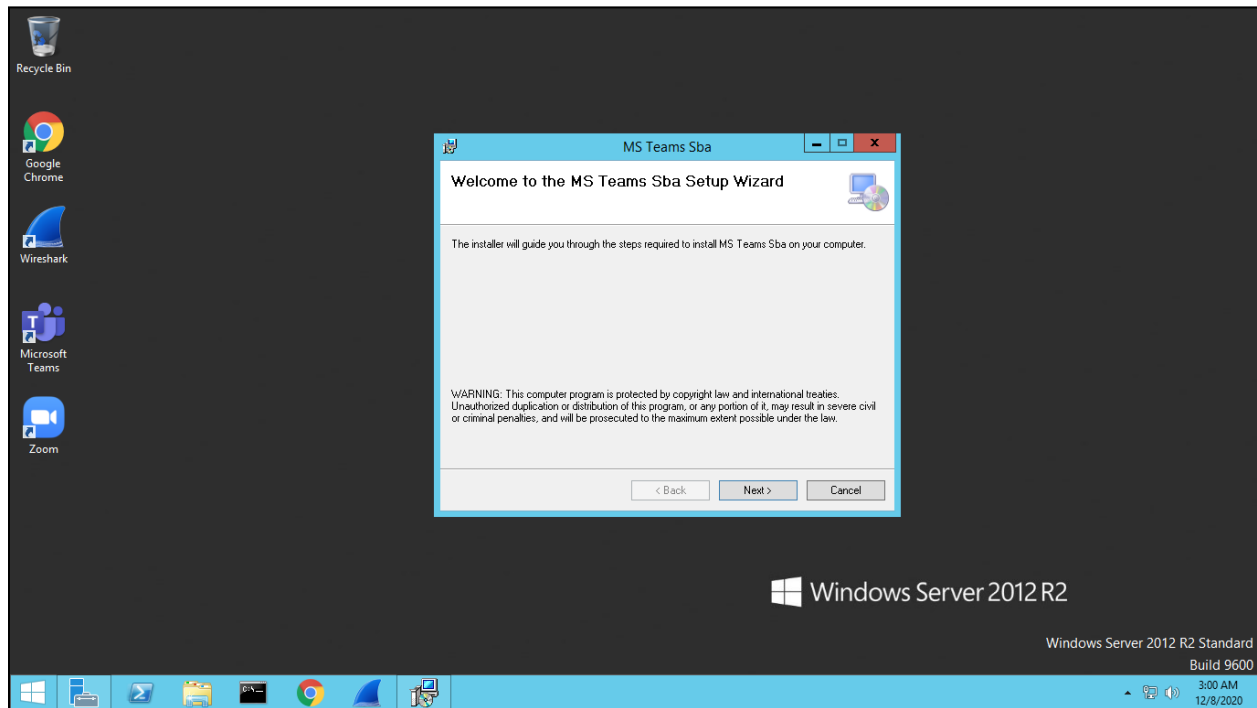
- Install the Microsoft SBA Application
- Create Azure Active Directory SBA Application
- Microsoft SBA API Configuration
- Configure Direct Routing Survivable Branch Appliance (SBA) in Microsoft 365

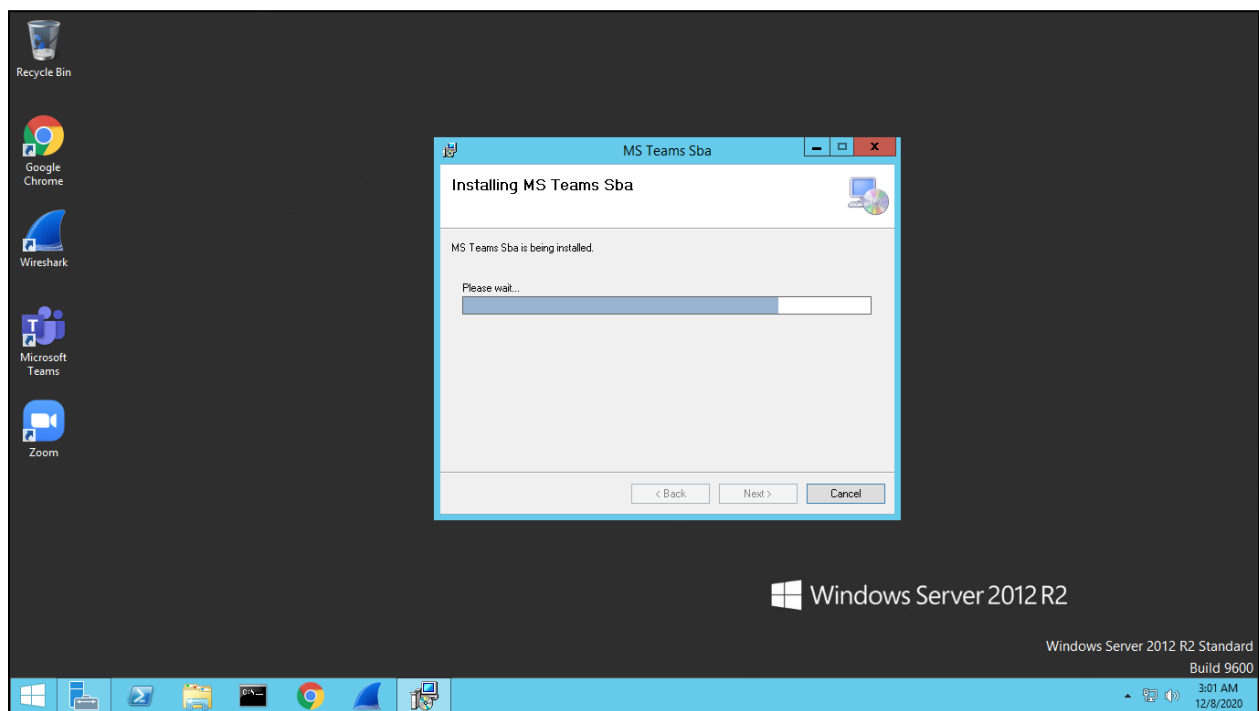
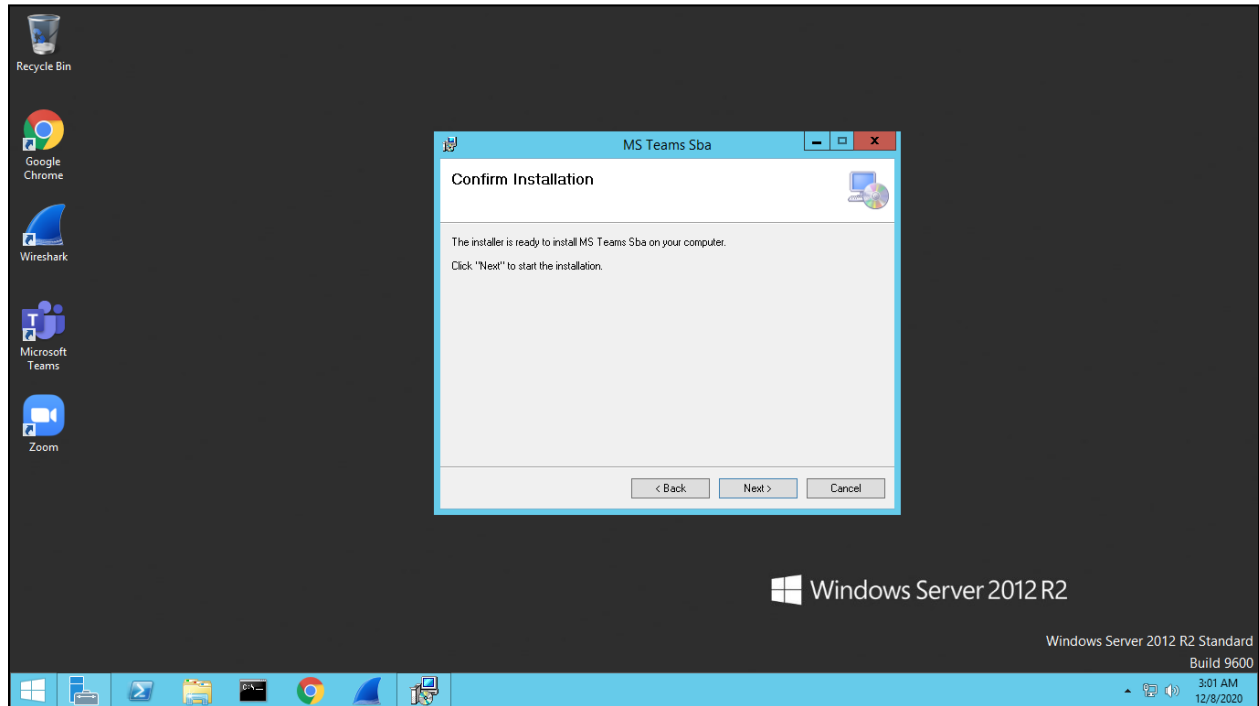
6.1 Install the Microsoft SBA Application

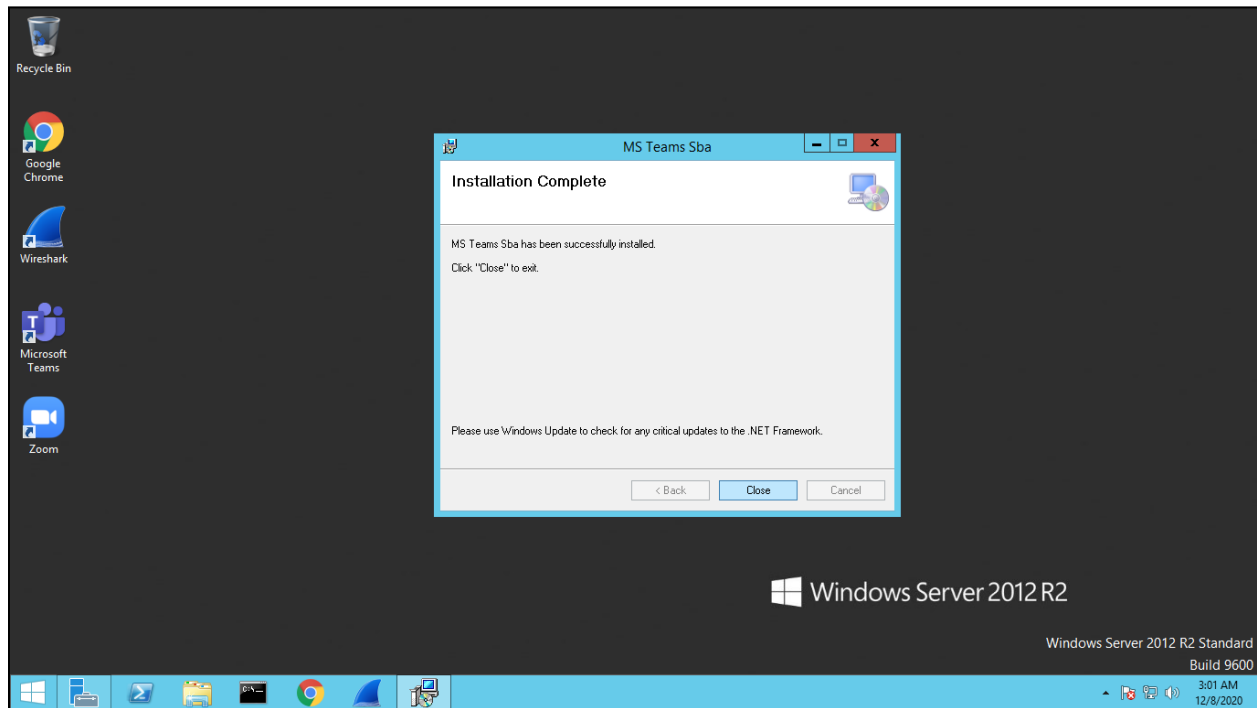
In this step we will provide steps on how to Deploy and configure Microsoft SBA.

Microsoft provides an easy to install Click and Run type Installer for the SBA Application. Transfer the Microsoft Teams SBA Installer package to the Windows Server and Start the Installer to install the SBA.

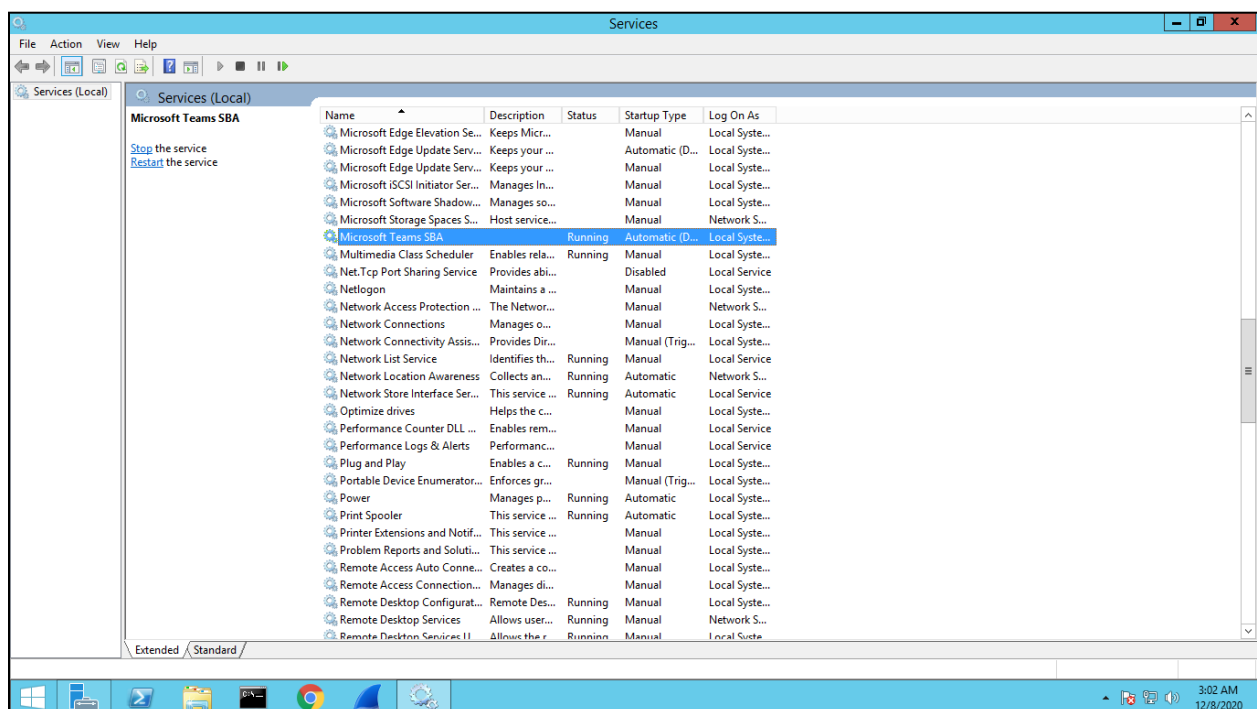
Please follow below snapshots for reference –







Once the Microsoft SBA Application is installed. Verify that the Microsoft SBA Service is running to validate successful completion of the installation.





6.2 Create Azure Active Directory SBA Application

To allow the different SBAs used within your tenant to read required data from Microsoft 365 you need to register an application for the SBA with Azure Active Directory.

For more information about application registration please see below link -

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/developer-guidance-for-integrating-applications>

<https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app>

You only need to register one application for use by all the SBA's in your tenant.

For the SBA registration, you need the following values created by the registration below:

These are the specific steps & notes to follow as reference specifically for the SBA application:

- The Name can be any Name, which you would like to use.
- Supported Account types = Account in this organizational directory only
- The Web Redirect Uri = <https://login.microsoftonline.com/common/oauth2/nativeclient>
- Implicit grant tokens = Access tokens and ID tokens
- API permissions = Skype and Teams Tenant Admin Access -> Application permissions -> application_access_custom_sba_appliance
- Client secret: you can use any description and expiration
- Remember to copy the client secret right away after you have created it
- The Application (client) id is shown on the Overview tab

6.2.1 SBA Connector registration on Microsoft Azure.

Create an AAD SBA Application following the steps mentioned below. The Application will be used for the communication of Local SBA Application with Microsoft 365.

Sign-in to Azure portal on behalf of your tenant and create new App registration

Note: Application should not be multi-tenant.

Register an application

* Name

The user-facing display name for this application (this can be changed later).

S8A

Supported account types

Who can use this application or access this API?

- ☒ Accounts in this organizational directory only (Single tenant)
- ☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)
- ☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- ☐ Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web

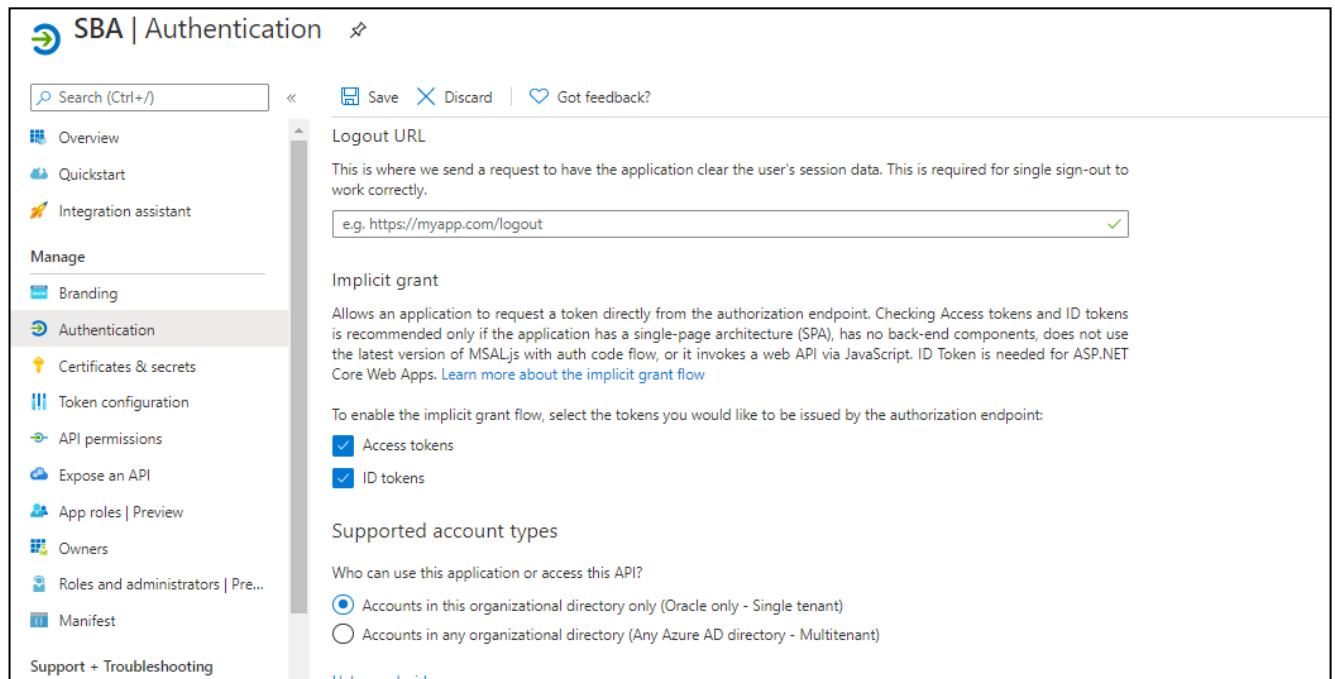
<https://login.microsoftonline.com/common/oauth2/nativeclient>

By proceeding, you agree to the [Microsoft Platform Policies](#)

Register

Put <https://login.microsoftonline.com/common/oauth2/nativeclient> into Redirect URIs as shown.

6.2.2 Setting Implicit Grant Token



The screenshot shows the 'SBA | Authentication' page in the Azure portal. The left sidebar contains a navigation menu with options: Overview, Quickstart, Integration assistant, Manage (Branding, Authentication, Certificates & secrets, Token configuration, API permissions, Expose an API, App roles | Preview, Owners, Roles and administrators | Pre..., Manifest), and Support + Troubleshooting. The main content area is titled 'Authentication' and includes a search bar, 'Save', 'Discard', and 'Got feedback?' buttons. The 'Logout URL' section has a text input field with the example 'e.g. https://myapp.com/logout' and a green checkmark. The 'Implicit grant' section explains that it allows an application to request a token directly from the authorization endpoint and is recommended for SPAs. It includes a link to 'Learn more about the implicit grant flow'. Below this, a section titled 'To enable the implicit grant flow, select the tokens you would like to be issued by the authorization endpoint:' shows two checked checkboxes: 'Access tokens' and 'ID tokens'. The 'Supported account types' section asks 'Who can use this application or access this API?' and has two radio button options: 'Accounts in this organizational directory only (Oracle only - Single tenant)' (selected) and 'Accounts in any organizational directory (Any Azure AD directory - Multitenant)'. A 'Help me decide' link is at the bottom.

6.2.3 Request API Permissions

Go to section API permissions to configure the SBA API permissions. Search 'Skype' Request API permissions and choose 'Skype and Teams Tenant API'

Select application_access_custom_sba_appliance.

Grant admin consent.

Home > Oracle > SBA

registrations ✕

«

+ New registration

Endpoints

Troubleshooting

Download

Preview features

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication. Applications will need to be upgraded to Microsoft Authentication Library.

All applications

Owning applications

Start typing a name or Application ID to filter these results

Display name

SBAConnector1

SBAConnector-27Oct

SBA

Request API permissions

« All APIs

Skype and Teams Tenant Admin API

https://api.interfaces.records.teams.microsoft.com

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

expand all

Start typing a reply url to filter these results

Permission

Admin consent required

Permissions (1)

application_access

application_access

Yes

application_access_custom_sba_appliance

application_access_custom_sba_appliance

Yes

Home > Oracle > SBA

SBA | API permissions ✕

Search (Ctrl+/)

«

Refresh

Got feedback?

Overview

Quickstart

Integration assistant

Manage

Branding

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles | Preview

Owners

Roles and administrators | Preview

Manifest

Configured permissions

Applications are authorized to call APIs when they are granted permissions. All the permissions the application needs. [Learn more about permissions](#)

+ Add a permission

✓ Grant admin consent for Oracle

API / Permissions name

Type

Description

Microsoft Graph (1)

User.Read

Delegated

Sign in and access user profile

Request API permissions

Select an API

Microsoft APIs

APIs my organization uses

My APIs

Apps in your directory that expose APIs are shown below

skype

Name

Application (client) ID

Skype and Teams Tenant Admin API

48ac35b8-9aa8-4d74-927d-1f4a14a0b239

Skype for Business

7557eb47-c689-4224-abcf-ae9bd7573df

Skype for Business Management Reporting and Analytics - Legacy

de17788e-c765-4d31-aba4-fb837cfff174

Skype for Business Online

00000004-0000-0ff1-ce00-000000000000

Skype For Business Powershell Server Application

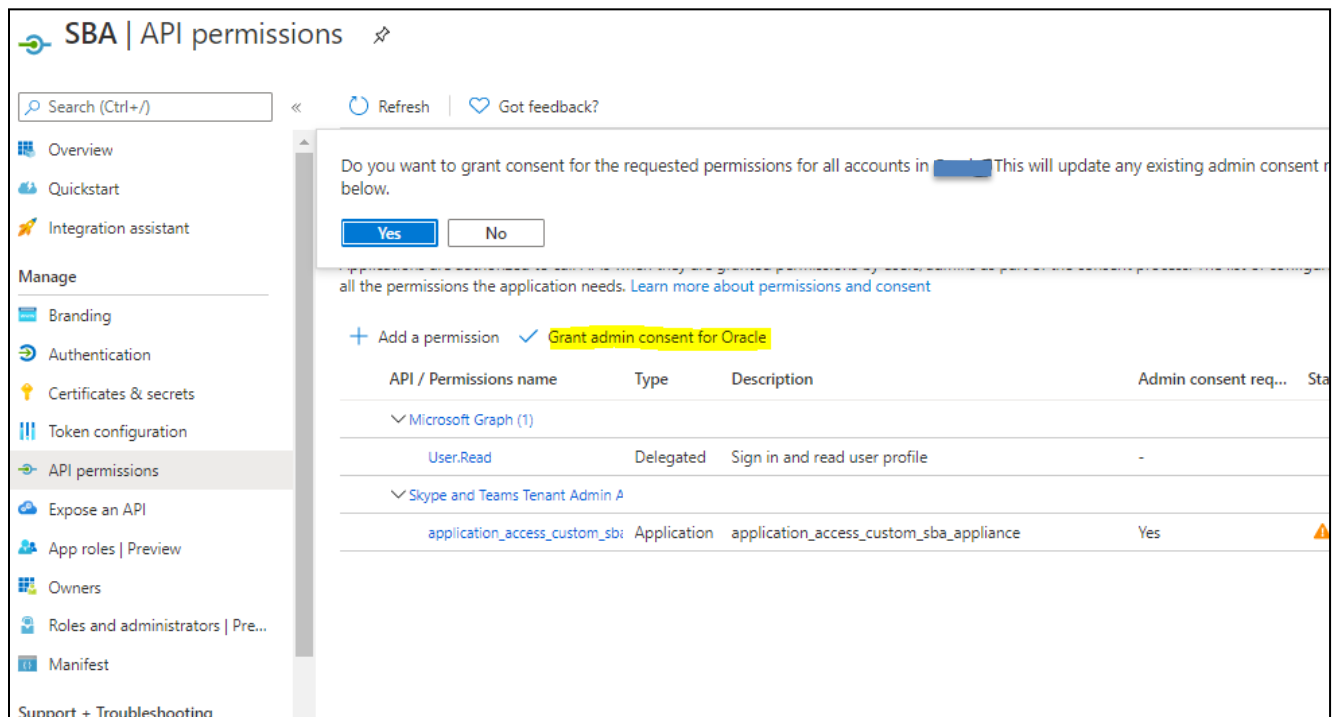
39624784-6cbe-4a60-afbe-9f46d10fdb27

Skype Presence Service

1e70cd27-4707-4589-8ec5-9bd20c472a46

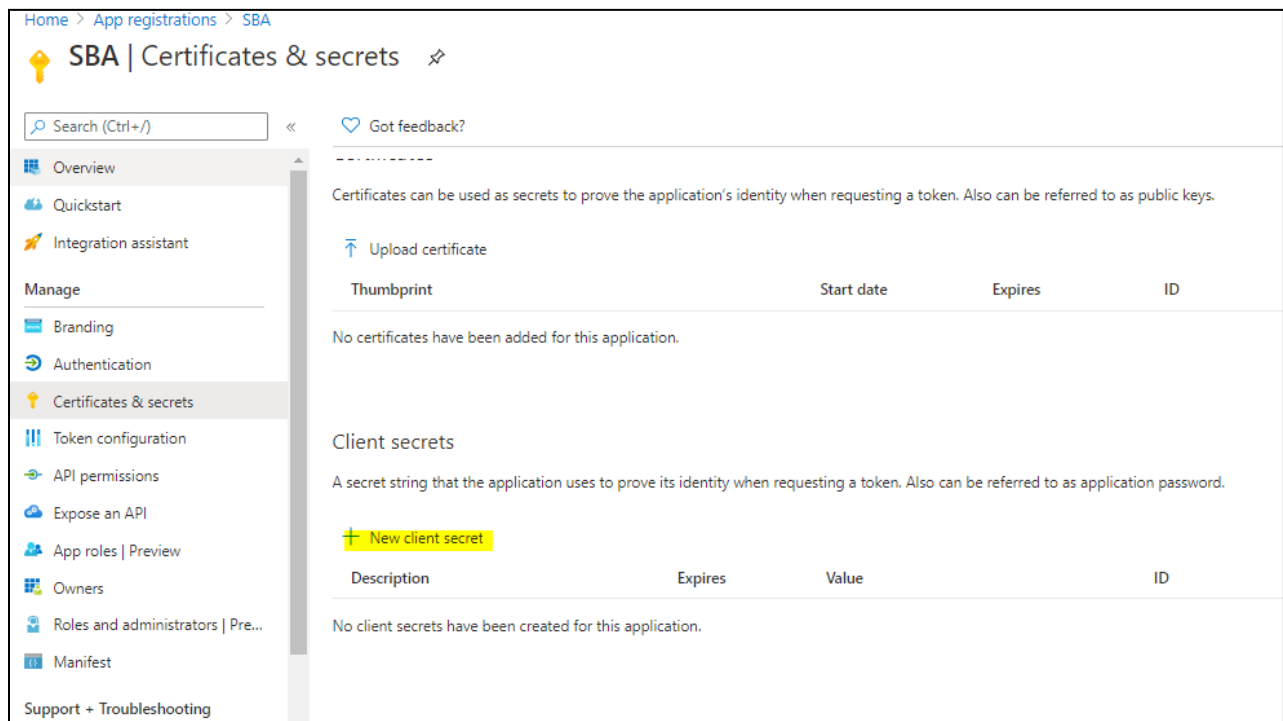
Skype Teams Firehose

cdccd920-384b-4a25-897d-75161a4b74c1



6.2.4 Create Client Secret

Navigate to Certificates and Secrets > New Client Secret and create new client secret as shown below.



SBA | Certificates & secrets

Search (Ctrl+ /)

Got feedback?

Overview

Quickstart

Integration assistant

Manage

Branding

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles | Preview

Owners

Roles and administrators | Pre...

Manifest

Support + Troubleshooting

Add a client secret

Description

SBA

Expires

☐ In 1 year
 ☐ In 2 years
 ☒ Never

Add

Cancel

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	ID
No client secrets have been created for this application.			

SBA | Certificates & secrets

Search (Ctrl+ /)

Got feedback?

Overview

Quickstart

Integration assistant

Manage

Branding

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles | Preview

Owners

Roles and administrators | Pre...

Manifest

Copy the new client secret value. You won't be able to retrieve it after you perform another operation or leave this blade.

Upload certificate

Thumbprint	Start date	Expires	ID
No certificates have been added for this application.			

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	ID
SBA	12/31/2299		

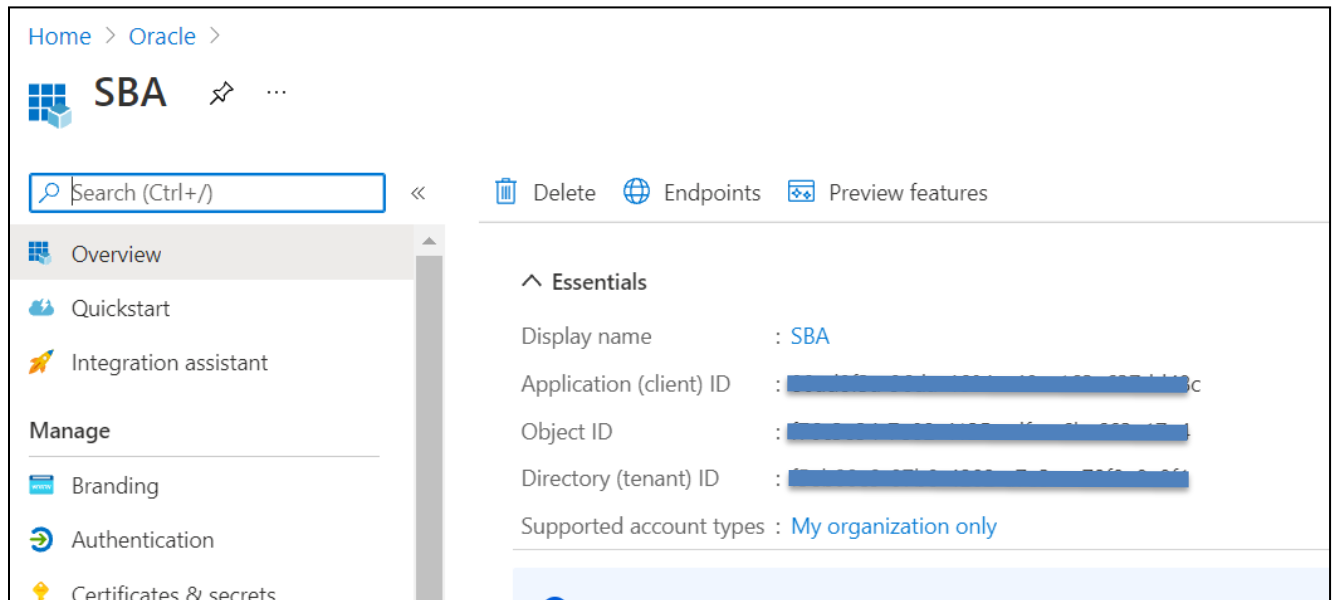
Copy to clipboard

Copy **Application Id** and **AppSecret**.

Application ID can be found under Overview Tab.

Value – is the App Secret

These will be used during SBA API configuration.



6.3 Configure Direct Routing Survivable Branch Appliance (SBA) in Office 365

This Section describes how to configure Direct Routing Survivable Branch Appliance (SBA) in Microsoft 365. This cover the following elements:

- Teams Survivability Branch Appliance
- Teams Branch Survivability Policy
- Assigning the policy to users

For the SBA feature to work the Microsoft Teams client needs to know, which SBA(s) are available in each branch site and are assigned to the users in that site. This is done via assigning a TeamsBranchSurvivabilityPolicy that contains one or more TeamsSurvivableBranchAppliance to individual users.

All the configuration is performed via Microsoft Teams Module on PowerShell.

Please note -

- When you add new branch appliances, it might take some time before you can use them in branch survivability policies.
- When you assign a branch survivability policy to a user it might take some time before it is shown in the output of Get-CsOnlineUser

6.3.1 Teams Survivable Branch Appliance

You create SBA's via the **New-CsTeamsSurvivableBranchAppliance** cmdlet in Skype for Business Online PS.

The parameters to the cmdlet are shown in Table 1.

Parameter	Description
Identity	The FQDN of the SBA
Fqdn	The FQDN of the SBA
Site	The TenantNetworkSite where the SBA is located. Used for Location Based Routing (LBR)
Description	Free format text

Table 1 Parameters for New-CsTeamsSurvivableBranchAppliance

An example is shown below:

```
C:\> New-CsTeamsSurvivableBranchAppliance -Fqdn sba1.contoso.dk -Description "SBA 1"
Identity : sba1.contoso.dk
Fqdn : sba1.contoso.dk
Site :
Description: SBA 1
```

Lab Snippet for reference -

```
PS C:\Users\solutionstest> New-CsTeamsSurvivableBranchAppliance -Identity teamssba.eastus.cloudapp.azure.com -Fqdn teamssba.eastus.cloudapp.azure.com
```

```
PS C:\Users\solutionstest> Get-CsTeamsSurvivableBranchAppliance -Identity teamssbaserver3.eastus.cloudapp.azure.com

Identity      : teamssbaserver3.eastus.cloudapp.azure.com
Fqdn          : teamssbaserver3.eastus.cloudapp.azure.com
Site          :
Description   : TeamsSBAServer3
```

6.3.2 Teams Branch Survivability Policy

This policy contains one or more SBA and you create it via the **New-CsTeamsSurvivableBranchAppliancePolicy** cmdlet in Skype for Business Online PS.

The parameters to the cmdlet are shown in Table 2.

Parameter	Description
Identity	The identity of the policy
BranchApplianceFqdns	The FQDN of the SBA(s) in the site

Table 2 Parameters for New-CsTeamsSurvivableBranchAppliancePolicy

An example is shown below:

```
C:\> New-CsTeamsSurvivableBranchAppliancePolicy -Identity CPH -BranchApplianceFqdns
"sba1.contoso.dk","sba2.contoso.dk"
```

Identity : Tag:CPH

BranchApplianceFqdns : {sba1.contoso.dk, sba2.contoso.dk}

You can add or remove SBA's from a policy by using the **Set-CsTeamsSurvivableBranchAppliancePolicy** like this:

```
Set-CsTeamsSurvivableBranchAppliancePolicy -Identity CPH -BranchApplianceFqdns
@{remove="sba1.contoso.dk"}
Set-CsTeamsSurvivableBranchAppliancePolicy -Identity CPH -BranchApplianceFqdns
@{add="sba1.contoso.dk"}
```

Lab Snippet for reference -

```
PS C:\Users\solutiontest>
PS C:\Users\solutiontest>
PS C:\Users\solutiontest> New-CsTeamsSurvivableBranchAppliancePolicy -Identity TeamsSBA3 -BranchApplianceFqdns teamssbaserver3.eastus.cloudapp.azure.com

Identity          : Tag:TeamsSBA3
BranchApplianceFqdns : {teamssbaserver3.eastus.cloudapp.azure.com}

PS C:\Users\solutiontest>
```

6.3.3 Assigning Teams Branch Survivability Policy to users

You assign the policy to individual users by using the **Grant-CsTeamsSurvivableBranchAppliancePolicy** cmdlet in Skype for Business Online PS.

The parameters to the cmdlet are shown in Table 3.

Parameter	Description
Identity	The identity of the user
Policy Name	The identity of the policy

Table 3 Parameters to Grant- CsTeamsSurvivableBranchAppliancePolicy

An example is shown below:

C:\> Grant- CsTeamsSurvivableBranchAppliancePolicy -PolicyName CPH -Identity user@contoso.dk

You can remove a policy from a user by granting the \$Null policy:

C:\> Grant- CsTeamsSurvivableBranchAppliancePolicy -PolicyName \$Null -Identity user@contoso.dk

Lab Snippet for reference -

```
PS C:\Users\solutiontest> Grant-CsTeamsSurvivableBranchAppliancePolicy -PolicyName TeamsSBA3 -Identity priyesh.mehrotra@telechat.o-test06161977.com
PS C:\Users\solutiontest> |
```

6.4 SBA API Configuration

Once the Microsoft SBA Package is installed and the SBA Service is running, mentioned steps should be performed in order to configure the Microsoft SBA.

The SBA configuration is done through API. The configuration can be performed using a REST API Client. Currently the SBA API is configured using a Freeware Client called POSTMAN, which can be downloaded from below link.

<https://www.postman.com/downloads/>

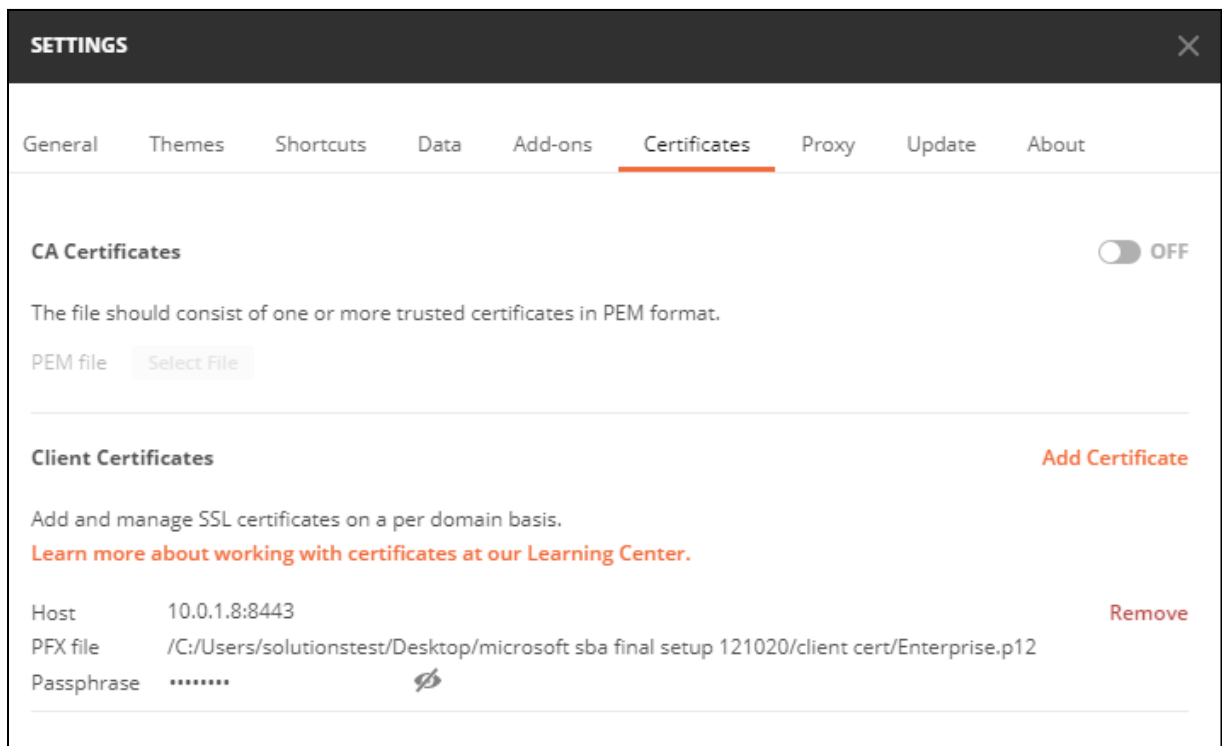
- The below query provides the state of SBA Application. The initial state is 'waiting initial parameters' SBA state: GET <http://localhost:8081/api/v1/diagnostics/state>

The screenshot shows the Postman interface for a GET request to `http://localhost:8081/api/v1/diagnostics/state`. The request is successful, returning a 200 OK status with a response time of 44 ms and a body size of 227 B. The response body is displayed in JSON format, showing the state of the SBA application.

KEY	VALUE	DESCRIPTION
Key	Value	Description

```
1 {
2   "state": "waitTenantInfo",
3   "status": "ok"
4 }
```

- A **200 OK** and **202 Accepted** is a successful response. 'GET' queries can be performed to get the state of existing item or return the existing configuration values.
- Please ensure that you are using right syntax during configuration of the API. Wrong Syntax would lead to return of error responses. Oracle recommends using **JSON** format for API queries.
- **SBA https port is 8443.**Please make sure that POSTMAN sends your client certificate on the PUT requests for general and secure configuration.
- Use **FQDN:PORT / SBA IP:PORT** combination when sending https API queries in the URI address
- Provide the SBC's Certificate and Key file or the PFX File along with the Passcode along with the API query to establish communication between Client and Server and update records.(Shown below)



6.4.1 Basic configuration

This step is needed for initial SBA API configuration and applies to localhost.

Server cert needs to be installed in Local Machine/My store for the configuration.

- **Server Certificate Common Name** – Common Name of the Microsoft SBA Server Certificate.

Note: If you are using a self-signed certificate, please ensure the certificate is present in the trusted certificate list of the Computer, which is running the Microsoft Teams Client. If not, the tls negotiation and the communication between Microsoft Teams Client and the Microsoft SBA Server will fail.

- **Client Certificate Thumbprints** – Use the Thumbprints of the Oracle SBC Certificate that are used for communication with Microsoft SBA. As part of Lab Setup and for the purpose of the document the same Certificate is used that are used with Microsoft Teams Direct Routing with the SBC.
- **Local SIP IP Address** – IP address that will be used by Microsoft SBA for communication. If not set, Default NIC is automatically selected.

Endpoint: <http://localhost:8081/api/v1/diagnostics/configurations/basic>

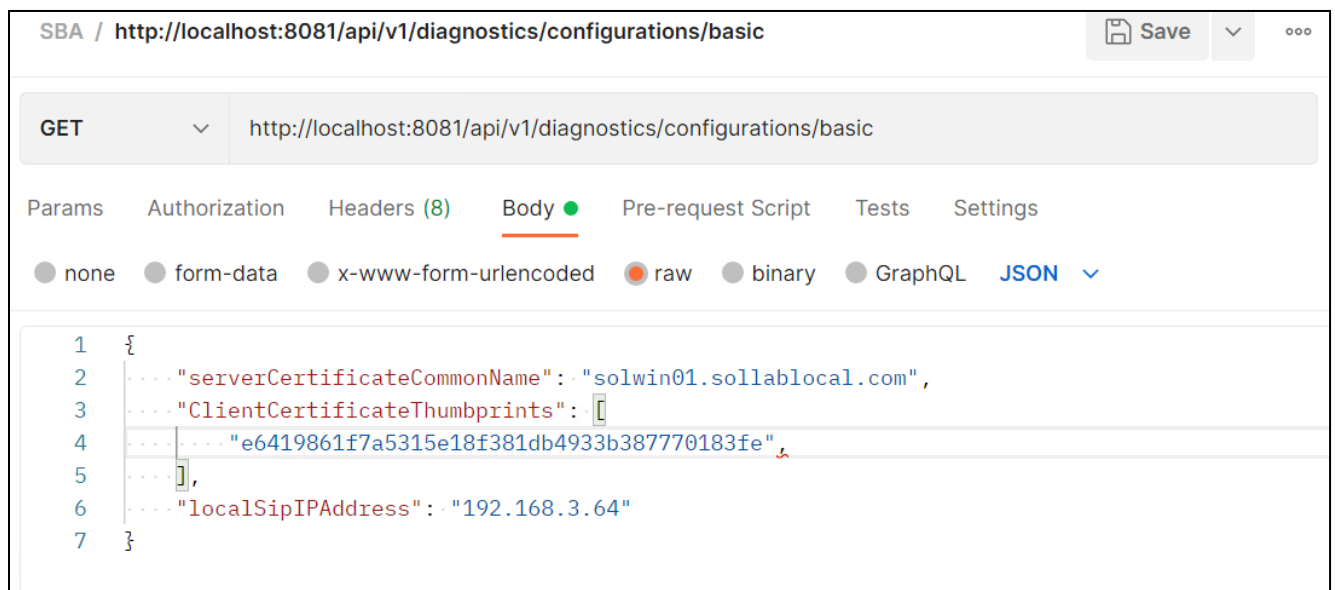
Allowed methods: GET, PUT, PATCH

Auth: N/A

SBA state: Wait initial parameters

```
{
  "serverCertificateCommonName": ""
  "ClientCertificateThumbprints": [
    "thumbprint1",
    "thumbprint2"
  ],
  "localSipIPAddress": null|"<local ip address>"|"0.0.0.0"
}
```

Lab Snippet for reference -



6.4.2 General configuration

The following step is the 2nd Step to configure the SBA Application.

- Use the SBA Server **FQDN** (Hostname) for the Endpoint.
- **Identity** - Identity of your Tenant, If you do not know the Tenant ID, It can be obtained from Powershell or the Microsoft O365 portal

- **Directory** – Is the SBA Logs Directory and can be set based on preference.

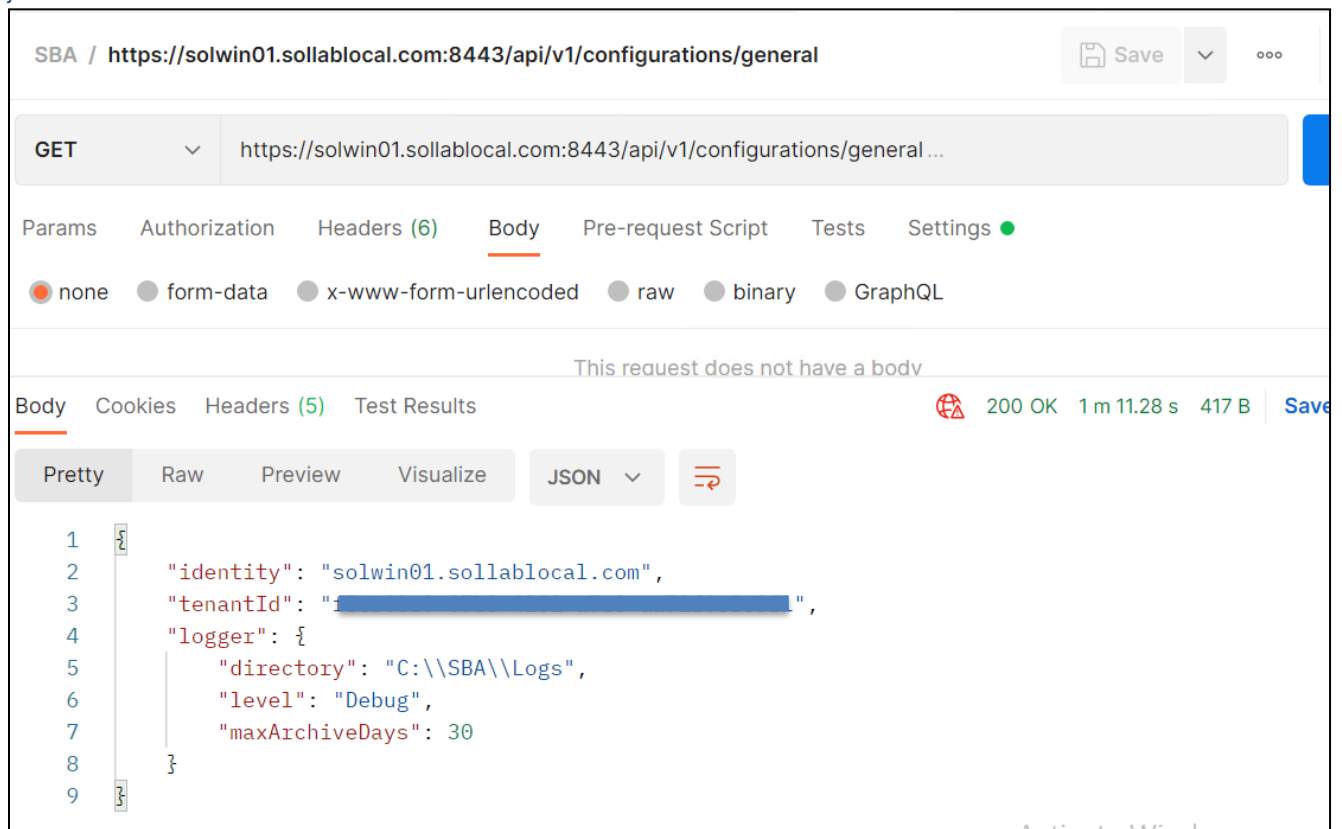
Endpoint: <https://fqdn/api/v1/configurations/general>

Allowed methods: GET, PUT, PATCH

Auth: mTLS (uses cert from Basic configuration "clientCertificateThumbprints")

SBA state: Wait tenant application credentials

```
{
  "identity": "", //sba identity when register with cmdlets- SBA FQDN
  "tenantId": "", //Identity of your Tenant
  "logger": {
    "directory": "C:\\logs"
    "level": "Critical| Error| Warning| Information| Debug| Trace|None",
    "maxArchiveFiles": 720 // range of 24-10000; default 720
  }
}
```



6.4.3 Secure configuration

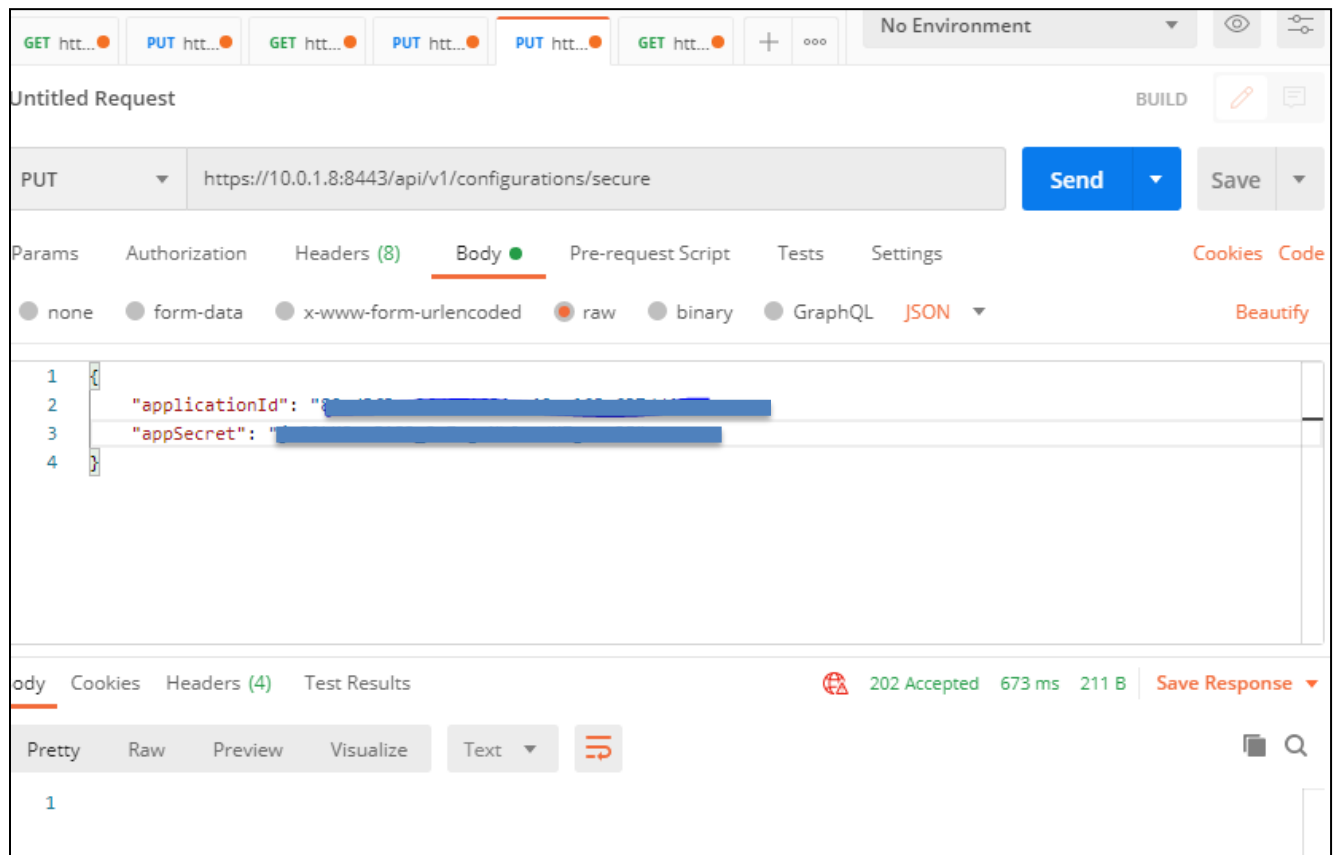
This is the last step of the configuration and is required for tenant information synchronization. Please use the Application ID and Application Secret which are generated in Step [6.2.4](#)

Endpoint: <https://fqdn/api/v1/configurations/secure>

Allowed methods: PUT, PATCH

Auth: mTLS (uses cert from Basic configuration "clientCertificateThumbprints")
SBA state: Wait tenant application credentials

```
{  
  "applicationId": ""  
  "appSecret": ""  
}
```



Restart the SBA Server once the Secured configuration step is complete.

7. Configuring the Oracle SBC

This section provides instructions to establish the communication of DR-SBA with Oracle SBC. In the setup, we are re-using many configuration elements that are already in place for direct routing with Microsoft Teams on the SBC. The document covers the additional steps that are required to configure the Microsoft SBA and enable calling functionality between the SBC and SBA. It is assumed that media bypass has been enabled on the Tenant.

The detailed steps to configure TLS between the Oracle SBC and Microsoft Teams can be referred from Oracle SBC with Microsoft Teams Media Bypass - Enterprise Model Application note

<https://www.oracle.com/a/otn/docs/OracleSBCwithMSFTTeamsMediaBypassEnabled.pdf>

Note : It is assumed the interconnection between Oracle SBC and the Carrier has been implemented and is operational with or without Public internet access. If Oracle SBC is unable to communicate with the Carrier, the PSTN calls will fail. The App note does not provide instructions to implement communication between Oracle SBC and Carrier. Visit our Application Note page which has instructions to internet multiple carriers with Oracle SBC.

7.1 Configure Physical Interface for DR-SBA

To configure physical Interface values,

Navigate to System->phy-interface.

ACL Path: config t->system->phy-interface

Here we have configured, phy-interface M11 for DR SBA communication.

The screenshot displays the 'Modify Phy Interface' configuration page. The left sidebar lists various configuration categories, with 'phy-interface' highlighted. The main configuration area includes the following fields and values:

Field	Value	Range
Name	M11	
Operation Type	Media	
Port	1	(Range: 0.5)
Slot	1	(Range: 0.2)
Virtual Mac		
Admin State	<input checked="" type="checkbox"/> enable	
Auto Negotiation	<input checked="" type="checkbox"/> enable	
Duplex Mode	FULL	
Speed	100	
Wancom Health Score	50	(Range: 0.100)
Network Alarm Threshold		

7.2 Configure Network Interface for DR-SBA

To configure network-interface, Navigate to system->Network-Interface.

ACL Path: config t->system->network-interface

Below Network interface enables the communication between Oracle SBC and DR-SBA.

Configuration

View Configuration

Q

media-manager

security

session-router

system

fraud-protection

host-route

http-client

http-server

network-interface

ntp-config

phy-interface

redundancy-config

snmp-community

spl-config

system-config

trap-receiver

Show All

Modify Network Interface

Name

M11

Sub Port Id

0

(Range: 0..4095)

Description

Hostname

IP Address

192.168.3.62

Pri Utility Addr

Sec Utility Addr

Netmask

255.255.255.0

Gateway

192.168.3.1

▲ Gw Heartbeat

State

☐ enable

Heartbeat

0

(Range: 0..65535)

Retry Count

0

(Range: 0..65535)

Retry Timeout

OK

Back

7.3 Configure Realm for DR-SBA

In this step will configure the DR-SBA Realm. Most of the Parameters will align with the Realm configured for communication with Microsoft Sip Proxies on the Teams Realm.

Navigate to media-manager -> realm-config

ACLI Path: config t->media-manger->realm-config

The name of the Realm can be any relevant name according to the user convenience. Use the following table as a configuration example for the three realms used in this configuration:

Configuration Parameter	Value
Identifier	SBA
Network Interface	M11
Mm in realm	<input checked="" type="checkbox"/>
Access Control Trust Level	High
Media Sec policy	sdesPolicy

rtcp-mux	enabled
ice-profile	Ice
teams-fqdn	telechat.o-test06161977.com
teams-fqdn-in-uri	enabled

Configuration
View Configuration
Q

media-manager
▼

codec-policy
media-manager
media-policy
realm-config
steering-pool
security
▶
session-router
▶
system
▶

Modify Realm Config

Identifier
SBA

Description

Addr Prefix
0.0.0.0

Network Interfaces
M1:0.4 ✕

Media Realm List

Mm In Realm
☒ enable

Mm In Network
☒ enable

Mm Same Ip
☒ enable

QoS Enable
☒ enable

Max Bandwidth
0 (Range: 0..999999999)

Max Priority Bandwidth
0 (Range: 0..999999999)

Parent Realm

DNS Realm

Show All
☐
OK
Back

media-policy
realm-config
steering-pool
security
▶
session-router
▶

Media Sec Policy
sdesPolicy
RTCP Mux
☒ enable
Ice Profile
ice
Teams Fqdn
customers.telechat.o-test06161977.com
Teams Fqdn In Uri
☒ enable

7.4 Create Microsoft SBA certificate-record

“Certificate-record” are configuration elements on Oracle SBC that captures information for a TLS certificate – such as common-name, key-size, key-usage etc.

A certificate record must be created on the Oracle SBC for the Microsoft SBA. This is the Certificate record for the Certificate Authority for Microsoft SBA.

The screenshot displays the Oracle SBC Configuration interface. On the left, a navigation pane lists various configuration categories: media-manager, security, authentication-profile, certificate-record (highlighted), tls-global, tls-profile, session-router, access-control, account-config, filter-config, ldap-config, local-policy, local-routing-config, media-profile, session-agent, session-group, and session-recording-group. Below this list is a 'Show All' button. The main area is titled 'Modify Certificate Record' and contains the following fields:

Name	sollablocal-SOLWIN01-CA
Country	US
State	MA
Locality	Burlington
Organization	Engineering
Unit	
Common Name	sollablocal-SOLWIN01-CA
Key Size	2048
Alternate Name	
Trusted	<input checked="" type="checkbox"/> enable
Key Usage List	digitalSignature X keyEncipherment X
Extended Key Usage List	serverAuth X
Key Algor	rsa

At the bottom right of the form are 'OK' and 'Back' buttons.

Oracle SBC Certificate “TeamsEnterpriseCert” already configured for Direct Routing will be reused in this setup. The certificate is shown below –

Configuration View Configuration 🔍

- media-manager ▶
- security ▼
 - authentication-profile
 - certificate-record**
 - tls-global
 - tls-profile
- session-router ▼
 - access-control
 - account-config
 - filter-config
 - ldap-config
 - local-policy
 - local-routing-config
 - media-profile
 - session-agent
 - session-group
 - session-recording-group

Show All ☐

Modify Certificate Record

Name	TeamsEnterpriseCert
Country	US
State	California
Locality	Redwood City
Organization	Oracle Corporation
Unit	
Common Name	telechat.o-test06161977.com
Key Size	2048 ▼
Alternate Name	
Trusted	<input checked="" type="checkbox"/> enable
Key Usage List	digitalSignature ✕ keyEncipherment ✕
Extended Key Usage List	serverAuth ✕
Key Algor	rsa ▼

OK Back

7.5 Create DR-SBA TLS Profile.

A TLS profile configuration on the SBC allows specific certificates to be assigned.

Go to security-> TLS-profile configuration element and configure the tls-profile

Below figure illustrates the TLS-Profile created for DR-SBA

Oracle SBC Certificate used to communicate with DR-SBA is present in End Entity Certificate. SBA-CA is added to the trusted Root CA to trust the communication from DR-SBA.

Configuration

View Configuration

Q

media-manager

security

authentication-profile

certificate-record

tls-global

tls-profile

session-router

access-control

account-config

filter-config

ldap-config

local-policy

local-routing-config

media-profile

session-agent

session-group

session-recording-group

Show All

Modify TLS Profile

Name

TLSSBA

End Entity Certificate

TeamsEnterpriseCert

Trusted Ca Certificates

SBA-Ca

Cipher List

DEFAULT

Verify Depth

10

(Range: 0..10)

Mutual Authenticate

enable

TLS Version

tlsv12

Options

Cert Status Check

enable

Cert Status Profile List

Ignore Dead Responder

enable

Allow Self Signed Cert

enable

OK

Back

7.6 Media Security

Media between Oracle SBC and the Microsoft SBA Server is secured with SRTP Protocol. To implement SRTP between Oracle SBA and Microsoft SBA we are using the existing SDES-Profile and the media-sec-policy which is used for communication with Microsoft Teams Direct Routing. Please refer to section 7 of the Oracle SBC with Microsoft Teams Non Media Bypass for detailed steps to configure SRTP.

Below is the snippet for the sdes-Profile “SDES” and media-sec-policy “sdesPolicy”.

7.6.1 SDES Profile

Wizards

Commands

cert-status-profile

certificate-record

ike

ipsec

media-security

dtls-srtp-profile

media-sec-policy

sdes-profile

sipura-profile

password-policy

security-config

ssh-config

Show All

Modify Sdes Profile

Name

SDES

Crypto List

AES_CM_128_HMAC_SHA1_32

AES_CM_128_HMAC_SHA1_80

Srtp Auth

☒ enable

Srtp Encrypt

☒ enable

SrTCP Encrypt

☒ enable

Mki

☐ enable

Egress Offer Format

same-as-ingress

Use Ingress Session Params

OK

Back

sdes-profile

sipura-profile

password-policy

security-config

ssh-config

Show All

Key

Salt

Srtp Rekey On Re Invite

☐ enable

Lifetime

31

(Range: 0,20..48)

OK

Back

7.6.2 Media-sec-policy

The image displays two screenshots of a network configuration interface for 'Modify Media Sec Policy'.

Top Screenshot:

- Left Sidebar:** A list of configuration items including *cert-status-profile*, *certificate-record*, *ike*, *ipsec*, *media-security* (expanded), *dtls-srtp-profile*, ***media-sec-policy*** (selected), *sdes-profile*, *sipura-profile*, *password-policy*, *security-config*, and *ssh-config*. A 'Show All' toggle is at the bottom.
- Main Panel:**
 - Title:** Modify Media Sec Policy
 - Name:** sdesPolicy
 - Pass Through:** ☐ enable
 - Options:** (Empty text box)
 - Inbound Section:**
 - Profile:** SDES
 - Mode:** srtp
 - Protocol:** sdes
 - Hide Egress Media Update:** ☐ enable
 - Outbound Section:**
 - Profile:** SDES
 - Buttons:** OK, Back

Bottom Screenshot:

- Left Sidebar:** Similar to the top, but *sdes-profile* is selected.
- Main Panel:**
 - Title:** (Same as top)
 - Outbound Section:**
 - Profile:** SDES
 - Mode:** srtp
 - Protocol:** sdes
 - Buttons:** OK, Back

7.7 Configure the SBA Session-Agent

Session-agents are configuration elements, which are trusted agents who can send/receive traffic from the SBC with direct access to trusted data path.

Configure the session-agent for Microsoft SBA with the following parameters.

Go to session-router- >Session-Agent and set the parameters as below-

- Hostname to "FQDN of your SBA Server"
- IP Address to "IP Address of your SBA Server"
- Port 5061
- Realm-id – needs to match the realm created for DR-SBA – in this case – "SBA"
- Transport set to "Statists"
- Ping-method – send OPTIONS message to Microsoft for health check

- Ping-interval to 30 secs
- Ping-response enable

Configuration
View Configuration
Q

media-manager
security
authentication-profile
certificate-record
tls-global
tls-profile
session-router
access-control
account-config
filter-config
ldap-config
local-policy
local-routing-config
media-profile
session-agent
session-group

Modify Session Agent

Hostname: solwin01.sollablocal.com

IP Address: 192.168.3.64

Port: 5061 (Range: 0,1025..65535)

State: ☒ enable

App Protocol: SIP

App Type:

Transport Method: StaticTLS

Realm ID: SBA

Egress Realm ID:

Description:

Match Identifier:

media-manager
security
session-router
access-control
account-config
filter-config
ldap-config
local-policy
local-routing-config
media-profile
session-agent
session-group
session-recording-group
session-recording-server
session-translation
sip-config

Modify Session Agent

Ping Method: OPTIONS

Ping Interval: 30 (Range: 0..4294967295)

Ping Send Mode: keep-alive

Ping All Addresses: ☐ enable

Ping In Service Response Codes:

Options:

SPL Options:

Media Profiles:

In Translationid:

Out Translationid:

Trust Me: ☐ enable

Local Response Map:

Ping Response: ☒ enable

In Manipulationid:

Note: Microsoft accepts the OPTIONS ping and other requests in a format as described in the section 4 of the Direct Routing Media Bypass document. Please refer and validate the message format to ensure the signaling is in accepted format required by Microsoft.

Requirements for “OPTIONS” messages syntax

```
OPTIONS sip:solwin01.sollablocal.com:5061;transport=tls SIP/2.0
Via: SIP/2.0/TLS 192.168.3.62:5061;branch=z9hG4bK827nmi1088j8asfav5n0
Call-ID: f6574f99d22a4514dbaad5ff6712cfa70200008gm3000@192.168.3.62
To: sip:ping@solwin01.sollablocal.com
From:<sip:ping@telechat.o-
test06161977.com>;tag=dedc857e7c327cff2f2e07600b881da20008gm3
Max-Forwards: 70
CSeq: 1261 OPTIONS
Contact: <sip:ping@telechat.o-test06161977.com:5061;transport=tls>;sip.ice
Expires: 10
Route: <sip:192.168.3.64:5061;lr>
X-MS-SBC: Oracle/NN4600/8.4.0p5A
```

1. **From header** When sending OPTIONS to DR SBA “FROM” header MUST have SBC FQDN in URI hostname:

Syntax: From: sip: @;tag=....

If the parameter is not set correctly, the OPTIONS are rejected with “403 Forbidden” message.

2. **Contact Header.** When sending OPTIONS to Teams Hybrid Voice Connectivity Interface “Contact” header should have SBC FQDN in URI hostname along with Port & transport parameter set to TLS.

Syntax: Contact: sip:

If the parameter is not set correctly, outbound OPTIONS won’t be sent by Teams The above requirements are automatically fulfilled in the referenced build of the software.

Configure SIP Interface

7.8 Configure the sip-interface

Navigate to session-router-> sip-interface and configure the sip-interface as shown below.

ACL Path: config t->session-router->sip-interface

Configure sip-interface for the DR-SBA as below-

- Tls-profile needs to match the name of the tls-profile previously created

- Set allow-anonymous to agents-only to ensure traffic to this sip-interface only comes from the Session agents added to the SBC.

Configuration View Configuration Q

Modify SIP Interface Show Configuration

State ☒ enable

Realm ID SBA

Description

SIP Ports

Action	Select	Address	Port	Transport Protocol	TLS Profile	Allow Anonymous	Multi Home Addr
	<input type="checkbox"/>	192.168.3.62	5061	TLS	TLSSBA	agents-only	

7.9 Configure steering-pool

Steering-pool config allows configuration to assign IP address(s), ports & a realm. They define sets of ports that are used for steering media flows through the Oracle SBC. These selected ports are used to modify the SDP to cause receiving session agents to direct their media toward this system.

Navigate to GUI Path: media-manger->steering-pool

ACLI Path: config t->media-manger->steering-pool

Configure a Steering pool for DR-SBA as below -

Configuration View Configuration Q

Modify Steering Pool

IP Address 192.168.3.62

Start Port 10000 (Range: 0,1..65535)

End Port 20000 (Range: 0,1..65535)

Realm ID SBA

Network Interface

7.10 Modification to local-policy

7.10.1 Outbound calls to Microsoft

Microsoft SBA is configured to accept calls in case of connectivity with Office 365 goes down, to achieve this Microsoft SBA is defined as an additional hop to the local-policy which is used to route calls from PSTN to Microsoft 365.

The existing local-policy routes the PSTN calls to the sag:TeamsGrp, which contains Microsoft SIP proxy FQDNs.

sip.pstnhub.microsoft.com

sip2.pstnhub.microsoft.com

sip3.pstnhub.microsoft.com

This local-policy is modified with Microsoft SBA Session-Agent “solwin01.sollablocal.com” defined as an additional next hop.

“solwin01.sollablocal.com” is the FQDN of the Oracle Lab Microsoft SBA Server that resolves to its communication IP address. Calls upon failure through O365 will be routed to DR-SBA as configured.

Below is the snippet of the modified local-policy. Microsoft returns a “480 Temporarily Unavailable” when the O365 endpoints fail to complete the call. After trying all the hops, the call is connected via Microsoft SBA Server.

Terminate recursion parameter should be disabled on the local-policy for SBC to try all the hops.

Stop recurse: parameter on the session-agent/sip-interface should not contain a 480-cause code, as this would result to failure of calls.

7.10.2 Inbound calls from Microsoft

Inbound calls from DR-SBA are routed to the PSTN from the SIP Trunk. Below is the snippet of Lab Local Policy for reference.

Configuration

View Configuration

media-manager

security

session-router

access-control

account-config

filter-config

ldap-config

local-policy

local-routing-config

media-profile

session-agent

session-group

session-recording-group

session-recording-server

Modify Local Policy

From Address

* x

To Address

* x

Source Realm

SBA x

Description

State

☒ enable

Policy Priority

none

Policy Attributes

Action

Select

Next Hop

Realm

Action

Terminate Recursion

Cost

State

App Protocol

Lookup

Next Key

⋮

☐

68.68.117.67

SIPTrunk

none

disabled

0

enabled

single

Note – It is important for the dialed number to be in the exact same format as configured for the Direct Routing calls. So that SBA to perform the User Number lookup in its database, hence do ensure to include the session-translations, sip-manipulation on the SBA Ream/Sip-Interface if you have configured any for direct routing calls.



CONNECT WITH US

 blogs.oracle.com/oracle

 facebook.com/Oracle/

 twitter.com/Oracle

 oracle.com

Oracle Corporation, World Headquarters

500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries

Phone: +1.650.506.7000
Fax: +1.650.506.7200

Integrated Cloud Applications & Platform Services

Copyright © 2020, Oracle and/or its affiliates. All rights reserved. This document is provided *for* information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 0615