

User Management Pack™ 365 Service Provider Edition

Version 8.0.300



Table of Contents

Table of Contents.....	ii
Notice	ix
WEEE EU Directive	ix
Customer Support.....	ix
Stay in the Loop with AudioCodes	ix
Abbreviations and Terminology	ix
Document Revision Record	ix
Documentation Feedback.....	x
1 Introduction	11
Part I	12
Preinstallation	12
2 Virtual Hardware Deployment Requirements	13
3 Securing SSL Connection	14
4 UMP Networking Configuration	21
4.1 UMP Firewall Configuration	22
4.2 VPN Configuration (Optional).....	22
4.3 OVOC Service Provider Firewall Configuration	24
5 SQL License Guidelines - Optional	28
6 Implementing Anti-virus on UMP server	30
6.1 SQL.....	30
6.2 ASP.NET	30
6.3 Create UMP Service Account.....	31
Part II	38
Installation and Setup	38
7 Installing the Prerequisites.....	39
8 Installing UMP-SP.....	40
8.1 Adding SSL Certificate to IIS Website	41
9 Creating Customer DNS Subdomains.....	43
9.1 Fully Automatic Provisioning.....	43
9.1.1 Before Provisioning	44
9.1.1.1 Registering DNS Application.....	44
9.1.1.2 Create A Records for Customer Sub Domains	48
9.1.1.3 Assign Access Control.....	50
9.1.1.4 Configure DNS API	54
9.1.2 Provisioning.....	58

9.2	Two-step Provisioning	70
9.2.1	Before Provisioning	70
9.2.2	Provisioning	72
9.3	Manual Provisioning	82
9.3.1	Registering a Subdomain Name on the Customer M365 Tenant	82
9.3.2	Activating the Providers Domain	88
10	Microsoft Teams Direct Routing SBC Configuration	95
11	App Registration For Background Replication	96
11.1	Assigning Administrator Roles to Customer IT Administrator	102
12	Configure Invitation Settings	107
13	Configure Email Settings	109
14	App Registration for Customer Admins	110
15	Configure License	114
15.1	Installing the UMP 365 License	114
16	Update Service Provider Logos	116
17	Secure UMP Interface Connection with OVOC and SBC	117
17.1	Configure UMP Interface for WebSocket Tunnel (Cloud Architecture Mode)	118
17.1.1	Configure WebSocket Tunnel (Cloud Architecture Mode) on OVOC	120
17.1.1.1	Add WebSocket Tunnel User	122
17.1.1.2	Change the WebSocket Tunnel Default Password	122
17.1.2	Configure SBC	122
17.2	Configure HTTPS SSL Connection to OVOC Public IP	126
17.3	Configure Connection to OVOC Azure Private IP	129
17.4	Managing Alarms	130
Part III	133
Upgrade	133
18	Getting Started	134
18.1	Overview	134
18.2	UMP 365 with Service Provider Admin Credentials	134
18.3	Tenants Global View	138
18.3.1	Configured Number of Licenses Users	139
18.3.2	Onboard SBC Devices for New Site Locations	140
18.3.3	Queue Replication	141
18.3.4	Undo Deployment	141
18.3.5	Upgrade Customer	141

19 UMP Backup– Disk Snapshot.....	144
20 Upgrade using Wyupdate.....	149
20.1 Prerequisites.....	149
20.2 Run Wyupdate Tool.....	149
20.2.1 Main UMP Tenant Update	149
20.2.2 Services Updates for each Tenant.....	154
21 UMP Snapshot Restore	157
22 UMP Upgrade Testing Checklist	161
23 Post Upgrade Actions	163
23.1.1 Remove Token Registration Permissions	163
23.1.2 Update Scripts	166
Part IV.....	167
Service Provider Management	167
24 SBC and M365 Onboarding Script Templates.....	168
24.1 SBC Template Scenarios	169
24.1.1 sbc-scenario7	169
24.1.2 sbc-scenario7Cleanup	171
24.1.3 add-ipx-user	172
24.1.4 sbc-add-prefix.....	173
24.1.5 sbc-remove-prefix	175
24.2 M365 Template Scenarios.....	175
24.2.1 Default M365 Tenant Onboarding Script	176
24.2.2 Default M365 Tenant Cleanup Script	176
24.3 Onboarding Wizard Defined Variables.....	177
24.4 Custom Variables.....	178
24.4.1.1 Custom Script	181
24.5 Scenario Scripts Templates Page.....	183
24.5.1 Script Scenario Comparison	184
24.5.2 Script Templates Updates	187
24.5.2.1 sbc-scenario7.....	187
24.5.2.2 sbc-scenario7Cleanup	189
24.5.2.3 sbc-add-prefix.....	189
24.5.2.4 sbc-remove-prefix	190
24.6 SQL DBA Script Pairing.....	191
25 Security Settings	196
25.1 Customer Admins	196
25.2 Customer Invitations	196
25.3 Auth Tokens.....	199

25.4	UMP Service Settings	202
26	Managing SBC Devices	203
26.1	Add an SBC Device.....	203
26.2	Show SBC Site Locations.....	205
26.3	Show Prefixes	206
27	Queued Tasks.....	207
Part V.....		208
Onboarding a New Tenant Customer		208
28	Introduction	209
29	Onboarding Prerequisites	210
30	Onboarding Teams Direct Routing Customers	211
30.1	Hosted Essentials.....	211
30.2	Hosted Essentials +	217
30.2.1	Configure Default Routing.....	221
30.2.2	Configure without Default Routing	227
30.2.3	Configure SBC Number Prefixes and Scripts	228
30.3	Hosted Pro.....	231
30.3.1	Configure Default Routing.....	235
30.3.2	Configure without Default Routing	243
30.3.3	Configure SBC Number Prefixes and Scripts	244
30.4	Provision M365 Domain and DNS Server Automatically.....	247
30.5	Running Token Authentication Invitation Wizard	249
30.5.1	Pending Requests	259
31	Managing Licensed Users	261
Part VI.....		262
2nd Day Operations		262
32	Introduction	263
33	Provider Self-Service Portal	264
33.1	Editing User Policies	264
33.2	Grant Admin Permissions to Service Provider IT Administrator User	264
33.3	Edit Users.....	266
33.4	Assigning Phone Numbers.....	268
33.5	Lifecycle Management	269
33.6	Managing Unassigned Number Ranges.....	269
33.6.1	Creating a Bundle	271
33.6.2	Editing a Bundle	274
33.6.3	Deleting a Bundle	275

33.6.3.1	Troubleshooting	276
33.7	Managing Templates	278
33.7.1	Importing Bulk Templates from a File	280
33.7.2	Create New Entry Manually	284
33.7.3	Export CSV	284
33.7.4	Binding Templates to Security Groups	285
33.8	Configuring Online Voice Routing	286
33.8.1	PSTN Usage.....	287
33.8.2	Voice Routing Policy.....	288
33.8.2.1	Adding Voice Routing Policy.....	288
33.8.2.2	Editing Voice Routing Policy	289
33.8.2.3	Deleting/Canceling Voice Routing Policy.....	290
33.8.2.4	Applying a Voice Routing Policy to a Group of Users	290
33.8.3	Voice Route	291
33.8.4	PSTN Gateways.....	292
33.8.5	Dial Plan & Normalization Rules.....	292
33.9	Reserving M365 Tenant Phone Numbers	296
33.10	Audit and Roll Back Historical Changes	297
33.11	Queued Changes	298
33.12	Microsoft 365 Settings	299
33.13	Manage Site Locations	300
33.13.1	Add SBC Site Locations	301
33.13.2	Configure SBC Prefixes	302
33.13.3	Import PBX Users	305
34	Multitier Admin Access	306
Part VII.....	308
Appendix	308
A	Browser setting - IETF Same Site Cookie Attribute	309
B	Backup and Restore Customer Tenant.....	311
B.1	Backup the Customer Tenant Database.....	311
B.2	Restore the Customer Tenant Database	313
B.2.1	Restore to a Point-in-Time	316
C	AudioCodes Sfb2Teams Migration Tool.....	319
C.1	Installing the Prerequisites.....	319
C.1.1	Install SkypeOnline PowerShell.....	319
C.1.2	Install .NET framework 4.8 Runtime	319
C.2	Create and Register the Azure App	319
C.3	Set Microsoft Graph API Permissions.....	321
C.4	Running the Sfb2Teams Application	324

C.5	Auto Call Routing To Teams	327
D	Renewing Expired Tokens	329
E	SQL Server Configuration	330
E.1	Setup Microsoft SQL Server for SBC	330
E.2	SQL Server Database Updates	331
E.3	Updates for Backend SQL Server	333
E.4	Configure SQL Server for Enhanced Capacity	334
E.5	Run Changes on the External SQL Server	335

Notice

Information contained in this document is believed to be accurate and reliable at the time of printing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee accuracy of printed material after the Date Published nor can it accept responsibility for errors or omissions. Updates to this document can be downloaded from <https://www.audiocodes.com/library/technical-documents>.

This document is subject to change without notice.

Date Published: June-07-2022

WEEE EU Directive

Pursuant to the WEEE EU Directive, electronic and electrical waste must not be disposed of with unsorted waste. Please contact your local recycling authority for disposal of this product.

Customer Support

Customer technical support and services are provided by AudioCodes or by an authorized AudioCodes Service Partner. For more information on how to buy technical support for AudioCodes products and for contact information, please visit our website at <https://www.audiocodes.com/services-support/maintenance-and-support>.

Stay in the Loop with AudioCodes



Abbreviations and Terminology

Each abbreviation, unless widely used, is spelled out in full when first used.



The UMP Multitenant interface Navigation pane includes Operator Connect related menu items. Operator Connect is not supported by this product.

Document Revision Record

LTRT	Description
26343	Initial release of this document.
26348	Update for software version 8.0.100
26349	Update for software version 8.0.220
26356	Added backup, upgrade and restore procedures. Update to Section Automatic Provisioning of DNS Records.

LTRT	Description
26357	Corrections to Section “Onboarding New Customers”
26358	Updates for version 8.0.300.
26359	Correction to procedure “App Registration for Customer Admins”

Documentation Feedback

AudioCodes continually strives to produce high quality documentation. If you have any comments (suggestions or errors) regarding this document, please fill out the Documentation Feedback form on our website at <https://online.audiocodes.com/documentation-feedback>.

1 Introduction

AudioCodes' User Management Pack 365 (UMP 365) SP Edition is a software application that simplifies Microsoft 365 Tenants onboarding automation, users MACD and lifecycle management of Microsoft Teams, and OneDrive policies with Microsoft Direct Routing capabilities. The application is an asynchronous model. This implies that changes to users will only be applied after replication takes place, either from scheduled tasks or by forcing a replication cycle from within the web application.



In this document, M365 is an acronym for Microsoft 365.

Part I

Preinstallation

2 Virtual Hardware Deployment Requirements

The following table describes the Base Configuration for up to 100 Tenants for Hosted Pro and Hosted Essentials + models with a single VM.

Table 2-1: Virtual Hardware Deployment Requirements

Deployment Size	Average Number of Users per Tenant	Maximum Number of Users per Environment	Azure Machine Size	CPU Processors	Disk Type	Memory RAM
Basic	500	50,000	Standard D4s v3	4 cores with at least 2.4 GHz per core	Premium SSD with 100 GB available disk space for application*	16 GB
Medium	2000	200,000	Standard D16s v3	16 cores with 2.4 GHz per core	Premium SSD with 400 GB available disk space for application*	64 GB
Large	20000	2,000,000	Standard D32s v3	32 cores with 2.4 GHz per core	Premium SSD with 1 Terabyte available disk space for application*	128 GB

- **Operating System:** Single Windows Server 2019-- US English
 - * Allocate an additional 80 GB of disk space for the Windows Server 2019 -- US English Operating System



Only Windows Server 2019 – US English is supported.

- ~20k users will run for 20 minutes
- Each tenant synchronizes every hour
- An additional Backend SQL VM server is recommended for disaster recovery and for security reasons
- For additional capacity, contact AudioCodes support.



The OS and SQL License are not included in the product pricing (UMP CPN). The basic CPN including 1 CAL For additional Admins customers must order separate licenses.

3 Securing SSL Connection

This section describes how to secure UMP HTTPS connections by installing an SSL certificate on the Windows server of the UMP platform.

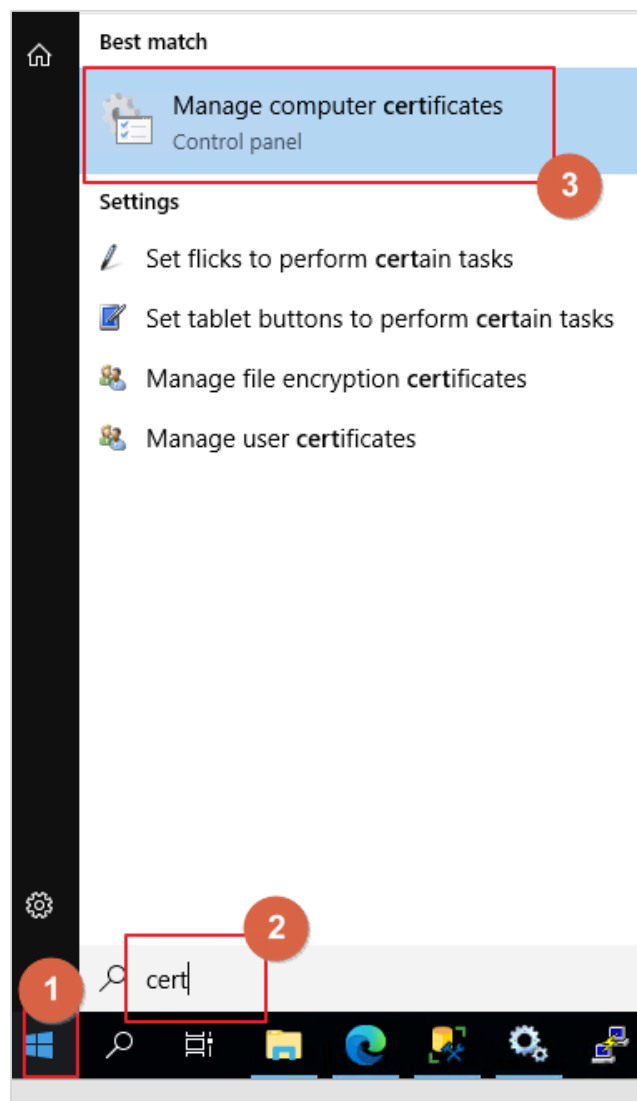


The UMP can only be accessed over **HTTPS**.

To secure SSL connection with Azure:

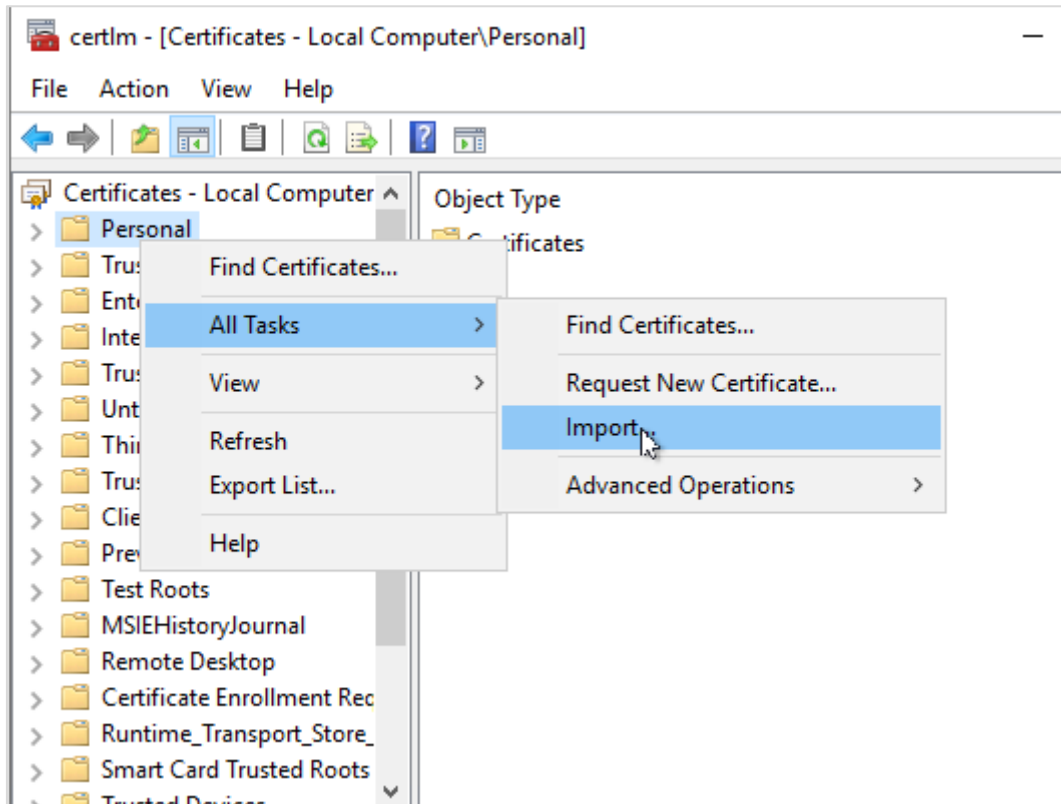
1. Make sure you have a valid SSL certificate with a private key available
2. From the server open Certlm (Manager computer certificates), type **cert** at Windows start button and select **Manage computer certificates**.

Figure 3-1: Manage computer certificates



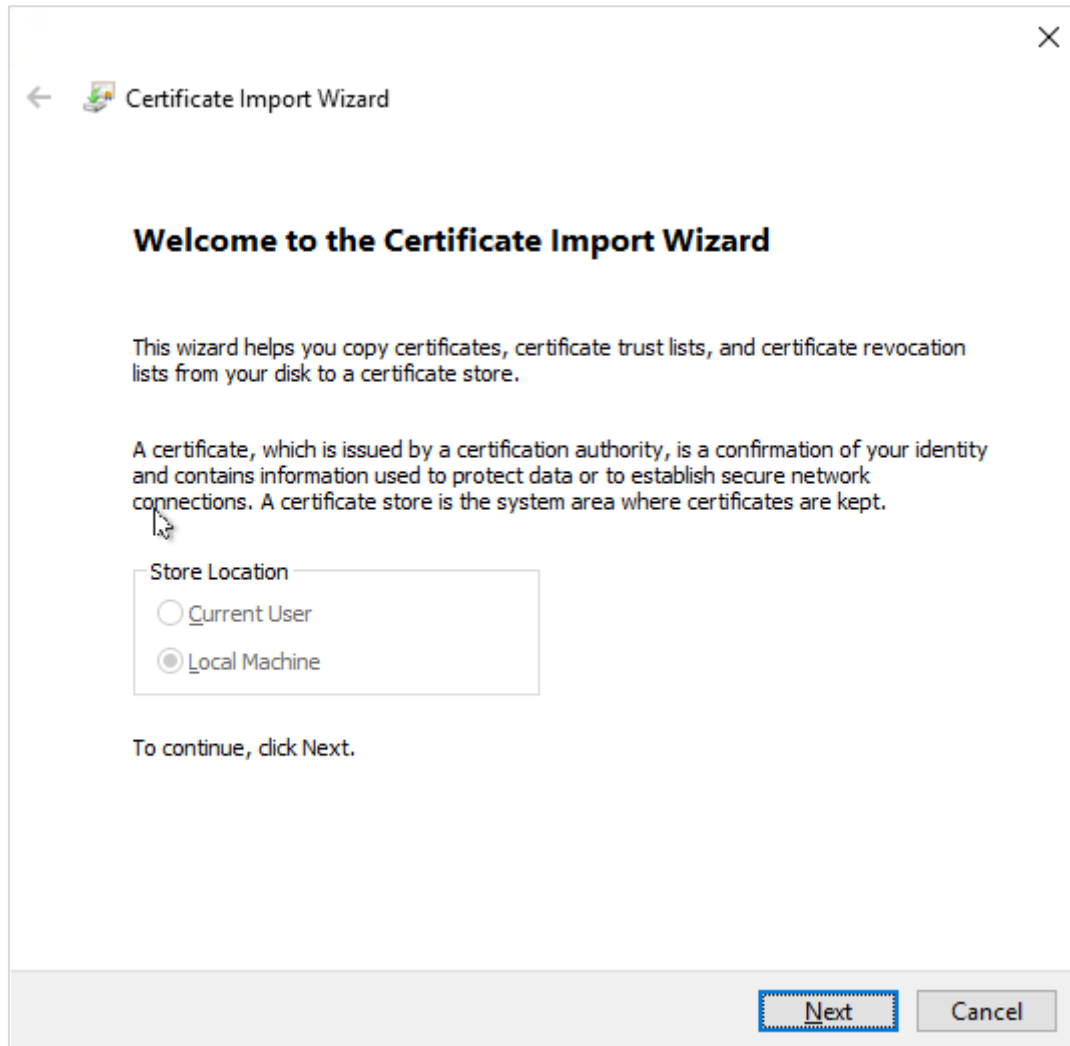
3. On Certlm select personal, right click and select All task then select **Import**.

Figure 3-2: Import Certificates



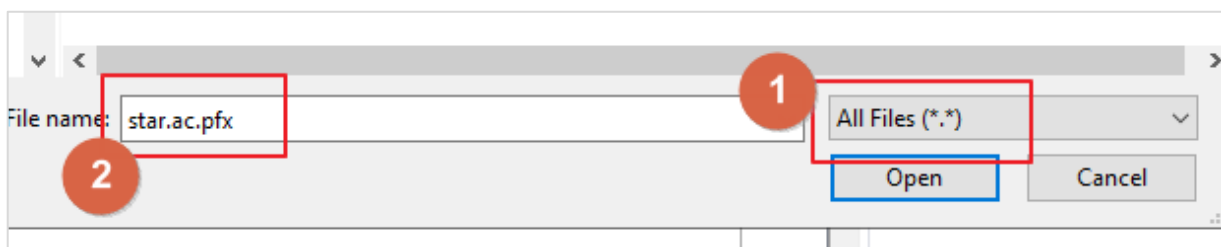
The Certificate Import Wizard is displayed.

Figure 3-3: Welcome Import Wizard



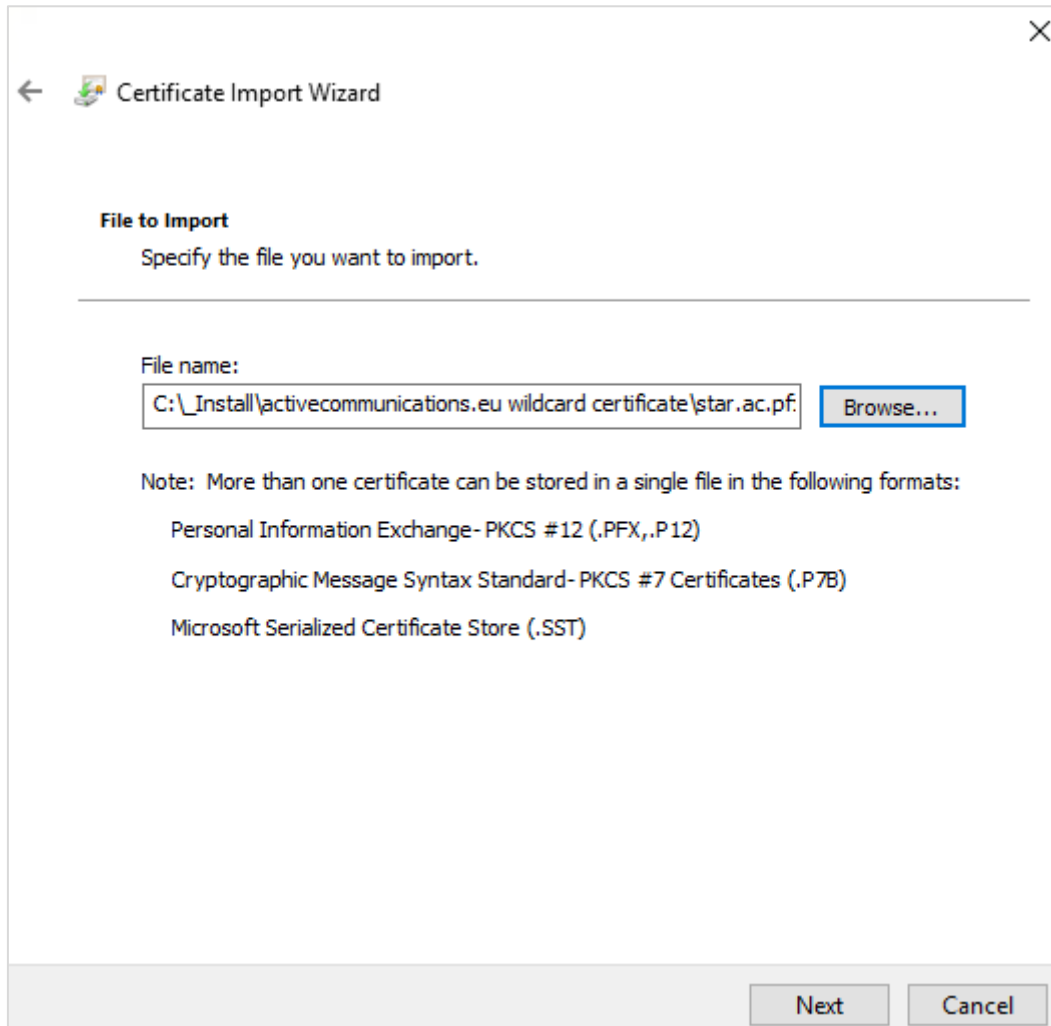
4. Click **Next** to continue.

Figure 3-4: Select Certificate File



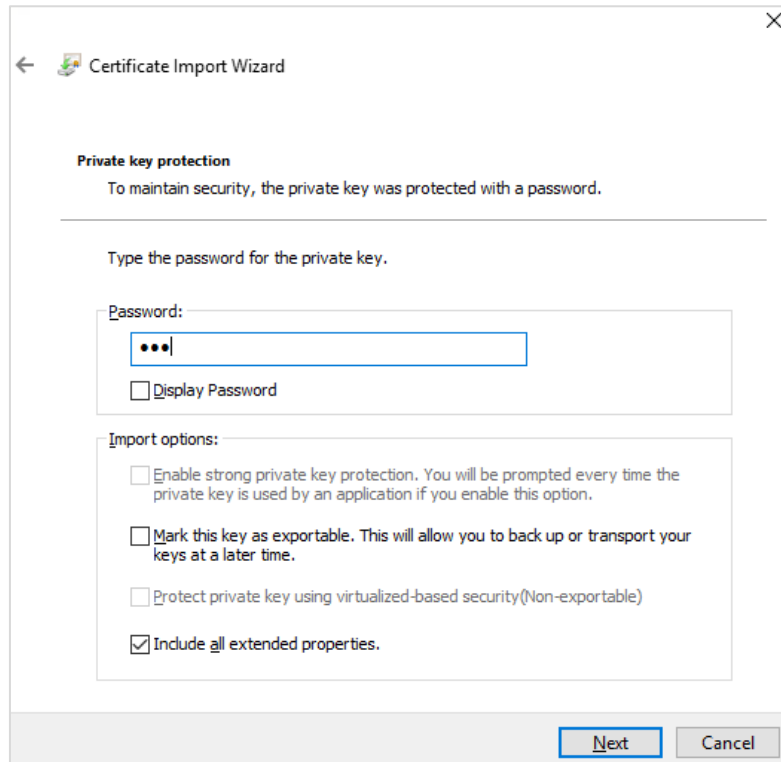
5. Select "all files" at the extension selector and browse to the pfx file from your certificate.

Figure 3-5: Browse to Certificate File



6. Select **Next**.

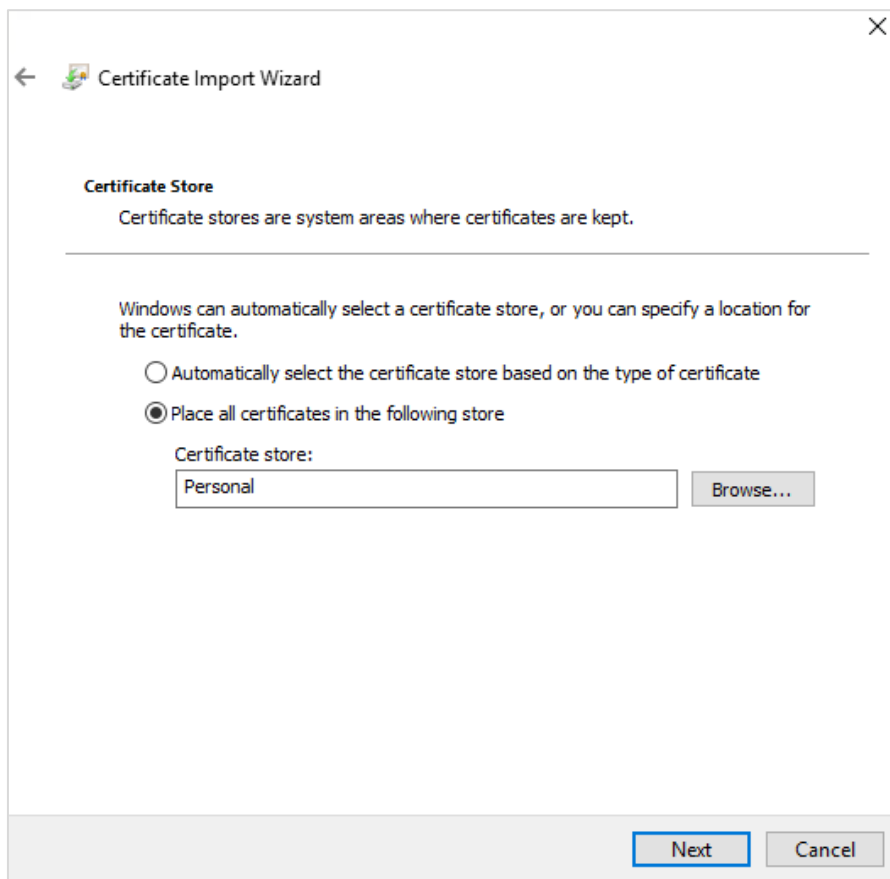
Figure 3-6: Enter Password



The screenshot shows the 'Certificate Import Wizard' dialog box at the 'Enter Password' step. The title bar includes a back arrow, a certificate icon, and the text 'Certificate Import Wizard'. The main content area is titled 'Private key protection' and contains the following text: 'To maintain security, the private key was protected with a password.' Below this is a horizontal line and the instruction 'Type the password for the private key.' A 'Password:' label is followed by a text input field containing three dots and a cursor. Below the input field is a checkbox labeled 'Display Password'. Underneath is the 'Import options:' section with four checkboxes: 'Enable strong private key protection...' (unchecked), 'Mark this key as exportable...' (unchecked), 'Protect private key using virtualized-based security(Non-exportable)' (unchecked), and 'Include all extended properties.' (checked). At the bottom right are 'Next' and 'Cancel' buttons.

7. Enter the password of your pfx file (optional select “Mark this key as exportable...(only if you want to be able to export the certificate again from this machine).

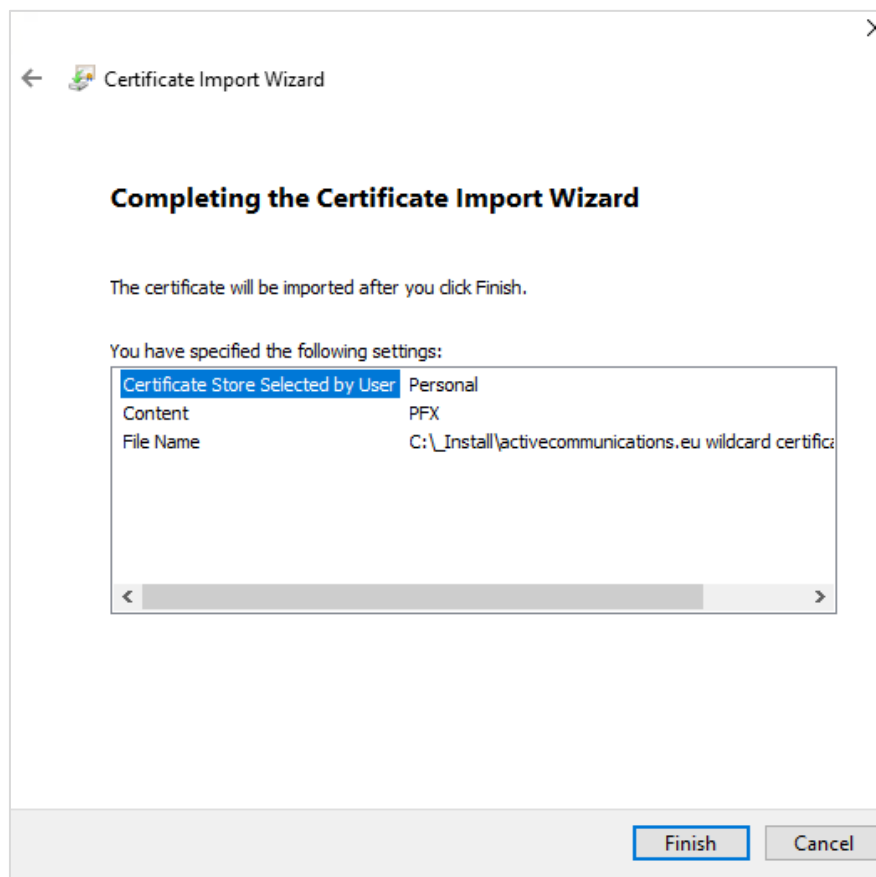
Figure 3-7: Certificate Store



The screenshot shows the 'Certificate Import Wizard' dialog box at the 'Certificate Store' step. The title bar includes a back arrow, a certificate icon, and the text 'Certificate Import Wizard'. The main content area is titled 'Certificate Store' and contains the text: 'Certificate stores are system areas where certificates are kept.' Below this is a horizontal line and the text: 'Windows can automatically select a certificate store, or you can specify a location for the certificate.' There are two radio button options: 'Automatically select the certificate store based on the type of certificate' (unselected) and 'Place all certificates in the following store' (selected). Below the second option is a 'Certificate store:' label followed by a text input field containing 'Personal' and a 'Browse...' button. At the bottom right are 'Next' and 'Cancel' buttons.

8. Browse to the location of the certificate store.

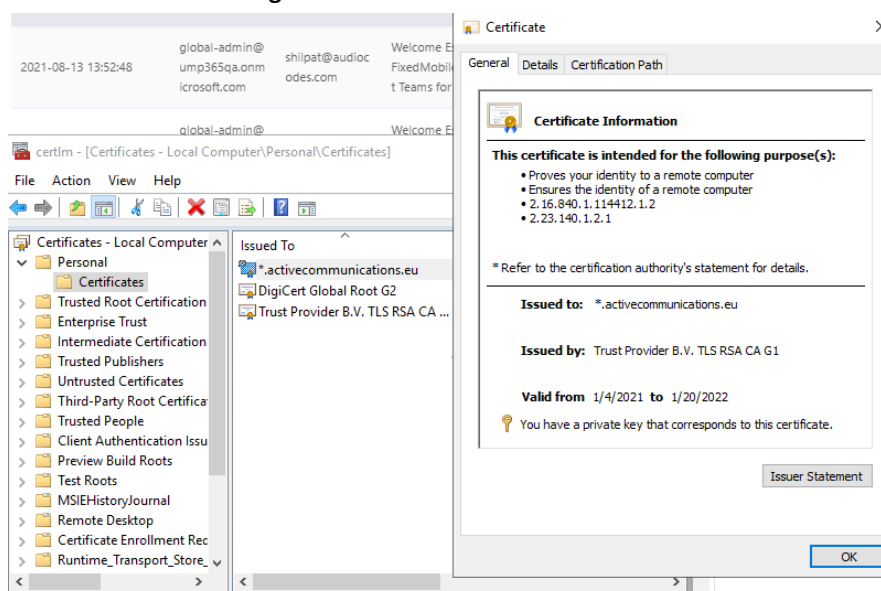
Figure 3-8: Completing the Certificate Wizard

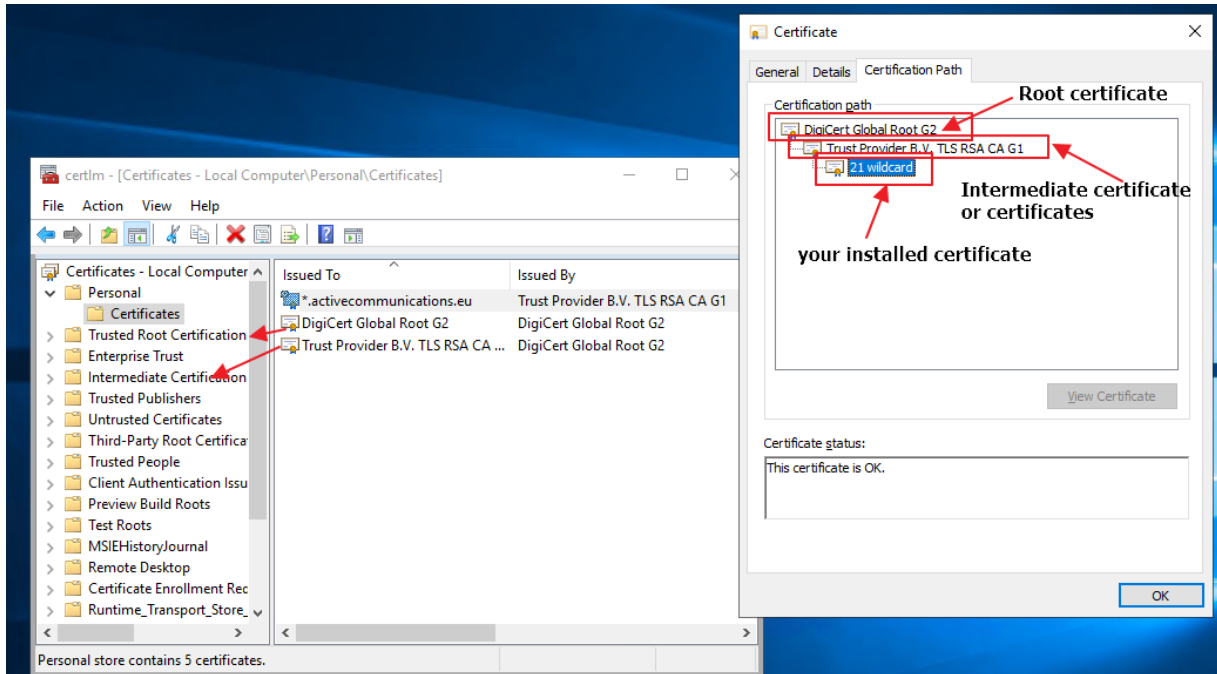
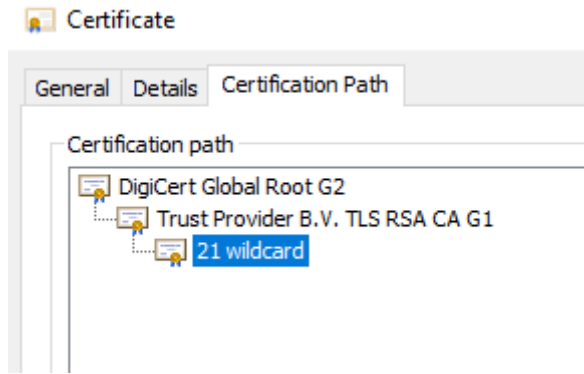


9. Click **Finish**.

The new certificates are installed and added to the Personal > Certificates folder. You now need to move the Trusted Root certificate and Intermediate Certificates to the corresponding folders. To identify which certificates have to be moved to which folder, open your certificate from certlm (double-click it).

Figure 3-9: Personal Certificate Store





4 UMP Networking Configuration

This chapter describes the networking ports recommendation. Networking topology can vary for different deployments according to the following factors:

- Are UMP, SBC and OVOC deployed in the same network environments ?
- Have different VNETs been defined ?
- Have different locations been defined ? For example, OVOC in Azure, UMP and SBC in Customer Data Center) ?

It is necessary to configure the Networking tunnel, ports and firewall:

- PowerShell:
 - PowerShell uses port 80 and 443 to communicate with Microsoft Azure
 - No VPN is required
 - Current Version require “basic” direct internet access without a proxy server
- HTTPS – Port 443:
 - Access to the Self-service portal
 - UMP → SBC (HTTP – port 80 also available)
 - Rest API (HTTP – port 80 also available)
- HTTP – Port 80:
 - Access to PowerShell
 - OVOC: OVOC → UMP
 - Add the Source IP (OVOC server IP address).
- SNMP – Ports 161,162 (OVOC)
- RDP – Port 3389 (Optional)
- MSFT address link – <https://docs.microsoft.com/en-us/microsoft-365/enterprise/urls-and-ip-address-ranges?view=o365-worldwide>

4.1 UMP Firewall Configuration

The following table describes the firewall configuration on the UMP for the connection with the provider's Data Center where OVOC is installed.

Table 4-1: UMP Ports Networking

Port/Protocol	UMP > Data Center (provider)	Data Center (provider) > UMP	Description
TCP 80 (HTTP)	√	√	Access to UMP 365 and SBC's GUI-Access to PowerShell (outbound).
TCP 3389 (RDP)	√	√	Access to Azure's Service Server using RDP (TCP 3389) from Data Center's Access to UMP (Data Center).
UDP 161 (SNMPv3)		√	SNMP Trap Manager port on UMP that is used to send traps to the OVOC server.
UDP 162 (SNMPv3)	√	-	SNMP trap listening port on OVOC.
UDP 1161 (Keep-alive)	√	-	Port used to send Keep-alive messages from UMP.
TCP 443 (HTTPS)	√	-	-

4.2 VPN Configuration (Optional)

- VPN is required if the connection to OVOC (or between the UMP and the SBC's) is over the public network. The VPN is used to connect the On-Premises UMP and SBC to the central OVOC service.

Table 4-2: VPN Configuration

Phase	Attribute	Customer		AudioCodes
Phase 1: ISAKMP- Main Mode	Peer IP Address	-		-
	SA Timeout (seconds)	1440		1440
	Hash Algorithm	SHA1		SHA1
	Encryption Algorithm	AES-256		AES-256
	Diffie-Hellman (DH) Group	Group 2 (1024)		Group 2 (1024)
	Pre-shared Key	Shared via Phone/Email		
Phase 2: IPSec – Quick Mode	SA Timeout (seconds)	3600	3600	-
	Hash Algorithm	SHA1	SHA1	-
	Encryption Algorithm	AES-256	AES-256	-
	PFS DH Group	Group 2 (1024)	Group 2 (1024)	-
	Encrypted Hosts/Subnets	TBD	TBD	-



- Authentication Header (AH) is not supported.
- Aggressive Mode is not supported
- If a PAT or hide NAT is used on either side of the tunnel, the VPN will require special configuration.

The VPN tunnel ports should allow traffic for the following protocols/ports.

Table 4-3: VPN Tunnel Ports

Transport/Port/Protocol	AudioCodes > Customer	Customer > AudioCodes
TCP 22 (SSH)	√	-
UDP 162 (SNMP)		√
UDP 161 (SNMP)	√	
TCP 443 (HTTPS)	√	-
TCP 3389 (RDP)	√	-
TCP; 636 (LDAPs)	-	-
The following ports are required if managed devices are monitored using central OVOC (AudioCodes Datacenter)		
UDP 1161 (SNMP)	Bi-directional	



The VPN tunnel ports above are just an example and can vary between different customers topologies. The table should include all the require protocols and ports, according to the networking topology.

4.3 OVOC Service Provider Firewall Configuration

This section describes how to configure the Enterprise Firewall between the OVOC Service provider network and the UMP/SBC.

To configure the Enterprise firewall on Microsoft Azure:

1. On Microsoft Azure, ensure that you have deployed the OVOC Virtual Machine as described in the OVOC IOM.
2. Configure the Enterprise firewall according to the ports below.

Table 4-4: Enterprise Firewall

Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
OVOC clients and OVOC server					
HTTPS/NBIF Clients ↔ OVOC server	TCP (HTTPS)	√	443	Connection for OVOC/ NBIF clients. Initiator: Client	OVOC server side / Bi-directional
WebSocket Client ↔ OVOC Server Communication	TCP (HTTP)	√	915	WebSocket Client and OVOC Server communication (internal) according to RFC 6455, used for managing the alarm and task notification mechanism in the OVOC Web. Initiator (internal): WebSocket Client	OVOC server side / Bi-directional
OVOC server and OVOC Managed Devices					
Device ↔ OVOC server (SNMP)	UDP	√	1161	Keep-alive - SNMP trap listening port (used predominantly for devices located behind a NAT). Used also by Fixed License Pool and Floating License Service. Initiator: AudioCodes device	OVOC server side / Receive only
	UDP	√	162	SNMP trap listening port on the OVOC. Initiator: AudioCodes device	OVOC server side / Receive only
	UDP	√	161	SNMP Trap Manager port on the device that is used to send traps to the OVOC server. Used also by Fixed License Pool and Floating License Service. Initiator: OVOC server	MG side / Bi-directional
Device ↔ OVOC server (NTP Server)	UDP (NTP server)	x	123	NTP server synchronization for external clock. Initiator: MG (and OVOC server, if configured as NTP client) Initiator: Both sides	Both sides / Bi-directional
Device ↔ OVOC server	TCP (HTTP)	x	80	HTTP connection for files transfer and REST communication.	OVOC server side / Bi-

Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction	
				Initiator: Both sides can initiate an HTTP connection	directional	
	TCP (HTTPS)	√	443	HTTPS connection for files transfer (upload and download) and REST communication. Initiator: Both sides can initiate an HTTPS connection.	OVOC server side / Bi-directional	
Device ↔ OVOC server Floating License Management	TCP (HTTPS)	√	443	HTTPS connection for files transfer (upload and download) and REST communication for device Floating License Management. Initiator: Device	OVOC server side / Bi-directional	
Devices Managed by the Device Manager						
OVOC server ↔ Device Manager Pro	TCP (HTTP)	x	80	HTTP connection between the OVOC server and the Device Manager Pro Web browser. Initiator: Client browser	OVOC server side / Bi-Directional.	
				HTTP connection that is used by endpoints for downloading firmware and configuration files from the OVOC server. Initiator: Endpoint		
	TCP (HTTPS)	√	443	HTTPS connection between the OVOC server and the Device Manager Pro Web browser. Initiator: Client browser		OVOC server side / Bi-Directional
				HTTPS connection used by endpoints for downloading firmware and configuration files from the OVOC server. Initiator: Endpoints		
OVOC server ↔ Endpoints (used for backward compatibility)	TCP (HTTP)	x	8080	HTTP connection that is used by endpoints for downloading firmware and configuration files from the OVOC server. Initiator: Endpoint	OVOC server side / Bi-directional	
	TCP (HTTP)	x	8081	HTTP REST updates connection. It is recommended to use this connection when managing more than 5000 IP Phones. In this case, you should change the provisioning URL port from 80 to 8081 in the phone's configuration file. Initiator: Endpoint	OVOC server side / Bi-directional	
	TCP	x	8082	HTTPS REST updates connection	OVOC server	

Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
	(HTTPS)			(encryption only without SSL authentication). It is recommended to use this connection when managing more than 5000 IP Phones. In this case, you should change the provisioning URL port from 443 to 8082 in the phone's configuration file. Initiator: Endpoint	side / Bi-directional
OVOC Voice Quality Package Server and Devices					
Media Gateways ↔ Voice Quality Package	TCP	x	5000	XML based communication for control, media data reports and SIP call flow messages. Initiator: Media Gateway	OVOC server side / Bi-directional
	TCP (TLS)	v	5001	XML based TLS secured communication for control, media data reports and SIP call flow messages. Initiator: AudioCodes device	OVOC server side / Bi-directional
LDAP Active Directory Server					
OVOC server ↔ Active Directory LDAP server (OVOC user authentication)	TCP	x	389	Connection between the OVOC server and the Active Directory LDAP server (OVOC Users). Initiator: OVOC server	Active Directory server side / Bi-directional
	TCP (TLS)	v	636	Connection between the OVOC server and the Active Directory LDAP server (OVOC Users) with SSL configured. Initiator: OVOC server	Active Directory server side / Bi-directional
AudioCodes Floating License Service					
OVOC server ↔ AudioCodes Floating License Service	TCP	v	443	HTTPS for OVOC/ Cloud Service Initiator: OVOC REST client	OVOC REST client side / Bi-directional
External Servers					
OVOC server ↔ Mail Server	TCP	v	25	Trap Forwarding to Mail server Initiator: OVOC server	Mail server side / Bi-directional
OVOC server ↔ Syslog Server	TCP	v	514	Trap Forwarding to Syslog server. Initiator: OVOC server	Syslog server side / Bi-directional
OVOC server ↔ Debug Recording Server	UDP	v	925	Trap Forwarding to Debug Recording server.	Debug Recording server / Bi-

Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
				Initiator: OVOC server	directional
OVOC server ↔ UMP-365 server	TCP RDP	√	3389	Remote Desktop access to UMP-365 server Initiator: OVOC server	UMP-365 server/Bi-directional
Voice Quality					
Voice Quality Package ↔ Endpoints (RFC 6035)	UDP	x	5060	SIP Publish reports sent to the SEM server from the endpoints, including RFC 6035 SIP PUBLISH for reporting device voice quality metrics. Initiator: Endpoint	SEM server / Bi-directional

5 SQL License Guidelines - Optional

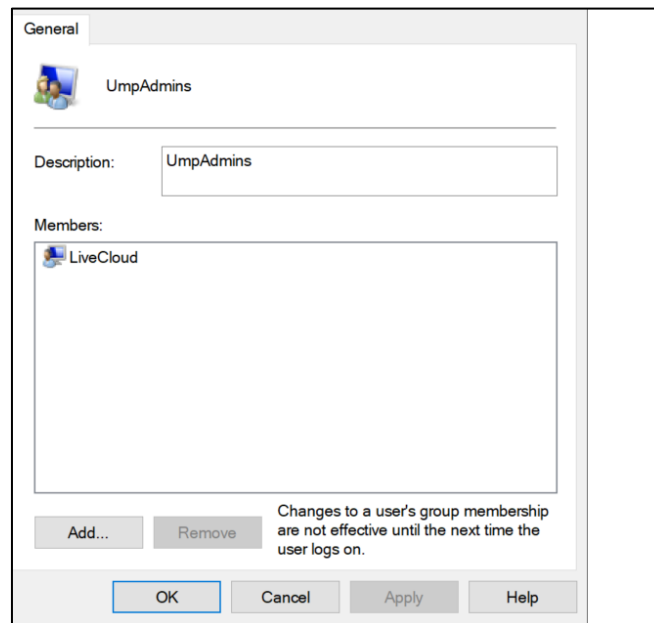
This chapter describes the SQL licensing guidelines. The UMP SP solution requires SQL 2019 Standard edition. Customers can do one of the following:

- Implement their own license agreement with MSFT ((UMP SP don't includes WIN OS or SQL license).
- AudioCodes can offer SQL standard edition (OEM) based on Server+CAL. Each Admin user with access to the system requires an SQL license.

The list of Admin users requiring a license is as follows:

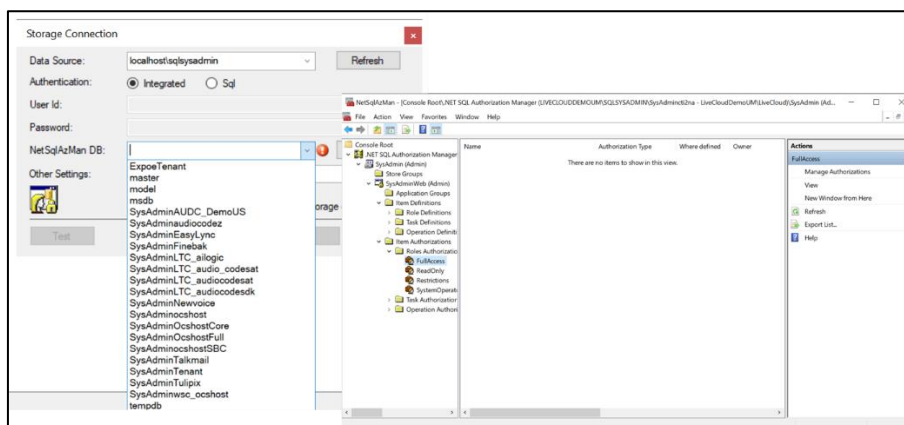
- **UMP SP Super Admin Users (Windows):**
 - All the users under Group “UmpAdmins”

Figure 5-1: UmpAdmins user members



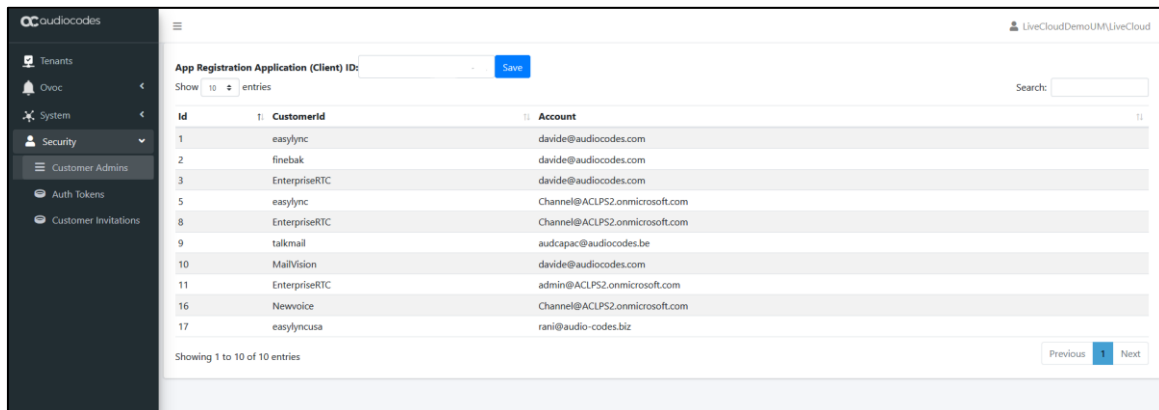
- UMP support two types of User Admin per Tenant:
 - UMP SP Windows users per Tenant (Customer) – Windows users per Tenant, our recommendation is to Grant Access to Account user (SSO with Azure AD). It is not recommended to create Windows users per Tenant (Customer). If you choose to create Window users per Tenant, this requires a license per user.

Figure 5-2: Tenant Admin User (Windows)



- **Grant Access to Users** – Customer/ Channel with Grant Access users (SSO Sign-In with Azure AD user):
- This information is displayed under **Security > Customer Admins**
- Accounts managing multiple customers only require one license.

Figure 5-3: Account List



Id	Customerid	Account
1	easylync	davide@audiocodes.com
2	finebak	davide@audiocodes.com
3	EnterpriseRTC	davide@audiocodes.com
5	easylync	Channel@ACLP52.onmicrosoft.com
8	EnterpriseRTC	Channel@ACLP52.onmicrosoft.com
9	talkmail	audcapac@audiocodes.be
10	MallVIsion	davide@audiocodes.com
11	EnterpriseRTC	admin@ACLP52.onmicrosoft.com
16	Newoice	Channel@ACLP52.onmicrosoft.com
17	easylyncusa	rani@audio-codes.biz

The guidelines are the follow:

- License per Admin
- **# License** = N (#Admin) x (SQL Server 2019 + 1 CAL per Admin User)
- CPN = SW/UMP/SP/1A



The OS and SQL license are not included in the product pricing (UMP CPN). Customers must order them separately.

6 Implementing Anti-virus on UMP server

This chapter describes the recommended guidelines for running anti-virus software on the UMP-365 server.

6.1 SQL

Running antivirus on a server with SQL installed, like the UMP server is not recommended. It is highly recommended prior to the roll out of any virus-protection project to test the entire system under a full load to measure any changes in stability and performance.

Virus protection software requires system resources to successfully execute tasks. Therefore you must perform testing before and after you install your antivirus software to determine whether there are any performance affecting issues that may arise on the computer that is running SQL Server.

When you configure your antivirus software settings, make sure that you exclude the following files or directories (as applicable) from virus scanning. This improves the performance of the files and helps make sure they are not locked when the SQL Server service must use them:

- Exclude database files (MDF, LDF, and NDF)
- Exclude the binaries / executable files (sqlservr.exe, SSAS, SSRS, SSIS etc.)
- Exclude the library files
- Exclude Backup files (full, differential or log)
- Exclude Audit and trace files
- Exclude Full-Text Catalog
- Exclude Analysis, Reporting or Integration Services files
- Exclude File Stream

For the UMP server also exclude the following directory:

- Exclude c:\acs
- Disable on access scan

6.2 ASP.NET

As UMP uses ASP.NET with IIS, the below folders should be excluded for Antivirus:

- The physical file folders for the web sites content, whether it's a local folder or a network share.
The default location is mentioned below, however note that your content may reside in a different directory as well. Check the path to your website and it's virtual directories to identify the correct path.
 - C:\inetpub\wwwroot
- .Net Framework config directory:
 - C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG
 - C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG
 - C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config
 - C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config
- ASP.net temp file directory:
 - C:\Windows\Microsoft.NET\Framework\v2.0.50727\Temporary ASP.NET Files
 - C:\Windows\Microsoft.NET\Framework64\v2.0.50727\Temporary ASP.NET Files

- C:\Windows\Microsoft.NET\Framework\v4.0.30319\Temporary ASP.NET Files
- C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files
- IIS config folder: In case you are running IIS in shared configuration and your server hosts the configuration on a different location, ensure to exclude it from the scan. More information regarding shared configuration can be found [here](#).
%SystemDrive%\Windows\System32\inetsrv\config\
- IIS Temporary Compressed Files:
%SystemDrive%\inetpub\temp\IIS Temporary Compressed Files

6.3 Create UMP Service Account

This procedure describes how to define users and administrators for the Windows login account service on the Service Provider domain. These users perform the following tasks to setup the UMP-365 for the Service Provider operator before they can start onboarding customers. The following actions are performed by the Windows Service account:

- Install UMP-365 (see Chapter 8)
- Create DNS Subdomains (see Chapter 9)
- App Registration for Background Processing (see Chapter 10)
- Define Invitation Settings (see Chapter 12)
- Define Email Settings (see Chapter 13)
- App Registration for Customer Admins (see Chapter 14)
- Configure License (see Chapter 15)
- Configure Service Provider Logos (see Chapter 16)
- Secure networking between UMP, SBC and OVOC (see Chapter 17)

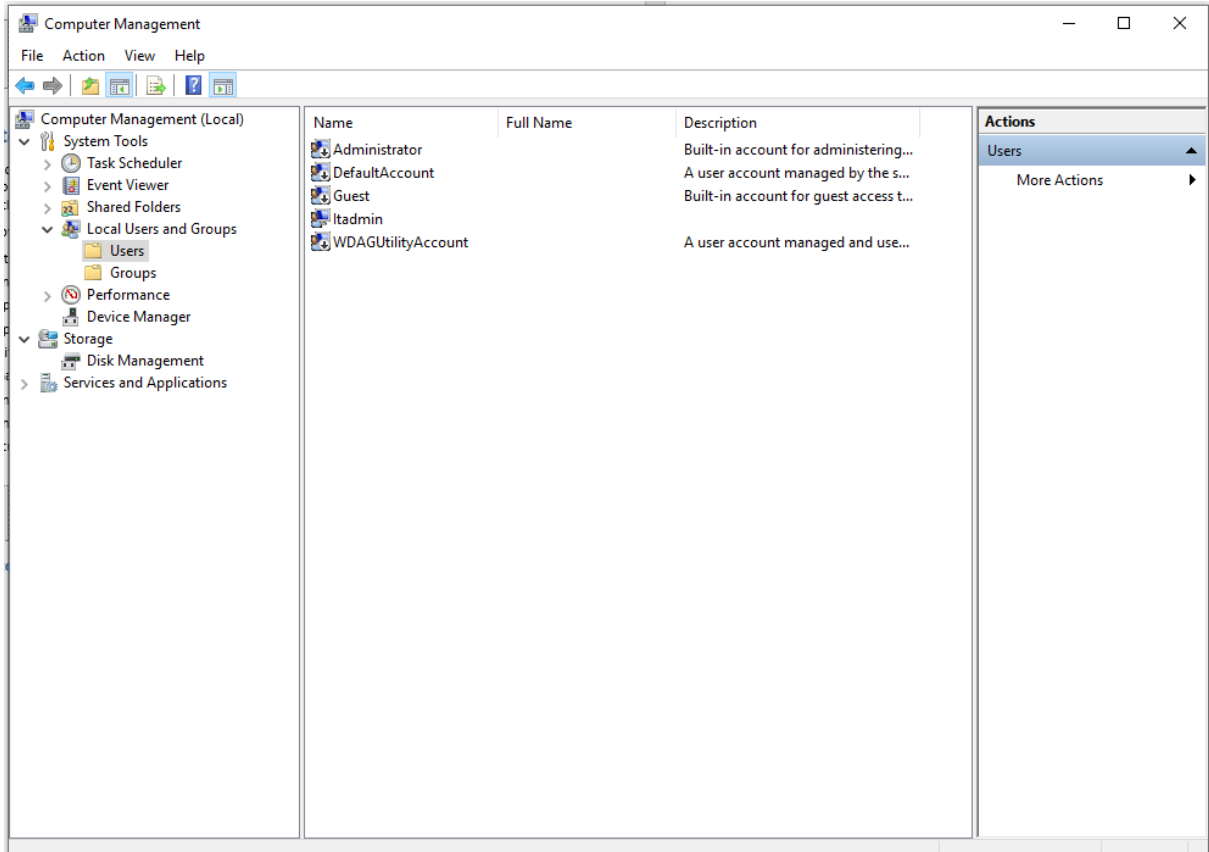


For configuration on the Microsoft Azure platform, ensure that you have Global Admin permissions for both the Main Tenant and Service Provider operator tenant platforms. If customers are using a backend SQL server, then the same account must be used to login to the SQL server on the backend server.

To create a Windows UMP Service account:

1. Open the Computer Management (Local) screen.
2. Open the Local Users and Groups folder.

Figure 6-1: Computer Management



3. On the right-hand side pane, select **Users > More Actions > New User**.

Figure 6-2: New User

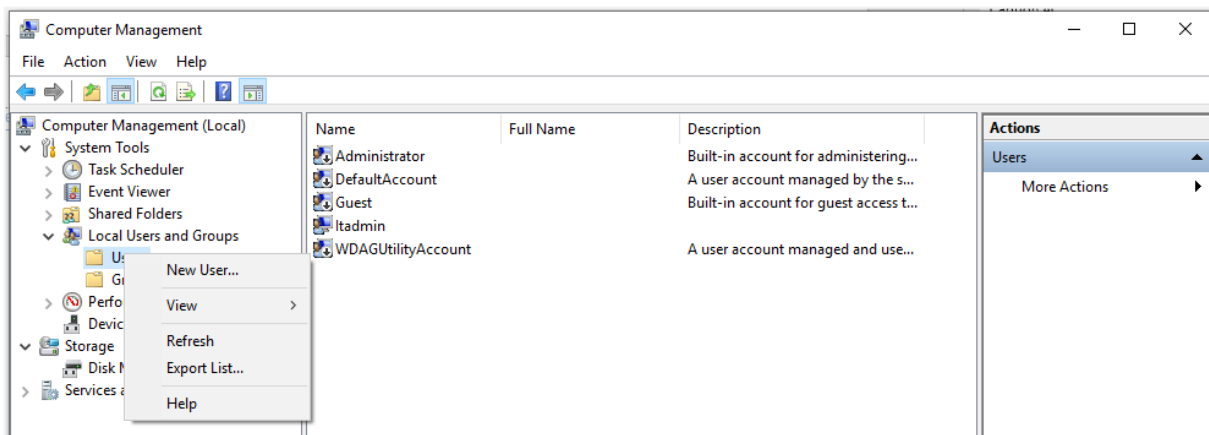


Figure 6-3: UMP Service Account

New User

User name: UMP Service Account

Full name: UMP Service Account

Description: UMP Service Account

Password: ●●●●●●

Confirm password: ●●●●●●

User must change password at next logon

User cannot change password

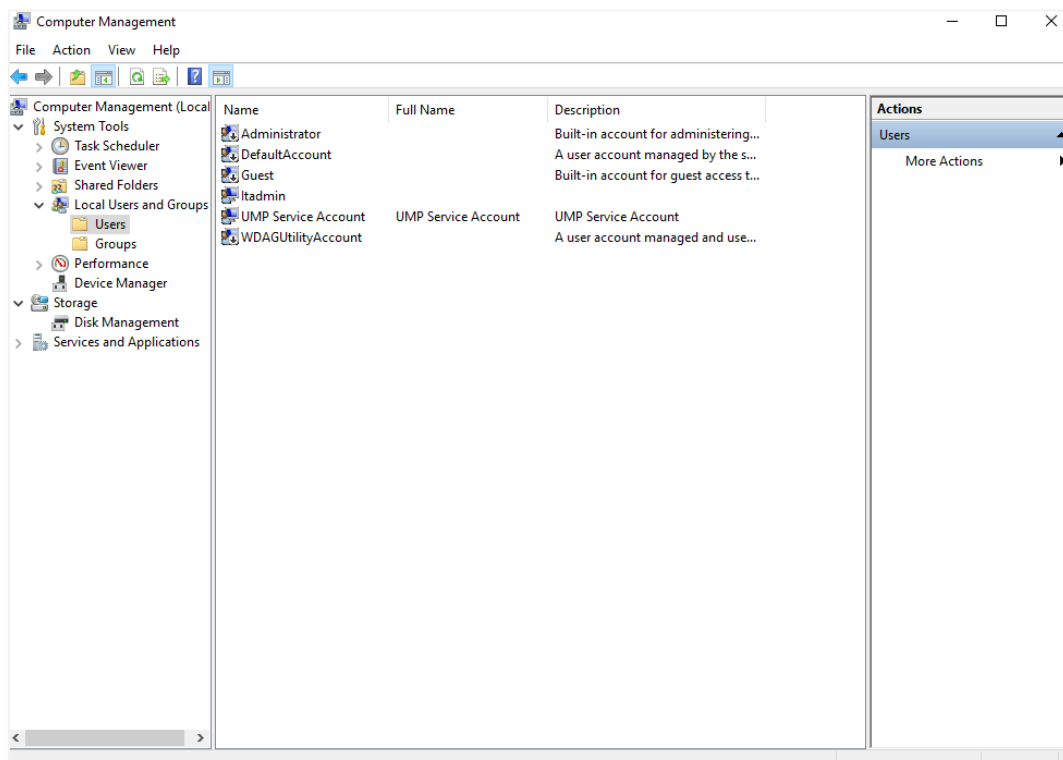
Password never expires

Account is disabled

Help Create Close

2. Enter the details of the new user to manage the UMP-365 Service Account(recommended to set Password never expires option) and then click **Create**. The new user is added.

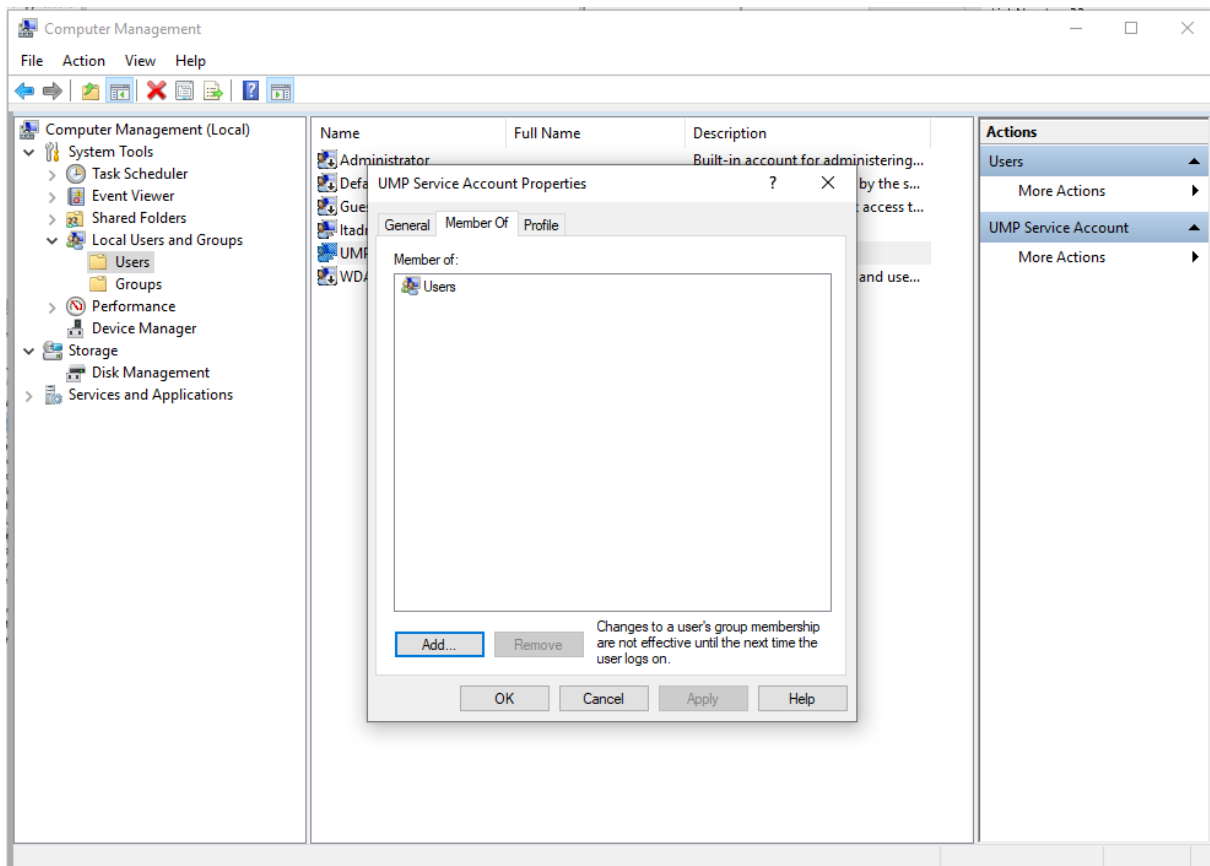
Figure 6-4: New UMP Service Account User



3. Right-click the user and select **Properties**.

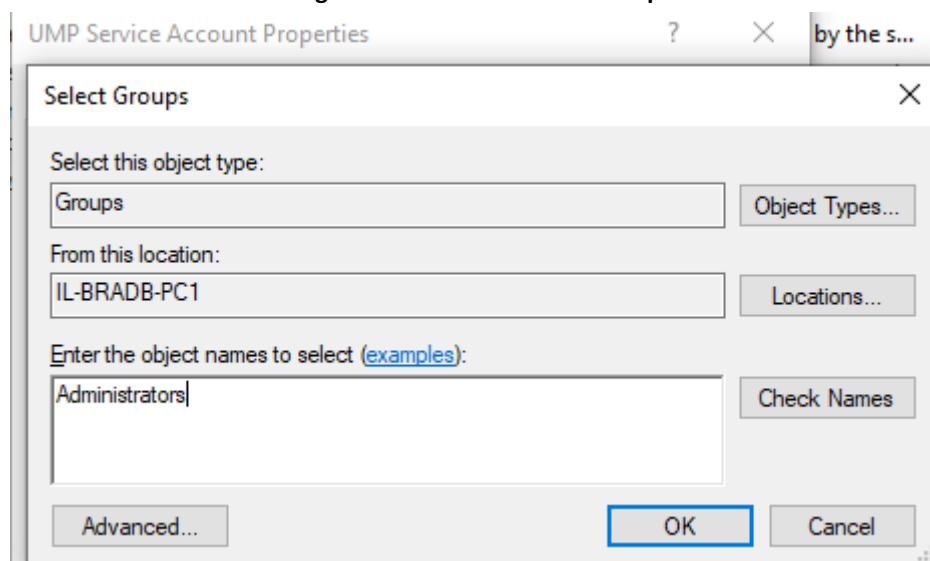
4. Select the **Member Of** tab.

Figure 6-5: Account Properties



5. Click **Add** to add the UMP Service Account user to the **Administrators** group.

Figure 6-6: Administrators Group



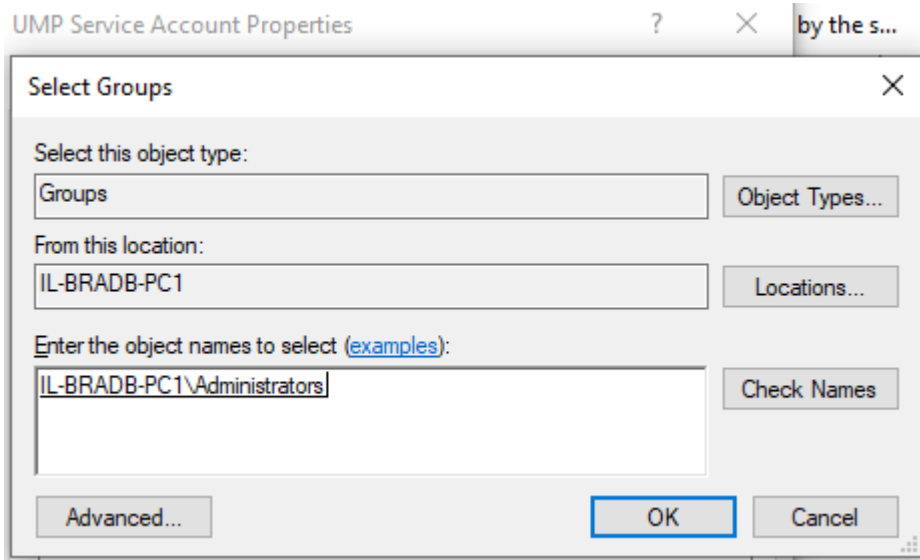


Figure 6-7: UMP Service Account Properties

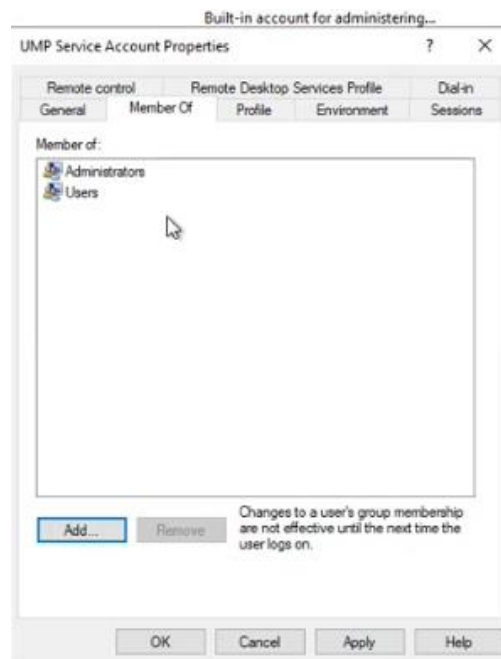
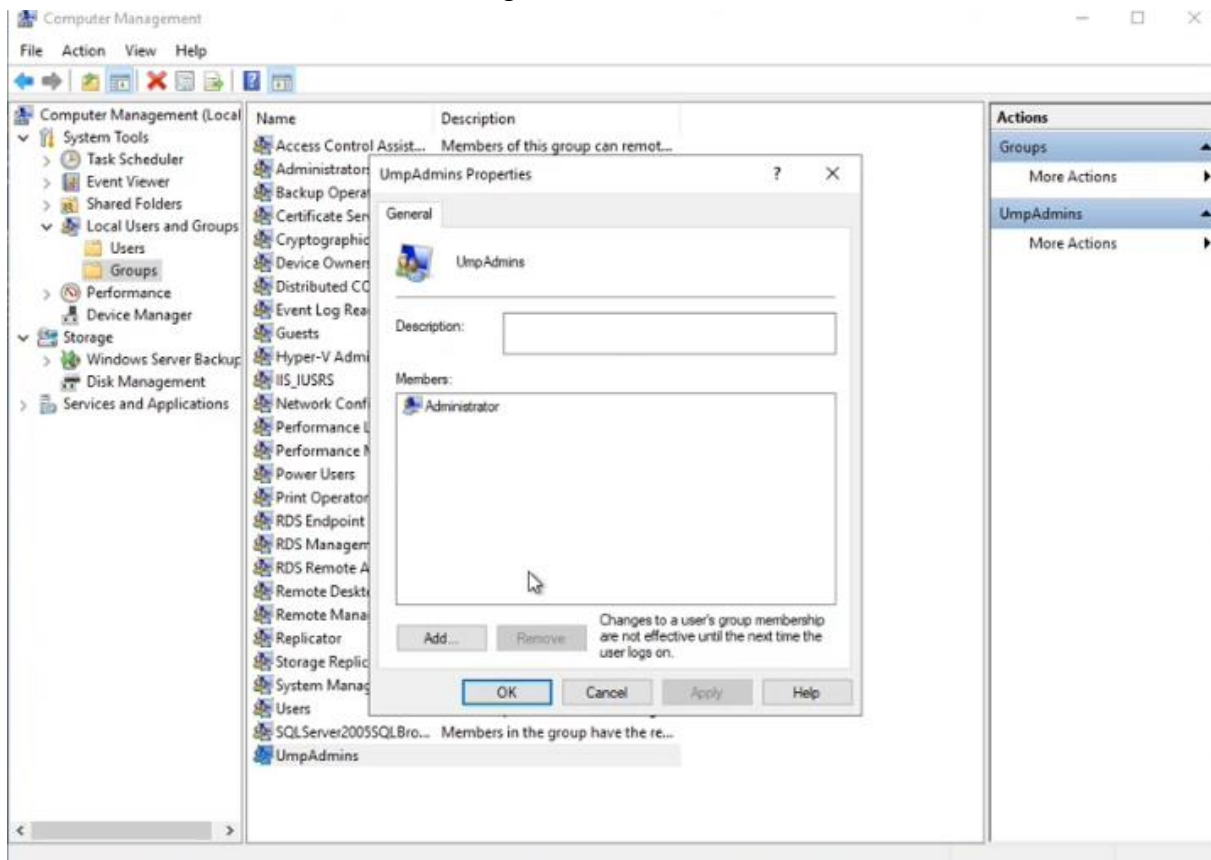


Figure 6-8: Administrators Properties



The example screen below shows a new group “UmpAdmins” that is created following the installation. The Administrator who ran the installation is automatically a member of this group.

Figure 6-9: UMPAdmins



6. Click **Add** to add other users to this group who you wish to administer the UMP-365.

Figure 6-10: UMP Admin User

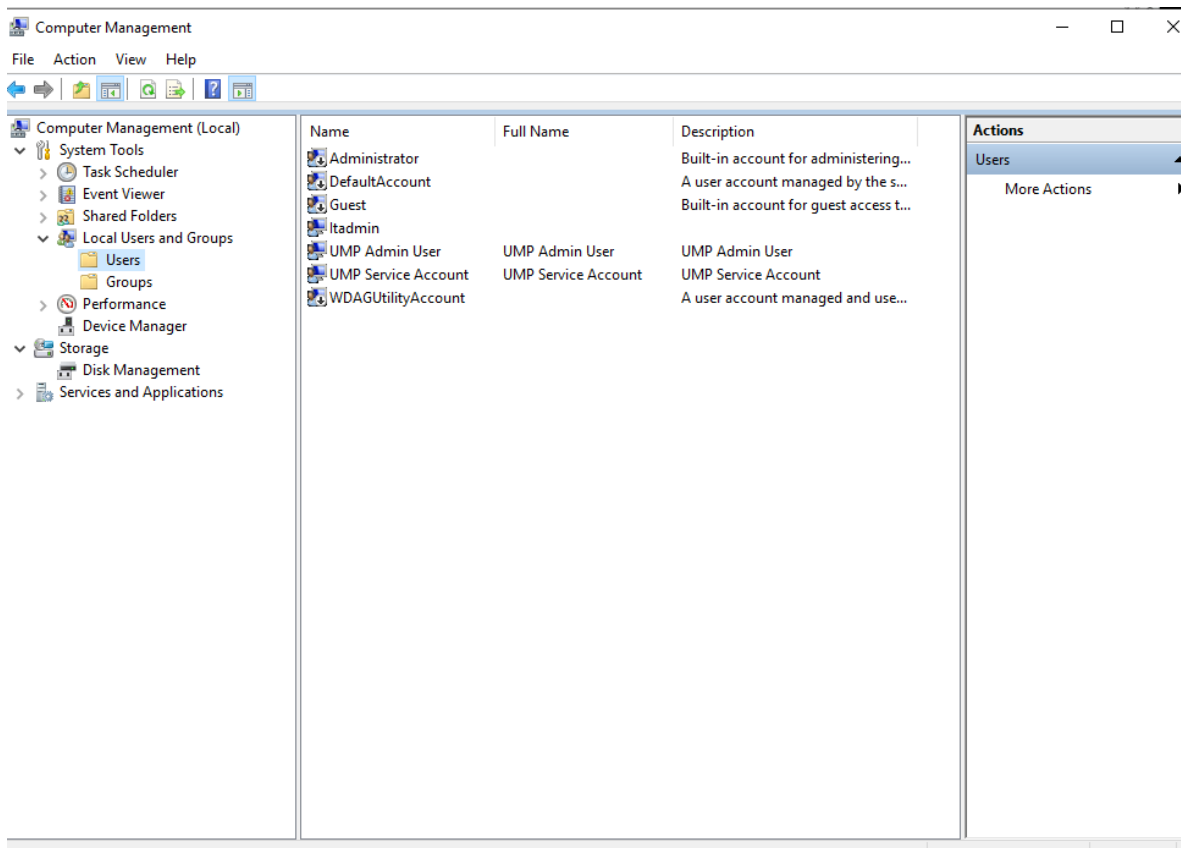
The 'New User' dialog box contains the following information:

- User name: UMP Admin User
- Full name: UMP Admin User
- Description: UMP Admin User
- Password: [Masked]
- Confirm password: [Masked]
- User must change password at next logon
- User cannot change password
- Password never expires
- Account is disabled

Buttons: Help, Create (highlighted), Close

7. Enter the details of the new user to manage the UMP-365 Service Account(recommended to set Password never expires option) and then click **Create**.
The new user is added.

Figure 6-11: New UMPAdmins User



Part II

Installation and Setup

7 Installing the Prerequisites

This section describes how to install the prerequisites.

Do the following:

1. Create service account with local admin rights.
2. Server login with new service account.
3. Download the installation package from the following location: https://downloads-audiocodes.s3.amazonaws.com/Download/AC_UMP_OVL_ISO.html
4. Mount the UMP-MT ISO file.
5. Before UMP SP can be installed, the server needs to be prepared by installing the prerequisites by running the Install-UMPSPPrerequisites.ps1 script file running with Administrator permissions (Admin mode).
6. Reboot server.



- Logfiles of the Prerequisites installation are placed in:%localappdata%\ump-sp\.
- To support the communication from the Frontend server (first server installed, running the web applications) to the backend servers running SQL server, all servers in the environment should use the same username and password, or be part of an Active Directory Domain, sharing the same security context.

8 Installing UMP-SP

This section describes how to install UMP-SP. This installation must be run by the Windows UMP Service account.

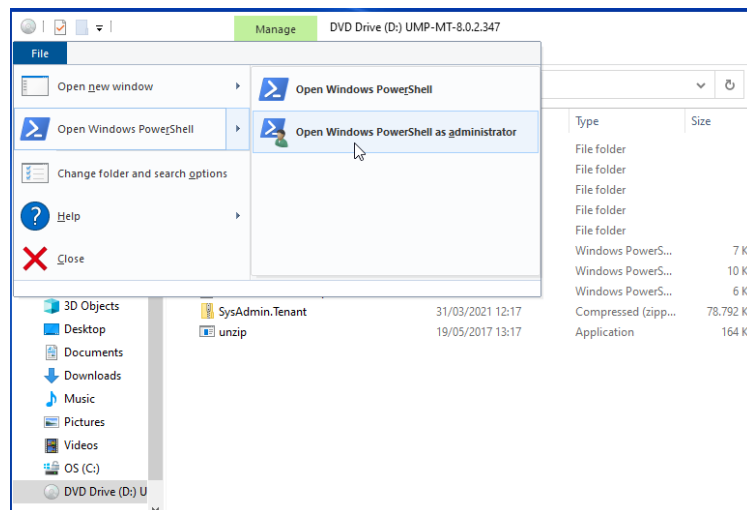


The details of the UMP Service account are displayed in the UMP Service Settings screen (see Section 06.3).

To install UMP-SP

1. Login With Service account with the UMP Service account credentials.
2. Mount ISO.
3. Open a PowerShell session, go to the iso partition (example d:\) and run the `install_multitenant.ps1` script.
4. From Mounted drive select:
file → Open Windows PowerShell → Open Windows PowerShell as administrator

Figure 8-1: Open Windows PowerShell



Important: Password is shown in clear text in PowerShell.

5. You are prompted for the domain/user/password of the local server (for workgroup use “.”) For the domain). The account entered must be the service account created above.

Figure 8-2: Installation Console

```
PS C:\multitenant>
PS C:\multitenant>
PS C:\multitenant> .\install_multitenant.ps1
What is your domain?: .
What is your username?: administrator
What is your password?:
```

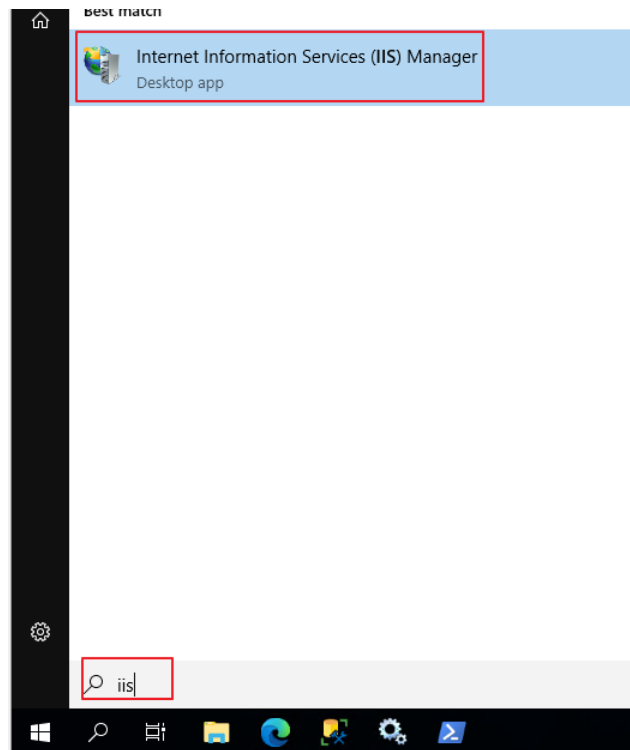
8.1 Adding SSL Certificate to IIS Website

After installing the UMP-SP you must install the SSL certificate to the IIS Website.

To install the certificate:

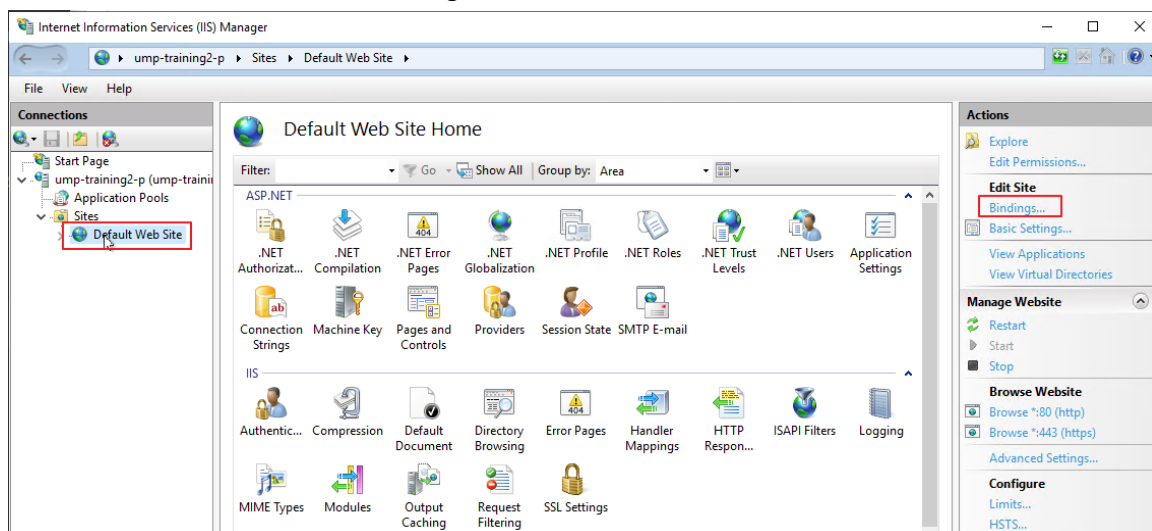
1. Open Internet Information Services (IIS) Manager.
2. Click Windows Start and type **IIS**.

Figure 8-3: IIS



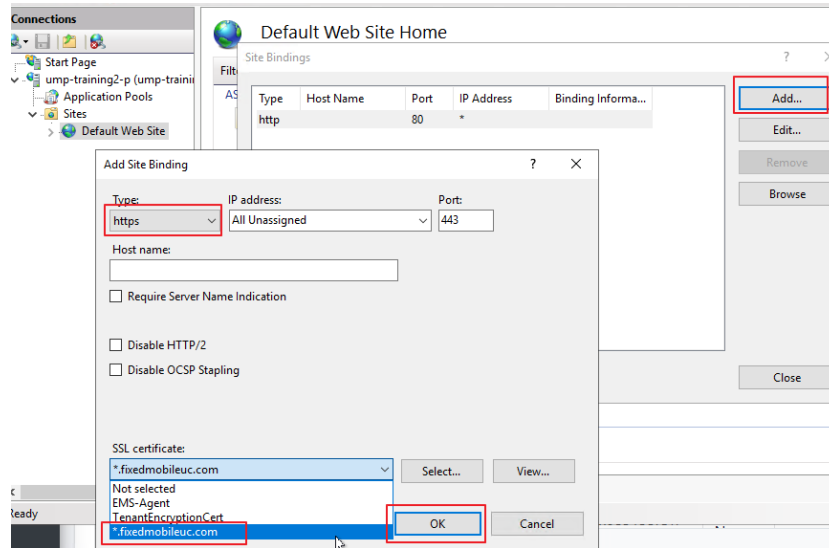
3. Browse in the Connections pane to Default Web Site and select **Bindings**.

Figure 8-4: Default Web Site



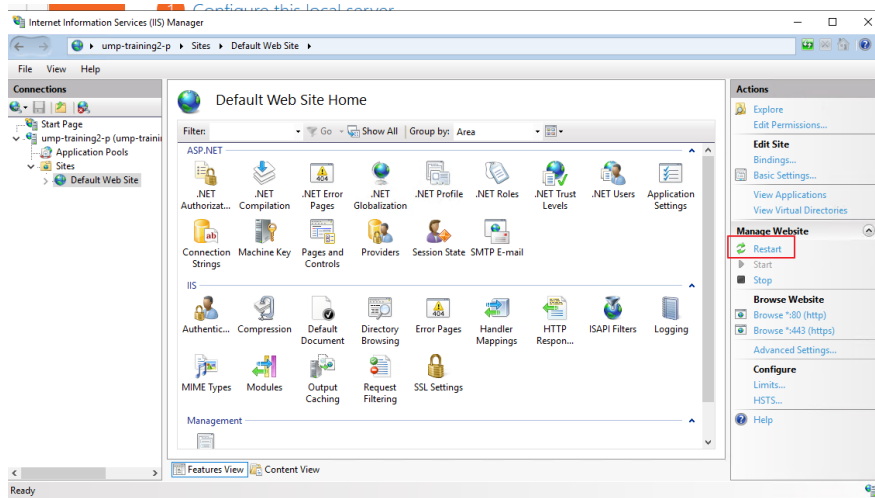
4. Click **Add**, select **https**, select your SSL certificate and click **OK**.

Figure 8-5: Add Site Binding



5. Click Close.

Figure 8-6: Default Web Site



6. Restart IIS.

9 Creating Customer DNS Subdomains

You can setup the DNS server connection between the customer's domain and the service provider domain using the following methods:

- **Fully Automatic process (DNS Hosting Provider resides on Azure):** The creation of the DNS subdomain including the creation of the TEXT and A-record is fully automated using the Onboarding Wizard. This setup requires configuration on the backend UMP-365 device (see Section 9.1)
- **Semi-automatic process (DNS Hosting Provider does not reside on Azure):** (Two-step provisioning semi-automatic process):
For this option the customer starts the Onboarding process with option to automatically create a DNS subdomain. However, this option is semi-automated because during the Onboarding process the customer is prompted to create a TEXT record for validating their subdomain and an A-record for IP address translation to the FQDN of the SBC device used to manage calls on the customer site (see Section 09.2).
- **Manual process (DNS Hosting Provider resides on Azure):** The DNS subdomain is created manually (see Section 9.3).



The Carrier tenant must keep at least one available license assigned to the tenant for one of the following Microsoft Office 365 Phone System user license types:

- E1 with Phone System
- E3 with Phone System
- Office 365 E5

The UMP-365 SQL database can be configured to support other license types upon customer request.

9.1 Fully Automatic Provisioning

This section describes how to setup the customer subdomain using automatic provisioning. This process runs the procedures described in Section 9.3 automatically.

Automatic DNS configuration requires one of the following roles:

- Domain Name Administrator
- Global Administrator

For details, see [Add a domain to Microsoft 365 - Microsoft 365 admin | Microsoft Docs](#)



The automatic provisioning of the DNS subdomains requires pre-configuration as described in Section 9.1.

9.1.1 Before Provisioning

Automatic provisioning of DNS records and derived trunk domain fully automates the onboarding process for a new tenant deploying the Microsoft direct routing model for service providers. The wizard adds the new domain in the customer M365 tenant and validates it by an automated process including:

- The creation of a TXT record in the Service Provider Azure DNS environment.
- The creation of a temporary activation user in the customer tenant with the newly created domain assigned and licensed with a Microsoft Office 365 Phone System user license.

9.1.1.1 Registering DNS Application

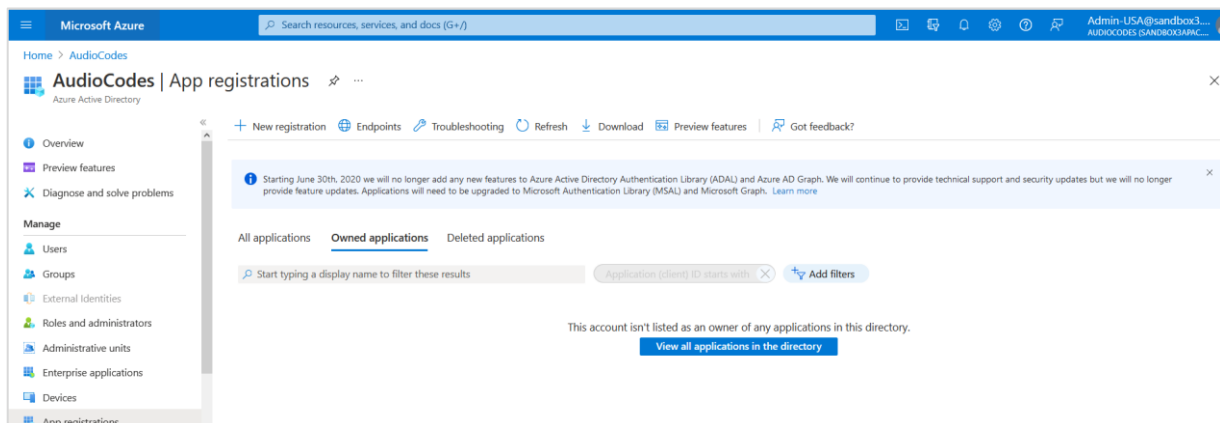


This registration includes the generation of a Client Secret that is only displayed once. It should be captured and saved for later configuration in the UMP Multitenant interface.

To register the DNS domain:

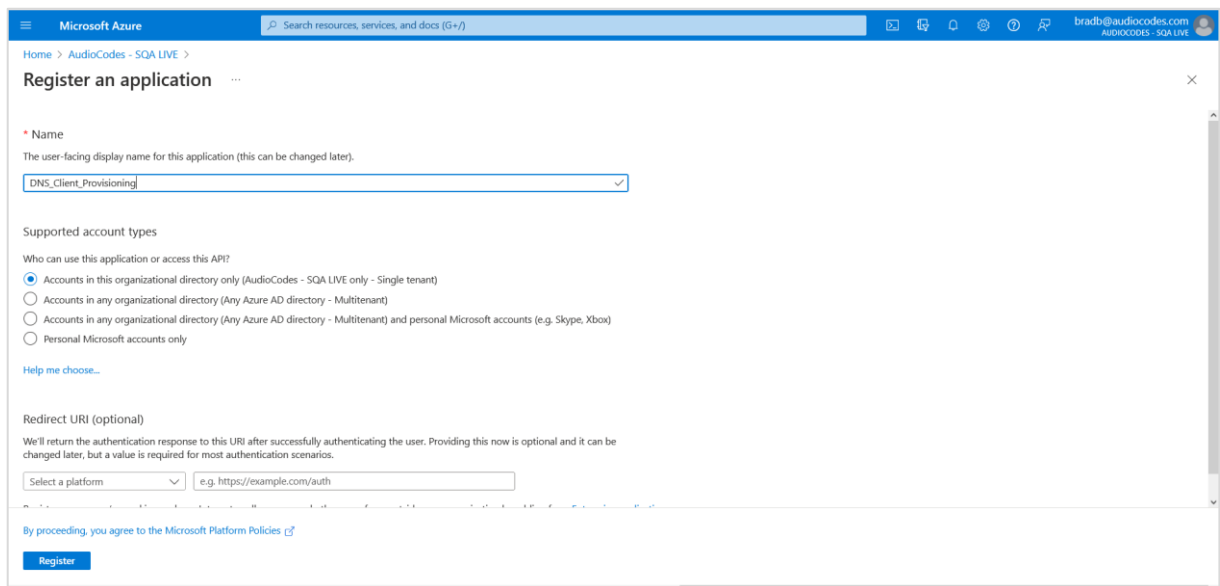
1. In the Navigation pane, select **App registrations** and then click **New registration**.

Figure 9-1: DNS Registration



2. Enter the name of the new registration e.g. **DNS_Client_Provisioning** and then click **Register**.

Figure 9-2: Dns_Client_Provisioning



A new registration is created.

Figure 9-3: DNS Application Registration

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the Microsoft Azure logo, a search bar, and the user profile 'bradb@audiocodes.com'. The main content area is titled 'DNS_Client_Provisioning' and displays the following details:

- Essentials:**
 - Display name: `DNS_Client_Provisioning`
 - Application (client) ID: `bd2e21ca-bd43-49d3-a9c1-ac0519c14e7d`
 - Object ID: `e9380a70-765e-4a60-8c36-c882374c0e25`
 - Directory (tenant) ID: `6a217d07-8f6d-43da-bcd5-2cd8b8be3b17`
 - Supported account types: `My organization only`
 - Client credentials: `0 certificate, 3 secret`
 - Redirect URIs: `Add a Redirect URI`
 - Application ID URI: `Add an Application ID URI`
 - Managed application in L: `DNS_Client_Provisioning`

Below the details, there is a 'Get Started' section with a 'Documentation' link and a large banner that reads: 'Build your application with the Microsoft identity platform'. The banner text states: 'The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create modern, standards-based authentication solutions, access and protect APIs, and add sign-in for your users and customers. Learn more'.

3. In the Navigation pane, select **App registrations**. The new registration is listed.

Figure 9-4: New App Registration

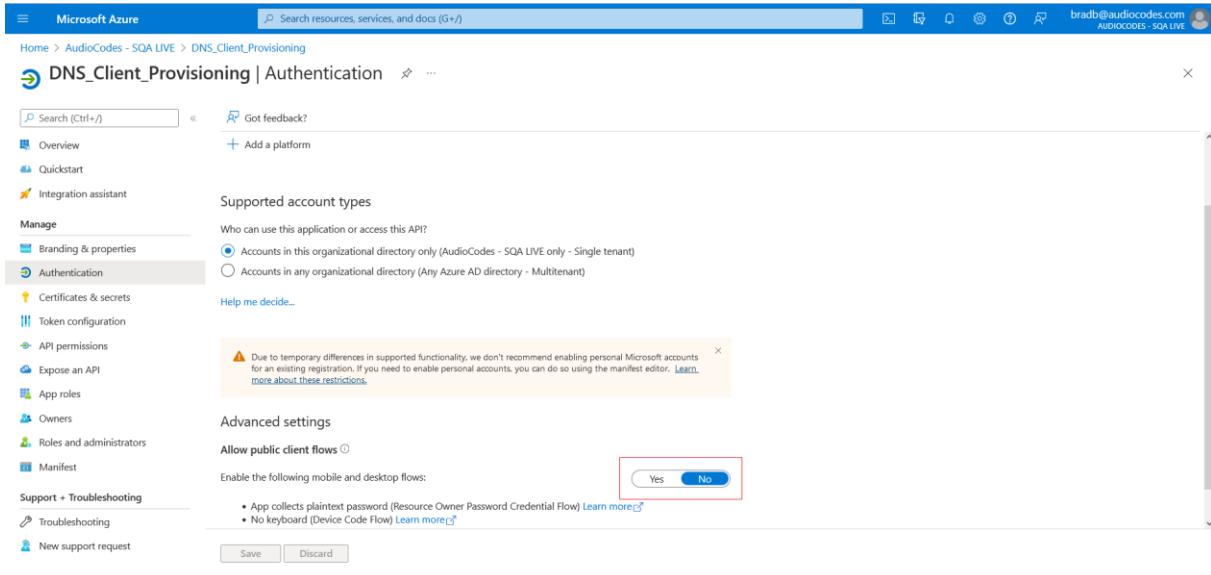
The screenshot shows the Microsoft Azure portal interface for 'AudioCodes - SQA LIVE | App registrations'. The left navigation pane is expanded to 'App registrations'. The main content area shows a list of applications with the following details:

- All applications:**
 - Search filter: `DNS`
 - 1 applications found

Display name ↑↓	Application (client) ID	Created on ↑↓	Certificates & secrets
<code>DNS_Client_Provisioning</code>	<code>bd2e21ca-bd43-49d3-a9c1-ac0519c14e7d</code>	10/13/2021	Current

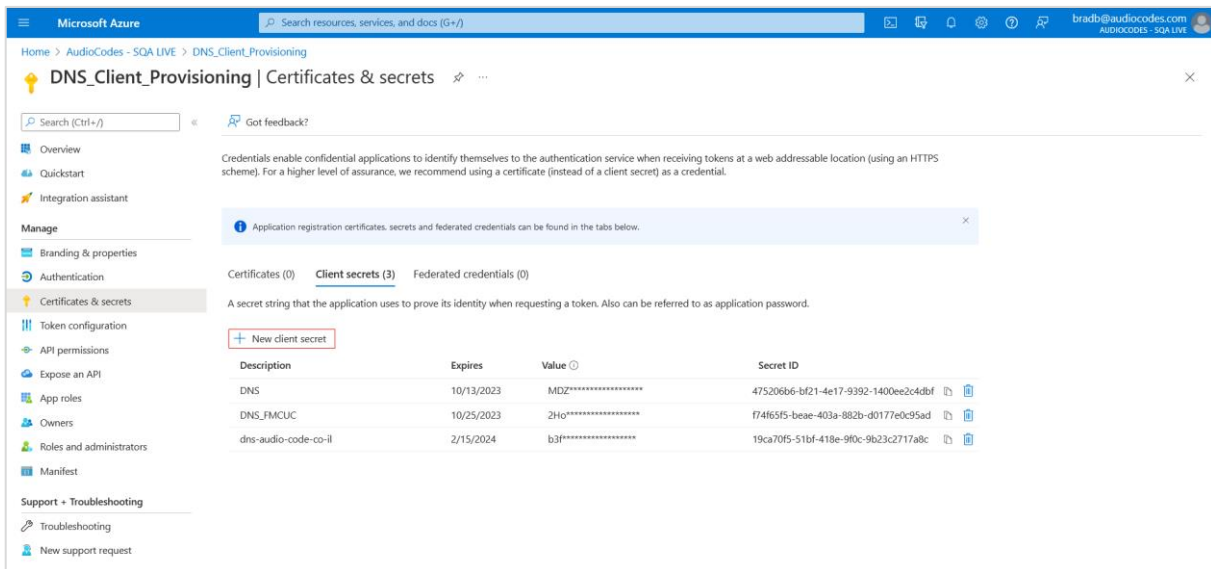
4. Click the new registration (`Dns_Client_Provisioning`) and then in the Navigation pane, select **Authentication**.
5. Under Advanced Settings, select **No** to disable mobile and desktop flows.

Figure 9-5: Advanced Settings



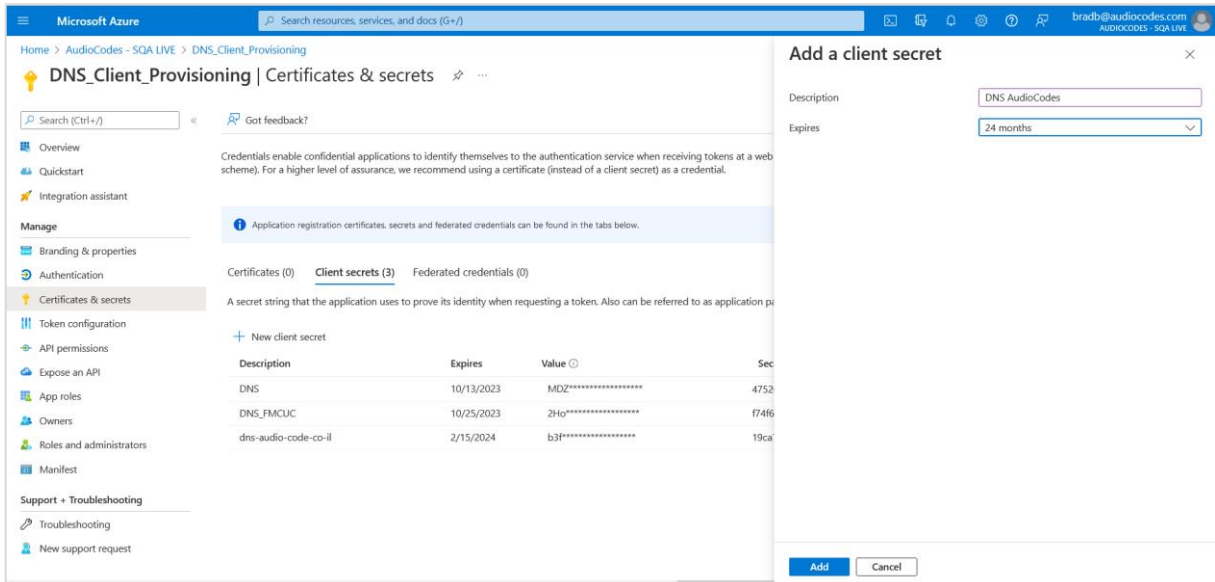
6. Click **Save**.
7. In the Navigation pane, select **Certificate & secrets**.

Figure 9-6: Certificates & secrets



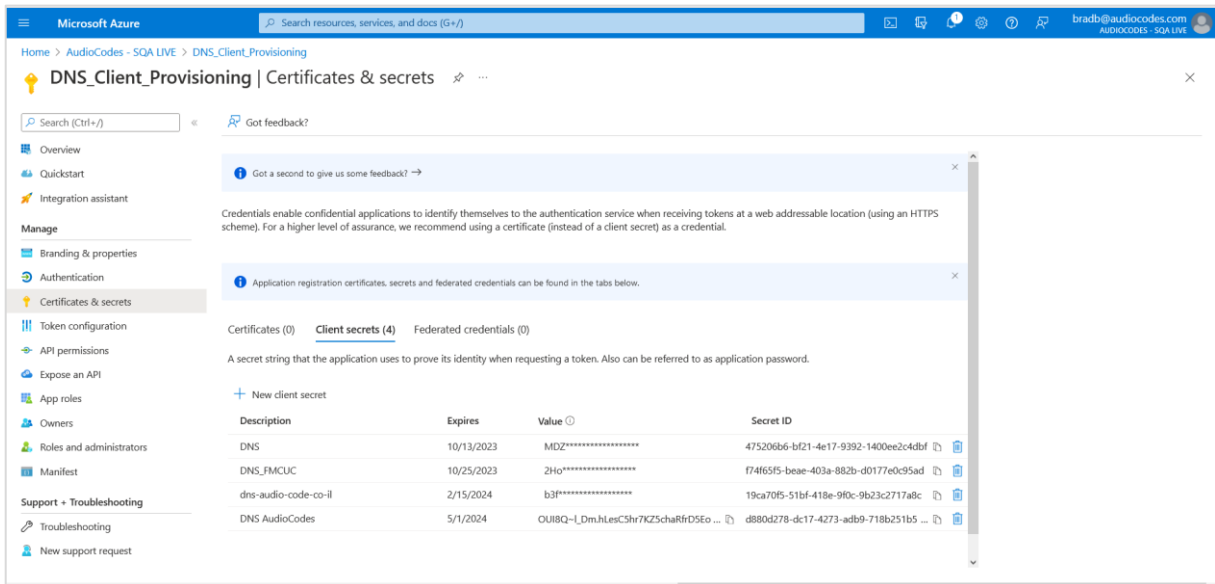
8. Click **New client secret**.

Figure 9-7: New Client Secret



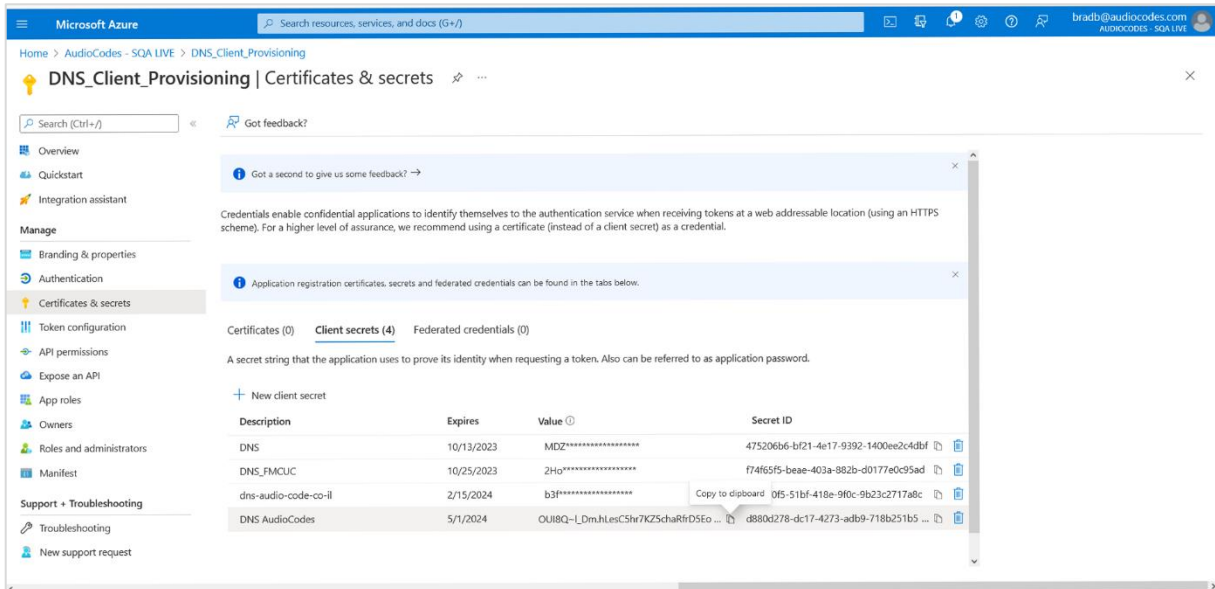
9. Enter a description, Set the Expires field to **24 months** and then click **Add**.

Figure 9-8: Client Secret Added



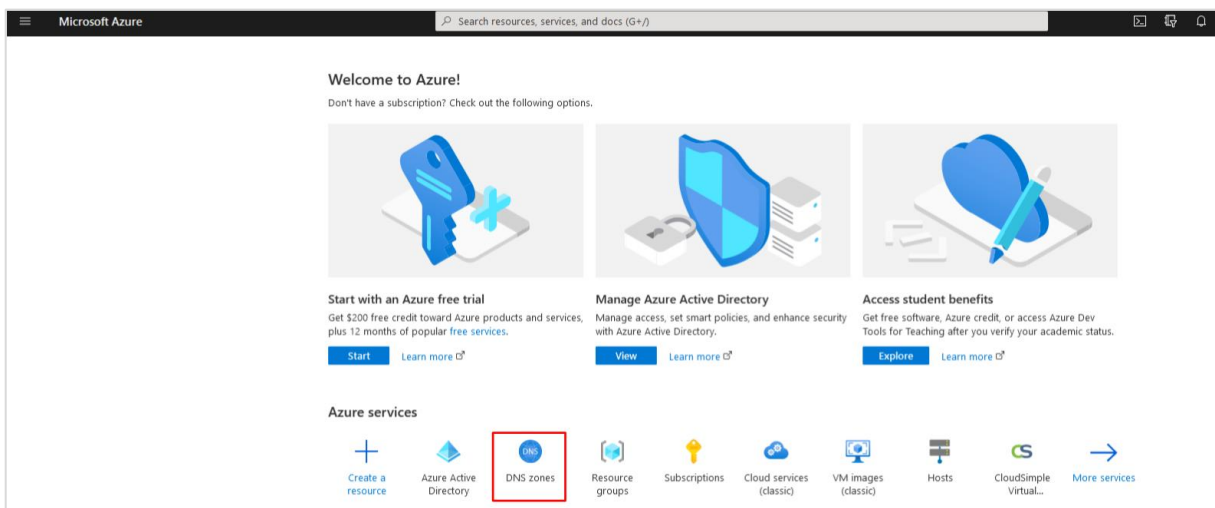
10. Copy the Value to notepad as it must later be configured in the UMP interface.

Figure 9-9: Copy Secret Value



11. In the Azure Portal Home page pane, select **DNS Zones**.

Figure 9-10: DNS zones



9.1.1.2 Create A Records for Customer Sub Domains

It's necessary to configure the Service Provider domain that is used by its' customers for direct routing registered in Azure DNS, so that it can be configured by the UMP.

An A record should be created that points to the SBC site location FQDN. For example:

- EMEA SBC = emeasbc.audiocodes.be = IP of EMEA SBC

If the customer wishes to create a site that uses EMEA SBC, an A record similar to the following example should be created: **emeasbc**.audiocodes.co.il

- US SBC = ussbc.audiocodes.be = IP of US SBC

If the customer wishes to create a site that uses US SBC, an A record similar to the following example should be created: **ussbc**.audiocodes.co.il

During the Onboarding process, the TXT record is generated consisting of the SBC Site Name (Customer Shortname) appended to the subdomain name i.e. <shortcustomername>.emeasbc.audiocodes.co.il. For example, EnterpriseA.emeasbc.audiocodes.co.il.

To create an A-record:

1. In the relevant DNS Zone, click **+ Record Set**.

Figure 9-11: Add Record Set

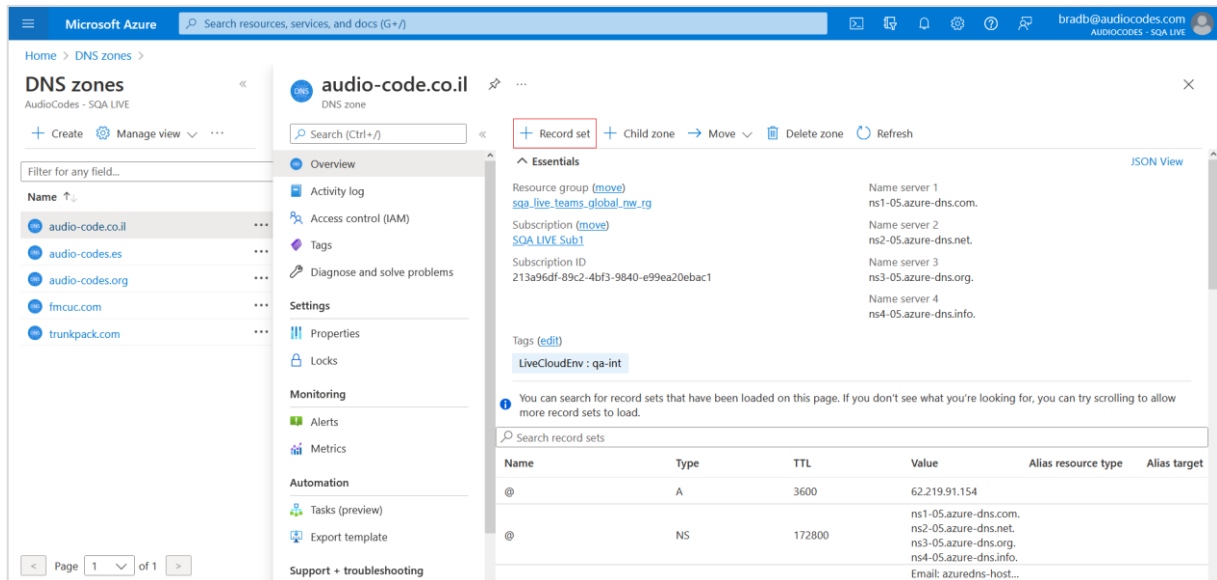


Figure 9-12: Add A Record

Add record set

audio-code.co.il

Name
 .audio-code.co.il

Type

Alias record set Yes No

Alias type
 Azure resource Zone record set

Choose a subscription *

Azure resource *

TTL * TTL unit

OK

2. Add an A-record to translate the site SBC shortname to its' IP address and FQDN:

- Enter the name of the customer subdomain.
- From the Type drop-down list, select **A-Alias record to IPv4 address**.
- Set the Alias record set to **Yes**.
- Set the Alias type to **Azure resource**.
- From the Azure resource field drop-down list, select the relevant SBC device.
- Click **OK**.

The following confirmation prompt is displayed.



The figure below displays the newly added records.

Figure 9-13: Added DNS Records

Name	Type	TTL	Value	Priority	Target
customers	A	3600	-	-	Public IP Address qa-int-sbc1-ip
alogics.customers	A	3600	51.13.97.95	-	-
alogics.customers	TXT	3600	MS=ms27839176	-	-
alogdnsprotest.customers	A	3600	51.13.97.95	-	-
alogdnsprotest.customers	MX	3600	0	10	alogdnsprotest-cus...
alogdnsprotest.customers	TXT	3600	MS=ms73743276 v=spf1 includespf.pr...	-	-
autodiscover.alogdnsprotest.customers	CNAME	3600	autodiscover.outlook...	-	-
alogcs.customers	A	3600	51.13.97.95	-	-
alon.customers	A	3600	51.13.97.95	-	-
audio00codes.customers	A	3600	-	-	Public IP Address qa-int-sbc1-ip
brad.customers	A	3600	51.13.97.95	-	-
m365x950135.customers	A	3600	-	-	Public IP Address qa-int-sbc1-ip
m365x950135.customers	TXT	3600	MS=ms30004690	-	-
ocl.customers	A	3600	-	-	Public IP Address qa-int-sbc1-ip
ocl.customers	MX	3600	0	10	ocl1-customers-audi...

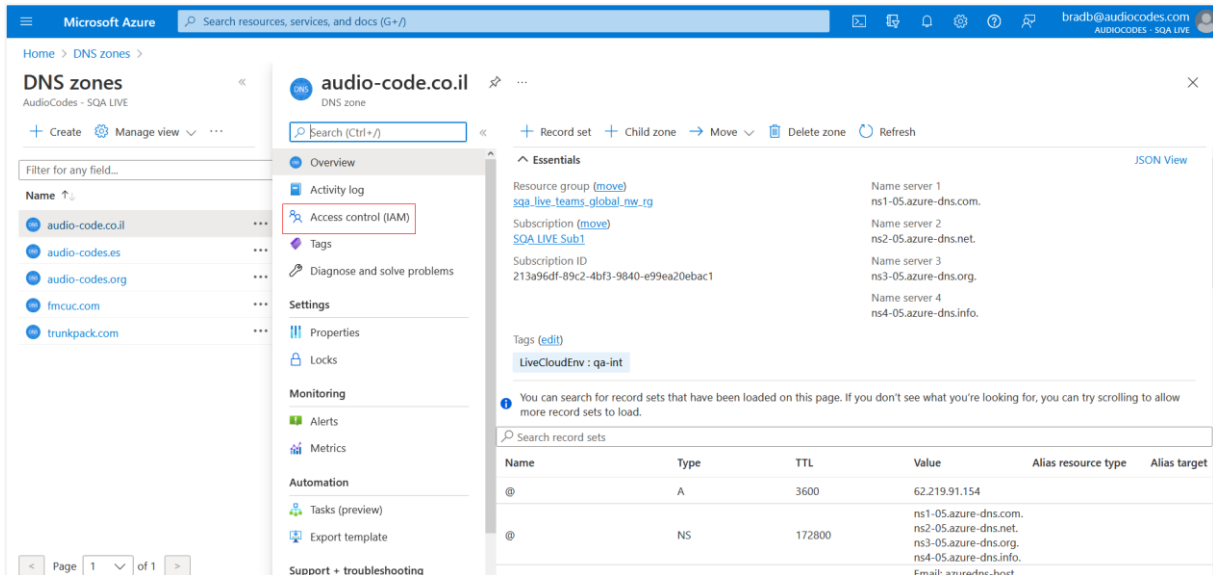
9.1.1.3 Assign Access Control

On the created subdomain, assign access control to the app registration to allow the DNS Application registration (Enterprise Application) to access the DNS zone. In this example, the DNS Application DNS_Client_Provisioning needs access to the subdomain customers.audio-code.co.il. The permission used to authorize this access is "DNS Zone Contributor".

To assign access control:

1. In the DNS zone, select **Access control (IAM)**.

Figure 9-14: Access Control (IAM)



- click Add > Add role assignment.

Figure 9-15: Add Access Control

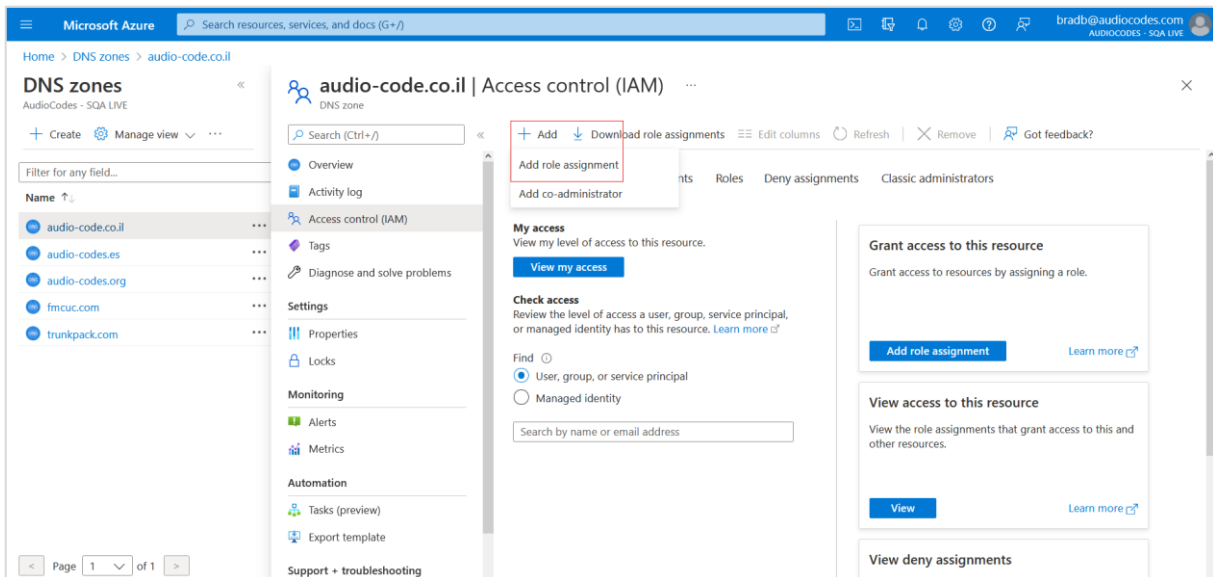
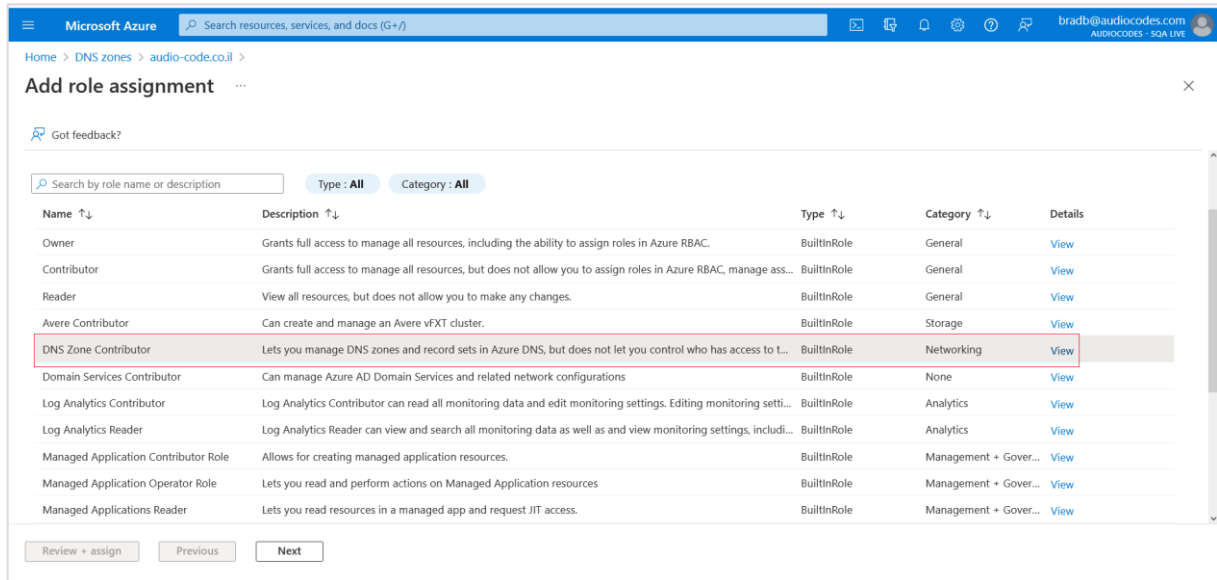
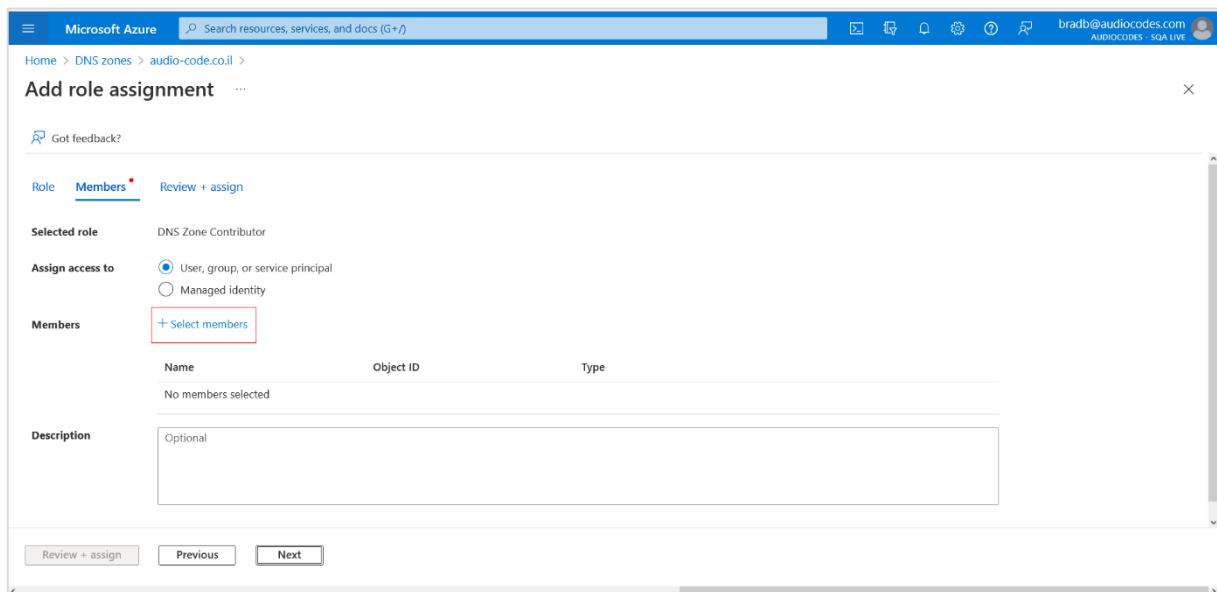


Figure 9-16: DNS Zone Contributor' role



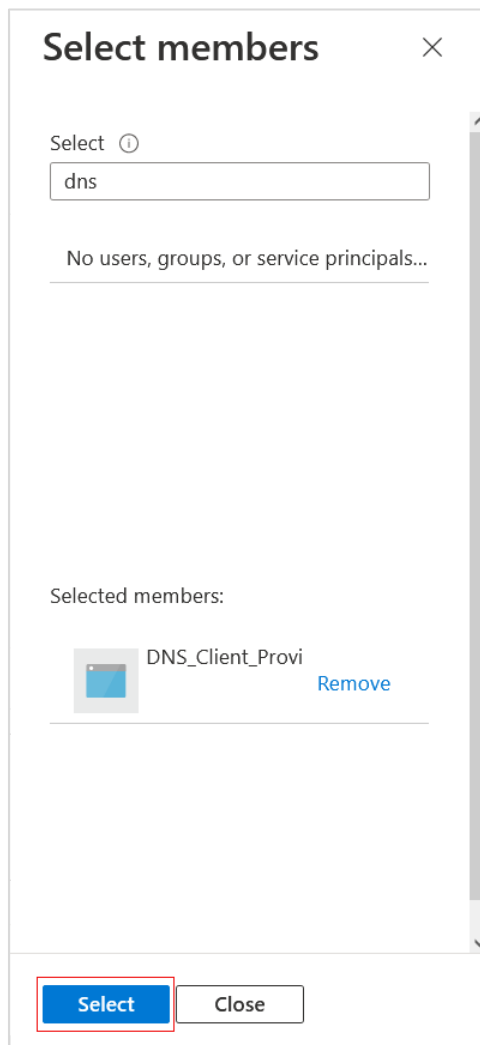
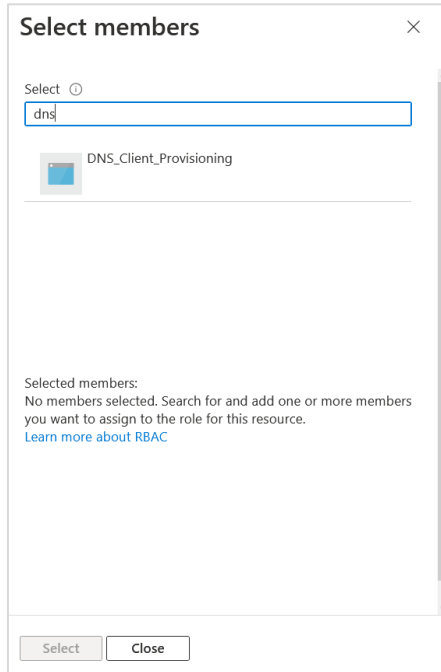
3. Configure the role assignment as shown in the figure below.

Figure 9-17: Add role assignment



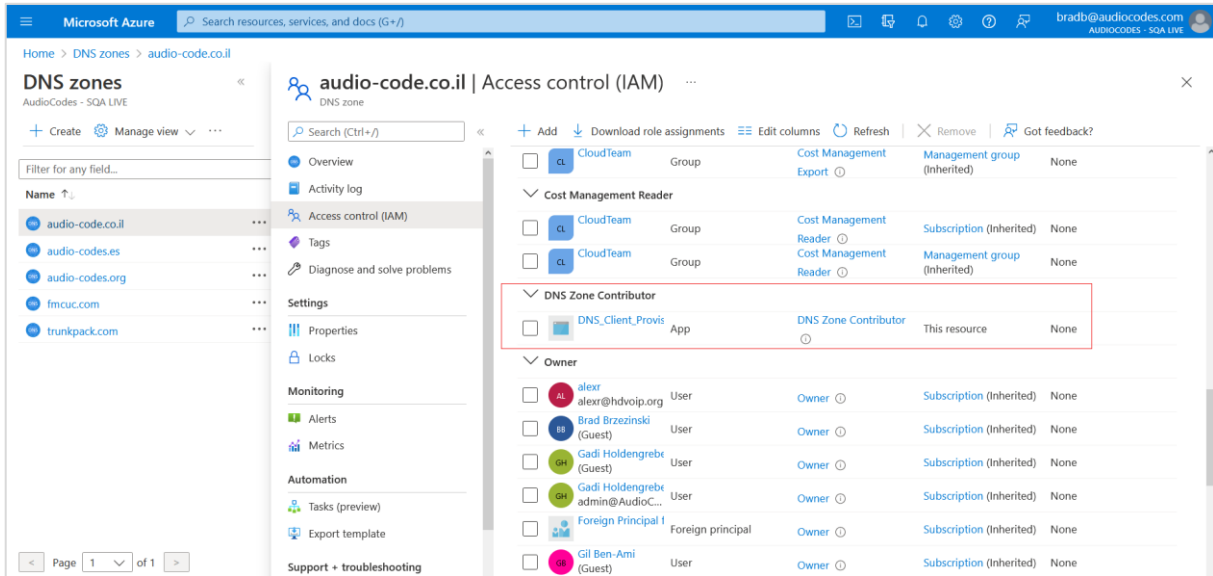
4. Search for the DNS Registration that you created in Section 9.1.1.1 and then click **Select**.

Figure 9-18: Select Members



- Return to the Access Control (IAM) tab. The new DNS Zone Contributor permission is displayed.

Figure 9-19: DNS Zone Contributor Permission Added



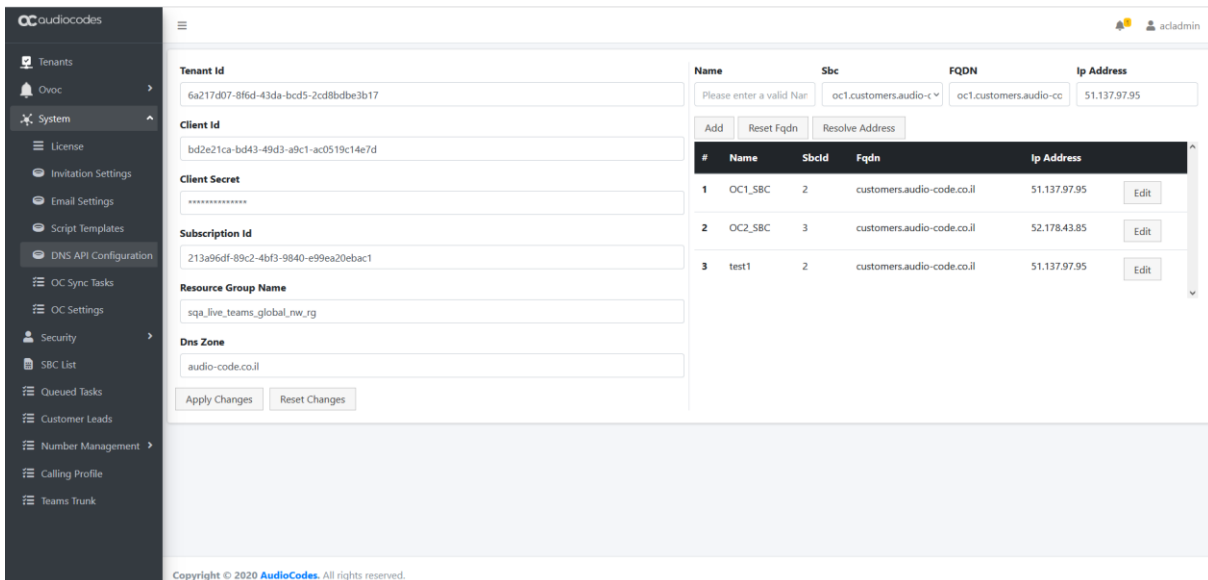
9.1.1.4 Configure DNS API

This section describes how to configure the DNS API after you have completed the Microsoft Azure configuration. This configuration includes the Azure settings based on the configuration in Section 9.1.1.1 and the adding of DNS records for each region site locations based on the configuration in Section 9.1.1.2.

To configure DNS API:

- In the UMP SP Main Tenant Main Page, open the DNS API Configuration screen (**System > DNS API Configuration**).

Figure 9-20: DNS API Configuration- Azure DNS Hosting Platform



2. Configure parameters as described in the table below.

Table 9-1: DNS API Configuration

Parameter	Description
Tenant Id	Directory (tenant) ID for the UMP (extracted from the Overview page in the Azure Portal for registered UMP).
Client Id	Application (Client) id for the UMP (extracted from the Overview page in the Azure Portal for registered UMP).
Client Secret	Client Secret for the UMP (extracted from the Certificates & Secrets page for the registered UMP).
Subscription Id	Azure Subscription Id for the Service Provider account.
Resource Group Name	Resource Group name of the Azure subscription.
Dns Zone	DNS zone of the Azure subscription.

- Client ID is the ID from the Registered App Application (client) ID
- Tenant ID is the Service Provider M365 Tenant ID and can be taken from the App Registration Directory (tenant) ID
- Client Secret is the value taken from the Registered App and only shown during creation

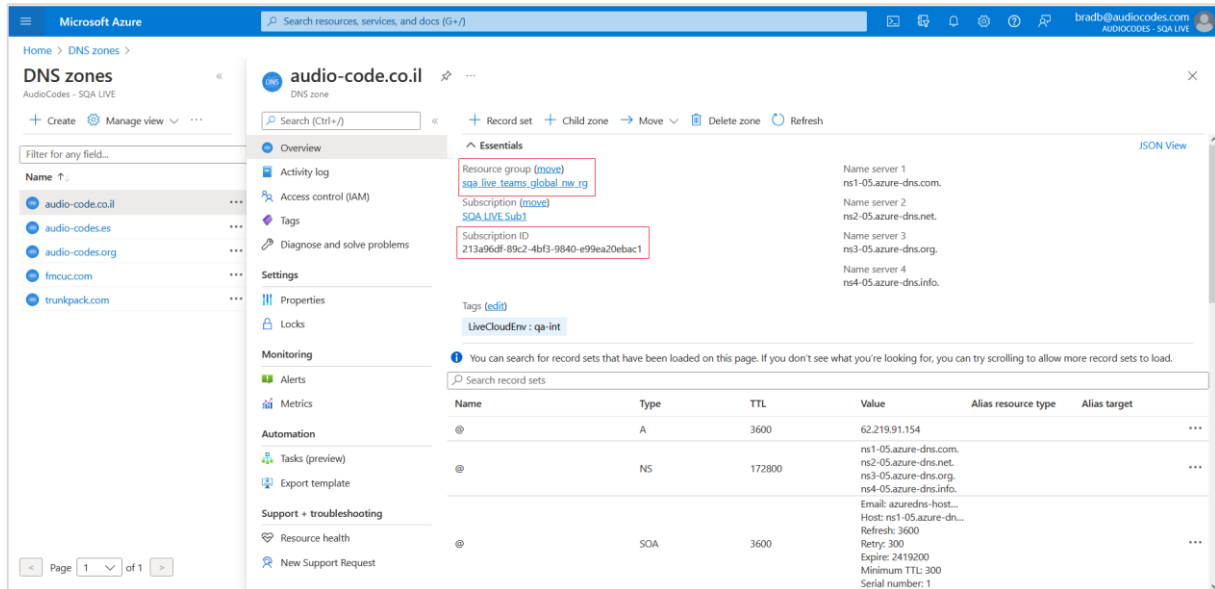
Figure 9-21: Extract IDs

The screenshot shows the Azure portal interface for a registered application. The 'Essentials' section contains the following information:

- Display name: [DNS_Client_Provisioning](#)
- Application (client) ID: [bd2e21ca-bd43-49d3-a9c1-ac0519c14e7d](#)
- Object ID: [e9380a70-765e-4a60-8c36-e882374c0e25](#)
- Directory (tenant) ID: [6a217d07-8f6d-43da-bcd5-2cd9bdbe3b17](#)
- Client credentials: [0 certificate_3.secret](#)
- Redirect URIs: [Add a Redirect URI](#)
- Application ID URI: [Add an Application ID URI](#)
- Managed application in L.: [DNS_Client_Provisioning](#)
- Supported account types: [My organization only](#)

A notification banner at the bottom states: "Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)"

Figure 9-22: DNS zones



- Subscription ID is the Subscription ID taken from the DNS Zone
 - Resource Group Name is the Resource group where the DNS Zone is created
 - DNS Zone is the name of the DNS Zone
3. On the right side of the screen, click **Add** to configure a new DNS subdomain region for the customer:
 - **Name:** Region SBC name. During the Onboarding process, this name is appended to the subdomain name (FQDN below) to form the TXT record. For example 'oc1_sbc.customers.audio-code.co.il'. In the Onboarding wizard DNS setup, this entry appears as in the Regions drop-down list (see Section 9.1.20 below).
 - **Sbclid:** Id of the SBC device in the SQL database.
 - **Fqdn:** A-Record added for the region SBC in Section 9.1.1.2.
 - **IP Address:** IP address of the region SBC device.

Figure 9-23: DNS Regions Table

Name	Sbc	FQDN	Ip Address		
<input type="text" value="Please enter a valid Name"/>	<input type="text" value="oc1.customers.audio-code.⌵"/>	<input type="text" value="oc1.customers.audio-code.cc"/>	<input type="text" value="51.137.97.95"/>		
<input type="button" value="Add"/>	<input type="button" value="Reset Fqdn"/>	<input type="button" value="Resolve Address"/>			
#	Name	Sbclid	Fqdn	Ip Address	
1	OC1_SBC	2	customers.audio-code.co.il	51.137.97.95	<input type="button" value="Edit"/>
2	OC2_SBC	3	customers.audio-code.co.il	52.178.43.85	<input type="button" value="Edit"/>
3	test1	2	customers.audio-code.co.il	51.137.97.95	<input type="button" value="Edit"/>

Another example below shows two different DNS regions configured, one for region APAC “customers.audiocodes.be” and one for EMEA “customerslatam.audiocodes.be”.

Figure 9-24: DNS Subdomain Mapping

The screenshot shows the AudioCodes management console interface for DNS Subdomain Mapping. On the left, there is a navigation sidebar with options: Tenants, Ovoc, System, License, Invitation Settings, Email Settings, Script Templates, DNS API Configuration, Security, SBC List, and Queued Tasks. The main configuration area is split into two columns. The left column contains input fields for: Tenant Id (1911c65c-893b-42f9-83fa-66c1b86fd85), Client Id (f57a202d-ec0b-4fd7-8de5-b412b20b6907), Client Secret (masked with asterisks), Subscription Id (c1d216b3-fc1c-4578-a97c-81e101dde515), Resource Group Name (audiocodesbe), and Dns Zone (audiocodes.be). Below these fields are 'Apply Changes' and 'Reset Changes' buttons. The right column features a table for mapping subdomains to SBC devices. At the top, there are input fields for Name (with a placeholder 'Please enter a valid Name'), Sbc (51.124.68.108_SBC), FQDN (customers.audiocodes.t), and Ip Address (13.80.148.30). Below these are 'Add', 'Reset Fqdn', and 'Resolve Address' buttons. The table below has columns: #, Name, SbcId, Fqdn, Ip Address, and an Edit button. It contains two rows: Row 11: APAC, 1, customers.audiocodes.be, 13.80.148.30; Row 12: EMEA, 2, customerslatam.audiocodes.be, 23.97.197.41. The bottom of the page shows 'Activate Windows' and 'Go to Settings to activate Windows' text.

Table 9-2: DNS Subdomain Mapping

Parameter	Description
Name	The name of the managed SBC device.
SBCID	The ID of the SBC device.
FQDN	The FQDN of the SBC device.
IP Address	The IP address of the SBC device.

9.1.2 Provisioning

This section describes how to automatically create the DNS record using the Onboarding wizard.

To create the subdomain:


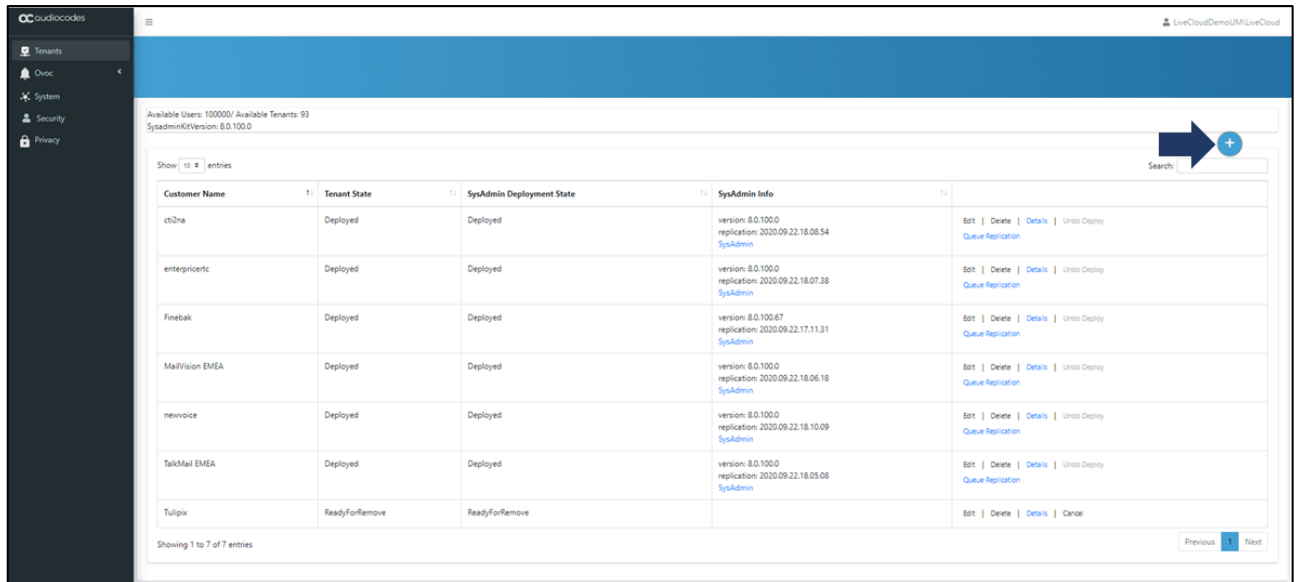
1. From the Main Provider Dashboard / Tenant view, select **Actions** .

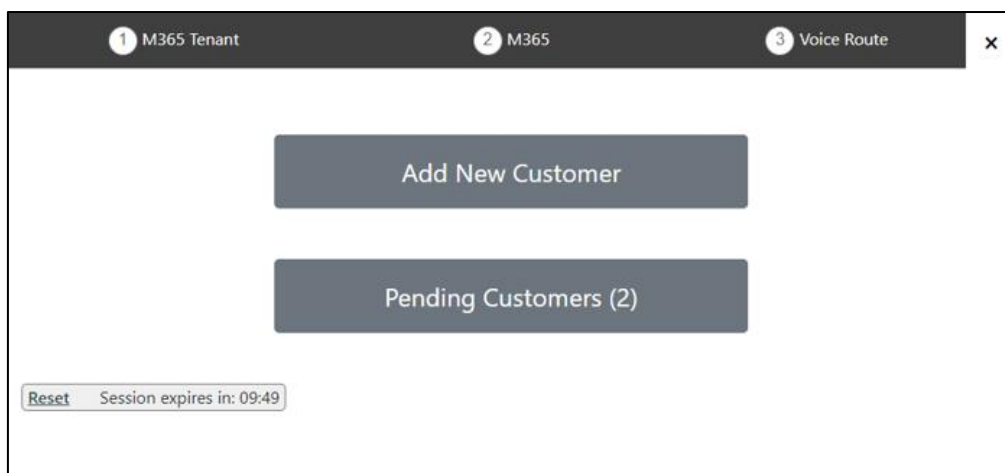
Figure 9-25: M365 Tenants



Customer Name	Tenant State	SysAdmin Deployment State	SysAdmin Info	
ct2na	Deployed	Deployed	version: 8.0.100.0 replication: 2020-09-22:18:08:54 SysAdmin	Edit Delete Details Undo Deploy Queue Replication
enterpricctc	Deployed	Deployed	version: 8.0.100.0 replication: 2020-09-22:18:07:38 SysAdmin	Edit Delete Details Undo Deploy Queue Replication
Finebak	Deployed	Deployed	version: 8.0.100.0 replication: 2020-09-22:17:11:31 SysAdmin	Edit Delete Details Undo Deploy Queue Replication
MailVision EMEA	Deployed	Deployed	version: 8.0.100.0 replication: 2020-09-22:18:06:18 SysAdmin	Edit Delete Details Undo Deploy Queue Replication
newvoice	Deployed	Deployed	version: 8.0.100.0 replication: 2020-09-22:18:10:09 SysAdmin	Edit Delete Details Undo Deploy Queue Replication
TalkMail EMEA	Deployed	Deployed	version: 8.0.100.0 replication: 2020-09-22:18:05:08 SysAdmin	Edit Delete Details Undo Deploy Queue Replication
Tulpix	ReadyForRemove	ReadyForRemove		Edit Delete Details Cancel

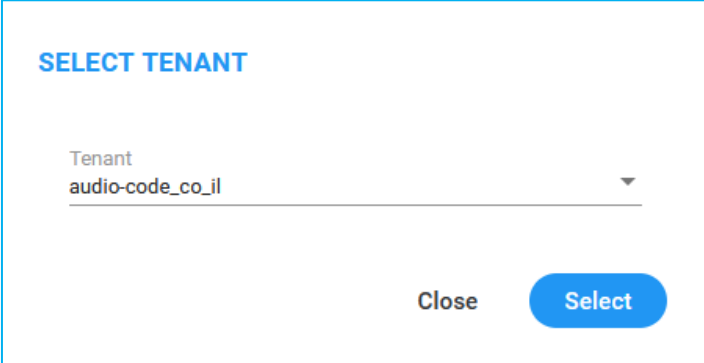
The Onboarding interface opens.

Figure 9-26: Add New Customer



2. Click **Add New Customer**.
3. Select the tenant of the new customer.

Figure 9-27: Select Tenant

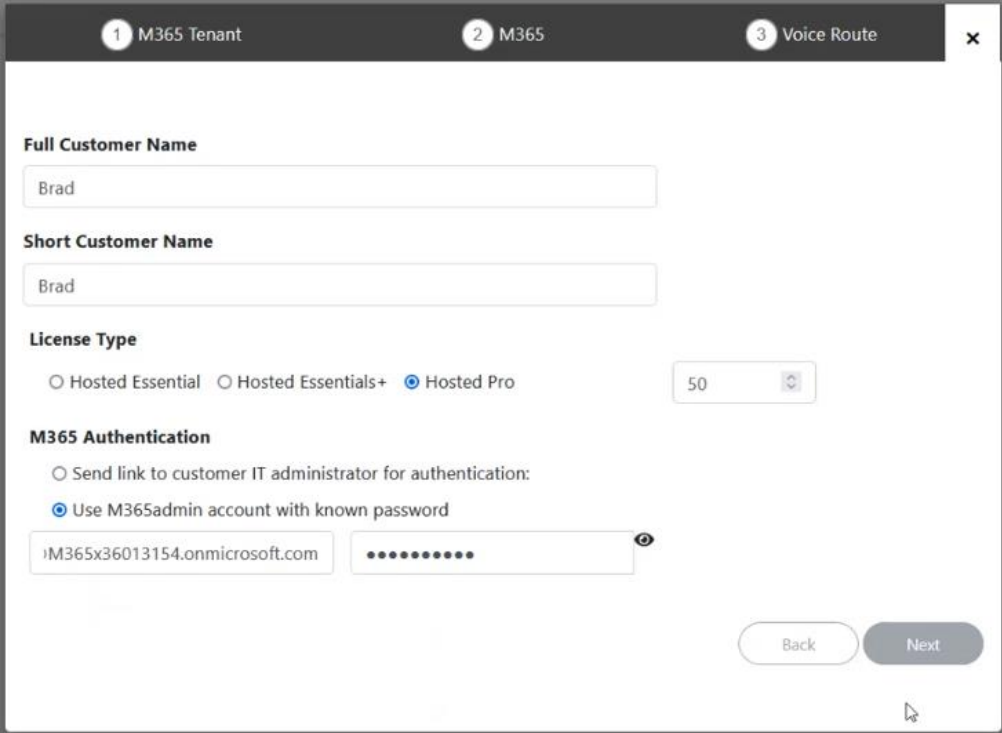


SELECT TENANT

Tenant
audio-code_co_il

Close Select

Figure 9-28: New Customer



1 M365 Tenant 2 M365 3 Voice Route

Full Customer Name
Brad

Short Customer Name
Brad

License Type
 Hosted Essential Hosted Essentials+ Hosted Pro 50

M365 Authentication
 Send link to customer IT administrator for authentication:
 Use M365admin account with known password
M365x36013154.onmicrosoft.com

Back Next

4. Enter the Full Customer Name and the Short Customer Name (this name will be used to identify the site SBC).
5. Select either the Hosted Essentials+ or Hosted Pro License Types.
6. Enter the number of user licenses required.
7. Enter the M365admin account credentials or send a token link to the administrator (see Section 30.5).

Figure 9-29: Validating Credentials

1 M365 Tenant 2 M365 3 Voice Route

Validating credentials, please wait! On succesfull authentication the wizard will continue.

Back Next

Figure 9-30: DNS Provisioning

1 M365 Tenant 2 M365 3 Voice Route

Region/Country
OC1_SBC

Ip Address
51.137.97.95

Sbc
oc1.customers.audio-code.co.il [51.137.97.95]

Domain Name
customers.audio-code.co.il

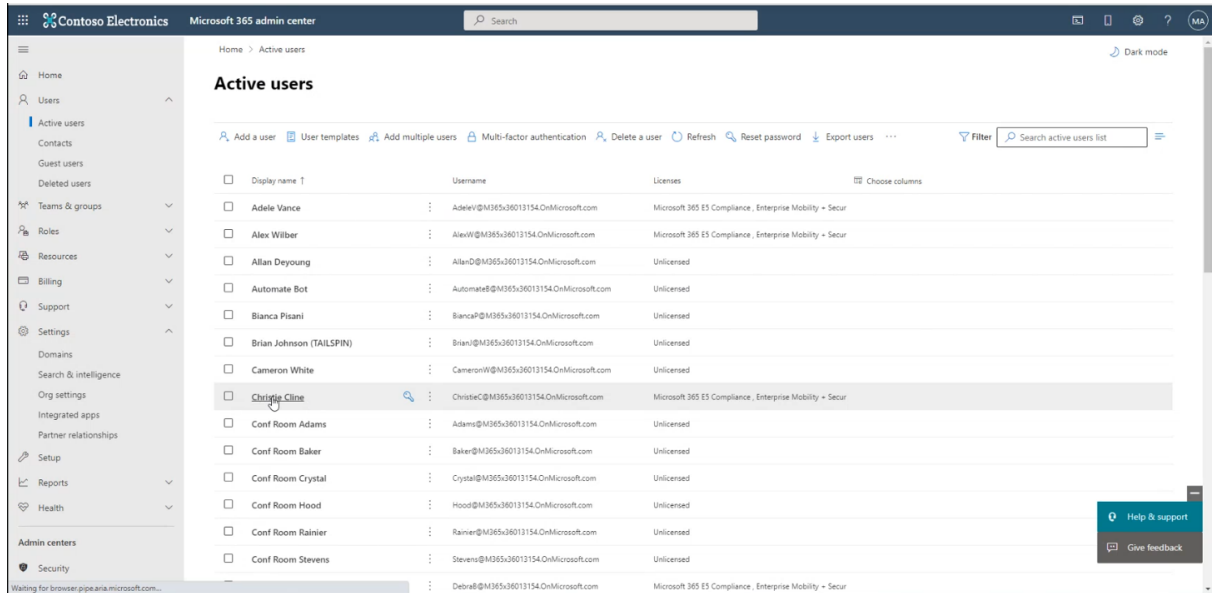
Sbc Site Name Note: You won't be able to change the sbc site name after adding the PSTN Gateway!
Brad

License Plan
No License Plan Available! Make sure to free the license(s) for a plan and reload

Back Next

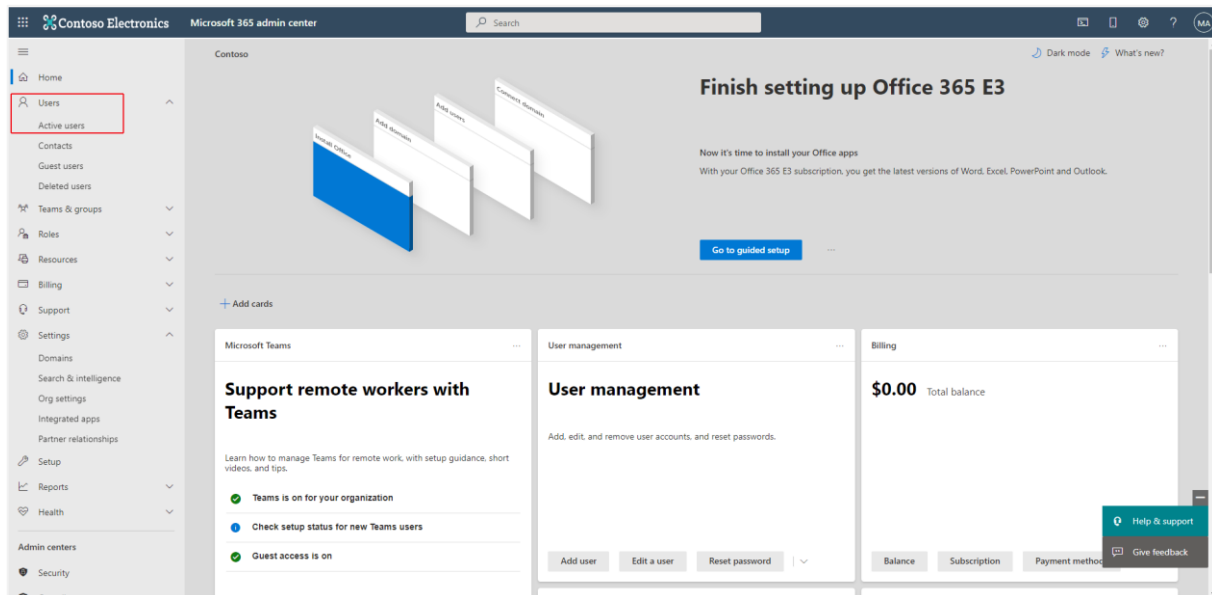
8. From the Region/Country drop-down list, select the relevant region of the customer site SBC.

Figure 9-31: Active users



9. Open the **Microsoft 365 admin center** for the customer tenant.
10. In the Navigation pane, select **Users > Active users**.

Figure 9-32: Active Users



11. Select any licensed user.

Figure 9-33: Select User

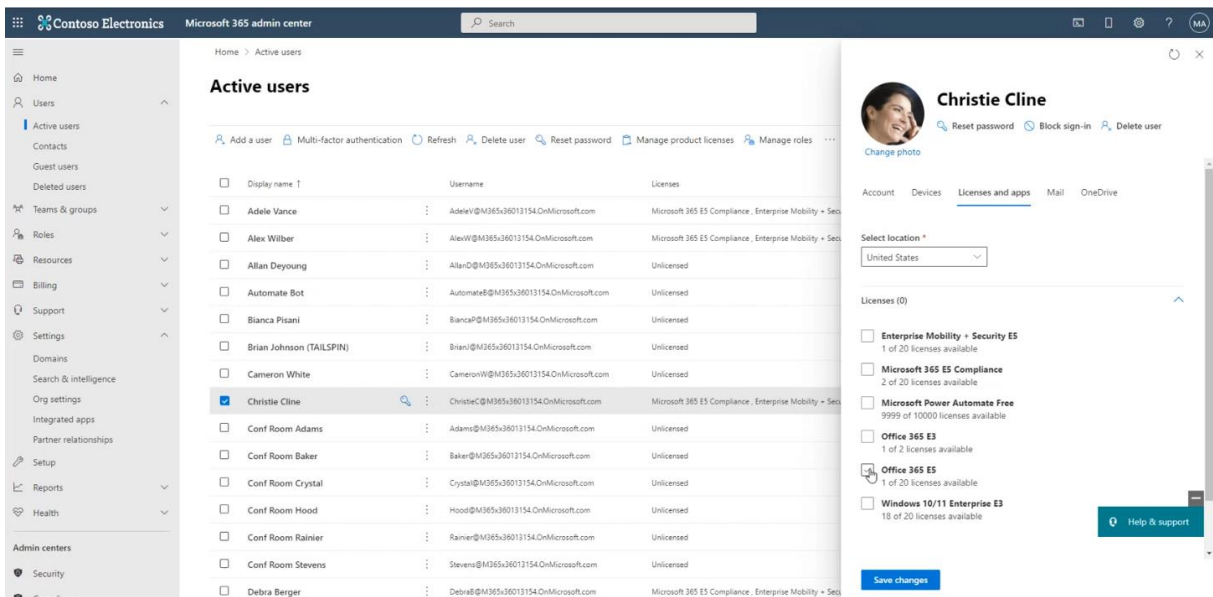
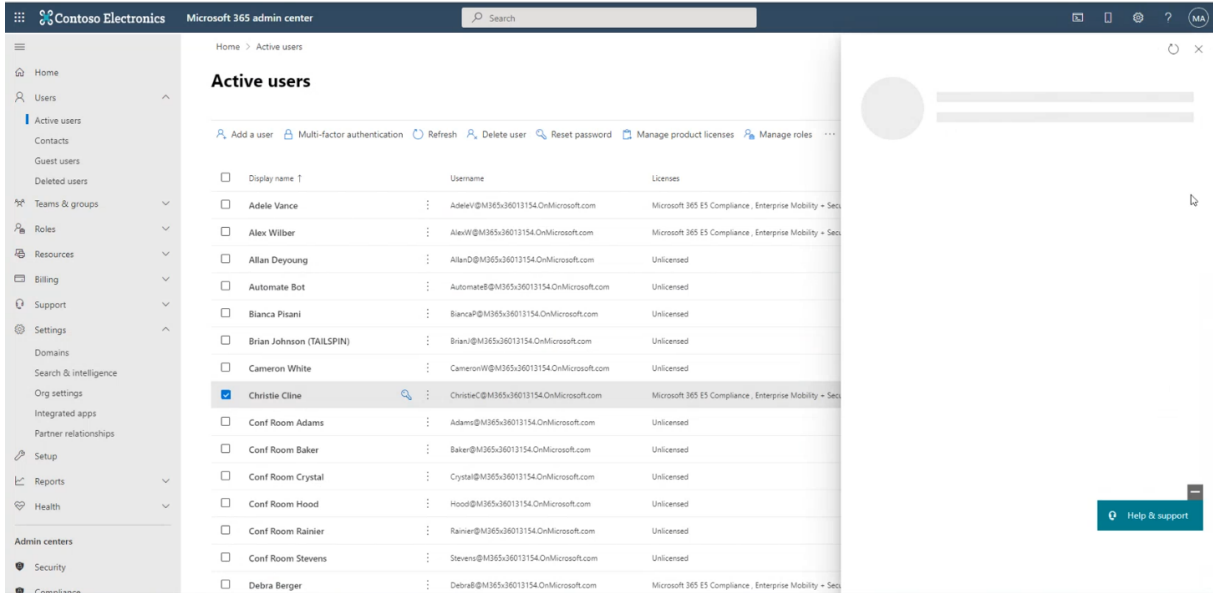


Figure 9-34: Disable License

The screenshot shows the Microsoft 365 Admin Center interface. On the left is a navigation pane with options like Home, Users, Active users, Contacts, Guest users, Deleted users, Teams & groups, Roles, Resources, Billing, Support, Settings, Domains, Search & intelligence, Org settings, Integrated apps, Partner relationships, Setup, Reports, Health, Admin centers, and Security. The main area is titled 'Active users' and contains a table of users. The user 'Christie Cline' is selected. To the right of the table is a profile card for 'Christie Cline' with options to 'Reset password', 'Block sign-in', and 'Delete user'. Below the profile card is a 'Licenses and apps' section with a 'Save changes' button. A green notification bar at the top of the license section says 'Your changes have been saved.'

Display name	Username	Licenses
Adele Vance	AdeleV@M365x36013154.OnMicrosoft.com	Microsoft 365 E5 Compliance, Enterprise Mobility + Sec
Alex Wilber	AlexW@M365x36013154.OnMicrosoft.com	Microsoft 365 E5 Compliance, Enterprise Mobility + Sec
Allan Deyoung	AllanD@M365x36013154.OnMicrosoft.com	Unlicensed
Automate Bot	AutomateB@M365x36013154.OnMicrosoft.com	Unlicensed
Bianca Pisani	BiancaP@M365x36013154.OnMicrosoft.com	Unlicensed
Brian Johnson (TAILSPIN)	BrianJ@M365x36013154.OnMicrosoft.com	Unlicensed
Cameron White	CameronW@M365x36013154.OnMicrosoft.com	Unlicensed
Christie Cline	ChristieC@M365x36013154.OnMicrosoft.com	Unlicensed
Conf Room Adams	Adams@M365x36013154.OnMicrosoft.com	Unlicensed
Conf Room Baker	Baker@M365x36013154.OnMicrosoft.com	Unlicensed
Conf Room Crystal	Crystal@M365x36013154.OnMicrosoft.com	Unlicensed
Conf Room Hood	Hood@M365x36013154.OnMicrosoft.com	Unlicensed
Conf Room Rainier	Rainier@M365x36013154.OnMicrosoft.com	Unlicensed
Conf Room Stevens	Stevens@M365x36013154.OnMicrosoft.com	Unlicensed
Debra Berger	DebraB@M365x36013154.OnMicrosoft.com	Microsoft 365 E5 Compliance, Enterprise Mobility + Sec

12. Deselect the licenses that are currently enabled for the user, and then save the changes.



The following licenses can be made available:

- E1 with Phone System
- E3 with Phone System
- Office 365 E5

Figure 9-35: Reload License Plan

1 M365 Tenant 2 M365 3 Voice Route

Region/Country
OC1_SBC

Ip Address
51.137.97.95

Sbc
oc1.customers.audio-code.co.il [51.137.97.95]

Domain Name
customers.audio-code.co.il

Sbc Site Name Note: You won't be able to change the sbc site name after adding the PSTN Gateway!
Brad

License Plan
[Empty] Reload

No License Plan Available! Make sure to free the license(s) for a plan and reload

Back Next

13. Click the **Reload** button to reload the license plan for the customer. The system is refreshed and searches for an available license for the tenant. The license plan is loaded. In the figure below, the OFFICE 365 E5 license is loaded.

Figure 9-36: License Plan Loaded

1 M365 Tenant 2 M365 3 Voice Route

Region/Country
OC1_SBC

Ip Address
51.137.97.95

Sbc
oc1.customers.audio-code.co.il [51.137.97.95]

Domain Name
customers.audio-code.co.il

Sbc Site Name Note: You won't be able to change the sbc site name after adding the PSTN Gateway!
Brad

License Plan
OFFICE 365 E5 Reload

Back Next

The new tenant is added.

Figure 9-37: New Tenant Added

1 M365 Tenant 2 M365 3 Voice Route

Processing Add New Pstn Gateway...

-- CreatePstnGateway task started --

-- Getting configuration... --

-- Tenant Manager Configured --

Back

During the script processing, the TXT record is created, the domain is created, then the TXT record is deleted and the A-record is created, and then at the end of the process a user is created with an OFFICE 365 E5 license.

Figure 9-38: Domain Created

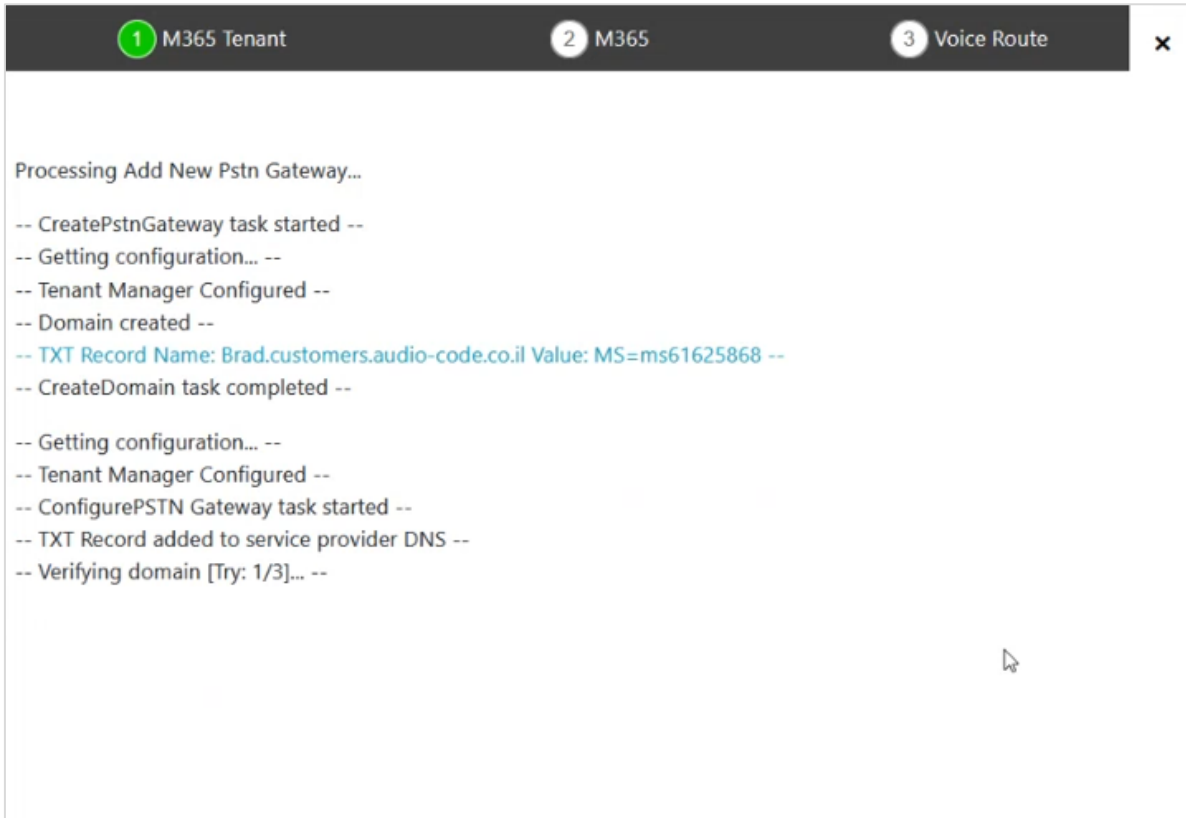


Figure 9-39: A-Record Created

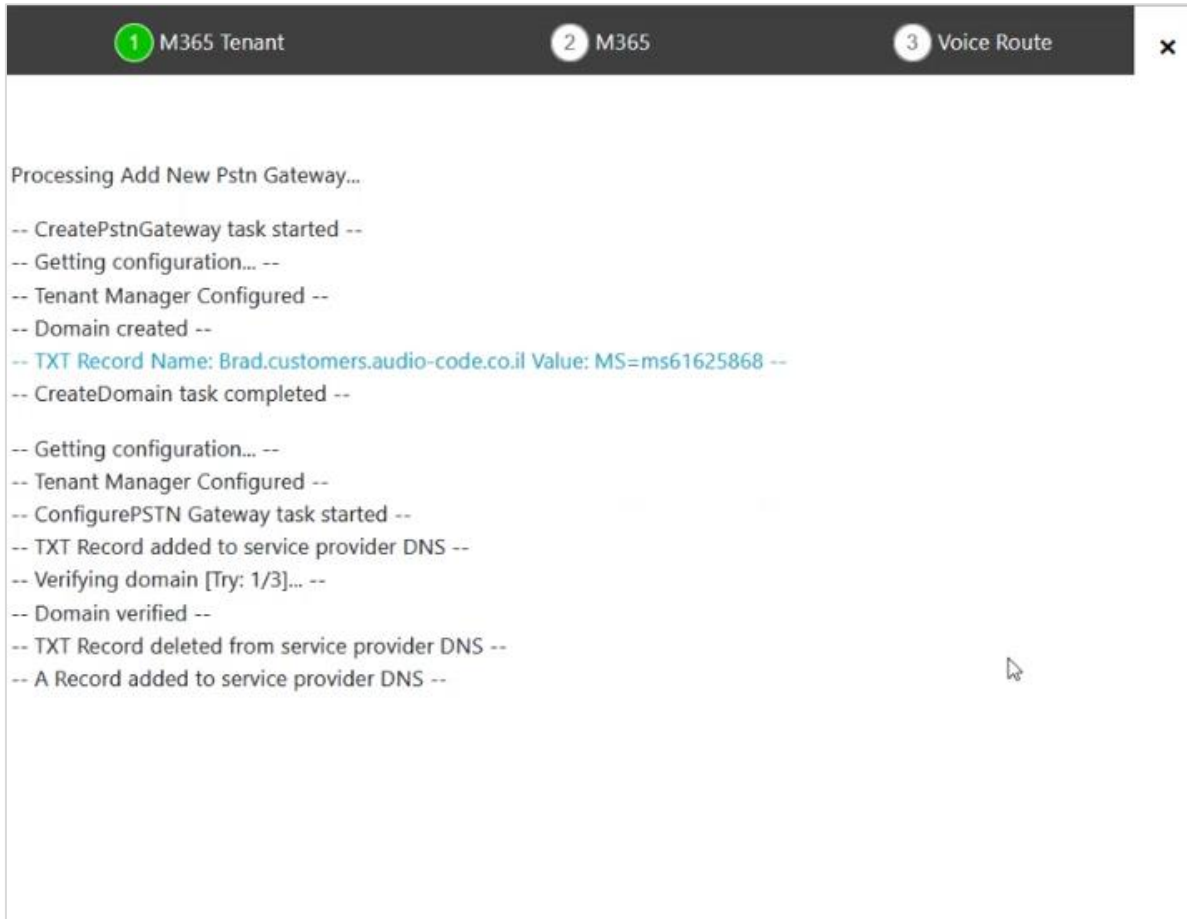
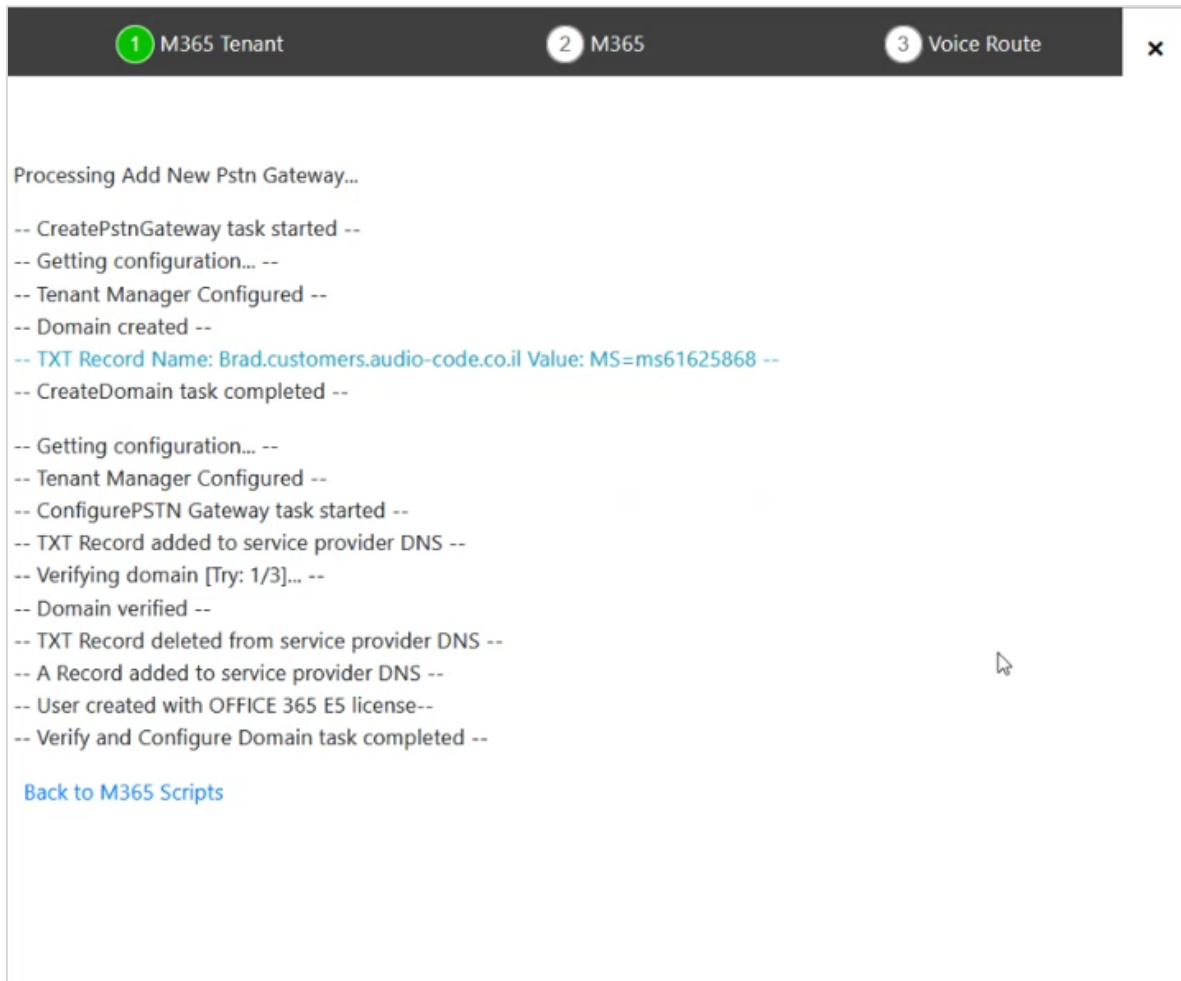


Figure 9-40: User Created



The newly created domain is displayed under Online PSTN Gateway drop-down list.

Figure 9-41: Online PSTN Gateway

1 M365 Tenant **2** M365 **3** Voice Route

Configure M365 default routing

Click [[Here](#)] to Provision M365 Domain and DNS Automatically

Online PSTN Gateway Brad.customers.audio-code.co.il

M365 Onboarding Script O365_PAI

M365 Cleanup Script Default Script

Customer Variables	Value
--------------------	-------

Back Next

14. Complete the Onboarding wizard as described in Section 30.2.1.

9.2 Two-step Provisioning

This procedure describes how to add the new customer subdomain in a partial automation process where during the Onboarding wizard run, the customer is prompted to generate the TXT and A-Record. Once created, the script creates the subdomain and adds it under the Custom domains on Azure.

9.2.1 Before Provisioning

Before proceeding, ensure that you have chosen a subdomain on your DNS hosting platform and added the entry to the DNS subdomain Mapping table as described in Section 9.1.1.1.

Do the following:

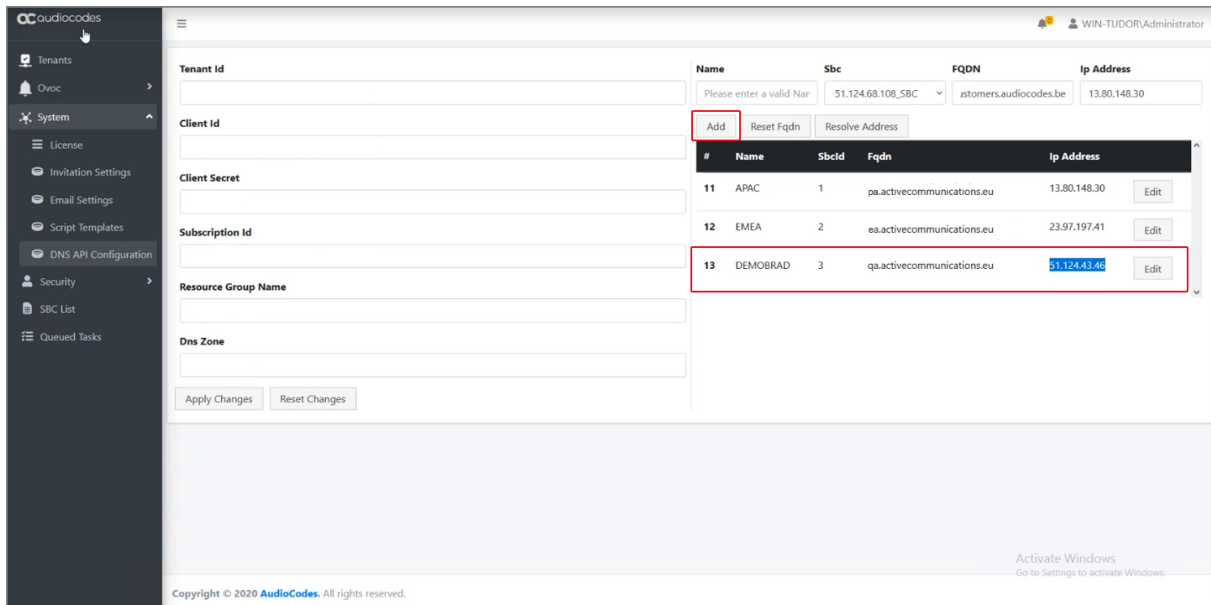
1. Open your custom DNS hosting platform and chose the desired subdomain.

Figure 9-42: Custom DNS Zone

Record Name	Type	Value	TTL	Actions
NL-QA-UMP-221.activecommunications.eu	A	20.93.133.186	14400	✕
officewebapps.activecommunications.eu	A	84.53.66.60	86400	✕
ProTokenCus11.activecommunications.eu	A	23.97.197.54	14400	✕
a.activecommunications.eu	A	51.124.43.46	14400	✕
sbc-tobi.activecommunications.eu	A	40.91.233.177	14400	✕
sip.activecommunications.eu	A	84.53.66.61	86400	✕
ump-access.activecommunications.eu	A	51.138.73.35	14400	✕
ump-walter.activecommunications.eu	A	52.178.102.123	14400	✕
wac.activecommunications.eu	A	84.53.66.60	86400	✕
autodiscover.activecommunications.eu	CNAME	autodiscover.outlook.com	86400	✕
transfer.activecommunications.eu	CNAME	acs-transfer.azureedge.net	3600	✕
ump-tobi.activecommunications.eu	CNAME	ump-tobi.westeurope.cloudapp.azure.com	14400	✕
www.activecommunications.eu	CNAME	www.audiocodes.com	86400	✕
activecommunications.eu	MX	100 2007.activecommunications.eu	86400	✕
activecommunications.eu	MX	50 activecommunications-eu.mail.protection.outlook.com	86400	✕

2. In the UMP SP Main Tenant Main Page, open the DNS API Configuration screen (**System > DNS API Configuration**).

Figure 9-43: DNS API Configuration- Custom DNS Hosting Platform



3. On the right side of the screen, click **Add** to create a new DNS subdomain for the customer with the following values:
 - Desired region name, for example APAC or EMEA
 - The domain name which may represent a specific region for a customer. For example, in the screen below, the domain for activecommunications.eu has three subdomains defined, one for region EMEA which is represented by **ea**.activecommunications.eu, one for the APAC region with **pa**.activecommunications.eu and a test region DEMOBRAD with **qa**.activecommunications.eu.
 - IP address of the SBC device used to manage SBC calls in the region

Table 9-3: DNS Subdomains Mapping Table

Parameter	Description
Name	The name of the managed SBC device.
SBCID	The ID of the SBC device.
FQDN	The FQDN of the SBC device.
IP Address	The IP address of the SBC device.

9.2.2 Provisioning

This procedure describes how to run the Onboarding Wizard to provision a DNS subdomain using the two-step method.

Do the following:


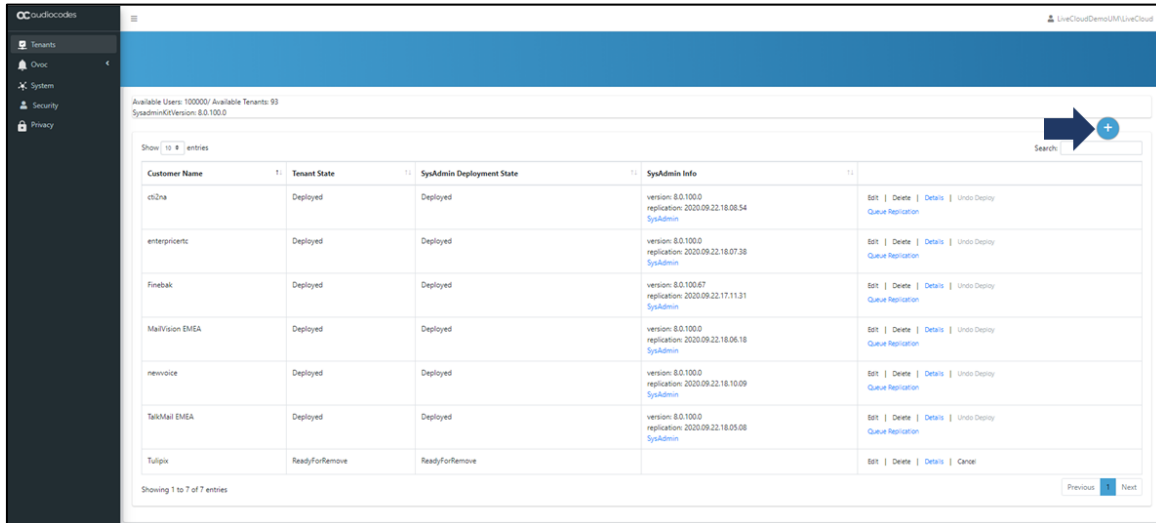
1. From the Main Provider Dashboard / Tenant view, select **Actions** .

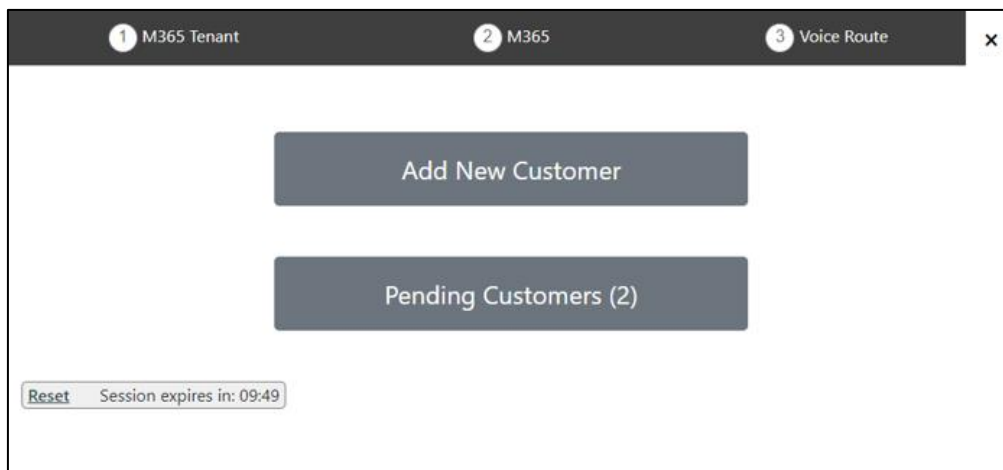
Figure 9-44: M365 Tenants



Customer Name	Tenant State	SysAdmin Deployment State	SysAdmin Info	
ct2na	Deployed	Deployed	version: 8.0.100.0 replication: 2020.09.22.18.08.54 SysAdmin	Edit Delete Details Undo Deploy Queue Replication
enterpricent	Deployed	Deployed	version: 8.0.100.0 replication: 2020.09.22.18.07.38 SysAdmin	Edit Delete Details Undo Deploy Queue Replication
Finbak	Deployed	Deployed	version: 8.0.100.67 replication: 2020.09.22.17.11.31 SysAdmin	Edit Delete Details Undo Deploy Queue Replication
MailVision EMEA	Deployed	Deployed	version: 8.0.100.0 replication: 2020.09.22.18.06.18 SysAdmin	Edit Delete Details Undo Deploy Queue Replication
neinvoice	Deployed	Deployed	version: 8.0.100.0 replication: 2020.09.22.18.10.09 SysAdmin	Edit Delete Details Undo Deploy Queue Replication
TalkMail EMEA	Deployed	Deployed	version: 8.0.100.0 replication: 2020.09.22.18.05.08 SysAdmin	Edit Delete Details Undo Deploy Queue Replication
Tulpix	ReadyForRemove	ReadyForRemove		Edit Delete Details Cancel

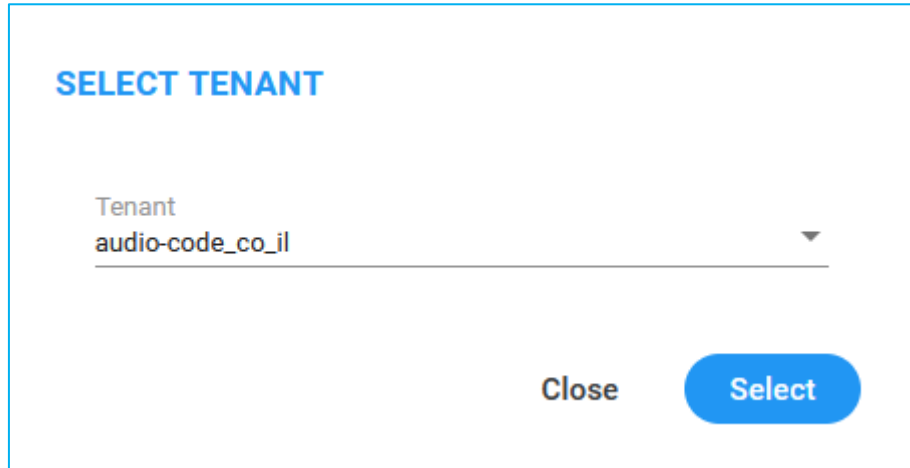
The Onboarding interface opens.

Figure 9-45: Add New Customer



2. Click **Add New Customer**.
3. Select the tenant of the new customer.

Figure 9-46: Select Tenant

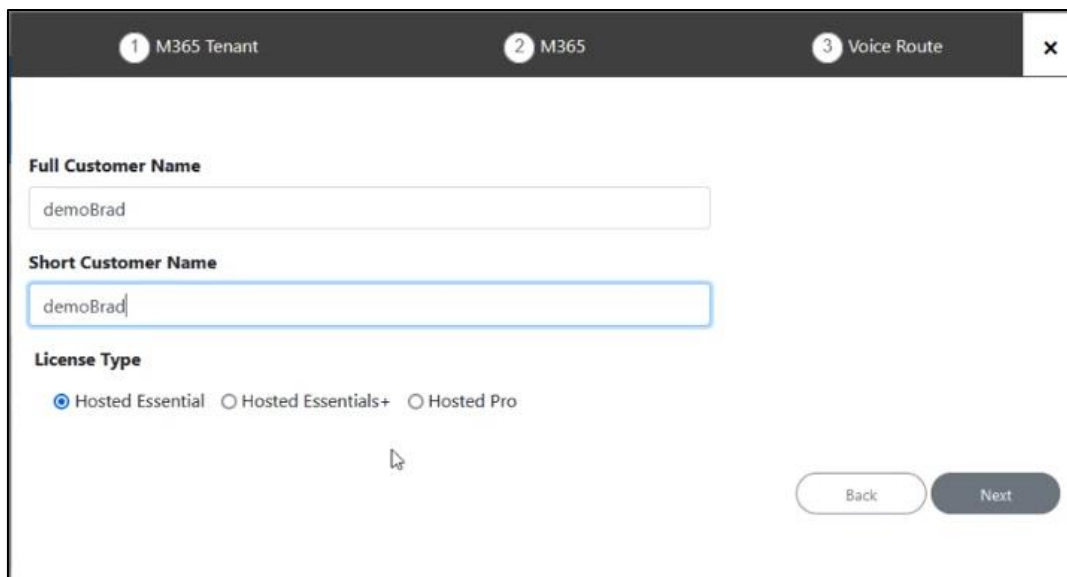


SELECT TENANT

Tenant
audio-code_co_il

Close Select

Figure 9-47: New Customer



1 M365 Tenant 2 M365 3 Voice Route

Full Customer Name
demoBrad

Short Customer Name
demoBrad

License Type
 Hosted Essential Hosted Essentials+ Hosted Pro

Back Next

4. Enter the names for the new customer, select either **Hosted Essentials+** or **Hosted Pro**, and then click **Next**.

Figure 9-48: Configure Default Routing

1 M365 Tenant **2** M365 **3** Voice Route

Configure M365 default routing

Click [[Here](#)] to Provision M365 Domain and DNS Automatically

Online PSTN Gateway: -- Please select --

M365 Onboarding Script: Default Script

M365 Cleanup Script: Default Script

Customer Variables	Value
--------------------	-------

Back Next

5. Click [Here](#) to Provision M365 Domain and DNS Automatically.

Figure 9-49: DNS Configuration

1 M365 Tenant **2** M365 **3** Voice Route

Region/Country
DEMOBRAD

Ip Address
51.124.43.46

Sbc
172.16.5.90_SBC

Domain Name
qa.activecommunications.eu

Sbc Site Name Note: You won't be able to change the sbc site name after adding the PSTN Gateway!
demoBrad

License Plan
OFFICE 365 E5 Reload

Back Next

6. From the Region/Country drop-down, select the newly created region e.g. DEMOBRAD that you added in Section 9.1.1.1.
7. Select the configured License Plan of the user e.g. Office 365 E5.

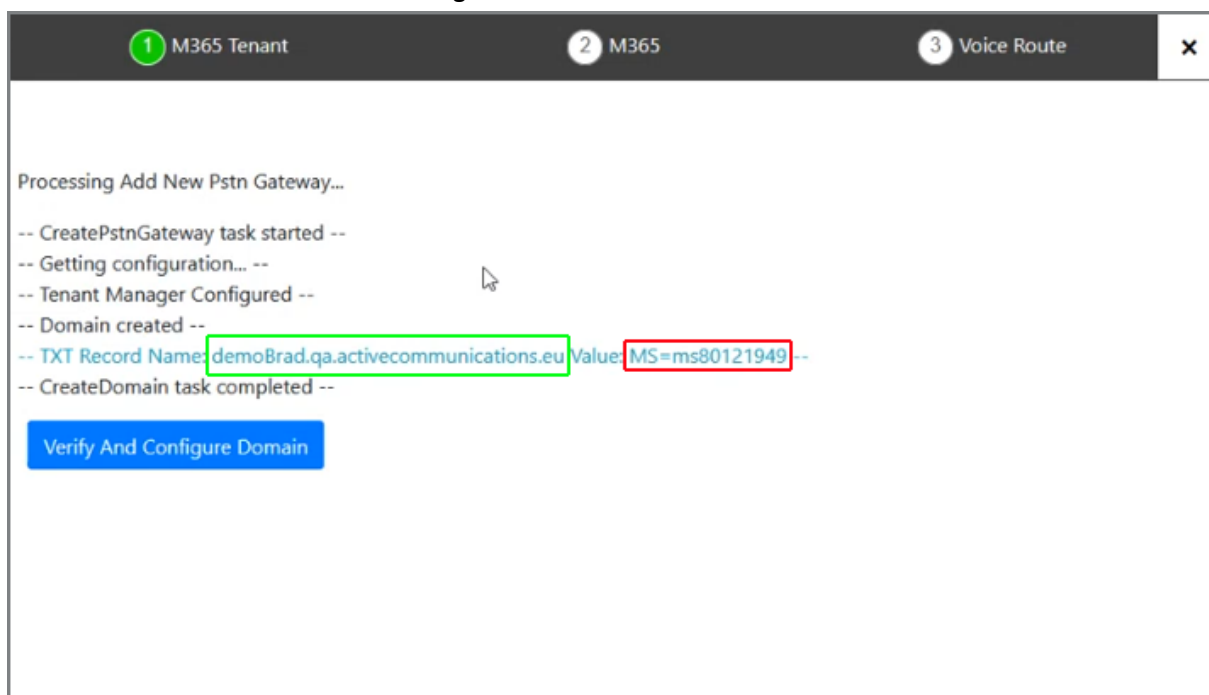


The Microsoft Office 365 Phone System user license should be preloaded as described in Section 9.3.2. If not, make a license available and then click **Reload**. The system is refreshed and searches for an available license for the tenant. The license plan is then loaded. The following license types can be made available:

- E1 with Phone System
- E3 with Phone System
- Office 365 E5

A new domain and DNS TXT record is created by the Onboarding script.

Figure 9-50: TXT Record Created



8. Copy the full record name <customername.domainname> and the TXT values to Notepad.
9. On your **DNS Hosting platform**, configure a new record with the values that you copied above, and then confirm.

Figure 9-51: Enter TXT String

activecommunications.eu	MX	100 2007.activecommunications.eu	86400	X
activecommunications.eu	MX	50 activecommunications-eu.mail.protection.outlook.com	86400	X
_sip._tls.activecommunications.eu	SRV	100 0 5061 access.activecommunications.eu	86400	X
_sipfederationtls._tcp.activecommunications.eu	SRV	100 0 5061 access.activecommunications.eu	86400	X
activecommunications.eu	TXT	v=spf1 include:spf.protection.outlook.com -all	14400	X
activecommunications.eu	TXT	dfcqn053hxy30pzz6dbmqj5fgqzz5mp	14400	X
14h.EMEA.activecommunications.eu	TXT	MS=ms40644176	14400	X
SBC-SIPTrunk.activecommunications.eu	A	82.79.139.25	3600	X
SBC-SIPTrunk.activecommunications.eu	TXT	MS=ms14688467	3600	X
NIEUWE RECORDS				
demoBrad.qa.activecommunications.eu	TXT	MS=ms80121949	14400	X

Let op: Je hebt niet alle wijzigingen opgeslagen.

+ Record toevoegen

Opslaan Ongedaan maken Sluiten

Activate Windows
Go to Settings to activate Windows.

Vragen? Start de chat

Figure 9-52: Verify and Configure Domain

1 M365 Tenant
2 M365
3 Voice Route X

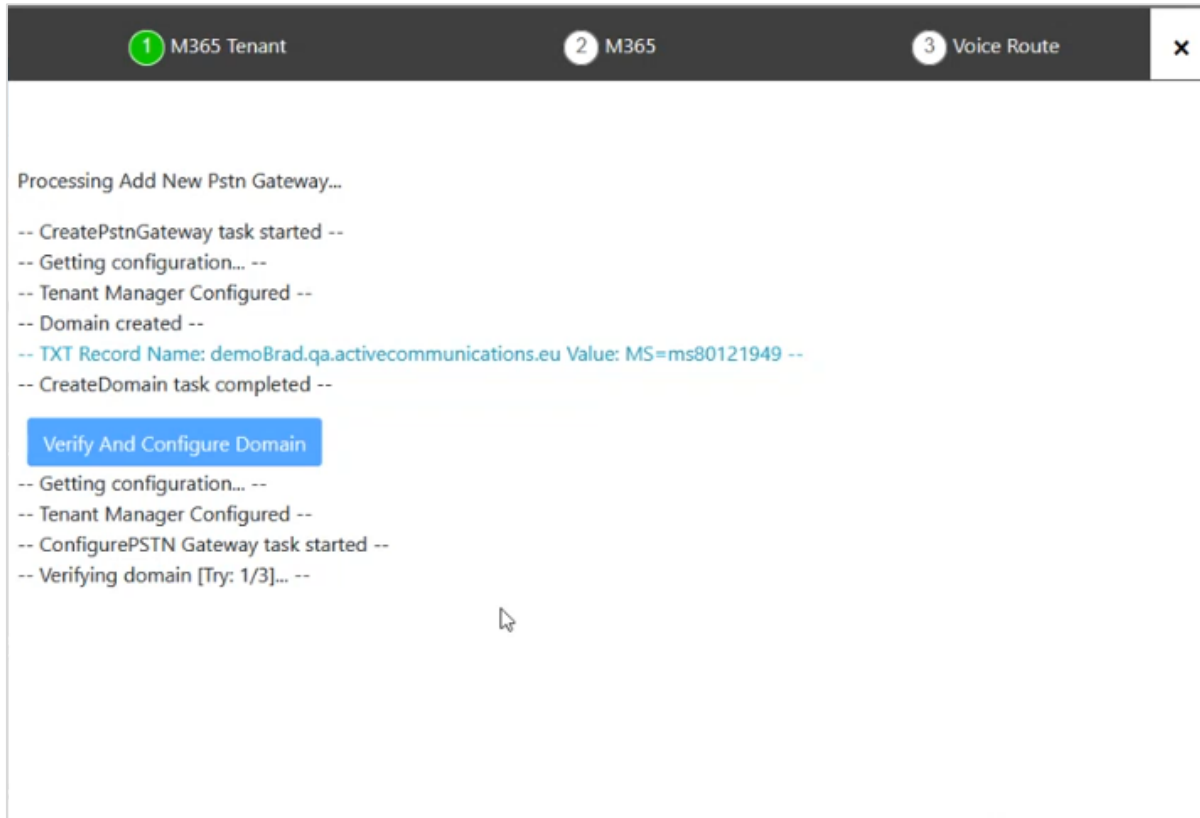
Processing Add New Pstn Gateway...

```
-- CreatePstnGateway task started --
-- Getting configuration... --
-- Tenant Manager Configured --
-- Domain created --
-- TXT Record Name: demoBrad.qa.activecommunications.eu Value: MS=ms80121949 --
-- CreateDomain task completed --
```

Verify And Configure Domain

10. Click **Verify and Configure Domain**.

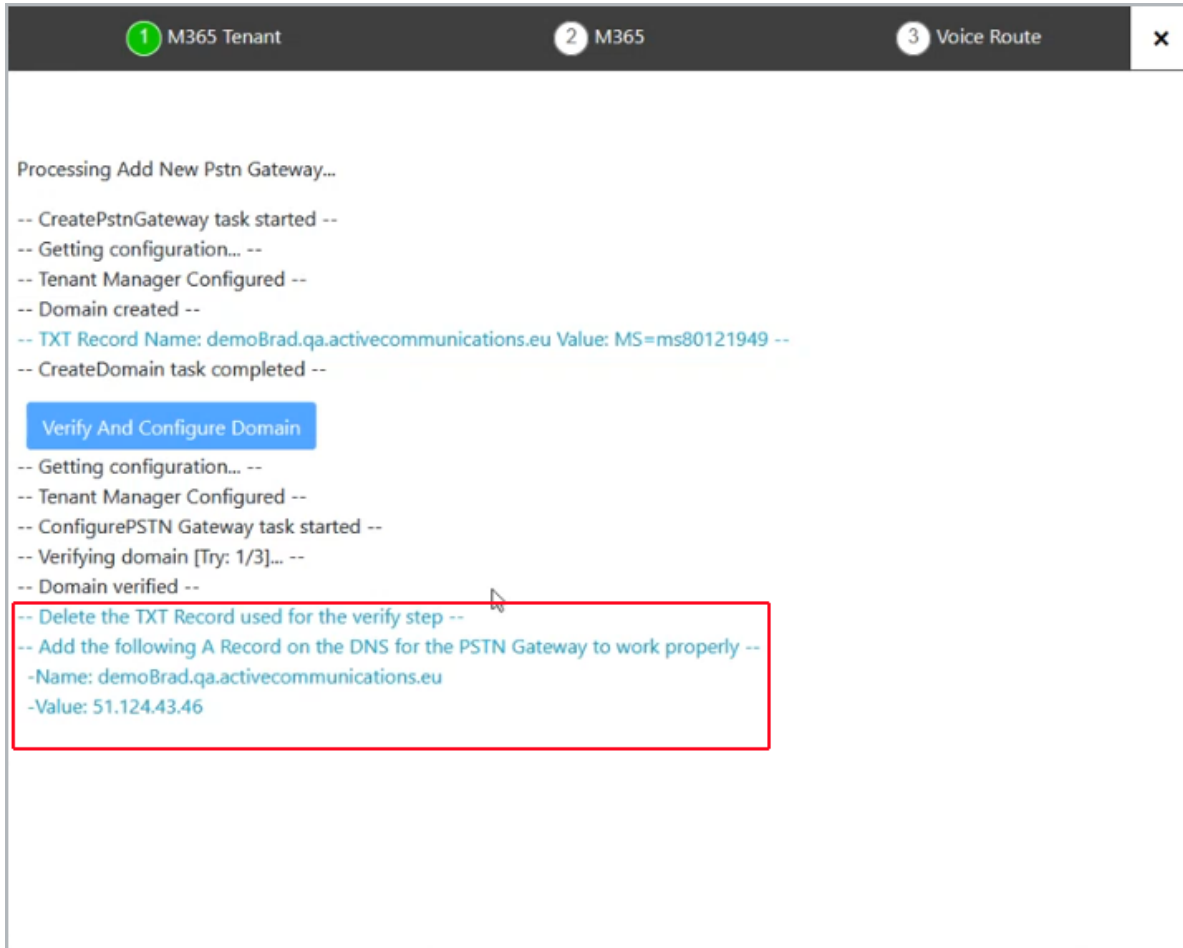
Figure 9-53: Domain is Verified



The verification process may take several tries to complete.

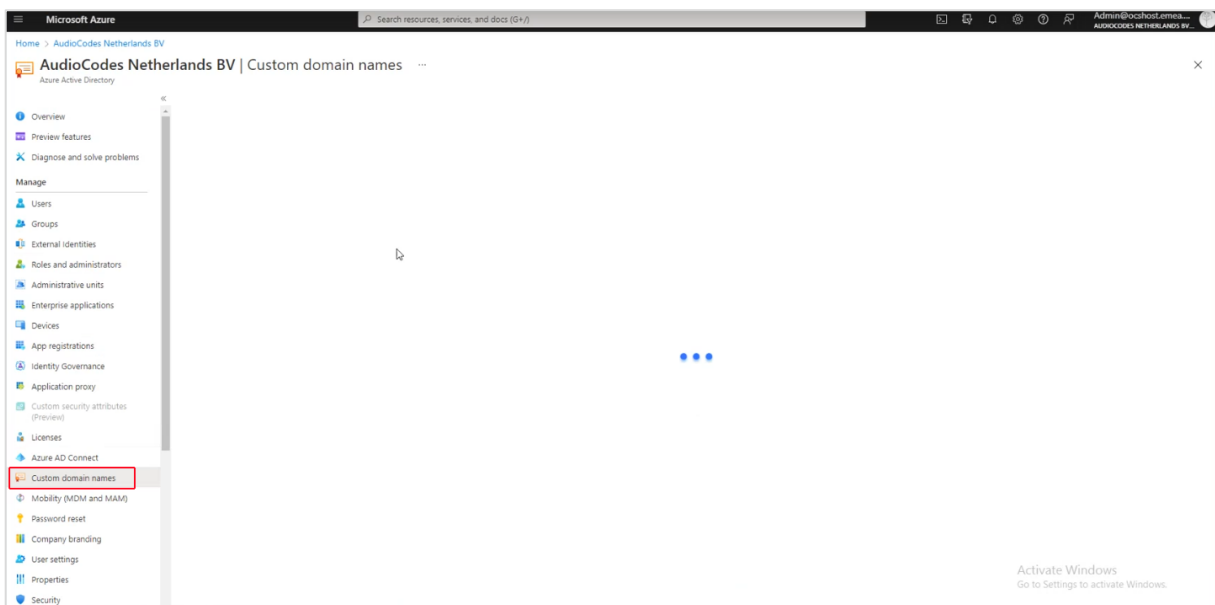
11. You are prompted to configure an A Record on the DNS Hosting platform.

Figure 9-54: Add A Record



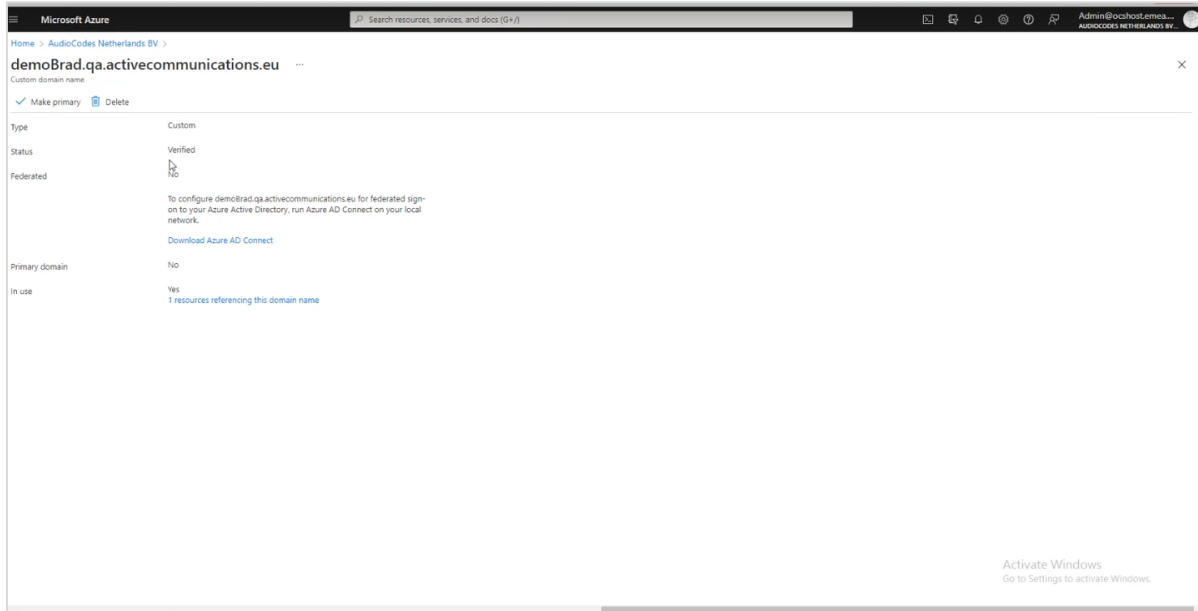
12. Open the customer Azure portal, and then in the Navigation pane, select **Custom domain names**.

Figure 9-55: Custom domain names



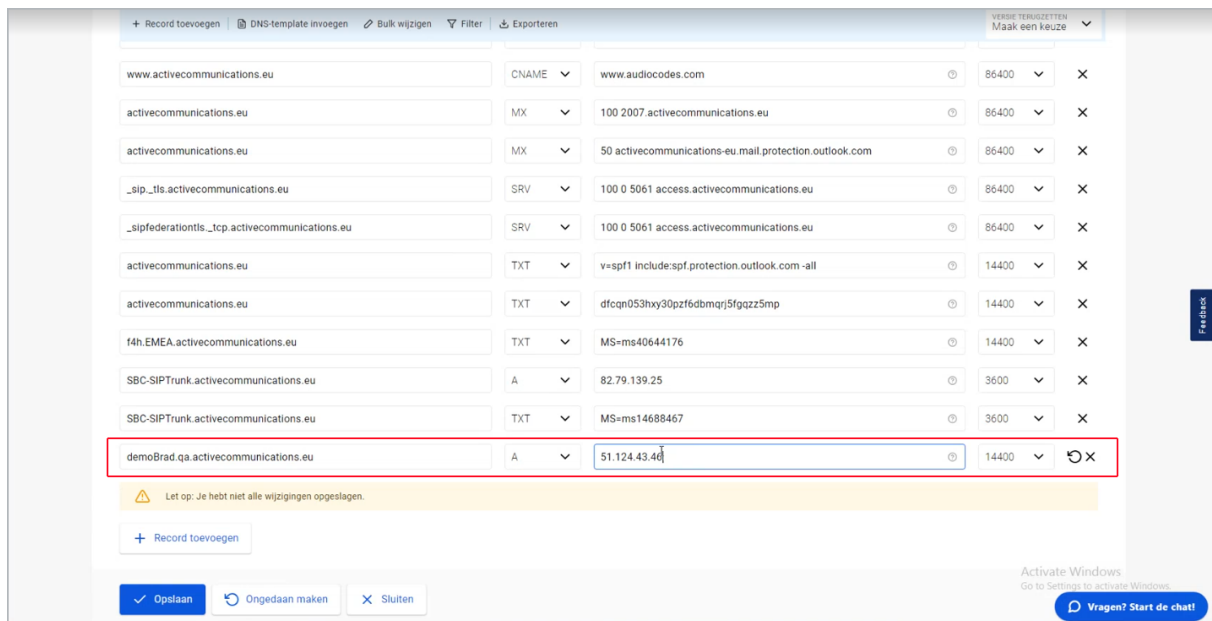
Notice the new domain that has been created.

Figure 9-56: Custom Domain



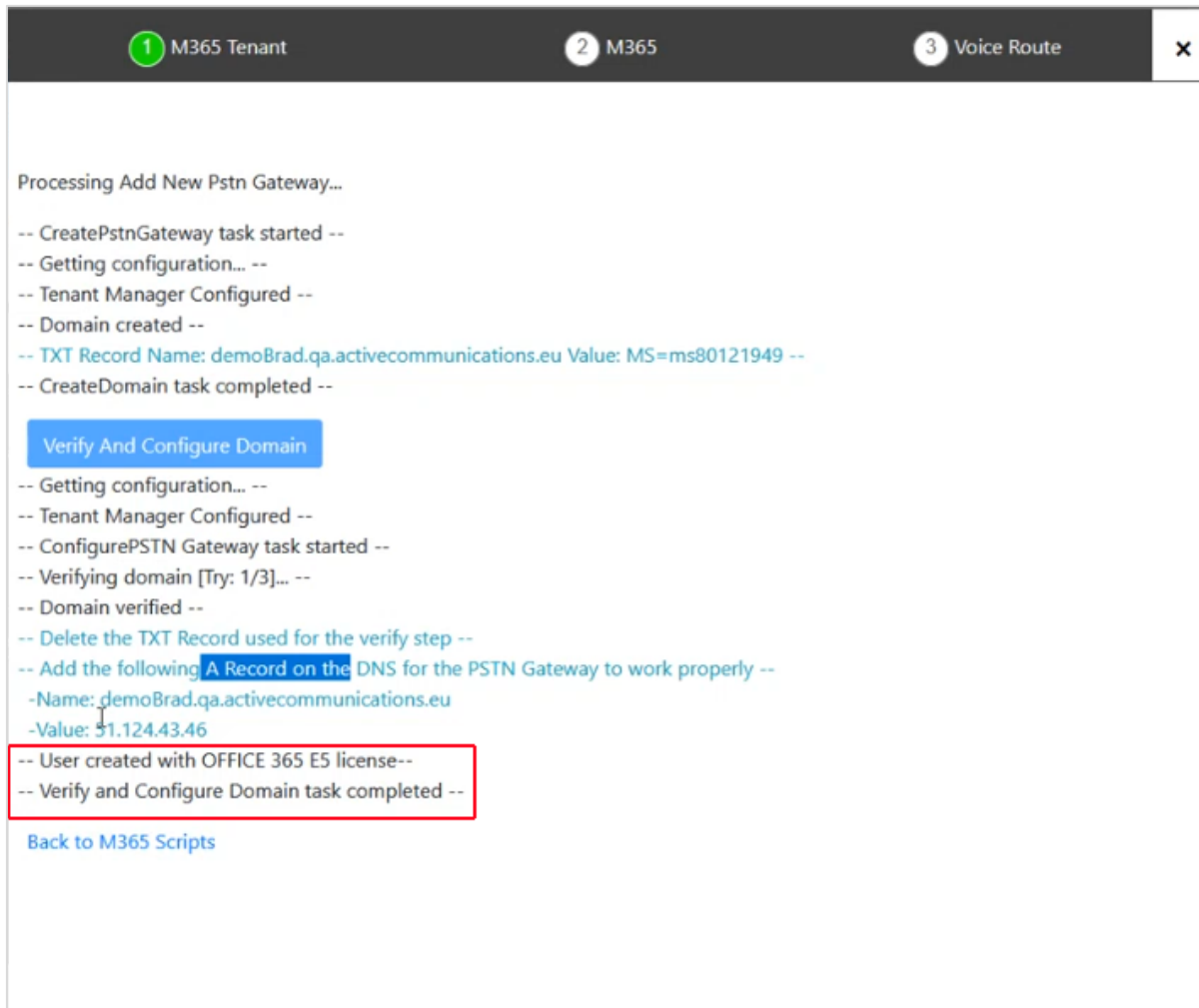
13. On the **DNS Hosting** platform, search for the TXT record that you create above, and then overwrite it by creating the A Record.

Figure 9-57: Create A Record



The user is created and the verification and configuration of the new domain is complete.

Figure 9-58: User Created



14. Return to the Onboarding wizard. Notice that the new domain now appears in the drop-down list for the Online PSTN Gateway field.

Figure 9-59: Online PSTN Gateway

1 M365 Tenant **2** M365 **3** Voice Route

Configure M365 default routing

Click [[Here](#)] to Provision M365 Domain and DNS Automatically

Online PSTN Gateway: demoBrad.qa.activecommunications.eu

M365 Onboarding Script: Default Script

M365 Cleanup Script: Default Script

Customer Variables	Value

Back Next

15. Click **Next** to continue.

Figure 9-60: New Domain Added

1 M365 Tenant **2** M365 **3** Voice Route

Customer: demoBrad

Configure SBC

Sbc Site Name: demoBrad

Online PSTN Gateway: demoBrad.qa.activecommunications.eu

Sbc Configuration: Sip Trunk IP PBX BYOC

Region: 172.16.5.90_SBC

Carrier: Select a Carrier from list

Carrier Registration

Enable Cac

Back Next

2. Complete the wizard as described in Complete the Onboarding wizard as described in Section 30.2.1.

9.3 Manual Provisioning

Manual provisioning of a DNS Azure customer subdomain involves configuration both on the Service Provider operator deployment and on the customer sites.

9.3.1 Registering a Subdomain Name on the Customer M365 Tenant

The registration of the customer subdomain is performed in the Microsoft 365 admin center of the Customer. The customer must generate a TXT record to validate with the Service Provider domain and an A-record to translate the customer site SBC shortname (configured in the Onboarding wizard) to its IP address and FQDN.

To register a subdomain for M365 customer tenant:

1. Login to the Microsoft 365 admin center with customer Tenant Admin permissions.
2. In the Navigation pane, select **Domains** and then click **Add a Domain**.

Figure 9-61: Add domain

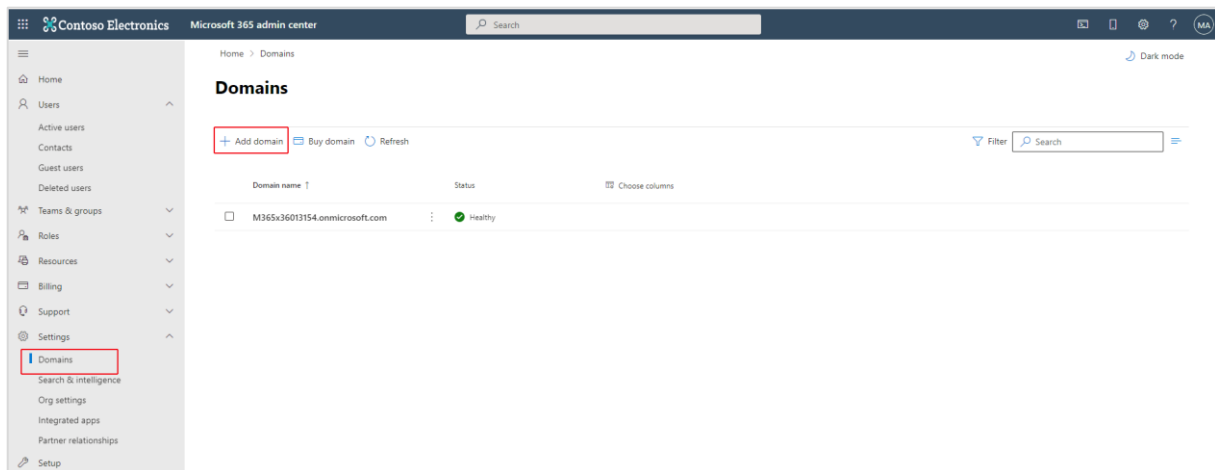
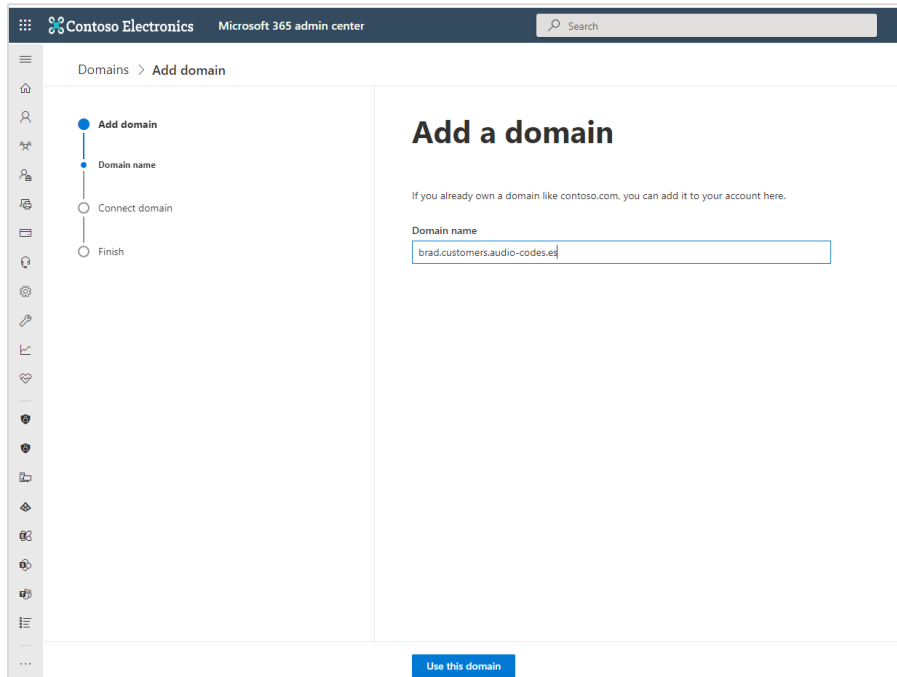
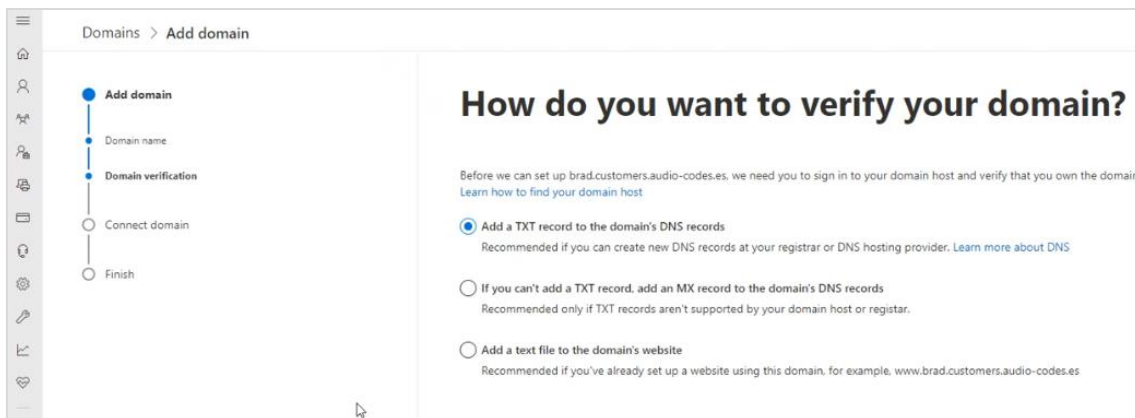


Figure 9-62: New Domain



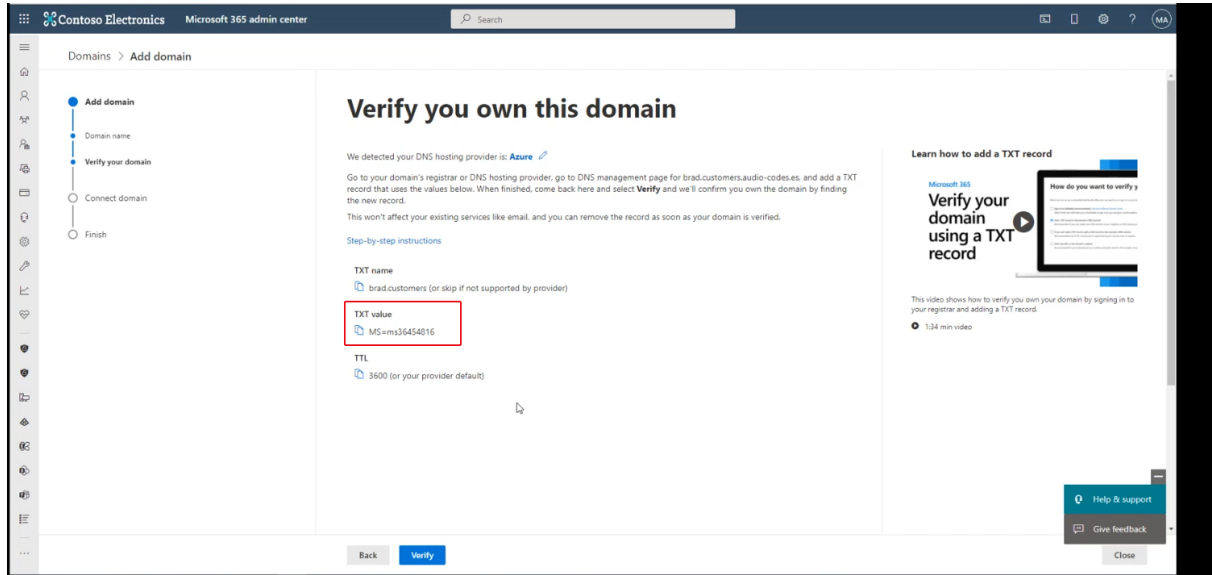
3. Enter the name for the customer subdomain e.g. **brad.customers.audio-codes.es**.
4. Click **Use this domain**.

Figure 9-63: Choose Verification Method



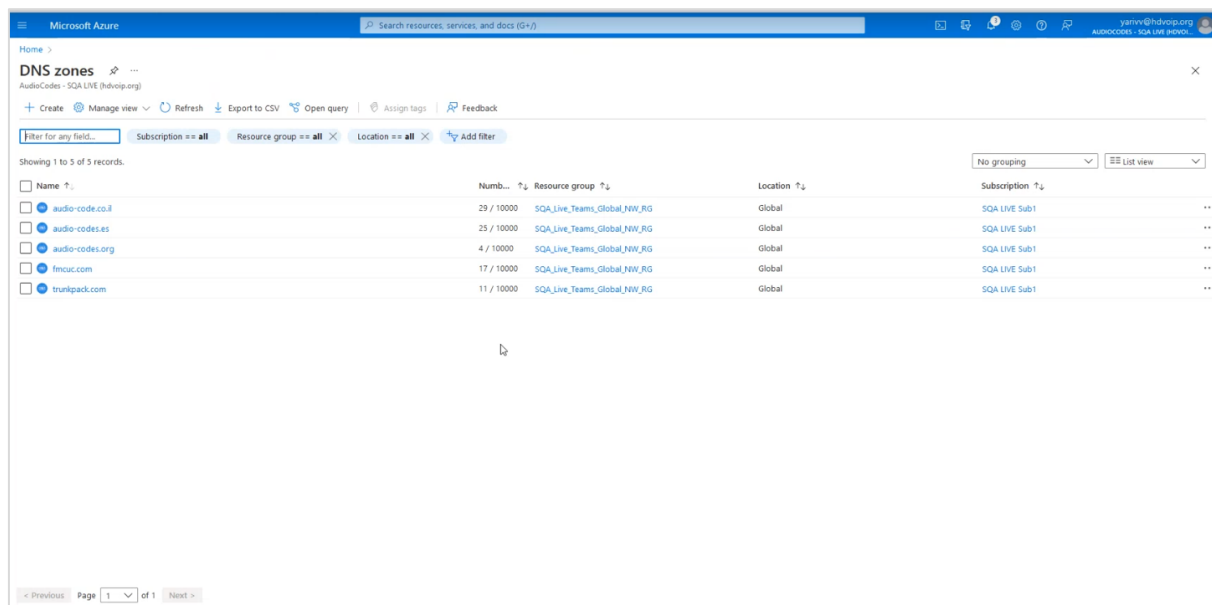
5. Select the "Add a TXT record to the domain's DNS records" checkbox.

Figure 9-64: Verify you own this domain



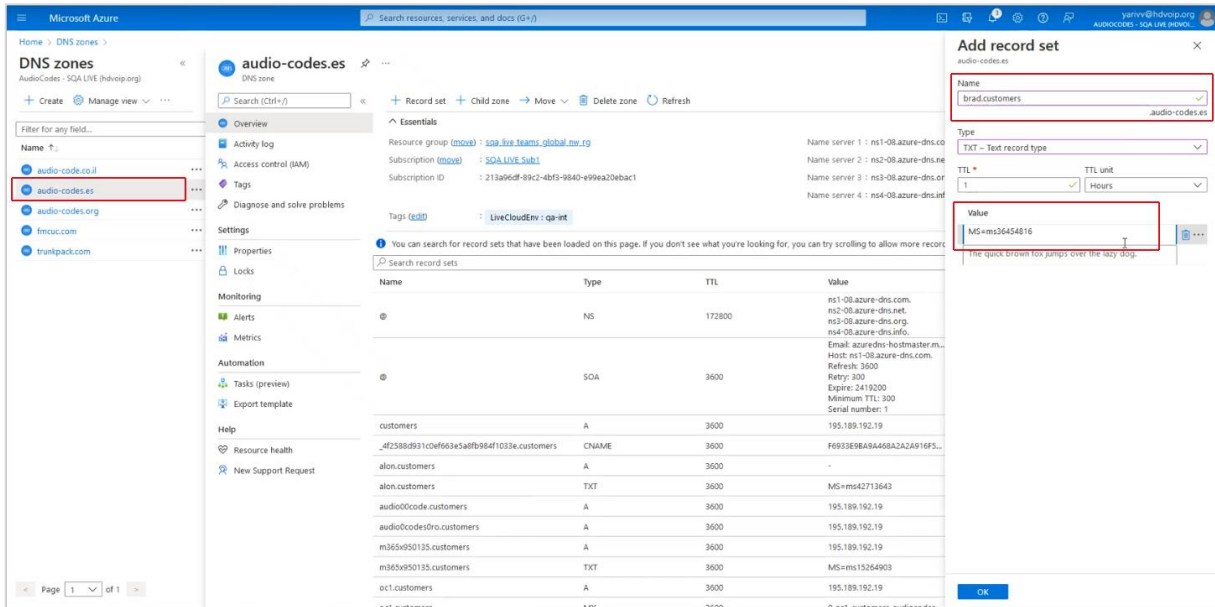
6. Copy the TXT value to clipboard.
7. Click **Verify** to verify you own this domain.
8. On the **Service Provider operator's hosting DNS Azure** platform, open the DNS zones screen.

Figure 9-65: DNS Zones

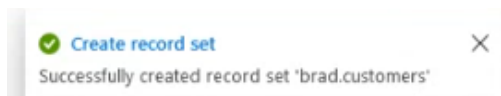


9. Select the relevant Service Provider Operator tenant DNS zone domain e.g. **audio-codes.es** and then add a record set for the customer's subdomain:
 - Enter the name of the customer domain.
 - In the Type drop-down list, select **TXT – Text record type**.
 - In the Value field, enter the TXT value that you saved above in Step 6.
 - Click **OK**.

Figure 9-66: Add Text Record



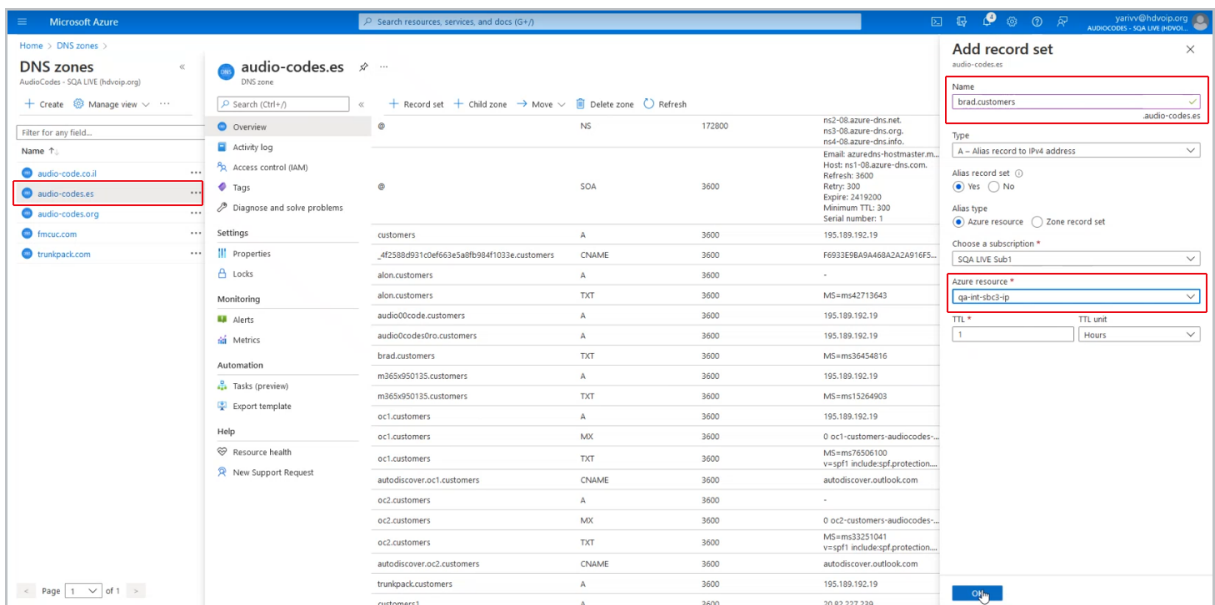
The following confirmation is displayed:



10. Add an A-record to translate the IP address of the site SBC to its FQDN:

- Enter the name of the customer subdomain.
- From the Type drop-down list, select **A-Alias record to IPv4 address**.
- Set the Alias record set to **Yes**.
- Set the Alias type to **Azure resource**.
- From the Azure resource field drop-down list, select the relevant SBC device.
- Click **OK**.

Figure 9-67: Add A Record



The following confirmation prompt is displayed.



The figure below displays the newly added records

Figure 9-68: Added DNS Records

Name	Type	TTL	Value	Alias resource type	Alias target
@	NS	172800	ns1-08.azure-dns.com ns2-08.azure-dns.net ns3-08.azure-dns.org ns4-08.azure-dns.info		
@	SOA	3600	Email: azure-dns-hostmaster.m... Host: ns1-08.azure-dns.com. Refresh: 3600 Retry: 300 Expire: 2419200 Minimum TTL: 3600 Serial number: 1		
customers	A	3600	195.189.192.19		
_4f258d931c0ff63e5a8fb984f1033e.customers	CNAME	3600	F6933E9BA4A68A2A24016F5...		
alon.customers	A	3600	-	Public IP Address	qa-int-ibc3-ip
alon.customers	TXT	3600	MS=ms42713643		
audio00code.customers	A	3600	195.189.192.19		
audio0code@ro.customers	A	3600	195.189.192.19		
brad.customers	A	3600	-	Public IP Address	qa-int-ibc3-ip
brad.customers	TXT	3600	MS=ms36454816		
m365d950135.customers	A	3600	195.189.192.19		
m365d950135.customers	TXT	3600	MS=ms15264903		
oc1.customers	A	3600	195.189.192.19		
oc1.customers	MX	3600	0 oc1-customers-audiocodes-...		
oc1.customers	TXT	3600	MS=ms76506100 v=spf1 include:spf.protection...		
autodiscover.oc1.customers	CNAME	3600	autodiscover.outlook.com		
oc2.customers	A	3600	-	Public IP Address	qa-int-ibc3-ip
oc2.customers	MX	3600	0 oc2-customers-audiocodes-...		

- Return to the Customer tenant Microsoft 365 admin center. Notice that the system has detected that the DNS hosting provider is on Azure.

Figure 9-69: Verify your own this domain

Verify you own this domain

We detected your DNS hosting provider is: **Azure**

Go to your domain's registrar or DNS hosting provider, go to DNS management page for brad.customers.audio-codes.es, and add a TXT record that uses the values below. When finished, come back here and select **Verify** and we'll confirm you own the domain by finding the new record.

This won't affect your existing services like email, and you can remove the record as soon as your domain is verified.

Step-by-step instructions

TXT name
brad.customers (or skip if not supported by provider)

TXT value
MS=ms36454816

TTL
3600 (or your provider default)

Learn how to add a TXT record

Microsoft 365
Verify your domain using a TXT record

This video shows how to verify you own your domain by signing in to your registrar and adding a TXT record.

134 min video

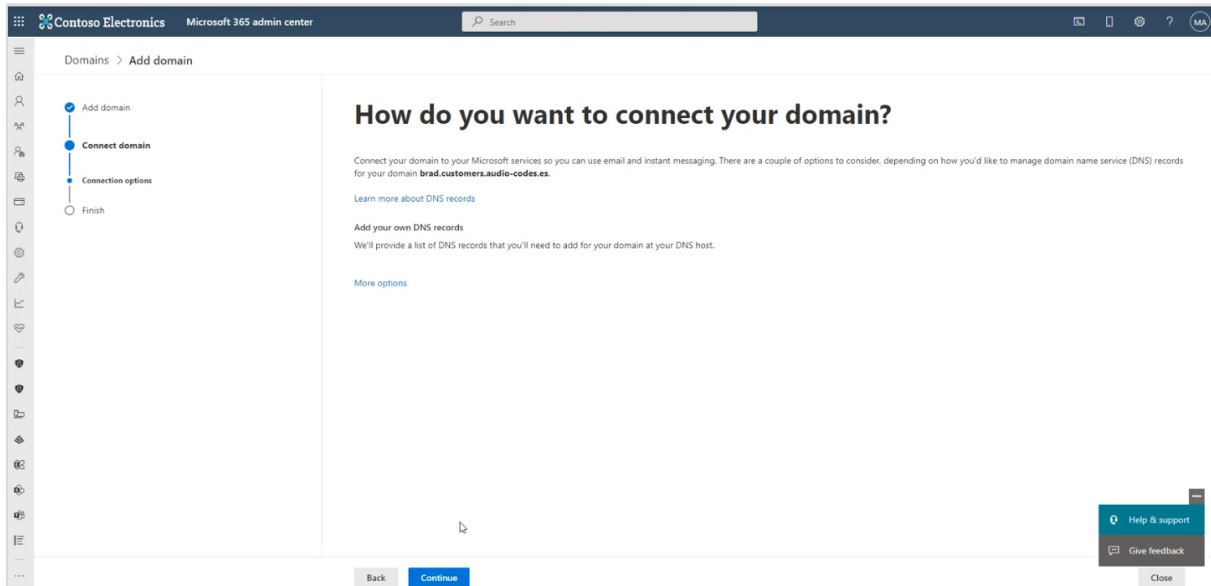
Back **Verify** Close

- Click **Verify**.

The customer's domain i.e. the Service Provider Operator domain **audio-codes.es** is verified.

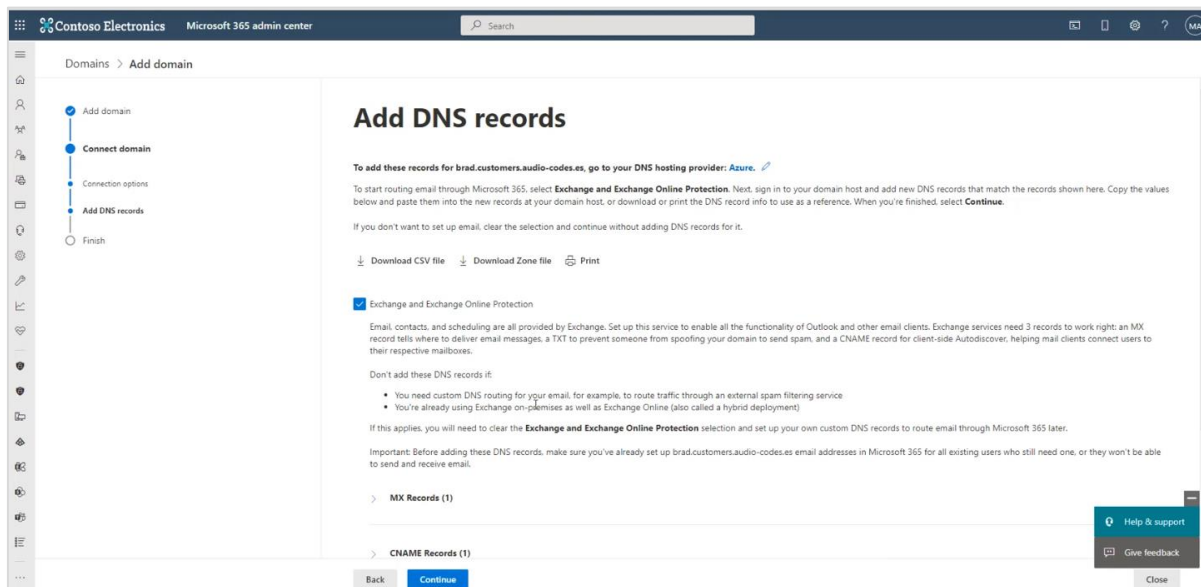


Figure 9-70: How do you want to connect your domain



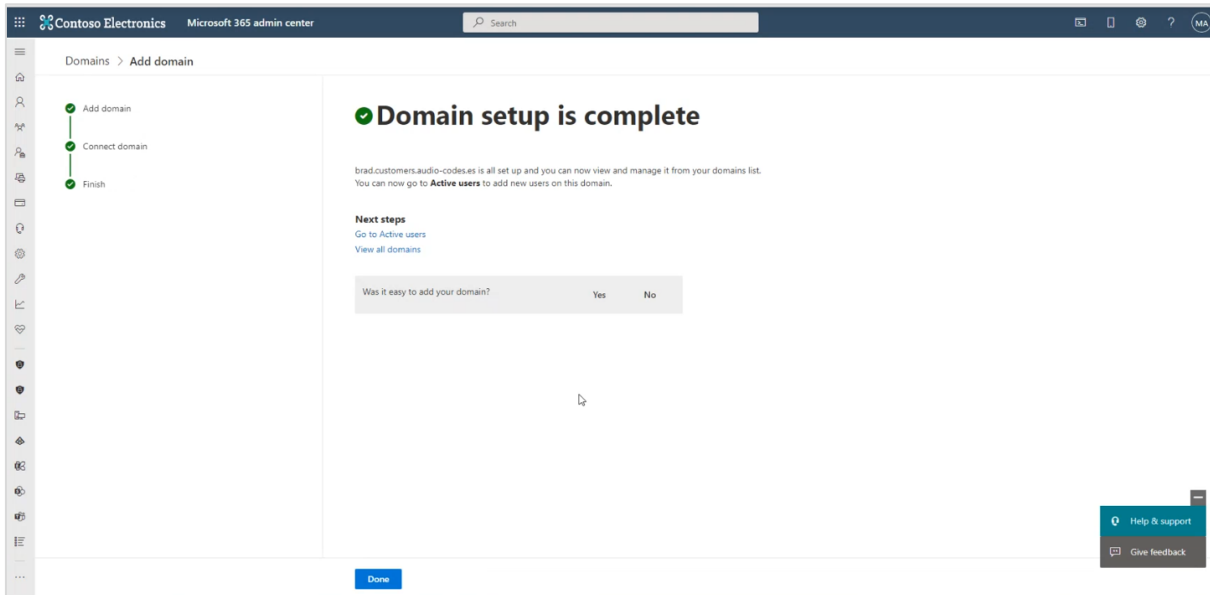
13. Click **Continue**.

Figure 9-71: Add DNS records



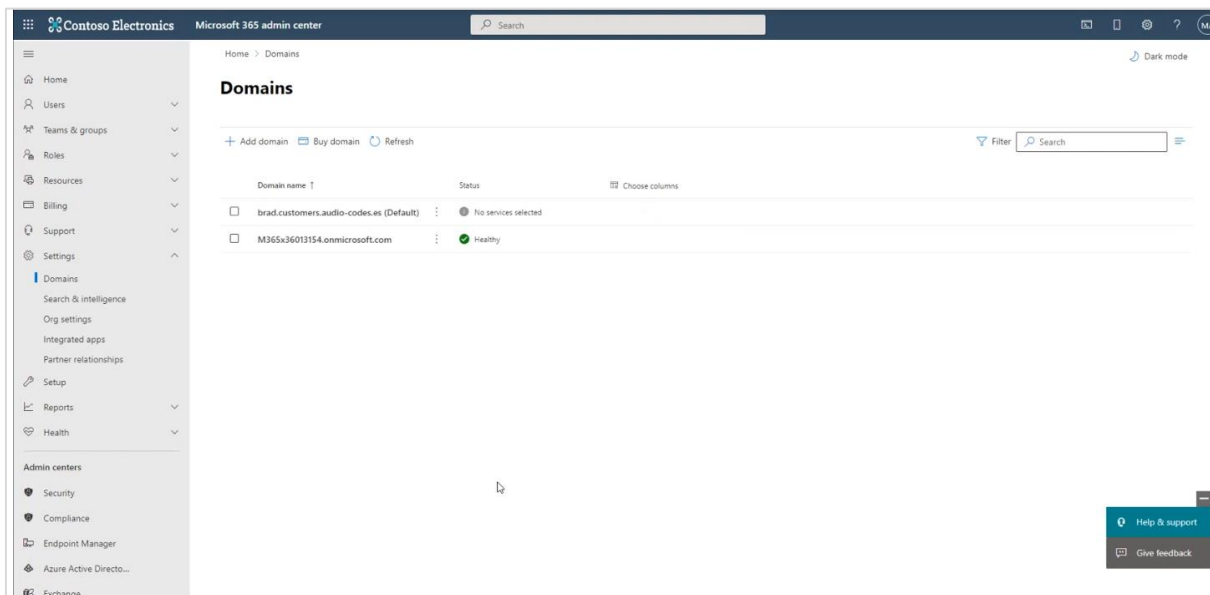
14. Deselect the **Exchange and Exchange Online Protection** checkbox and then click **Continue**.

Figure 9-72: Domain setup is complete



15. Click **Done**.

Figure 9-73: New Domain Created



9.3.2 Activating the Providers Domain

Activate the new domain created above by adding the licensed user with a Phone System license to your new subdomain. For example, a new user “UMP-365” and is assigned to the subdomain **brad.customers.audio-codes.es**. The License can be revoked after the domain activation (this may take up to 24 hours).

To activate a user:

1. In the Tenant’s Microsoft 365 admin center Navigation pane, select Active Users.
2. Select any user with an active license and click it.

Figure 9-74: Active users

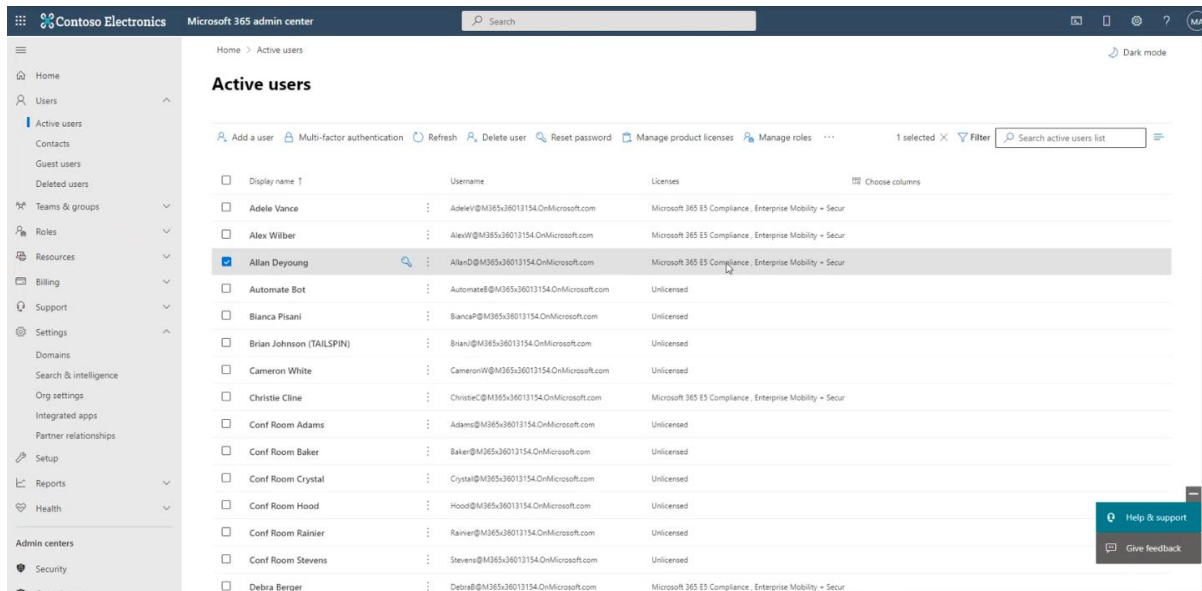
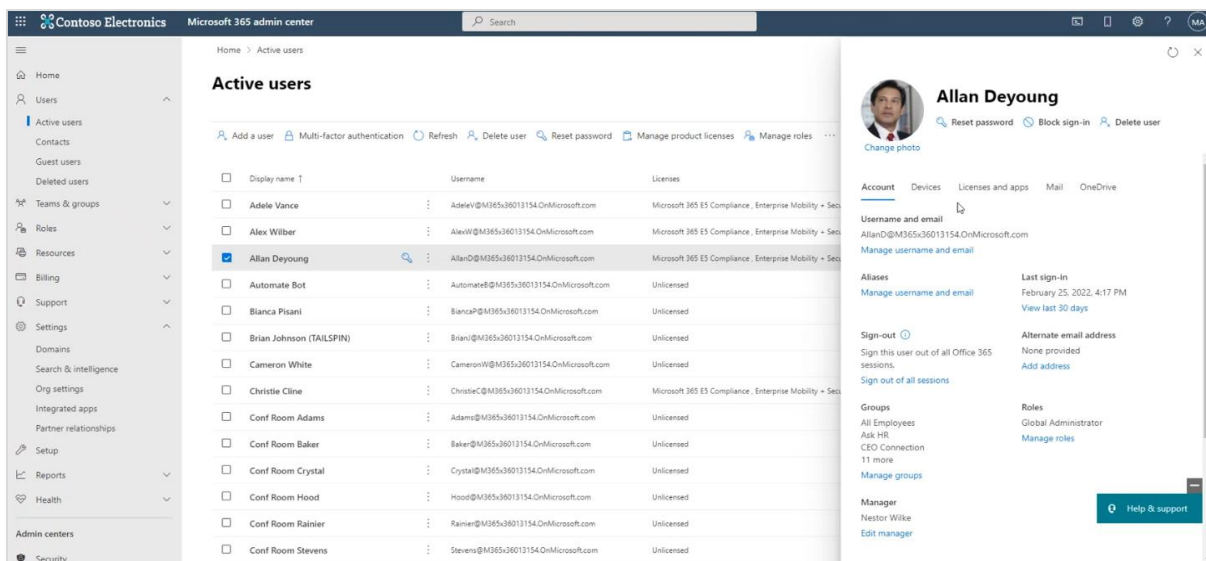


Figure 9-75: Disable User License



3. Select the License and apps tab.

Figure 9-76: License and apps

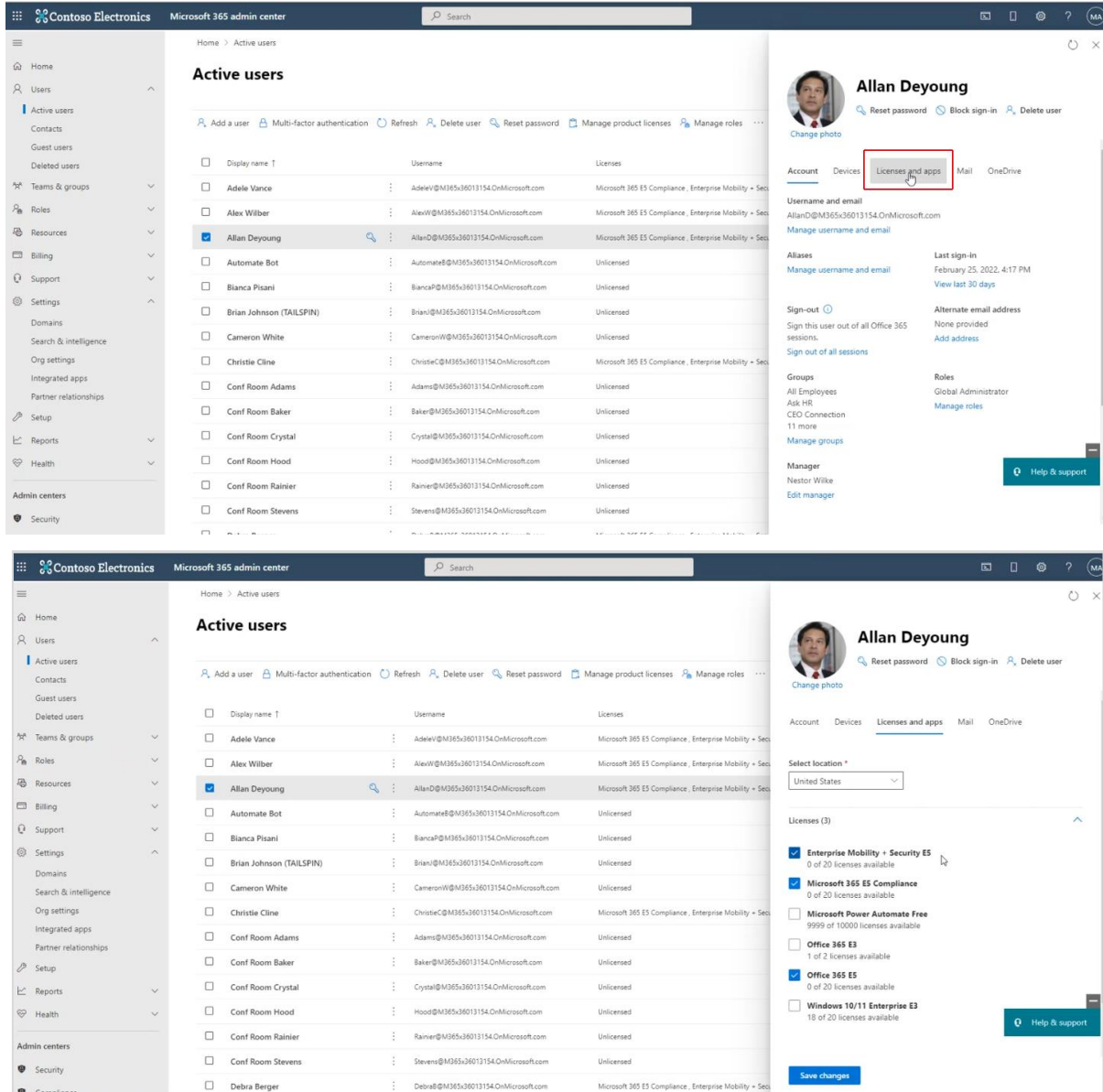


Figure 9-77: Disable User Licenses

The screenshot shows the Microsoft 365 admin center interface. On the left is a navigation pane with options like Home, Users, Active users, Contacts, Guest users, Deleted users, Teams & groups, Roles, Resources, Billing, Support, Settings, Domains, Search & intelligence, Org settings, Integrated apps, Partner relationships, Setup, Reports, Health, Admin centers, and Security. The main area is titled 'Active users' and contains a table of users. The user 'Allan Deyoung' is selected, and his profile is shown on the right. The 'Licenses and apps' section is open, showing a list of licenses with checkboxes. The 'Enterprise Mobility + Security E5' license is currently assigned to the user.

Display name	Username	Licenses
<input type="checkbox"/> Adele Vance	AdeleV@M365x36013154.OnMicrosoft.com	Microsoft 365 E5 Compliance, Enterprise Mobility + Security
<input type="checkbox"/> Alex Wilber	AlexW@M365x36013154.OnMicrosoft.com	Microsoft 365 E5 Compliance, Enterprise Mobility + Security
<input checked="" type="checkbox"/> Allan Deyoung	AllanD@M365x36013154.OnMicrosoft.com	Unlicensed
<input type="checkbox"/> Automate Bot	AutomateB@M365x36013154.OnMicrosoft.com	Unlicensed
<input type="checkbox"/> Bianca Pisani	BiancaP@M365x36013154.OnMicrosoft.com	Unlicensed
<input type="checkbox"/> Brian Johnson (TAILSPIN)	BrianJ@M365x36013154.OnMicrosoft.com	Unlicensed
<input type="checkbox"/> Cameron White	CameronW@M365x36013154.OnMicrosoft.com	Unlicensed
<input type="checkbox"/> Christie Cline	ChristieC@M365x36013154.OnMicrosoft.com	Unlicensed
<input type="checkbox"/> Conf Room Adams	Adams@M365x36013154.OnMicrosoft.com	Unlicensed
<input type="checkbox"/> Conf Room Baker	Baker@M365x36013154.OnMicrosoft.com	Unlicensed
<input type="checkbox"/> Conf Room Crystal	Crystal@M365x36013154.OnMicrosoft.com	Unlicensed
<input type="checkbox"/> Conf Room Hood	Hood@M365x36013154.OnMicrosoft.com	Unlicensed
<input type="checkbox"/> Conf Room Rainier	Rainier@M365x36013154.OnMicrosoft.com	Unlicensed
<input type="checkbox"/> Conf Room Stevens	Stevens@M365x36013154.OnMicrosoft.com	Unlicensed

4. Deselect all active licenses and then click **Save changes**. A confirmation is displayed.

Figure 9-78: User License Disabled

The screenshot shows the Microsoft 365 admin center interface. On the left is a navigation pane with options like Home, Users, Active users, Contacts, Guest users, Deleted users, Teams & groups, Roles, Resources, Billing, Support, Settings, Domains, Search & intelligence, Org settings, Integrated apps, Partner relationships, Setup, Reports, Health, Admin centers, and Security. The main area is titled 'Active users' and contains a table of users. The user 'Allan Deyoung' is selected, and his profile is shown on the right. The 'Licenses and apps' section is open, showing a list of licenses with checkboxes. The 'Enterprise Mobility + Security E5' license is now unassigned, and the 'Windows 10/11 Enterprise E3' license is selected. A green notification bar at the top of the profile section says 'Your changes have been saved.'

Display name	Username	Licenses
<input type="checkbox"/> Adele Vance	AdeleV@M365x36013154.OnMicrosoft.com	Microsoft 365 E5 Compliance, Enterprise Mobility + Security
<input type="checkbox"/> Alex Wilber	AlexW@M365x36013154.OnMicrosoft.com	Microsoft 365 E5 Compliance, Enterprise Mobility + Security
<input checked="" type="checkbox"/> Allan Deyoung	AllanD@M365x36013154.OnMicrosoft.com	Unlicensed
<input type="checkbox"/> Automate Bot	AutomateB@M365x36013154.OnMicrosoft.com	Unlicensed
<input type="checkbox"/> Bianca Pisani	BiancaP@M365x36013154.OnMicrosoft.com	Unlicensed
<input type="checkbox"/> Brian Johnson (TAILSPIN)	BrianJ@M365x36013154.OnMicrosoft.com	Unlicensed
<input type="checkbox"/> Cameron White	CameronW@M365x36013154.OnMicrosoft.com	Unlicensed
<input type="checkbox"/> Christie Cline	ChristieC@M365x36013154.OnMicrosoft.com	Microsoft 365 E5 Compliance, Enterprise Mobility + Security
<input type="checkbox"/> Conf Room Adams	Adams@M365x36013154.OnMicrosoft.com	Unlicensed
<input type="checkbox"/> Conf Room Baker	Baker@M365x36013154.OnMicrosoft.com	Unlicensed
<input type="checkbox"/> Conf Room Crystal	Crystal@M365x36013154.OnMicrosoft.com	Unlicensed
<input type="checkbox"/> Conf Room Hood	Hood@M365x36013154.OnMicrosoft.com	Unlicensed
<input type="checkbox"/> Conf Room Rainier	Rainier@M365x36013154.OnMicrosoft.com	Unlicensed
<input type="checkbox"/> Conf Room Stevens	Stevens@M365x36013154.OnMicrosoft.com	Unlicensed
<input type="checkbox"/> Debra Berger	DebraB@M365x36013154.OnMicrosoft.com	Microsoft 365 E5 Compliance, Enterprise Mobility + Security

5. Add a new user for the UMP-365.

Figure 9-79: Set up the basics

The screenshot shows the 'Add a user' page in the Microsoft 365 admin center. The 'Basics' step is selected in the left-hand navigation pane. The main content area is titled 'Set up the basics' and contains the following fields and options:

- First name:** UMP
- Last name:** (empty)
- Display name *:** UMP
- Username *:** UMP
- Domains:** brad.customers.audio-codes.es
- Automatically create a password
- Require this user to change their password when they first sign in
- Send password in email upon completion

Buttons for 'Next' and 'Cancel' are visible at the bottom of the form.

- Assign a product license for the new user and then click **Next**.

Figure 9-80: Assign product licenses

The screenshot shows the 'Add a user' page in the Microsoft 365 admin center, now on the 'Assign product licenses' step. The 'Product licenses' step is selected in the left-hand navigation pane. The main content area is titled 'Assign product licenses' and contains the following fields and options:

- Select location *:** United States
- Licenses (2)*:**
 - Assign user a product license
 - Enterprise Mobility + Security E5 (0 of 20 licenses available)
 - Microsoft 365 E5 Compliance (1 of 20 licenses available)
 - Microsoft Power Automate Free (9999 of 10000 licenses available)
 - Office 365 E3 (1 of 2 licenses available)
 - Office 365 E5 (0 of 20 licenses available)
 - Windows 10/11 Enterprise E3 (18 of 20 licenses available)
 - Create user without product license (not recommended)
 - They may have limited or no access to Office 365 until you assign a product license.

Buttons for 'Back', 'Next', and 'Cancel' are visible at the bottom of the form.

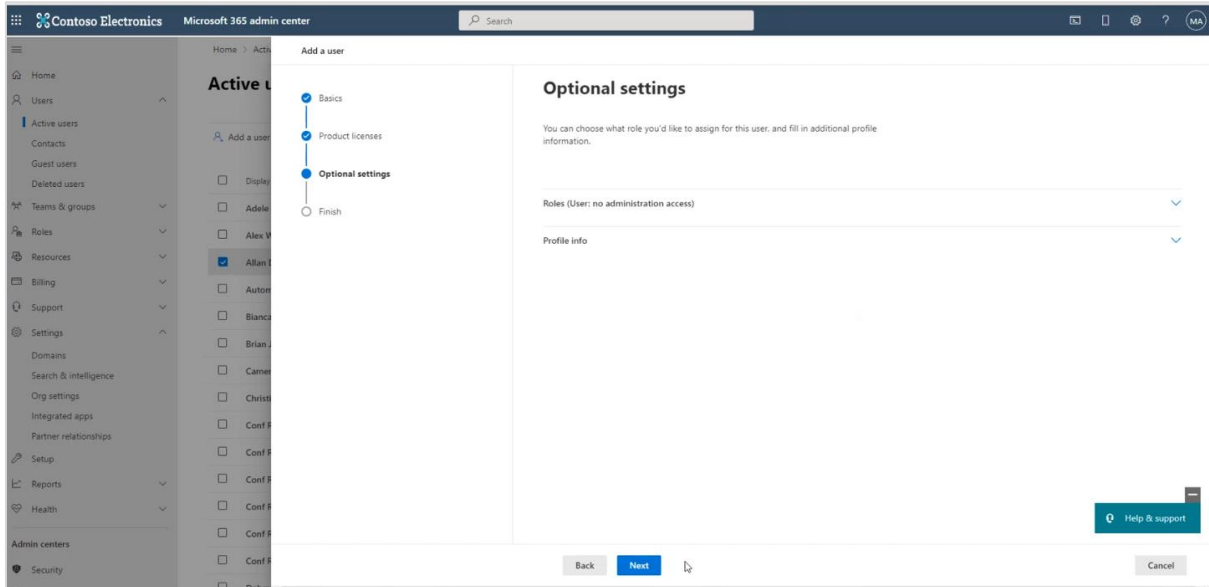


The following licenses can be configured:

- E1 with Phone System
- E3 with Phone System
- Office 365 E5

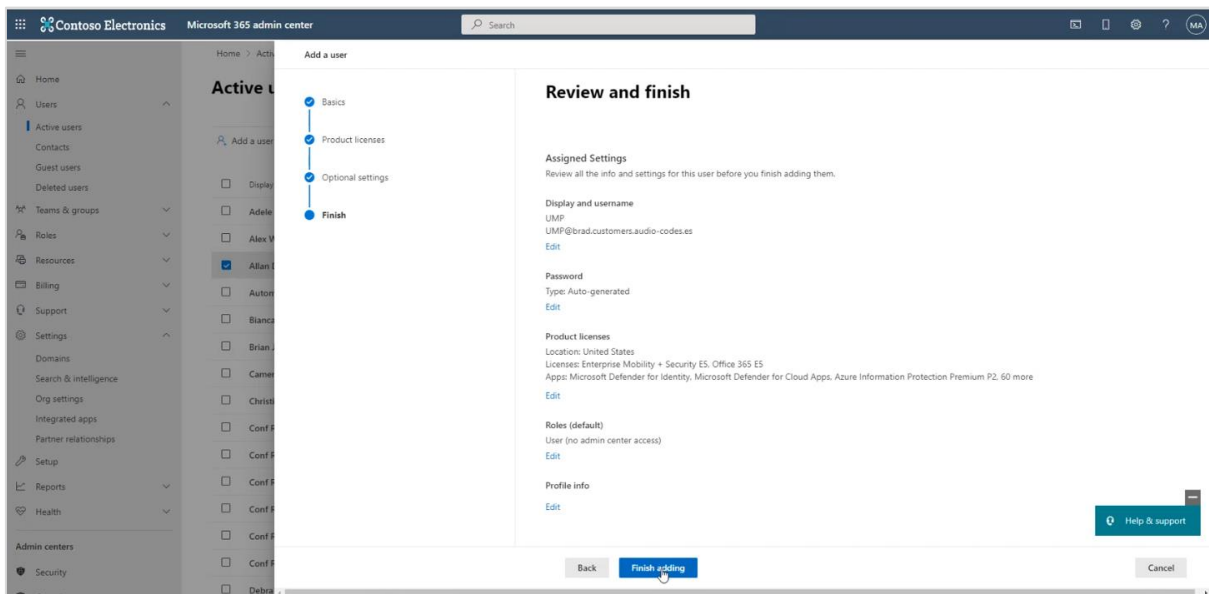
- Click **Next** to continue.

Figure 9-81: Optional settings



8. Click **Finish** adding.

Figure 9-82: Review and finish



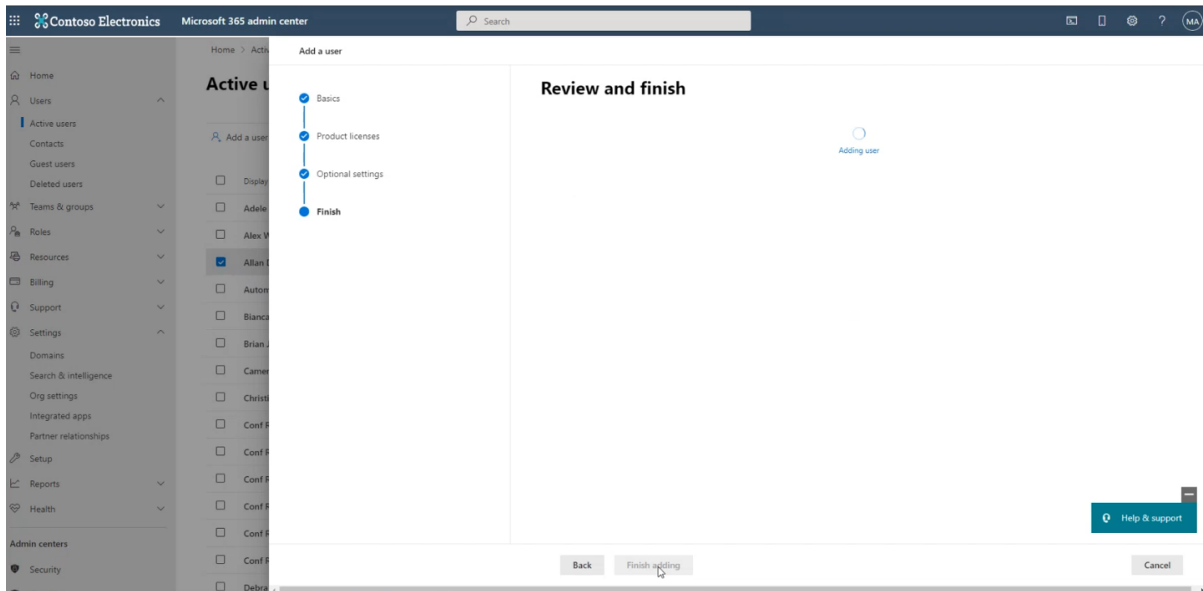
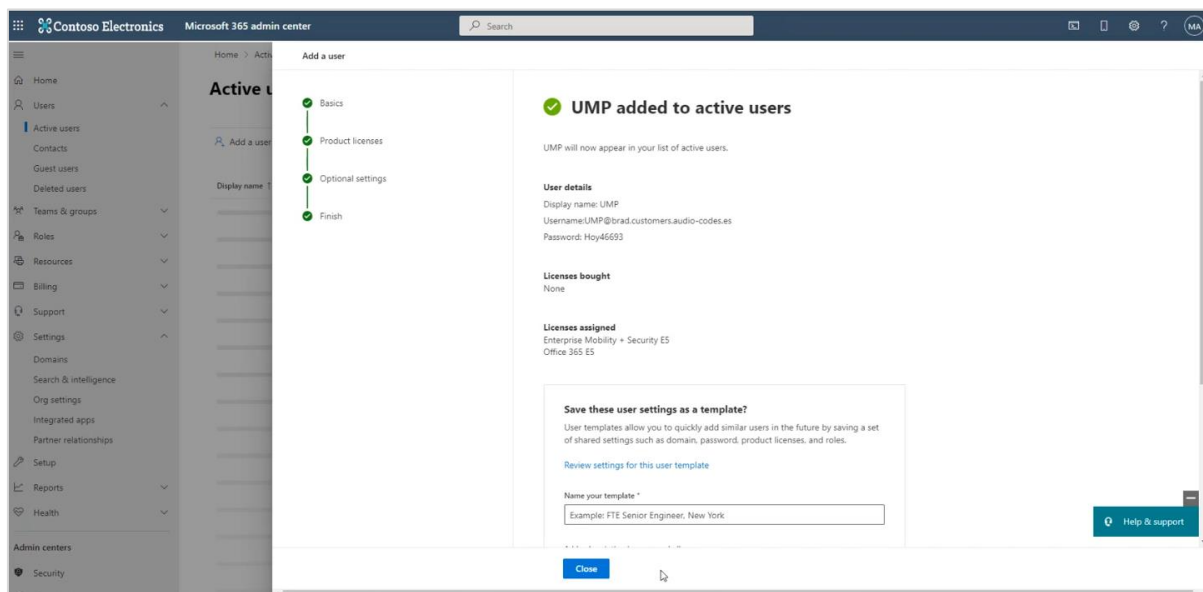


Figure 9-83: UMP added to active users



10 Microsoft Teams Direct Routing SBC Configuration

Microsoft Teams Direct Routing using AudioCodes SBC devices should be configured using one of the following topologies:

- **Single Tenant Enterprise Deployment:** Configuration of the **Enterprise** model should be performed according to the following:
<https://www.audiocodes.com/media/13181/connecting-audiocodes-sbc-to-microsoft-teams-direct-routing-enterprise-model-configuration-note.pdf>
- **Multitenant Deployment:** Configuration of the **SBC Direct Routing Hosting** model should be performed according to the following:
<https://www.audiocodes.com/media/13161/connecting-audiocodes-sbc-to-microsoft-teams-direct-routing-hosting-model-configuration-note.pdf>

11 App Registration For Background Replication

This section describes how to setup and configure the App registration for the background synchronization. The App Registration manages the automatic synchronization between the UMP-365 and the customer's Microsoft 365 platform. You must add the App registration under the Provider Tenant's Azure subscription for each UMP device. In this procedure, a redirect URL is configured which is used as part of the token authentication for requesting email consent from the customer tenant to connect to their Microsoft Office 365 platform (see Section 30.5).

In this procedure, the Client ID and the Redirect URL must be configured in the Auth Tokens screen in the Main Tenant interface (see Step below and described in Section 25.2). Once this registration is finished, the details of the M365 user configured in this procedure are displayed in the Multitenant portal in the Microsoft 365 Settings screen (see Section 33.12).

Once you complete this registration, administrator roles must be assigned to the customer IT administrator who provides consent to Service Provider IT administrator for using the token authentication (see Section 11.1).

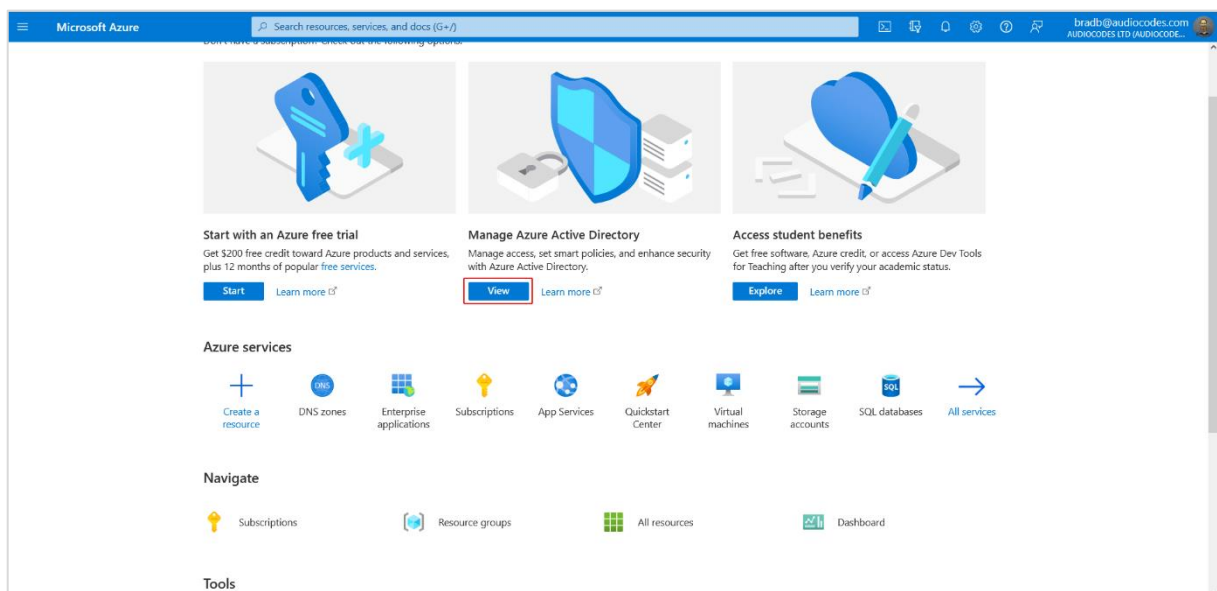


- The domain names shown in the procedure below are examples only.
- For each customer, a unique redirect URL is defined.
- This procedure must be performed by new customers running a clean installation. For existing customers, the registration must be updated as described in Chapter 23.

Do the following:

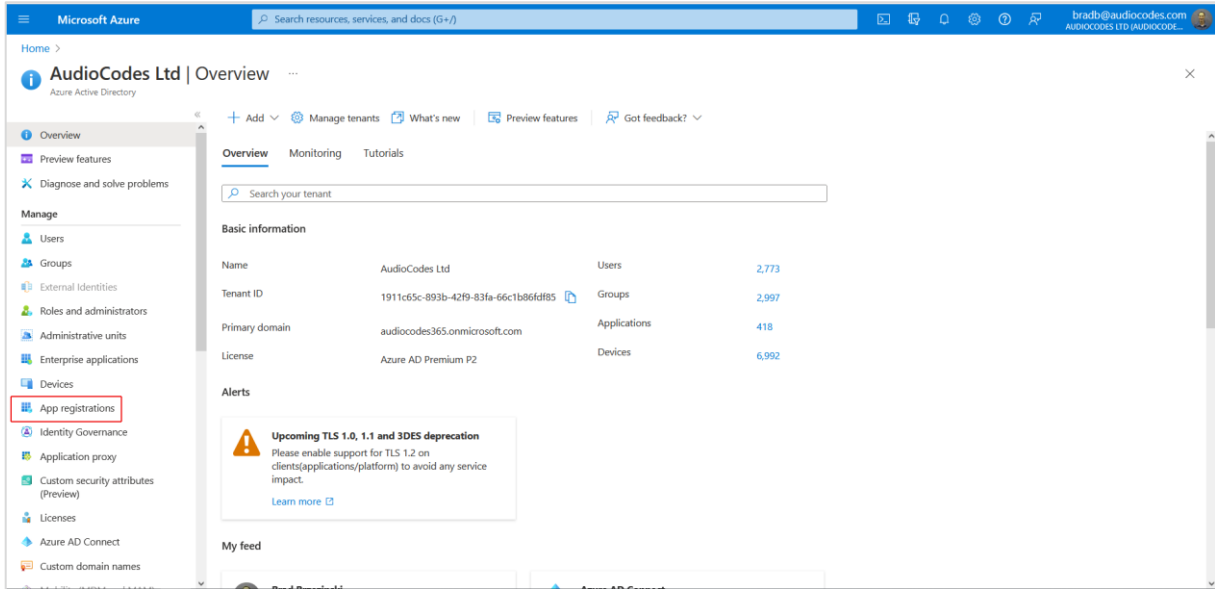
1. Sign-in to the Azure portal for the Service Provider operator tenant with Admin permissions.
2. Under Manage Azure Active Directory, select **View**.

Figure 11-1: View Azure Active Directory



3. In the Navigation pane, select **App registrations**.

Figure 11-2: App registrations



4. Click **New registration**.

Figure 11-3: New registration

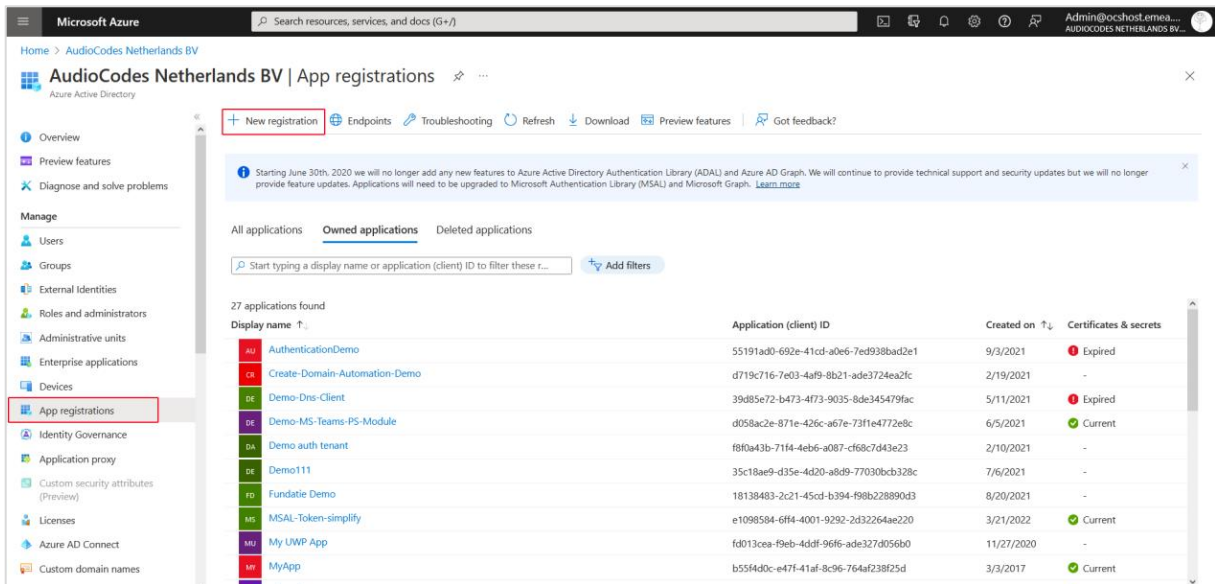


Figure 11-4: Register an Application

Microsoft Azure

Home > AudioCodes Netherlands BV > Register an application

* Name
The user-facing display name for this application (this can be changed later).
Demo-MS-Teams-PS-Module

Supported account types
Who can use this application or access this API?
 Accounts in this organizational directory only (AudioCodes Netherlands BV 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.
 Select a platform | e.g. https://example.com/auth

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

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

Register

5. Enter the following details:
 - **Name:** App registration name
 - **Select account type:** Accounts in any organizational directory (Any Azure AD directory - Multitenant)
6. Click **Register**.
7. Navigate to the **Overview** page.
8. Copy the Application (client) ID value to notepad as its required later in the configuration.

Figure 11-5: New Registration

Microsoft Azure

Home > AudioCodes Netherlands BV > Demo-MS-Teams-PS-Module

Search (Ctrl+F) | Delete | Endpoints | Preview features

Overview

Quickstart

Integration assistant

Manage

- Branding & properties
- Authentication
- Certificates & secrets
- Token configuration
- API permissions
- Expose an API
- App roles
- Owners
- Roles and administrators
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

Essentials

Display name	: Demo-MS-Teams-PS-Module	Client credentials	: Add a certificate or secret
Application (client) ID	: XXXXX-XXXX-XXXX-XXXX	Redirect URIs	: Add a Redirect URI
Object ID	: XXXXX-XXXX-XXXX-XXXX	Application ID URI	: Add an Application ID URI
Directory (tenant) ID	: XXXXX-XXXX-XXXX-XXXX	Managed application in L...	: Demo-MS-Teams-PS-Module

Supported account types: [Multiple organizations](#)

Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? [Learn more](#)

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

Starting November 9th, 2020 end users will no longer be able to grant consent to newly registered multitenant apps without verified publishers. [Add MPN ID to verify publisher](#)

Get Started | Documentation

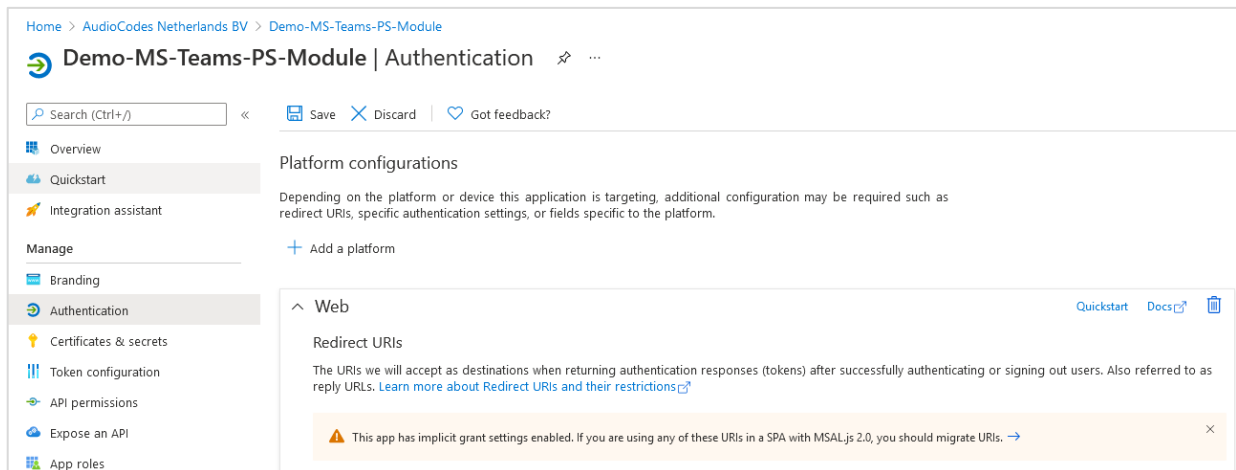
Build your application with the Microsoft identity platform

The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create modern, standards-based authentication solutions, access and protect APIs, and add sign-in for your users and customers. [Learn more](#)

9. Click the **Add a Redirect URI** link to add the Redirect URI.

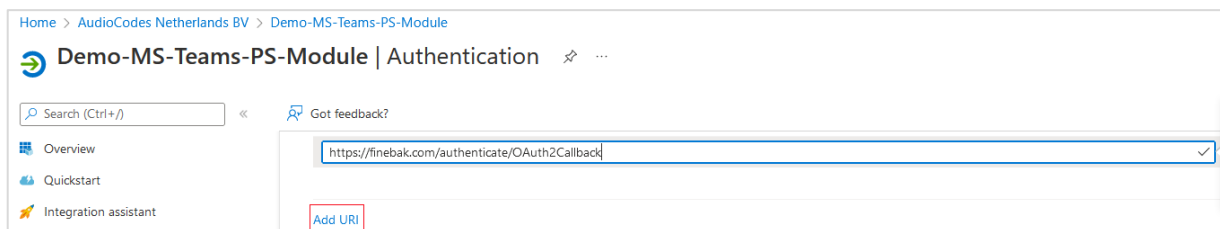
The Authentication screen is displayed.

Figure 11-6: Authentication



10. Under Platform configurations/Redirect URIs, click **Add URI**.

Figure 11-7: Add URI



11. Enter the HTTPS URI of the UMP installation VM (e.g. `https://finebak.com/authenticate/OAuth2Callback`)

where:

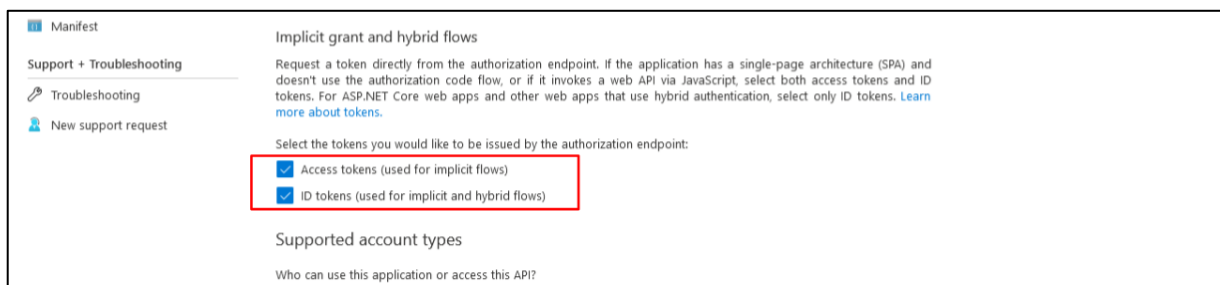
- “Finebak.com” is the FQDN of the Azure Virtual Machine where UMP is installed
- “OAuth2Callback” is the name of the token authentication page inside the registered application

12. Copy the URI to notepad as it is required later in the configuration.

13. Under Implicit grant and hybrid flows, select the following check boxes:

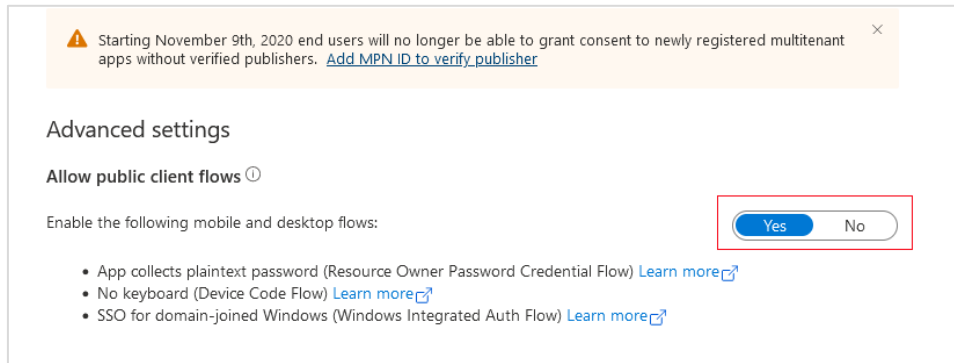
- Access tokens (used for implicit flows)
- ID tokens (used for implicit and hybrid flows)


Figure 11-8: Select Tokens



14. Under Advanced Settings, set to **Yes**.

Figure 11-9: Enable Mobile and Desktop Flows



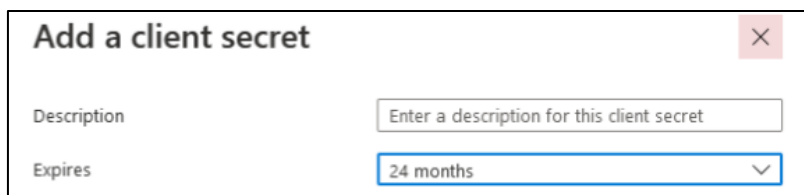
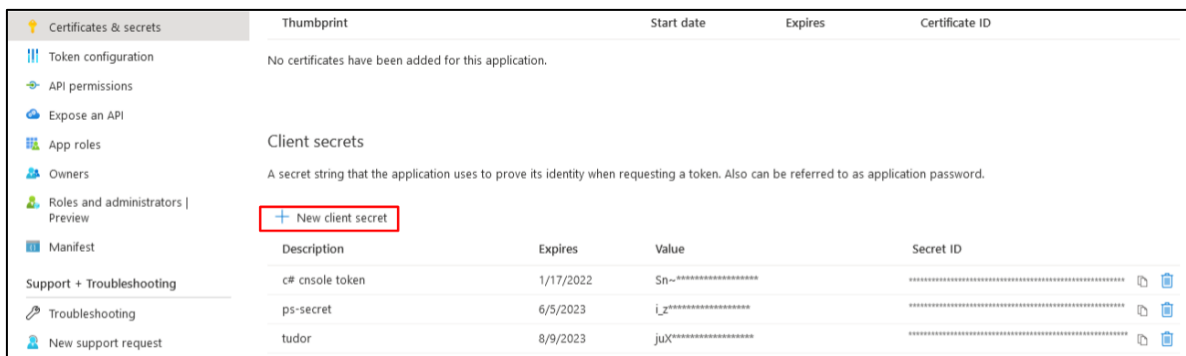
 Verify the MPN ID to ensure that the Consent dialog will automatically be set as a trusted application.

15. Click **Save** to apply changes.



16. In the Navigation pane, select **Certificates & Secrets** and then click **New Client secret**.

Figure 11-10: New Client Secret



17. Enter Description, set Expires to **24 months** and then click **Add**.

18. Copy the newly generated secrets' value to notepad.

Figure 11-11: Copy Client secret Value

Thumbprint	Start date	Expires	Certificate 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	Secret ID
c# console token	1/17/2022	Sn~*****	*****
ps-secret	6/5/2023	i_z*****	*****
tudor	8/9/2023	juX*****	*****
Key for UMP Token	8/10/2023	~h7*****	*****

19. In the UMP Main Tenant interface, open the Auth Tokens page (**Security > Auth Tokens**) and do the following:
 - Paste the Application (client) ID (see Step 8) and Client secret value to the respective fields.
 - Enter the Redirect URI that you configured in Step 911. For example <https://finebak.com/authenticate/OAuth2Callback>
20. Click **Apply Changes**.

Figure 11-12: AuthToken

AuthToken
Manage Authentication Tokens

Client Id

Client Secret

RedirectUri

Reload Verify All Update Used By

M365 Administrator	When Regenerated	Last Used	Used By Customer	Last Verification Status	Actions
admin@M365x52060359.onmicrosoft.com	April 11th 2022, 10:41	April 11th 2022, 10:41	tobi	✓	Verify Clear Send Invite

Showing 1 to 1 of 1 entries

Previous **1** Next

11.1 Assigning Administrator Roles to Customer IT Administrator

The following administrator roles must be granted to the Customer IT administrator who grants consent to the Service Provider operator to connect to their Microsoft 365 platform:

- Teams Admin
- Skype for Business Admin
- Application Administrator



These permissions are required because the background replication with the token or username password connects to Azure with the PowerShell connection string shown below:

```
connect-azuread -MsAccessToken $tokens.Item1 -AadAccessToken $tokens.Item3 -AccountId $m365username
```

To assign administrator roles:

1. Sign-in to the customer tenant with Admin permissions.
2. In the Users screen, choose the user who will have the role to grant consent in the organization.

Figure 11-13: Choose User

The screenshot shows the Microsoft Azure portal interface for the 'AudioCodes Netherlands BV' tenant. The main content area is titled 'Users | All users' and displays a table of users. The table has the following columns: Name, User principal name, User type, Directory synced, Account enabled, Identity issuer, Company name, and Creation type. Two users are listed:

Name	User principal name	User type	Directory synced	Account enabled	Identity issuer	Company name	Creation type
mike o' brian	mike.o'brian@OCSHOS...	Member	No	Yes	OCSHOST.onmicrosoft.cor		
TeamsITUser	TeamsITUser@ocshost.o...	Member	No	Yes	OCSHOST.onmicrosoft.cor		

The 'TeamsITUser' row is selected, indicated by a blue checkmark in the first column. The left sidebar contains navigation options such as 'All users', 'Deleted users', 'Password reset', 'User settings', 'Diagnose and solve problems', 'Activity', 'Sign-in logs', 'Audit logs', 'Bulk operation results', 'Troubleshooting + Support', and 'New support request'.

Figure 11-14: Teams User

The screenshot shows the Microsoft Azure portal interface for the user **TeamsITUser** (User Principal Name: TeamsITUser@ocshost.onmicrosoft.com). The navigation pane on the left is expanded to show the **Assigned roles** tab, which is highlighted with a red box. The main content area displays the user's profile, including a red circular profile picture with the initials 'TE', a 'User Sign-ins' chart showing activity from Mar 13 to Apr 3, and a table of identity information. The identity table includes fields for Name (TeamsITUser), First name (Brian), Last name (Brown), User Principal Name (TeamsITUser@ocshost.onmicrosoft.com), User type (Member), Object ID (2f807c26-80cb-461c-9b82-7b5d6493b99e), and Issuer (OCSSHOST.onmicrosoft.com). A 'Job info' section is partially visible at the bottom.

3. In the Navigation pane, select **Assigned Roles**.

Figure 11-15: Assigned Roles

The screenshot shows the Microsoft Azure portal interface for the user **TeamsITUser** under the **Assigned roles** section. The navigation pane on the left is expanded to show the **Assigned roles** tab, which is highlighted with a red box. The main content area displays the 'Administrative roles' section, which is currently empty. A table with columns for Role, Description, Resource Name, Resource Type, Assignment Path, and Type is shown, but it contains no data. The '+ Add assignments' button is highlighted with a red box.

4. Click **Add assignments**.

Figure 11-16: Teams administrator

Directory roles ✕

↑ Sort

i To assign custom roles to a user, your organization needs Azure AD Premium P1 or P2.

Choose admin roles that you want to assign to this user. [Learn more](#)

teams ✕ + Add filters

<input checked="" type="checkbox"/>	Teams administrator	Can manage the Microsoft Teams service.
<input type="checkbox"/>	Teams communications administrator	Can manage calling and meetings features within the Microsoft Teams service.
<input type="checkbox"/>	Teams Communications Support Engineer	Can troubleshoot communications issues within Teams using advanced tools.
<input type="checkbox"/>	Teams Communications Support Specialist	Can troubleshoot communications issues within Teams using basic tools.
<input type="checkbox"/>	Teams devices administrator	Can perform management related tasks on Teams certified devices.

Add

5. Add admin role “Teams administrator”.
6. Add admin role “Skype for Business Administrator”.

Figure 11-17: Skype for Business administrator

Directory roles

↑ Sort

i To assign custom roles to a user, your organization needs Azure AD Premium P1 or P2.

Choose admin roles that you want to assign to this user. [Learn more](#)

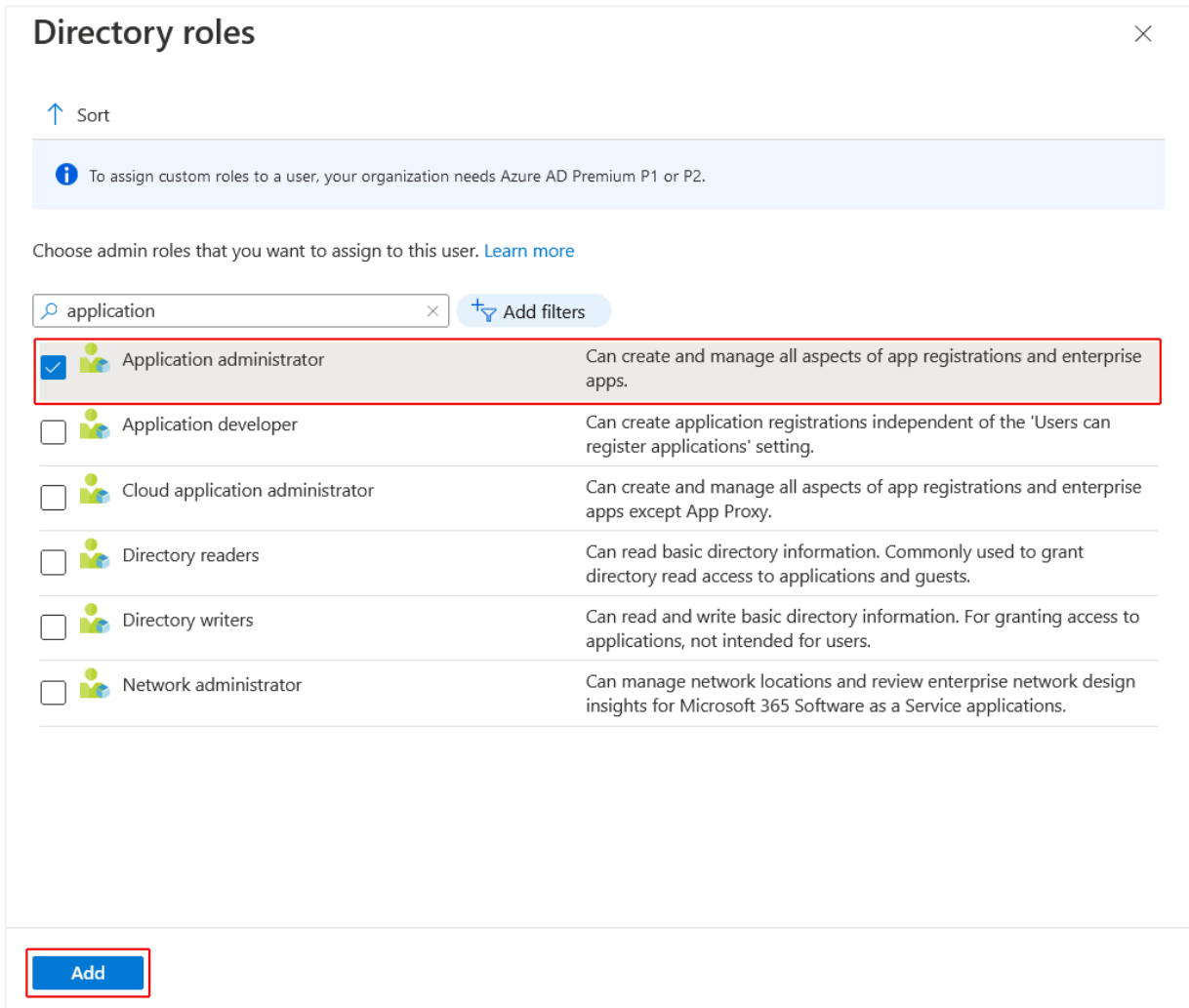
skype Add filters

<input checked="" type="checkbox"/>	Skype for Business administrator	Can manage all aspects of the Skype for Business product.
-------------------------------------	----------------------------------	-----------------------------------------------------------

Add

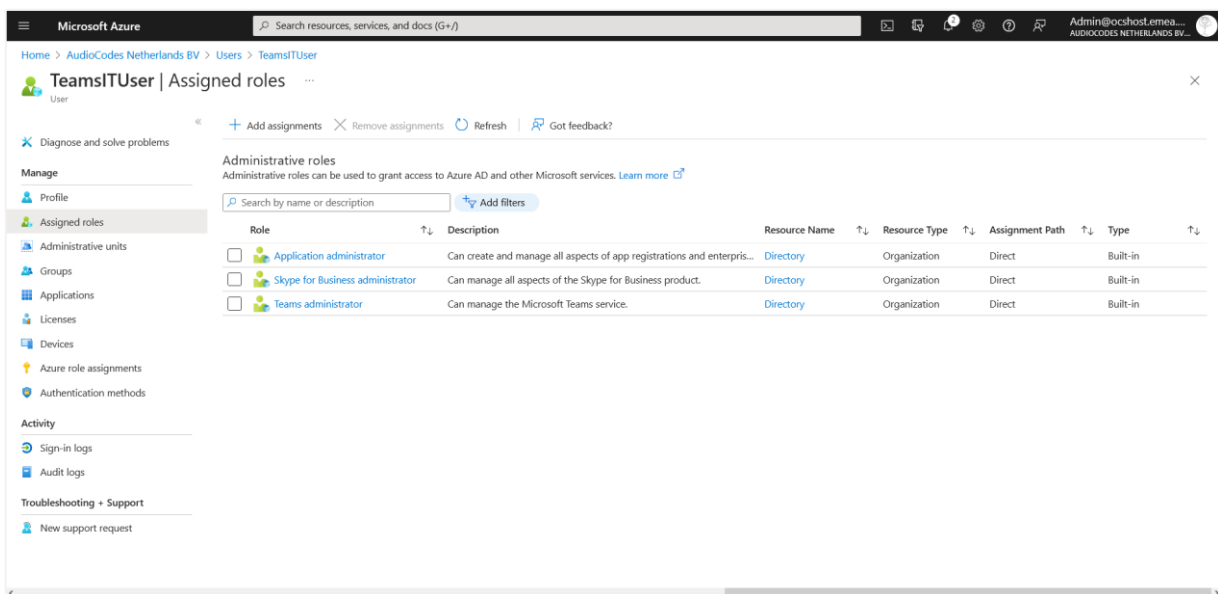
7. Add admin role "Application Administrator".

Figure 11-18: Application administrator



The following screen shows all added admin roles.

Figure 11-19: Assigned Admin Roles



12 Configure Invitation Settings

This step describes how to define Invitation Settings for requesting consent from customer IT administrators using the token authentication mechanism (See Section 30.5) to connect to their Microsoft 365 platform. The Invitation Settings define the template email that is sent to the customer administrator including the customer's name defined in the Onboarding wizard, the name of the Service Provider operator tenant who added the customer and the Invitation URL. This URL includes the subdomain name that was defined in Chapter 9. Once the invitations have been sent to the customer IT administrator, the outgoing request details can be viewed in the Customer Invitations screen in the Multitenant portal (see Section 25.2).

Do the following:

1. Login to the UMP Main Tenant interface with Windows UMP Service account created in Section 6.3.
2. In the UMP SP Main Tenant open the Invitation Settings page (**System > Invitation Settings**).

Figure 12-1: Invitation Settings

The screenshot shows the 'Invitation Settings' page in the UMP interface. The page has a dark sidebar on the left with navigation options like 'Tenants', 'System', 'License', 'Invitation Settings', 'Email Settings', 'Script Templates', 'DNS API Configuration', 'Security', 'SBC List', and 'Queued Tasks'. The main content area is titled 'Invitation Settings' and contains three main sections:

- Invitation Subject ***: A text input field containing the text: "Welcome {{CustomerId}} for joining the Finebak 'AudioCodes UMP-365 for Service Providers' service".
- Invitation Email ***: A text area containing a template email:


```
Dear Administrator of {{CustomerId}}.

We at Finebak welcome you to join our "AudioCodes UMP-365 for Service Providers" service.
Please activate your tenant by connecting to the link below and authenticate with your M365 UC Administrator account:
{{CustomerAuthenticationPortalUri}}/{{InvitationId}}

Please Note:
- UC admin role requirements:
```
- Customer Authentication Portal Uri ***: A text input field containing the URL: "https://finebak.com/authenticate".

At the bottom of the form, there is an 'Apply Changes' button. The footer of the page reads: 'Copyright © 2020 AudioCodes. All rights reserved.'

3. Enter the following details:
 - Invitation Subject: Edit the email invitation.
 - Invitation Email: Edit the email content
 - Invitation Subject and Invitation Email include the follow place holders
 - {{CustomerId}} – The CustomerID, Unique per Customer Name (from onboarding new customer flow)
 - {{CustomerAuthenticationPortalUri}}/{{InvitationId}} – unique invitation (Customer Authentication Portal Url / InvitationId)
4. In the Customer Authentication portal URL field define a public Portal URL for the provider.
For Example: https://finebak.com/authenticate

Create a DNS A record for domain. For example, **Finebak.com** to a Public IP xxx.xxx.xxx.xxx (UMP – IP address).

See example email below.

Figure 12-2: Example Email

Dear Administrator of {{CustomerId}},

We at Finebak welcome you to join our "AudioCodes UMP-365" service.

Please activate your tenant by connecting to the link below and authenticate with your M365 UC Administrator account:

{{CustomerAuthenticationPortalUrl}}/{{InvitationId}}

Please Note:

- UC admin role requirements:
 - Teams Admin
 - Skype for Business Admin
 - Application Administrator
- The Authentication process will run against your Microsoft M365 Tenant, we will not know or save your password.
- Revoke Token Authentication: you are able to revoke the authentication at any time. Revoking the authentication will stop the service.

Thank you and best regards,

Finebak Support Team

This email and any files transmitted with it are confidential material. They are intended solely for the use of the designated individual or entity to whom they are addressed. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, use, distribution or copying of this communication is strictly prohibited and may be unlawful.

If you have received this email in error please immediately notify the sender and delete or destroy any copy of this message

13 Configure Email Settings

This step describes how to define the email server settings for sending the invitation requests (configured in Chapter 12) to the customer IT administrator for connecting to the Multitenant portal.

Do the following:

1. In the UMP SP Main Tenant open the Email Settings page (**System > Email Settings**).

Figure 13-1: Email Server Settings

The screenshot shows the 'Email Server Settings' page in the UMP SP Main Tenant. The page has a dark sidebar on the left with a navigation menu. The main content area is white and contains the following fields:

- From ***: LTC_Support@audio-codes.co.il
- Username**: apikey
- Password already saved**: (empty)
- ConfirmPassword**: (empty)
- Host ***: smtp.sendgrid.net
- Port ***: 587
- EnableSsl**:
- Network**: (dropdown menu)
- Apply Changes**: (button)

2. Enter the following details:
 - From: Sender email
 - Username: Your email server account/username
 - Password: Email server account Password / API key
 - Confirm Password
 - Host: SMTP server
 - Port: SMTP server / port
 - Enable SSL: True
 - Select Network
3. Click **Apply Changes**.

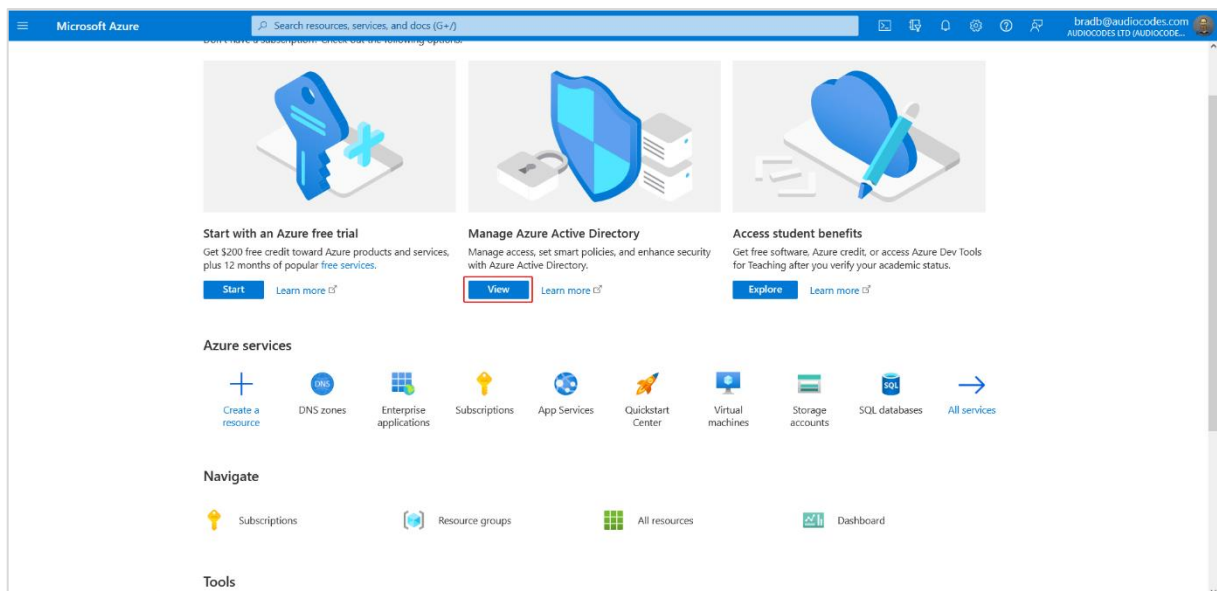
14 App Registration for Customer Admins

The Customer Admins App Registration enables the Azure sign-on for end user customer IT administrators (see Section 33.2). Once this registration is complete, the Application (Client) ID must be added in the Customer Admins screen in the Main Tenant interface. When the customer IT administrator logs into UMP-365, they can then view their Microsoft 365 tenant.

Do the following:

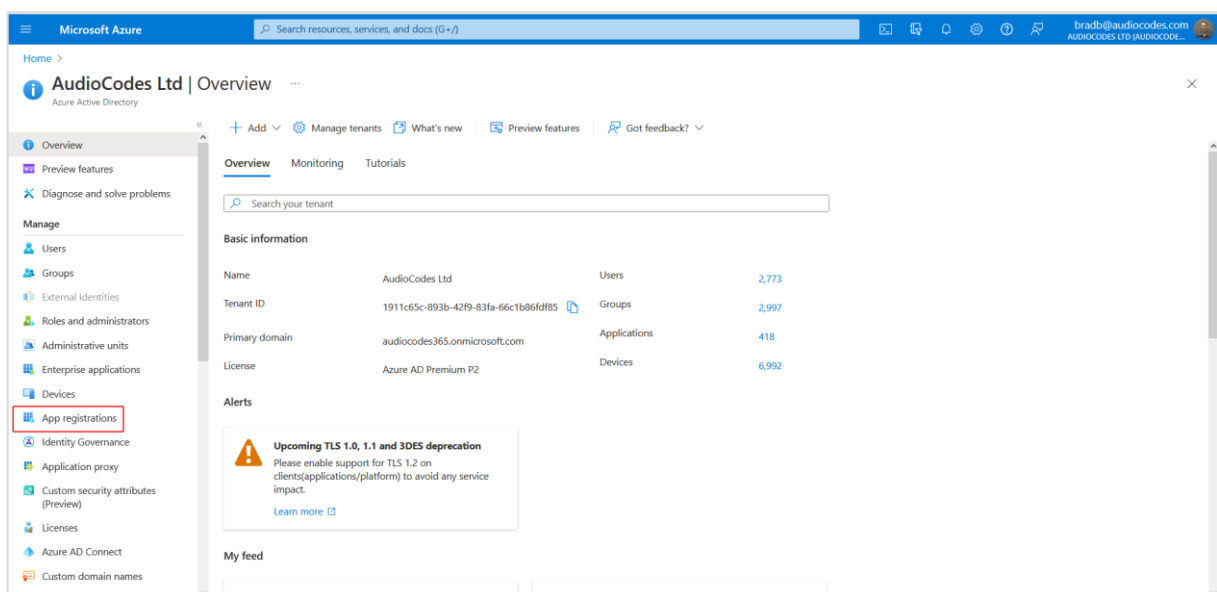
1. Sign-in to the Azure portal for the Service Provider operator tenant with Admin permissions.
2. Under Manage Azure Active Directory, select **View**.

Figure 14-1: View Azure Active Directory



3. In the Navigation pane, select **App registrations**.

Figure 14-2: App registrations



4. Click **New registration**.

Figure 14-3: New registration

The screenshot shows the 'App registrations' page in the Microsoft Azure portal. The 'New registration' button is highlighted with a red box. Below the navigation pane, a table lists 27 applications with columns for Display name, Application (client) ID, Created on, and Certificates & secrets.

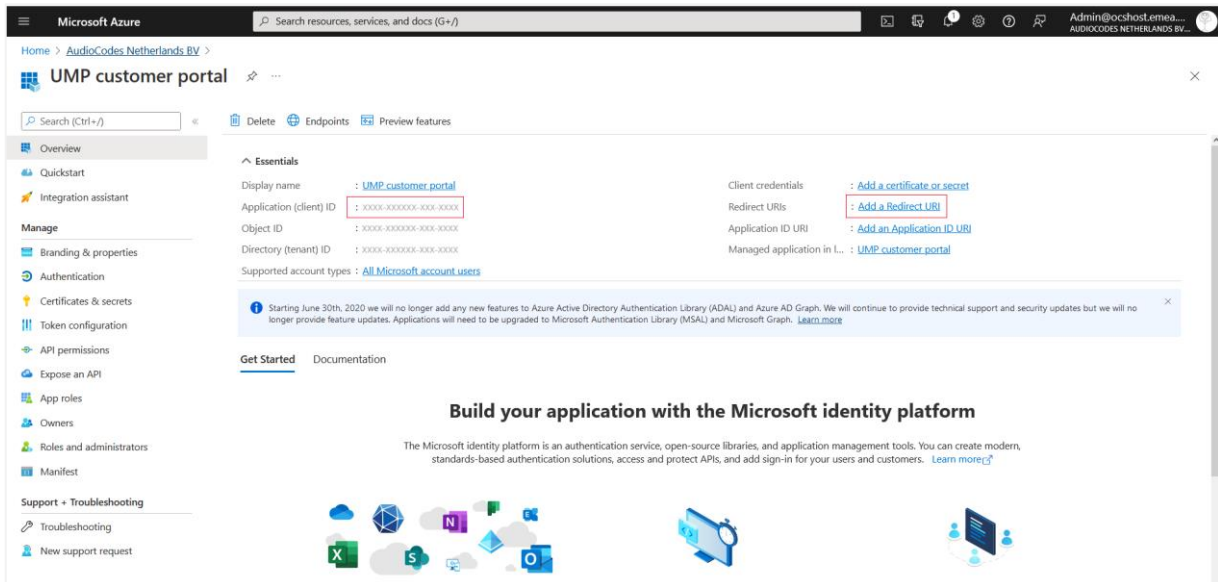
Display name	Application (client) ID	Created on	Certificates & secrets
AuthenticationDemo	55191ad0-692e-41cd-a0e6-7ed938bad2e1	9/3/2021	Expired
Create-Domain-Automation-Demo	d719c716-7e03-4af9-8b21-ade3724ea2fc	2/19/2021	-
Demo-Dns-Client	39d85e72-b473-4f73-9035-8de345479fac	5/11/2021	Expired
Demo-MS-Teams-PS-Module	d058ac2e-871e-426c-a67e-7311e4772e8c	6/5/2021	Current
Demo auth tenant	f8f0a43b-7114-4eb6-a087-d68c7d43e23	2/10/2021	-
Demo111	35c18ae9-d35e-4d20-a8d9-77030bcb328c	7/6/2021	-
Fundatie Demo	18138483-2c21-45cd-b394-f98b228890d3	8/20/2021	-
MSAL-Token-simplify	e1098584-6ff4-4001-9292-2d32264ae220	3/21/2022	Current
My UWP App	fd013cea-f9eb-4ddf-96f6-ade327d056b0	11/27/2020	-
MyApp	b55f4d0c-e47f-41af-8c96-764af238f25d	3/3/2017	Current

Figure 14-4: New App Registration

The screenshot shows the 'Register an application' page in the Microsoft Azure portal. The 'Name' field is filled with 'UMP customer portal'. The 'Supported account types' section has 'Accounts in any organizational directory (Any Azure AD directory - Multitenant)' selected. The 'Register' button is highlighted with a red box.

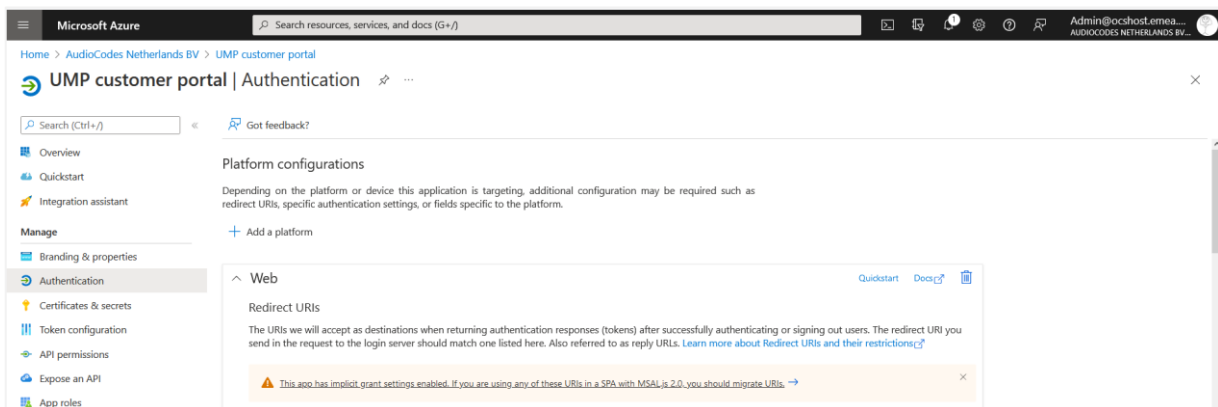
5. Enter the following details:
 - **Name:** App registration name
 - **Select account type:** Recommendation - Accounts in any organizational directory (Any Azure AD directory - Multitenant)
6. Click **Register**.
The new registration is created.
7. Navigate to the Overview page and copy the Application (client) ID to notepad (it must be configured later in this procedure).

Figure 14-5: Redirect URI's



- Click the **Add a Redirect URI** link to add the WEB redirect URI for the provider's public portal. The Authentication screen is displayed.

Figure 14-6: Authentication Screen



- Click **Add URI** and add the Public Portal DNS subdomain name for the provider that you defined in Chapter 9 with the appended string `"/tenantui/signin-aad"` as shown in the example figure below.

Figure 14-7: Add URI



- Scroll down the screen and enable the Implicit grant and hybrid flows; select the following tokens to be issued by the authorization endpoint:
 - Access tokens (used for implicit flow)
 - ID tokens (used for Implicit and hybrid flows)

Figure 14-8: Implicit Grant Flow

https://finebak.com/tenantui/signin-aad ✓

Add URI

Front-channel logout URL

This is where we send a request to have the application clear the user's session data. This is required for single sign-out to work correctly.

Implicit grant and hybrid flows

Request a token directly from the authorization endpoint. If the application has a single-page architecture (SPA) and doesn't use the authorization code flow, or if it invokes a web API via JavaScript, select both access tokens and ID tokens. For ASP.NET Core web apps and other web apps that use hybrid authentication, select only ID tokens. [Learn more about tokens.](#)

Select the tokens you would like to be issued by the authorization endpoint:

Access tokens (used for implicit flows)

ID tokens (used for implicit and hybrid flows)

Save Discard

11. Click **Save** to apply changes.
12. In the UMP-365 Main Tenant interface, open the Customer Admins page (**Security > Customer Admins**).
13. In the App Registration Application (Client) ID field, paste the value that you saved in Step 7 and then click **Save**.

Figure 14-9: Paste the Application (client) ID Value

App Registration Application (Client) ID: Save

Show 10 entries Search:

Id	Customerid	Account
64	M365x202362	AlexW@M365x202362.OnMicrosoft.com
66	essentials	admin@oachost.emea.microsoftonline.com
67	M365x202362	isaiah@m365x202362.onmicrosoft.com

Showing 1 to 3 of 3 entries Previous Next

14. Open PowerShell and type the following command:

```
iisreset [enter]
```

Figure 14-10: PowerShell

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\umpadmin> iisreset

Attempting stop...
Internet services successfully stopped
Attempting start...
Internet services successfully restarted
PS C:\Users\umpadmin>
```

15 Configure License

UMP365 supports the follow licensing schemes:

- **Tenant License:** Tenants license includes the following features support:
 - Quick Connect
 - Tenant Online voice routing
 - User view only
- **User License:** User license includes the following features support:
 - User MACD (Teams, and Voice policies)
 - Lifecycle management
 - Create and Edit Templates
 - DID management
 - Support Microsoft Teams
 - Support OneDrive policies (Future)
 - Manage emergency call Routing (Future)
- A Tenant License is mandatory requirement for Onboarding a new customer M365 Tenant and for managing the Voice Routing.



A User License is not mandatory. The provider can offer this service as an upscale service for selected customers (M365 Tenant).

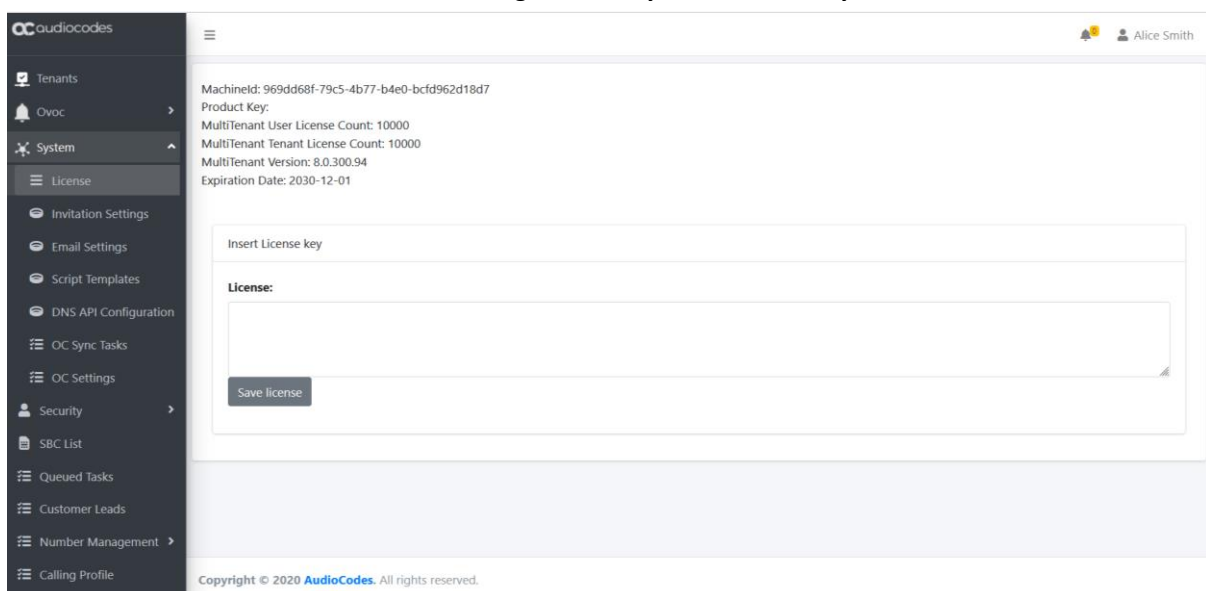
15.1 Installing the UMP 365 License

This section installs the UMP 365 license.

To configure the license:

1. In the UMP Main Tenant interface, open the License page (**System > License**) and extract the Machine ID.

Figure 15-1: System/License Key View



2. Activate your product through the AudioCodes License Activation tool at <http://www.audiocodes.com/swactivation>. You need your Product Key and Fingerprint (MachineID) for this activation process. An e-mail will subsequently be sent to you with your Product License.
3. Insert License Key and save.
4. Save License.

This page includes the follow information:

- MachineID – required for the license generator tool
- MultiTenant User License Count: # of Users License, Pool License between the Customers Tenant
- MultiTenant Tenant License Count: # of Tenants Licenses
- MultiTenant Version: SW Version
- Expiration Date

The 'Product Key' is a unique key that represents the UMP 365 / CloudBond 365 initial order and is used for online license generation. The 'Product Key' is used for future orders for the same system, such as a license upgrade.

When the maximum number of licensed users has been reached, a pop-up window appears on the individual user edit page indicating that there are no more licenses remaining. Previously edited users can still be edited.



Warning: When the maximum number of licensed users has been reached, it is no longer possible to automatically add users through Lifecycle management, nor is it possible to import users or onboard new Tenants (Tenant license). The license should be allocated based on the total number of users in the Active Directory.

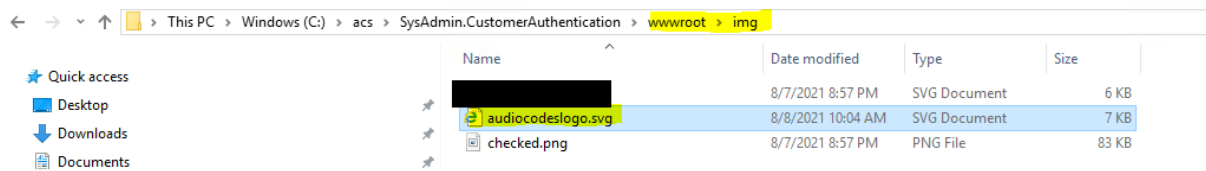
16 Update Service Provider Logos

This step describes how to replace the logo that appears in the Token Invitation wizard.

Do the following:

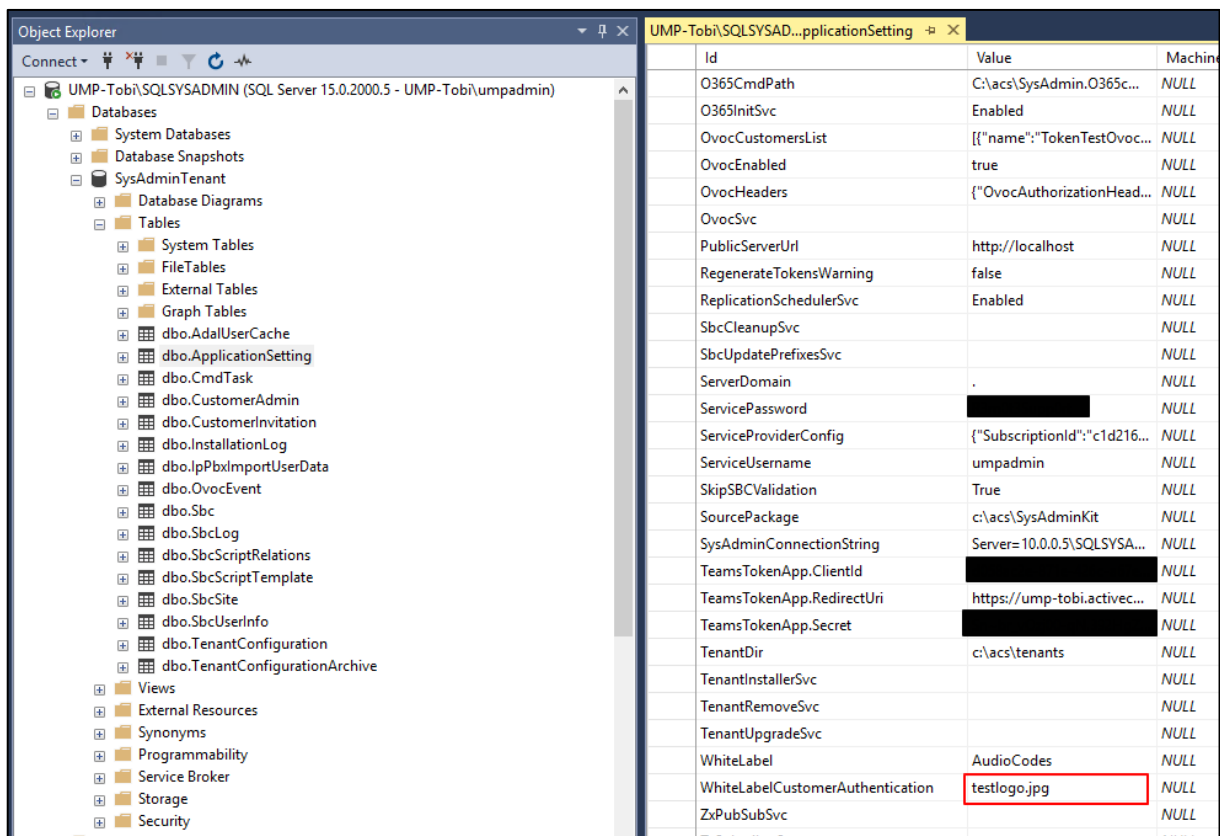
1. Update the customer logo image in the following folder:
 ..\acs\SysAdmin.CustomerAuthentication\wwwroot\img

Figure 16-1: Update Logo



2. Open the SQL database dbo.ApplicationSettings table and update parameter WhiteLabelCustomerAuthentication with the customer logo image:

Figure 16-2: SQL Updates



17 Secure UMP Interface Connection with OVOC and SBC

This section describes how to setup the connection between the UMP Web interface and the OVOC and UMP on Azure. Connection to the OVOC Server on Azure can be established using one of the following methods:

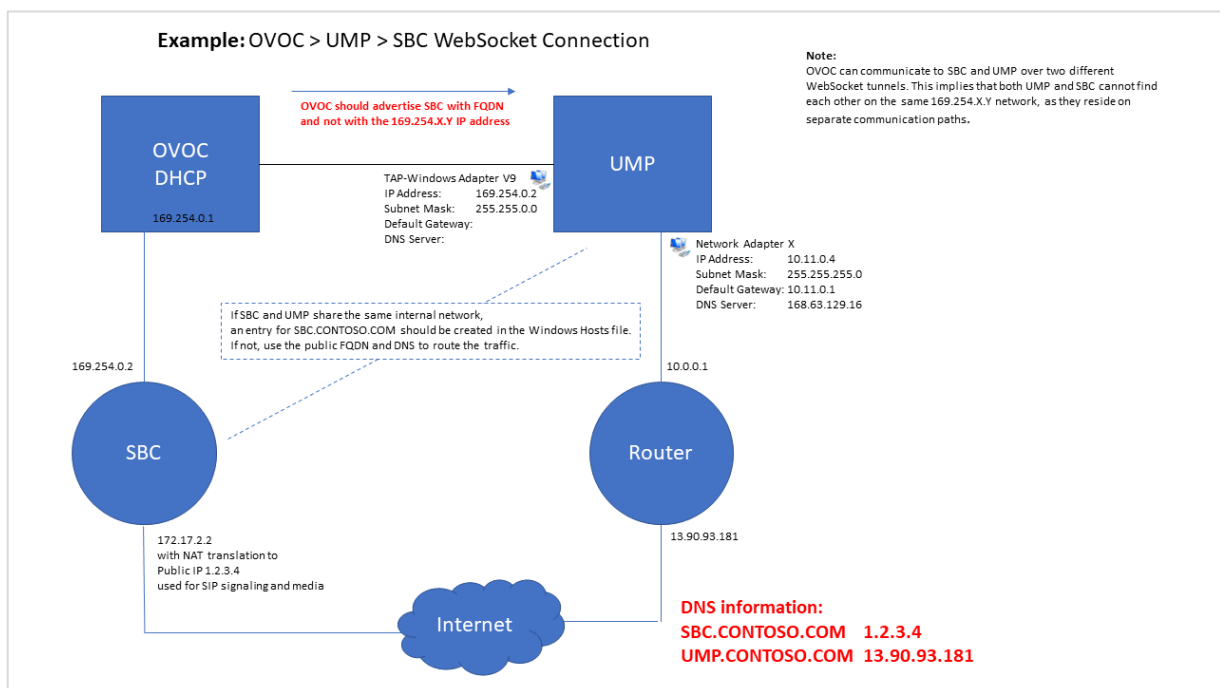
- OVOC Azure Public IP over WebSocket Tunnel (Cloud Architecture Mode). See Section 17.1.
- OVOC Azure Public IP over HTTPS SSL certificate with mutual authentication. See Section 017.2.
- OVOC Azure Private IP. See Section 17.3.



The SSO Connection to the UMP on Azure is always established using the Private IP of UMP on Azure.

The figure below illustrates the OVOC > UMP > SBC WebSocket connectivity architecture.

Figure 17-1: WebSocket Connection Architecture



17.1 Configure UMP Interface for WebSocket Tunnel (Cloud Architecture Mode)

This section describes how to secure the connection to the OVOC server public IP address using WebSocket tunnel.

Do the following:

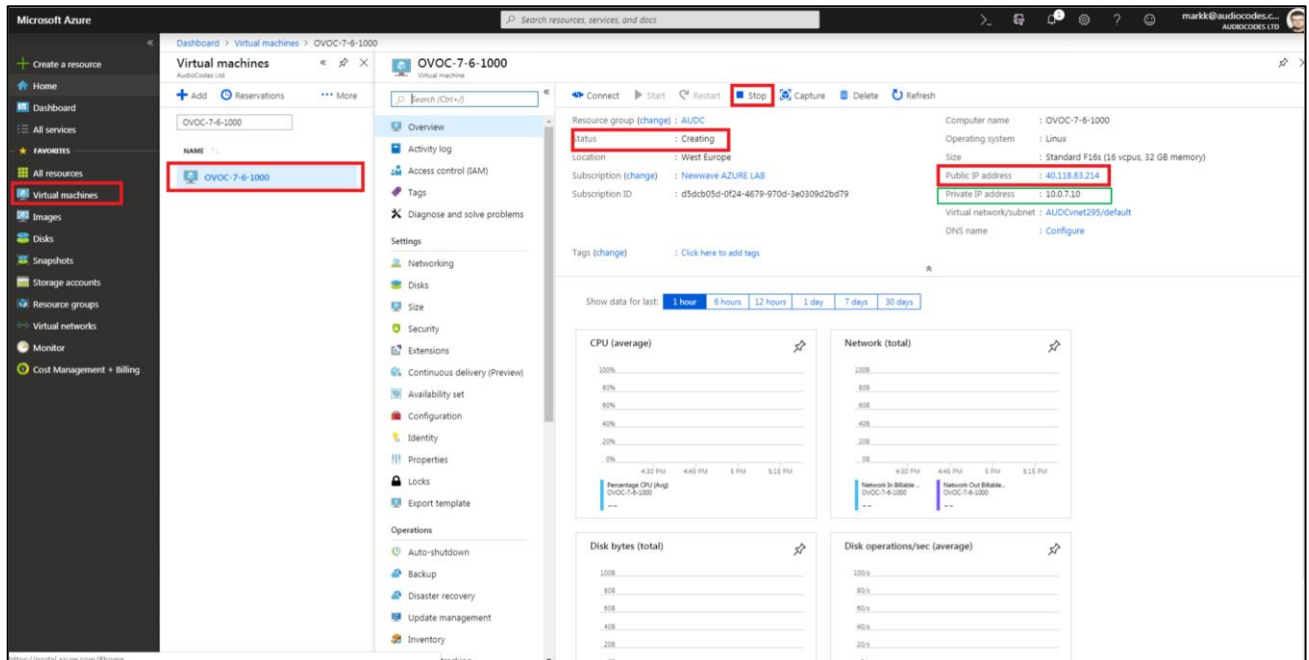
1. In the UMP Multi-Tenant GUI, open the OVOC Settings page (**System Configuration > OVOC Settings**).

Figure 17-2: OVOC Settings with Public IP

2. Select the Use Public IP checkbox to connect to the public IP address of the OVOC server on Azure.
3. In the Public IP Address, enter the Public IP address of OVOC on Azure.
4. In the Public User field, enter the Username for connecting to OVOC WebSocket Tunnel. Default: VPN
5. In the Public Password field, enter the Password for connecting to OVOC WebSocket Tunnel (Cloud Architecture Mode only). Default: 123456 (note that after initial connection is established, you can change this password and add new users to manage this connection, see below).

The figure below shows where to extract the OVOC server IP address on Azure.

Figure 17-3: OVOC on Azure



6. Enter Trap Port: 162
7. Enter Keep Alive Port: 1161
8. Select **SNMPv2** and in the Community Read and Community Write fields enter **public**
9. Uncheck the 'SBC monitor' flag.
10. Enter the following System Settings:
 - System Name
 - Location
11. For the **Login URL** (used for logging in to UMP from UMP Device Page in OVOC and REST connection initiated from OVOC): Enter the **Private IP address** of the UMP on Azure and not its Public IP address/FQDN (e.g. <http://127.0.0.1/tenantui>).



Once the initial Single Sign-on connection to the UMP VM is established, the "Login Url" field is automatically updated to <http://169.254.x.x> ; **do not change this value.**

12. Click Apply Changes.

17.1.1 Configure WebSocket Tunnel (Cloud Architecture Mode) on OVOC

This option configures the OVOC server in Cloud Architecture mode (WebSocket tunnel). When configured, a "secure tunnel" overlay network" is established between the connected devices and the OVOC server. This connection is secured over a WebSocket connection. The Tunnel Status indicates the status for all sub-processes running for this architecture.



- It's recommended to add new users to manage this connection (see below).
- It's recommended to change the default password for this connection (see below).

Do the following:

1. Login into the OVOC server by SSH, as 'acems' user and enter password *acems*.
2. Switch to 'root' user and provide root password (default password is root):

```
su - root
```
3. Type the following command:

```
# EmsServerManager
```
4. From the Network Configuration menu, choose **Cloud Architecture**.

Figure 17-4: Cloud Architecture

```

Main Menu > Network Configuration > Cloud Architecture
-----
Cloud Architecture Status:      ENABLED
Tunnel Interface:               eth0 (main)
Tunnel Status:                  UP
>1. Disable Cloud Architecture  (The server will be rebooted)
 2. Add new user
 3. Edit user password
  b. Back
  q. Quit to main Menu

```

5. Select option Enable Cloud Architecture.
6. Select the IPv4 interface for which to enable this mode and then press Enter.

Figure 17-5: Choose IP Interface

```

Choose Interface:
1) ens160 (main) IPv4
2) ens192 IPv6
3) ens256 IPv4
4) ens224 IPv4
5) Quit
: █

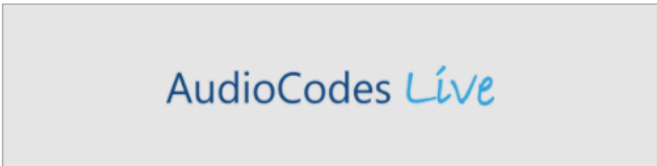
```

The OVOC server is restarted.

7. In the OVOC Web interface, ensure that device and tenant connections are enabled for HTTPS (default).
8. In the OVOC Web interface, ensure that the SBC Devices Communication parameter is set to "IP Based" (**System** menu > **Administration** tab > **OVOC server** folder > **Configuration**).

Figure 17-6: OVOC Hostname-IP-based

GENERAL SETTINGS

OVOC Hostname	<input type="text" value="tlc-ovoc.trunkpack.com"/>
Description	<input type="text" value="Audiocodes"/>
SBC Devices Communication	<input type="text" value="IP Based"/>
Privacy Mode	<input type="checkbox"/>
Global Logo	<input type="text" value="globalLogo.png"/>
	
Service Request URL	<input type="text" value="https://acext1--tst2.custhelp.com/ci/pta/login/redirect_to/app/account/q"/>
Service Request Password	<input type="password" value="....."/>

[Submit](#)



If this parameter is set to "Hostname Based" and the Cloud Architecture feature is enabled in the OVOC Server Manager, then the connected SBC devices cannot be managed for this OVOC instance.

9. Verify that the DNS resolves for the OVOC FQDN is successful, for example Google.com:

```
C:\Users\enterpriseluser>nslookup www.google.com
Server: tlc-ovoc.trunkpack.com
Address: 10.1.1.10
Non-authoritative answer:
Name: www.google.com
Addresses: 2a00:1450:4006:801::2004
          172.217.18.36
```

10. In the OVOC Server Manager install Custom Certificates (see Section "Server Certificates Updates").

17.1.1.1 Add WebSocket Tunnel User

This procedure describes how to create new WebSocket tunnel users.

Do the following:

1. Select option **2 Add New User**.
2. Create new Cloud Architecture User.
3. Enter the name of the new user and the password.

17.1.1.2 Change the WebSocket Tunnel Default Password

This procedure describes how to change the default WebSocket Tunnel password.

Do the following:

1. Select Option 3 Edit User Password.
2. Edit User Password.
3. Select the desired user whose password you wish to change and confirm.
4. Enter the new password and confirm.

17.1.2 Configure SBC

This section describes the actions to perform on the SBC

Do the following:

1. Install SSL certificates on managed SBC devices (refer to *Section Install Custom Certificates on OVOC Managed Devices in the IOM manual*). You must define two TLS contexts, one for the UMP-365 Management connection and one for the Microsoft Teams connection (Wildcard certificate) i.e. a separate TLS context must be defined for each service provider.

Figure 17-7: TLS Context-UMP-365 Management

⊕ TLS Context [#0] > Certificate Information

PRIVATE KEY

Key size:	2048 bits
Status:	OK

CERTIFICATE

Certificate:
 Data:
 Version: 3 (0x2)
 Serial Number:
 5d:05:f2:e8:77:f3:d9:5c:b9:03:95:f2:6d:13:c3:38
 Signature Algorithm: sha256WithRSAEncryption
 Issuer: C=IL, O=Domain The Net Technologies Ltd, CN=Domain The Net Technologies Ltd CA for SSL R2
 Validity
 Not Before: Aug 29 14:44:08 2021 GMT
 Not After : Aug 29 14:44:08 2022 GMT
 Subject: CN=customers.audio-code.co.il
 Subject Public Key Info:
 Public Key Algorithm: rsaEncryption
 RSA Public-Key: (2048 bit)
 Modulus:
 00:e5:70:02:b6:fd:74:56:c6:be:ef:ac:84:36:b0:
 e4:bc:47:8f:73:3a:71:30:33:10:68:41:7f:f6:e4:
 6f:a8:ff:9b:ee:3d:83:53:a6:f6:7b:4d:3b:42:48:
 41:33:9f:da:9f:12:9e:79:c2:e0:73:88:5d:39:e0:
 3d:94:a8:11:b7:66:93:41:0f:49:e9:4e:c9:7a:d4:
 71:91:cd:49:6e:c1:ce:05:4c:8b:1c:7e:1b:67:4b:
 99:d3:32:dd:7f:29:25:97:1c:68:cf:7d:e8:d9:3f:
 2e:a8:a1:cd:8c:5f:22:6f:f0:85:a8:ca:9f:14:90:
 75:6c:60:eb:54:58:6f:bd:ce:fc:69:cf:9a:70:ee:
 50:3c:fd:f7:9d:57:33:be:d9:04:ca:25:d6:e5:5b:
 84:37:55:f0:54:8f:04:cc:ed:7a:8b:7f:d3:7f:83:
 b5:db:e1:d9:dd:ea:c6:c2:09:1e:bc:9a:bf:d3:2a:
 25:7a:12:bc:3e:66:ed:2c:40:df:5e:45:a6:f1:7f:

Figure 17-8: Wildcard TLS Context for Teams (Service Providers)

CERTIFICATE

Certificate:
 Data:
 Version: 3 (0x2)
 Serial Number:
 f4:73:19:e0:b6:45:ed:e3:d1:00:e3:f8:fd:b5:39:92
 Signature Algorithm: sha256WithRSAEncryption
 Issuer: C=US, O=SSL.com, OU=www.ssl.com, CN=SSL.com DV CA
 Validity
 Not Before: Jun 17 00:00:00 2021 GMT
 Not After : Jun 17 23:59:59 2022 GMT
 Subject: CN=*.customers.audio-code.co.il
 Subject Public Key Info:
 Public Key Algorithm: rsaEncryption
 RSA Public-Key: (2048 bit)
 Modulus:
 00:b0:69:4d:22:71:89:e6:80:78:b1:3f:78:a9:a0:
 b6:2e:2c:f8:e7:af:a8:ef:2c:b8:78:66:9b:7a:8c:
 4a:74:df:ab:89:24:d5:87:ca:28:02:dc:5c:c9:c5:
 a9:69:90:df:15:fe:82:f1:ca:4a:16:5a:b8:83:27:
 7c:46:27:a9:5e:6a:7c:77:14:f5:1c:3c:e1:41:b8:
 ac:a8:17:93:a4:d8:f5:b8:76:3e:1a:d6:7f:23:74:
 9d:4f:2f:ba:3a:2a:1c:70:4b:99:c9:ca:18:95:04:
 5d:49:45:58:a0:9d:47:0c:e0:c9:97:03:a4:64:d6:
 14:ba:31:f9:ce:b1:04:37:b7:92:db:e8:b7:76:cf:
 57:52:8d:b6:65:ae:62:02:c1:d7:2f:22:3c:4e:76:
 65:d3:21:cc:73:c0:af:2a:cf:14:f4:88:f5:c6:95:
 71:4f:b1:08:e0:88:a5:6d:e1:ff:23:08:3f:88:1e:
 ed:19:01:fc:1a:23:f0:89:95:8e:bc:24:1f:da:e5:
 a0:1c:06:db:43:d4:1a:78:35:65:e4:01:a0:d5:85:
 33:85:e4:30:21:8f:2a:0e:87:94:0a:27:58:be:35:
 7a:06:9e:dd:4d:4a:1b:9d:19:33:b3:39:fa:3a:91:
 18:eb:b1:8e:14:a9:ac:0f:f7:20:58:bd:af:0a:dd:
 81:d1

2. Configure the OVOC Tunnel parameters that you configured in Section 17.1.10.

Figure 17-9: Web Service Settings

Web Service Settings

GENERAL

Topology Status: Enable

Quality Status:

Quality Status Rate: 60

Debug Level: 1

Routing Server Registration Status: Disable

OVOC TUNNEL

OVOC WebSocket Tunnel Server Address: 13.94.226.66

Path: tun

Username: VPN

Password:

Secured (HTTPS):

Verify Certificate:

3. Set parameter **Secured Web Connection (HTTPS)** to one of the following:

- HTTP and HTTPS
- HTTPS Only

Figure 17-10: Secured Web Connection (HTTPS)

Web Settings

GENERAL

Secured Web Connection (HTTPS): HTTP and HTTPS

Require Client Certificates for HTTPS connection: Disable

SESSION

Password Change Interval (minutes): 0

User Inactivity Timeout (days): 90

Session Timeout (minutes): 15

17.2 Configure HTTPS SSL Connection to OVOC Public IP

This section describes how to configure an HTTPS connection to the OVOC server public IP address.



The root certificate loaded to the UMP server and the OVOC server must be signed by the same Root CA.

Do the following:

1. In the UMP Multi-Tenant GUI, do the following:
 - Open the OVOC Settings page (**System Configuration > OVOC Settings**).
 - In the Public IP Address, enter the Public IP address of OVOC on Azure.

Figure 17-11: OVOC Settings with Public IP

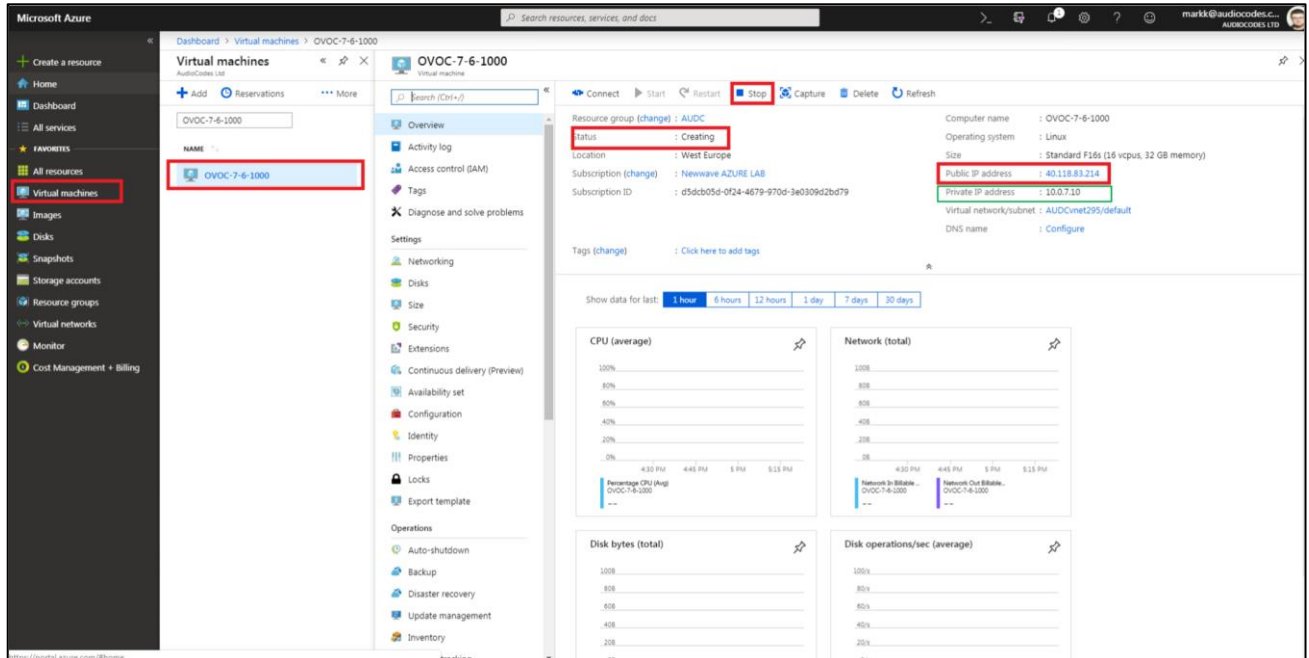
The screenshot displays the 'OVOC Settings' configuration page. On the left is a navigation sidebar with 'Settings' selected. The main content area is titled 'OVOC Settings' and is organized into several sections:

- Connection:** Includes a checked 'Use public OVOC' checkbox, a 'Public IP Address' field with the value '13.94.226.66', a 'Public User' field with 'VPN', a 'Public Password' field with a placeholder 'Please enter a valid OvocPublicPassword', a 'Trap Port' field with '1161', and a 'Keep Alive Port *' field with '1161'.
- System Settings:** Includes a 'System Name *' field with 'OnPremUMP1' and a 'Location' field with 'onPrem'.
- SNMP:** Features radio buttons for 'SNMPv2' (selected) and 'SNMPv3'. Below are 'Community Read *' and 'Community Write *' fields, both containing the value 'public'.
- Access Settings:** Includes a 'Login Uri' field with the value 'http://169.254.2.151/tenantui'.
- Managed Components:** Shows a checkbox for 'SBC' which is selected.

At the bottom of the configuration area, there are two buttons: 'Apply Changes' and 'Reset Changes'.

The figure below shows where to extract the IP address of OVOC server on Azure.

Figure 17-12: OVOC on Azure



- Enter Trap Port: 162
- Enter Keep Alive Port: 1161
- Select **SNMPv2** and in the Community Read and Community Write fields enter **public**
- Uncheck the 'SBC monitor' flag.
- Enter the following System Settings:
 - ◆ System Name
 - ◆ Location
- For the **Login URL** (used for Single Sign-on and REST connection initiated from OVOC side): Enter the **Private IP address** of the UMP on Azure and not its Public IP address/FQDN (e.g. <http://127.0.0.1/tenantui>).



Once the initial Single Sign-on connection to the UMP VM is established, the "Login Url" field above is automatically updated to `http://169.254.x.x`; **do not change this value.**

- Click **Apply Changes**.
2. In the OVOC Web interface, do the following:
 - Ensure that device and tenant connections are enabled for HTTPS (default).
 - In the General Settings page(**System** menu >**Administration** tab > **OVOC Server** folder > **Configuration** > **General Settings** tab), configure the SBC Devices Communication parameter to "**Hostname Based**"- FQDN host name that is specified in the OVOC server certificate file used to authenticate the connection with devices.

Figure 17-13: OVOC Hostname

GENERAL SETTINGS

OVOC Hostname: tlc-ovoc.trunkpack.com

Description: Audiocodes

SBC Devices Communication: Hostname Based

Privacy Mode:

Global Logo: globalLogo.png

Service Request URL: https://acext1-tst2.custhelp.com/ci/pta/login/redirect_to/app/account/q

Service Request Password:

Submit

- Verify that the DNS resolves for the OVOC FQDN is successful, for example Google.com:

```
C:\Users\enterpriseluser>nslookup www.google.com
Server: tlc-ovoc.trunkpack.com
Address: 10.1.1.10
Non-authoritative answer:
Name: www.google.com
Addresses: 2a00:1450:4006:801::2004
172.217.18.36
```

3. In the OVOC Server Manager install Custom Certificates (see Section “Server Certificates Updates”).
4. On the managed SBC devices, do the following:
 - Install SSL certificates on managed SBC devices (refer to *Section Install Custom Certificates on OVOC Managed Devices in the IOM manual*). You must define the following TLS contexts:
 - ◆ OVOC Management connection (Context #0)
 - ◆ UMP-365 Management connection (Context #1)
 - ◆ Microsoft Teams connection (Wildcard certificate) i.e. a separate TLS context must be defined for each service provider. (Context #3)
 - Set parameter **Secured Web Connection (HTTPS)** to one of the following:
 - ◆ HTTP and HTTPS
 - ◆ HTTPS Only

Figure 17-14: Secured Web Connection (HTTPS)

The screenshot displays the 'Web Settings' configuration page. On the left is a navigation menu with categories: TIME & DATE, WEB & CLI (selected), Local Users (2), Authentication Server, Web Settings (highlighted), CLI Settings, Access List, Additional Management Interfaces (0), and Customize Access Level (0). Below these are expandable sections for SNMP, LICENSE, MAINTENANCE, and PERFORMANCE MONITORING. The main content area is titled 'Web Settings' and is divided into 'GENERAL' and 'SESSION' sections. In the 'GENERAL' section, 'Secured Web Connection (HTTPS)' is set to 'HTTP and HTTPS', and 'Require Client Certificates for HTTPS connection' is set to 'Disable'. The 'SESSION' section includes input fields for 'Password Change Interval (minutes)' (0), 'User Inactivity Timeout (days)' (90), and 'Session Timeout (minutes)' (15).

17.3 Configure Connection to OVOC Azure Private IP

This section describes how to configure the connection to the OVOC server with its private IP address.

Do the following:

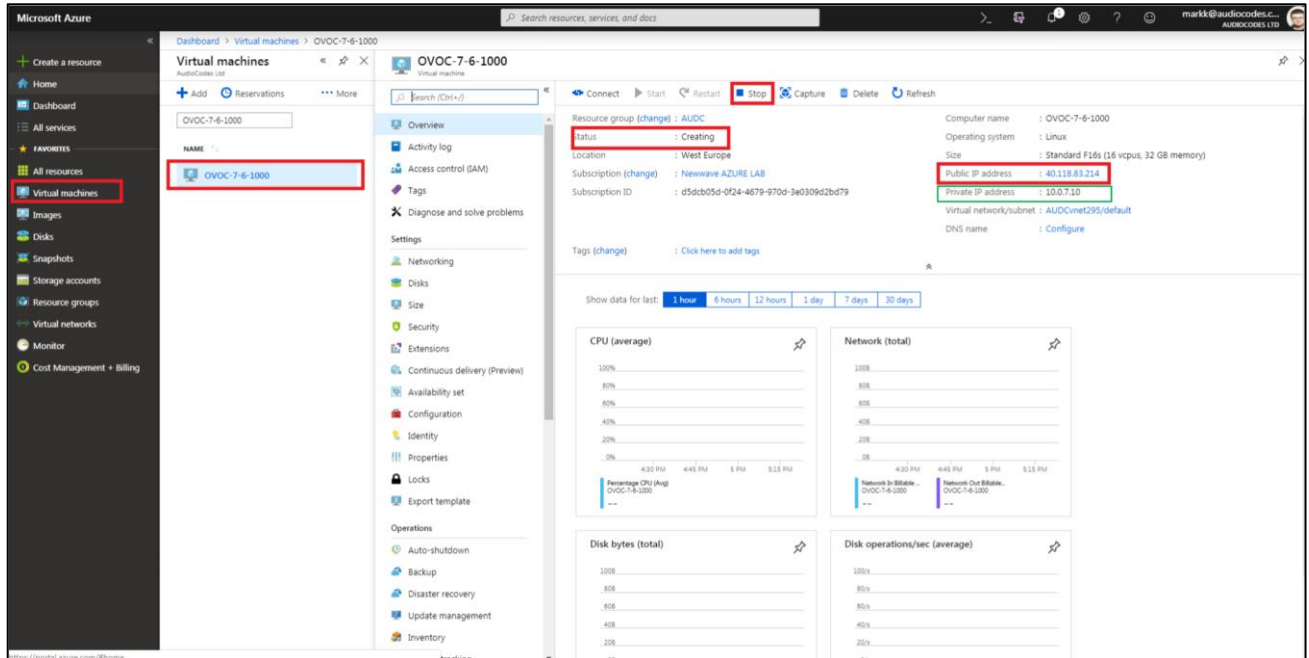
1. In the UMP Multi-Tenant GUI, open the OVOC Settings page (**System Configuration > OVOC Settings**).
2. In the IP Address enter the Private IP address of OVOC Azure

Figure 17-15: OVOC Setting with OVOC Private IP

The screenshot shows the 'OVOC Settings' page in the UMP Multi-Tenant GUI. The left sidebar contains navigation options: Tenants, Ovoc, Settings (selected), Alarms, System, and Security. The main content area is titled 'OVOC Settings' and includes a 'Connection' section with the following fields: 'Use public OVOC' (checked), 'IP Address' (169.254.0.1), 'Trap Port' (162), and 'Keep Alive Port *' (1161). Below this is the 'SNMP' section with 'SNMPv2' selected and 'Community Read *' (public) and 'Community Write *' (public) fields. The 'Managed Components' section shows 'SBC' with 'Apply Changes' and 'Reset Changes' buttons. On the right side, there are 'System Settings' (System Name: ump-qa-upgrade, Location: West Eu) and 'Access Settings' (Login Url: http://169.254.3.89/tenantui). The footer contains the copyright notice: 'Copyright © 2020 AudioCodes. All rights reserved.'

The figure below shows where to extract the IP address of OVOC on Azure.

Figure 17-16: OVOC on Azure



3. Enter Trap Port: 162
4. Enter Keep Alive Port: 161
5. Select **SNMPv2** and in the Community Read and Community Write fields enter **public**
6. Uncheck the 'SBC monitor' flag.
7. Enter the following System Settings:
 - System Name
 - Location
8. For the **Login URL** (used for Single Sign-on and REST connection initiated from OVOC side): Enter the **Private IP address** of the UMP on Azure and not its Public IP address/FQDN (e.g. `http://127.0.0.1/tenantui`).



Once the initial Single Sign-on connection to the UMP VM is established, the "Login Url" field above is automatically updated to `http://169.254.x.x` ; **do not change this value.**

9. Click Apply Changes.

17.4 Managing Alarms

The Alarms screen displays alarms that are raised for the OVOC connection into the following categories:

- Current alarms
- Cleared alarms
- Agent Alarms
- OVOC Events
- For each alarm the following information is displayed:

Table 17-1: Alarm Fields

Field	Description
Id	SNMP OID
Alarm Time	The time that the alarm was raised.
Name	The alarm name
Source	The source of the alarm (different for each alarm type). For example, for Agent Alarms <VM Name>/<Name of Service> of raised alarm
Text	Text description that is displayed in the alarm
Severity	Alarm severity displayed from the variable-binding tgTrapGlobalsSeverity. There may be several conditions for each severity.
Cleared	In the current alarms table indicates that the raised alarm has been cleared.
Actions	Recommended actions to take.

Figure 17-17: Current Alarms

The screenshot shows the 'Alarms' management interface. At the top, there are tabs for 'Current Alarms', 'Cleared Alarms', 'Agent Alarms', and 'Ovoc Events'. Below the tabs, there is a 'Reload' button, a 'Show 10 entries' dropdown, and a search field. The main table area displays a message: 'No data available in table'. At the bottom, it says 'Showing 0 to 0 of 0 entries' and includes 'Previous' and 'Next' navigation buttons.

Figure 17-18: Agent Alarms

The screenshot shows the 'Alarms' management interface with the 'Agent Alarms' tab selected. The table contains the following data:

Name	AlarmTime	Component	Source	Text	Severity
acCbCompSrvAlarm	July 26th 2021, 12:39		OVL_UMP_MT_UMP-TOBI/SysAdmin.CacheSrv.NewCustTest	Service SysAdmin.CacheSrv.NewCustTest stopped	Warning
acCbCompSrvAlarm	July 26th 2021, 12:39		OVL_UMP_MT_UMP-TOBI/SysAdmin.CacheSrv.TokenTest	Service SysAdmin.CacheSrv.TokenTest stopped	Warning
acCbCompSrvAlarm	July 26th 2021, 12:39		OVL_UMP_MT_UMP-TOBI/SysAdmin.CacheSrv.NewCustTest1	Service SysAdmin.CacheSrv.NewCustTest1 stopped	Warning
acCbCompSrvAlarm	July 27th 2021, 15:22		OVL_UMP_MT_UMP-TOBI/SysAdmin.CacheSrv.Plus_Cust_Test	Service SysAdmin.CacheSrv.Plus_Cust_Test stopped	Warning
acCbCompSrvAlarm	July 28th 2021, 09:41		OVL_UMP_MT_UMP-TOBI/SysAdmin.CacheSrv.SysOpera_Plus	Service SysAdmin.CacheSrv.SysOpera_Plus stopped	Warning
acCbCompSrvAlarm	July 28th 2021, 12:42		OVL_UMP_MT_UMP-TOBI/SysAdmin.CacheSrv.TokenAuth_Pro	Service SysAdmin.CacheSrv.TokenAuth_Pro stopped	Warning
acCbCompSrvAlarm	July 28th 2021, 12:42		OVL_UMP_MT_UMP-TOBI/SysAdmin.CacheSrv.OVOCTeams_SN	Service SysAdmin.CacheSrv.OVOCTeams_SN stopped	Warning

Figure 17-19: OVOC Events

Alarms

Current Alarms Cleared Alarms Agent Alarms Ovoc Events

Reload Show 10 entries Search:

Id	Event Time	Name	Source	Text	Severity
4702	October 8th 2021, 10:54	acUmpO365CommandExEvent	ancafromovoc	Removed Customer ancaFromOvoc	Indeterminate
4703	October 8th 2021, 12:26	acUmpUserSettingsFailEvent	TobiTestPro/lcm	unable to allocate a number from NumberRange for sip:MiriamG@M365x694040.OnMicrosoft.com	Warning
4704	October 8th 2021, 12:26	acUmpUserSettingsFailEvent	TobiTestPro/lcm	unable to allocate a number from NumberRange for sip:AdeleV@M365x694040.OnMicrosoft.com	Warning
4705	October 8th 2021, 12:35	acUmpUserSettingsFailEvent	TobiTestPro/lcm	unable to allocate a number from NumberRange for sip:MiriamG@M365x694040.OnMicrosoft.com	Warning
4706	October 8th 2021, 12:35	acUmpUserSettingsFailEvent	TobiTestPro/lcm	unable to allocate a number from NumberRange for sip:PattiF@M365x694040.OnMicrosoft.com	Warning
4707	October 8th 2021, 12:35	acUmpUserSettingsFailEvent	TobiTestPro/lcm	unable to allocate a number from NumberRange for sip:MeganB@M365x694040.OnMicrosoft.com	Warning
4708	October 8th 2021, 12:35	acUmpUserSettingsFailEvent	TobiTestPro/lcm	unable to allocate a number from NumberRange for sip:saiahL@M365x694040.OnMicrosoft.com	Warning

Part III

Upgrade

18 Getting Started

18.1 Overview

Microsoft 365 Tenant setups require deep PowerShell expertise and SBC configuration knowledge, where the acquisition of such skills involves high costs and is time consuming. The UMP 365 SP Edition application significantly simplifies the implementation of these skills through a sophisticated Microsoft 365 Tenant onboarding and service automation solution. On the 2nd day management UMP 365 SP edition application simplifies the daily operation work with user lifecycle and identity management of their M365 customers Tenants. As a result, they can adjust their configuration topology to best fit the rapidly changing requirements for voice services and fully leverage the rich capabilities of Office 365. This includes assigning templates with sets of Teams policies, managing the M365 Tenant DID range and telephony settings and assigning these templates to security groups.

The Provider (Service Provider or Hosted Provider) Admin is defined as a SuperAdmin with permissions to view their managed M365 Tenants (Customer). The Providers Admin can access their customers M365 Tenants, view the Users configuration, edit users with LifeCycle Management, manage their customer DID range and configure the Tenant Voice routing configuration. UMP 365 SP Edition application is a white-label managed application.

In a typical Microsoft 365 Tenant deployment, performing day-to-day administration tasks can be quite complex. Teams relies on the creation of user accounts using Azure Active Directory and then modifying user accounts, and other Teams Policies settings using the Teams Admin Center, and PowerShell commands.

User Management Pack 365 is a powerful software application that simplifies User Lifecycle & Identity management across Microsoft Teams environments, maintaining the availability of all these Microsoft tools; however, providing a much simpler web-based administration utility. UMP 365 does not attempt to remove or re-write these Microsoft tools, and they remain available for other purposes.

UMP 365 provides a simplified web-based administration utility (aka SysAdmin) with a strong focus on telephony, Teams and Microsoft 365 features that allows System Administrators to carry out day-to-day maintenance activities, without the need for access to multiple complicated Microsoft Management Tools and challenging PowerShell commands, requiring lengthy professional training.

18.2 UMP 365 with Service Provider Admin Credentials

The UMP 365 application is web-based and can be accessed via any web browser (Chrome, Microsoft Edge or Firefox) **over HTTPS only**. The provider can either access the Customer Portal using the Windows user or the Azure AD SSO user.

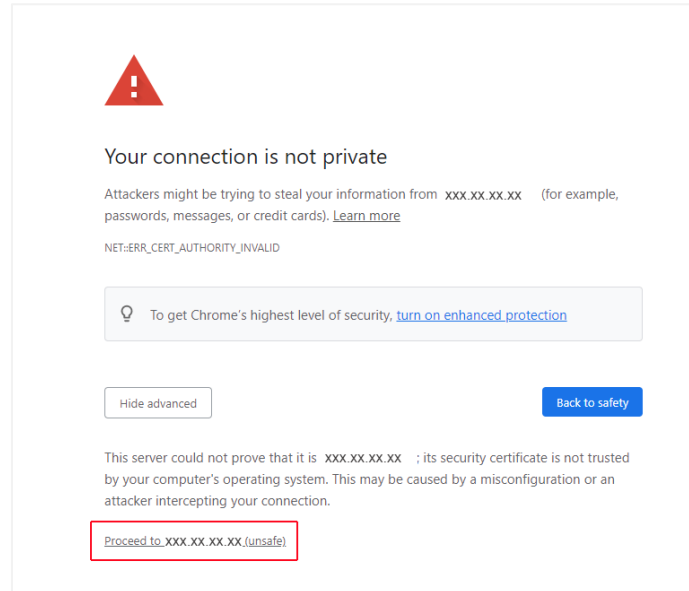


The minimum screen resolution for the Web browser page is 1920 X 1080.

One of the following Login URLs can be used:

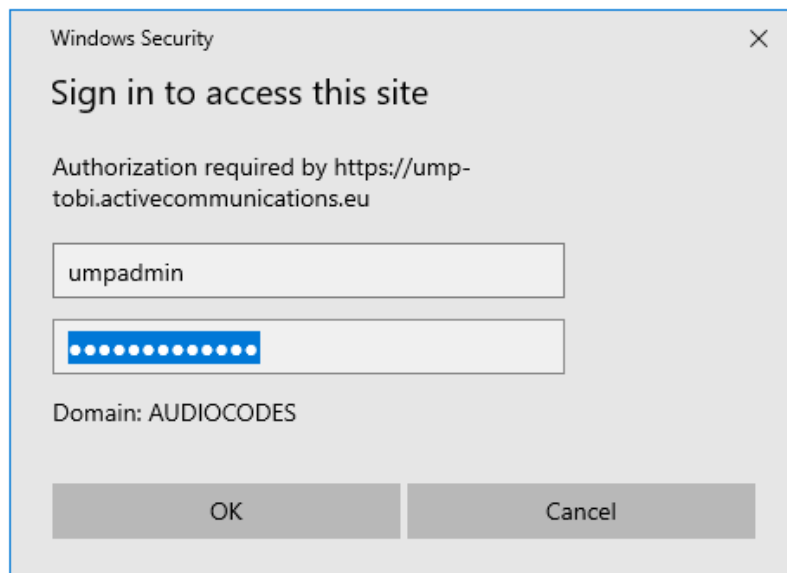
- `https:\\[DNSname]\\tenantui`
- `https:\\localhost\\tenantui`

If you are connecting with localhost, a certificate error message will be displayed, confirm to continue with insecure connection.

Figure 18-1: Private Connection

The provider can access User Management Pack 365 with the following Admin User types:

- **SuperAdmin:** a predefined Windows User Account which must be a member of Group UmpAdmins)
 - Access to Multi-Tenant level and to all the Customers Tenant

Figure 18-2: Multi-Tenant Access (Provider Only)

The following screen shows the UMP-365 interface after a clean installation for new customer.

Figure 18-3: UMP 365 Authentication

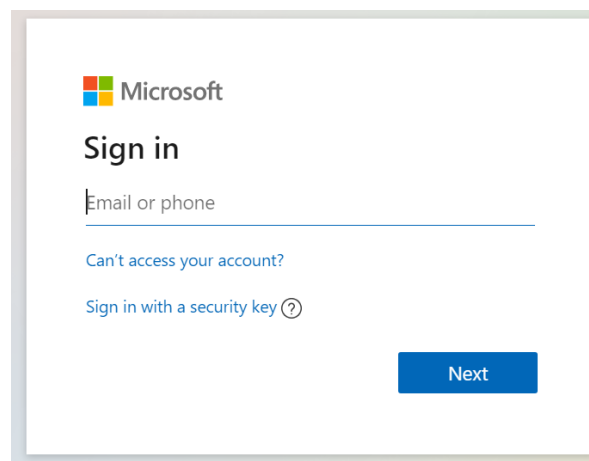
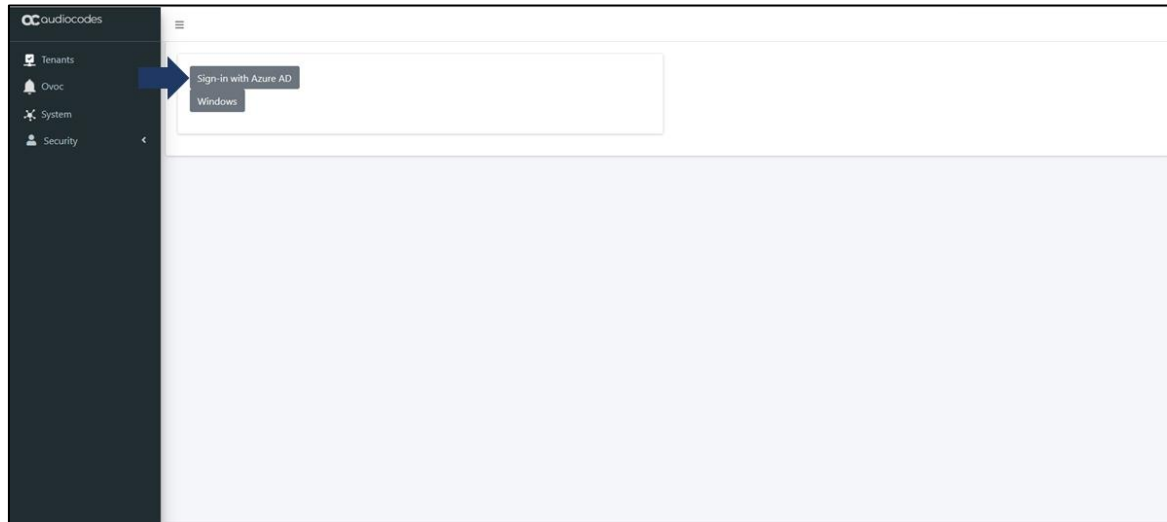
The screenshot shows the UMP-365 interface. On the left is a dark sidebar with the AudioCodes logo and navigation items: Tenants (selected), Ovoc, System, Security, SBC List, and Queued Tasks. The main content area has a blue header bar. Below it, system status is shown: Available Users: 100, Available Customers: 100, SysadminKit Version: 8.0.300.130. A search bar and a '+ Add' button are present. Below is a table with the following columns: Customer Name, State, SysAdmin Info, Licensing (licensed users), and Queued commands status. The table is empty, displaying 'No data available in table'. At the bottom of the table area, it says 'Showing 0 to 0 of 0 entries' with 'Previous' and 'Next' buttons. The footer contains the copyright notice: Copyright © 2020 AudioCodes. All rights reserved.

- **Admin User: SSO Sign-In with Azure AD user**
 - Access to the customers Tenant that received Grant access



Logging in with an Azure AD is only possible after a tenant has been created and assigned an administrator to this tenant as described in Chapter 14.

Figure 18-4: Customer Link UMP 365 Authentication



The following screen shows the Tenants screen for a login to the multitenant portal.

Figure 18-5: UMP 365 Authentication

Available Users: 247, Available Customers: 3
SysadminKit Version: 8.0.220.26

Show 10 entries Search:

Customer Name	State	SysAdmin Info	Licensing (licensed users)		Queued commands status
ancaFromOvoc	Deployed	version: 8.0.220.26 replication: 2021.08.22.10.49.44 SysAdmin	M365 - Pro (162)	Edit Delete Undo Deploy Add SBC Site Queue Replication	Queued commands: 0 Executing commands: 0 Replication in progress: no
Automation_Essential_BYOC_Cust omer	Deployed	SysAdmin	M365 - Essential (0)	Edit Delete Undo Deploy	Queued commands: 0 Executing commands: 0 Replication in progress: no
bcb	Deployed	SysAdmin	M365 - Essential (0)	Edit Delete Undo Deploy	Queued commands: unkown Executing commands: unkown Replication in progress: unkown
BradTrunk	Deployed	version: 8.0.220.26 replication: 2021.08.22.10.49.34 SysAdmin	M365 - EssentialPlus (10)	Edit Delete Undo Deploy Add SBC Site Queue Replication	Queued commands: 0 Executing commands: 0 Replication in progress: no
Pro_Token_With_Teams	Deployed	version: 8.0.220.26 replication: 2021.08.22.10.50.46 SysAdmin	M365 - Pro (120)	Edit Delete Undo Deploy Add SBC Site Queue Reicaltion	Queued commands: 0 Executing commands: 0 Replication in progress: no

18.3 Tenants Global View

The figure below displays an example screen including a list of M365 customer tenants:

Figure 18-6: Main Screen View

Available Users: 9885, Available Customers: 19
SysadminKit Version: 8.0.300.135

Show 10 entries Search:

Customer Deployment Status Opens Customer Portal Configure Number of Licensed Users

Customer Name	State	SysAdmin Info	Licensing (licensed users)		Queued commands status
essentials	Deployed	SysAdmin	M365 - Essential (0)	Edit Delete Undo Deploy Upgrade Customer	Queued commands: 0 Executing commands: 0 Replication in progress: no
M365x202362	Deployed	version: 8.0.300.135 replication: 2022.03.23.10.43.42 SysAdmin	M365 - Pro (30)	Edit Delete Undo Deploy Add SBC Site Queue Replication	Queued commands: 0 Executing commands: 0 Replication in progress: no
M365x35102214	Deployed	version: 8.0.300.135 replication: 2022.03.23.10.43.42 SysAdmin	M365 - Pro (25)	Edit Delete Undo Deploy Add SBC Site Queue Replication	Queued commands: 0 Executing commands: 0 Replication in progress: no
M365x45661692	Deployed	version: 8.0.300.135 replication: 2022.03.23.10.44.24 SysAdmin	M365 - Pro (25)	Edit Delete Undo Deploy Add SBC Site Queue Replication	Queued commands: 0 Executing commands: 0 Replication in progress: no
M365x78596656	Deployed	version: 8.0.300.135 replication: 2022.03.23.10.44.25 SysAdmin	M365 - Pro (25)	Edit Delete Undo Deploy Add SBC Site Queue Replication	Queued commands: 0 Executing commands: 0 Replication in progress: no
petre	Deployed	version: 8.0.300.135 replication: 2022.03.23.10.44.47 SysAdmin	M365 - Pro (10)	Edit Delete Undo Deploy Add SBC Site Queue Replication	Queued commands: 0 Executing commands: 0 Replication in progress: no

Annotations: Add new customers, Upgrade customer to latest version, Add new site locations, Replicate Database queue, Reset Deployment for M365 tenant

The M365 Tenant / Links screen displays a quick glance status and monitoring summary of the customer-specific M365 Tenants. Information displayed includes:

- Total number of available Tenants and Users (per system)
- Search box
- UMP SP version
- Customer Name

- Tenant State: Ready for Deployment, Deploying, Deployed, Ready for remove
- SysAdmin Info:
 - Version: Tenant Web application software version
 - Replication: last replication time

Table 18-1: Global Actions

Link	Action
SysAdmin	Opens the Service Provider portal (see Chapter 33).
Edit	Configured number of licensed users for M365 tenant (see 18.3.1).
Add SBC Site	Onboards SBC devices (see Section 33.13.10)
Delete	Removes the tenant from the UMP instance.
Undo Deploy	Resets the current deployment configuration for the M365 tenant.
Queue Replication	Replicates the database for the queue (See Section 18.3.3).
Upgrade Customer	Indicates whether the customer needs to be upgraded to the latest version.

18.3.1 Configured Number of Licenses Users

You can configure the number of licenses users to the M365 tenant.

To configure the number of licensed users:

1. In the Main View, select the desired M365 tenant and then click **Edit**.

Figure 18-7: Configure Number of Licensed Users

The screenshot shows a web interface for configuring a tenant. On the left is a dark sidebar with icons and labels for 'Tenants', 'Ovoc', 'System', 'Security', 'SBC List', and 'Queued Tasks'. The main area is light gray and contains a form. The form has a 'Customer Id' field with the value 'BBB123'. To its right is a 'Licensed users' section showing 'Currently assigned: 10' and a dropdown menu currently set to '10'. A green 'Save' button is to the right of the dropdown. Below the form is a blue button with a left-pointing arrow and the text 'BackToTenantsList'.

2. Change the number of currently assigned users and then click 

18.3.2 Onboard SBC Devices for New Site Locations

Once the new M365 tenant has been added you can onboard additional SBC devices that are deployed at new sites.

To onboard an SBC to a new site:

1. In the Tenants screen click **Add SBC Site**.

Figure 18-8: Add SBC Site

The screenshot shows the Tenants screen with a table of tenants. The table has columns for Customer Name, State, SysAdmin Info, Licensing (licensed users), and Queued commands status. The 'Add SBC Site' button is highlighted in red in the 'M365 - Pro (162)' row.

Customer Name	State	SysAdmin Info	Licensing (licensed users)	Queued commands status
ancaFromOvoc	Deployed	version: 8.0.220.26 replication: 2021.08.22.10.49.44 SysAdmin	M365 - Pro (162)	Queued commands: 0 Executing commands: 0 Replication in progress: no
Automation_Essential_BYOC_Customer	Deployed	SysAdmin	M365 - Essential (0)	Queued commands: 0 Executing commands: 0 Replication in progress: no
bcb	Deployed	SysAdmin	M365 - Essential (0)	Queued commands: unknown Executing commands: unknown Replication in progress: unknown
BradTrunk	Deployed	version: 8.0.220.26 replication: 2021.08.22.10.49.34 SysAdmin	M365 - EssentialPlus (10)	Queued commands: 0 Executing commands: 0 Replication in progress: no
Pro_Token_With_Teams	Deployed	version: 8.0.220.26 replication: 2021.08.22.10.50.46 SysAdmin	M365 - Pro (120)	Queued commands: 0 Executing commands: 0 Replication in progress: no

Below the table is a modal window with a progress bar showing three steps: 1 M365 Tenant, 2 M365, and 3 Voice Route. The modal contains the text "ADD NEW SITE PRESS NEXT" and a "Next" button.

2. Click **Next** to continue. Credentials are validated and the Onboarding wizard opens.

Figure 18-9: Configure Default Routing

The screenshot shows a modal window with a progress bar showing three steps: 1 M365 Tenant, 2 M365, and 3 Voice Route. The modal contains a checkbox labeled "Configure M365 default routing" and a "Next" button.


Configure M365 default routing

By selecting this check box, the wizard will create default routing in the customer M365 tenant, based on the derived trunk model for service providers and optionally configure the service provider DNS automatically if selected.

3. Proceed to Chapter 30.

18.3.3 Queue Replication

After successful authentication, the User Management Pack 365 loads the Users section under User Management, where the users and devices that are enabled for Microsoft Teams are shown.

 If the initial replication has not been completed yet, the Users list will be empty. Right-click the “Last Sync Never” message on the upper right-hand corner to initiate a full replication cycle.

EnterpriseRTC	Deployed	Deployed	version: 8.0.100.112 replication: 2020.11.12.21.37.51 SysAdmin	Edit Delete Un Queue Replication
---------------	----------	----------	----------------------------------------------------------------------	-----------------------------------------

18.3.4 Undo Deployment

If you wish to configure the M365 tenant deployment from scratch you can select the **Undo Deployment**.

18.3.5 Upgrade Customer

This feature lets you upgrade a Hosted Essentials customer to Hosted Essentials+ or Hosted Pro.

Figure 18-10: Upgrade Customer

Available Users: 9885, Available Customers: 19
SysadminKit Version: 8.0.300.135

Show 10 entries

Search:

Customer Name	State	SysAdmin Info	Licensing (licensed users)		Queued commands status
essentials	Deployed	SysAdmin	M365 - Essential (0)	Edit Delete Undo Deploy Upgrade Customer	Queued commands: 0 Executing commands: 0 Replication in progress: no
M365x202362	Deployed	version: 8.0.300.135 replication: 2022.03.23.10.43.42 SysAdmin	M365 - Pro (30)	Edit Delete Undo Deploy Add SBC Site Queue Replication	Queued commands: 0 Executing commands: 0 Replication in progress: no
M365x35102214	Deployed	version: 8.0.300.135 replication: 2022.03.23.10.43.42 SysAdmin	M365 - Pro (25)	Edit Delete Undo Deploy Add SBC Site Queue Replication	Queued commands: 0 Executing commands: 0 Replication in progress: no
M365x45661692	Deployed	version: 8.0.300.135 replication: 2022.03.23.10.44.24 SysAdmin	M365 - Pro (25)	Edit Delete Undo Deploy Add SBC Site Queue Replication	Queued commands: 0 Executing commands: 0 Replication in progress: no
M365x78596656	Deployed	version: 8.0.300.135 replication: 2022.03.23.10.44.25 SysAdmin	M365 - Pro (25)	Edit Delete Undo Deploy Add SBC Site Queue Replication	Queued commands: 0 Executing commands: 0 Replication in progress: no
petre	Deployed	version: 8.0.300.135 replication: 2022.03.23.10.44.47 SysAdmin	M365 - Pro (10)	Edit Delete Undo Deploy Add SBC Site Queue Replication	Queued commands: 0 Executing commands: 0 Replication in progress: no

To upgrade a Hosted Essentials customer:

1. Click **Upgrade Customer**.

Figure 18-11: Start Upgrade Customer

1 M365 Tenant 2 M365 3 Voice Route

Start Upgrade Customer
PRESS NEXT

Next

2. Click **Next** to continue.

Figure 18-12: Select License Type

1 M365 Tenant 2 M365 3 Voice Route

Full Customer Name
essentials

Short Customer Name
essentials

License Type
 Hosted Essential
 Hosted Essentials+
 Hosted Pro

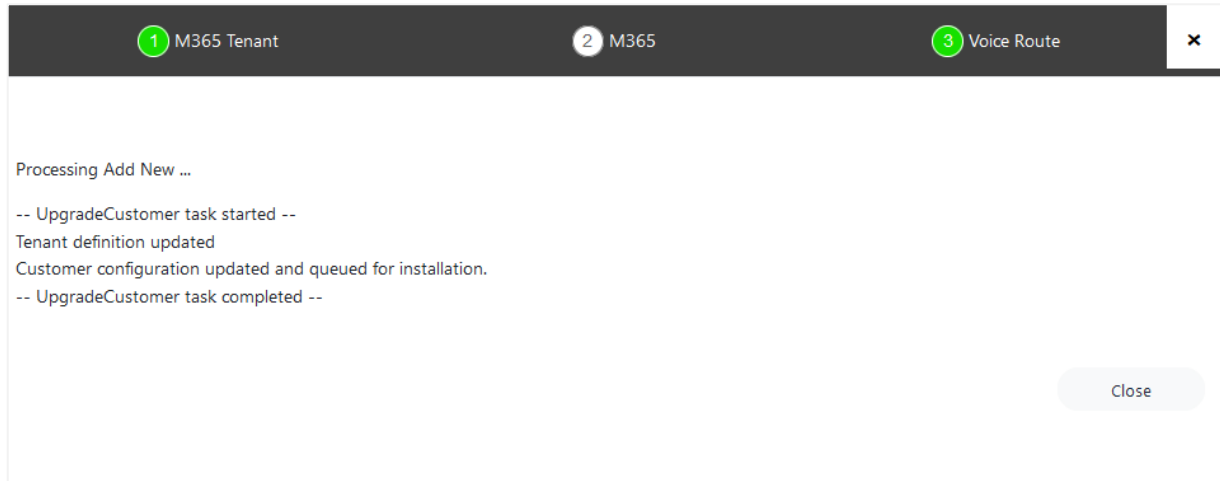
Licensed Users: 1

M365 Authentication
 Send link to customer IT administrator for authentication:
 Use M365admin account with known password

admin@ocshost.emea.microsoftonline.com ●●●●●●●●

Back Next

3. Select either Hosted Essentials + or Hosted Pro checkboxes, enter the number of Licensed users, and then click **Next**.
4. Continue with the Onboarding Wizard as described in Sections 30.2 and 30.3. At the end of the process, the following confirmation message is displayed:

Figure 18-13: Upgrade Customer Task

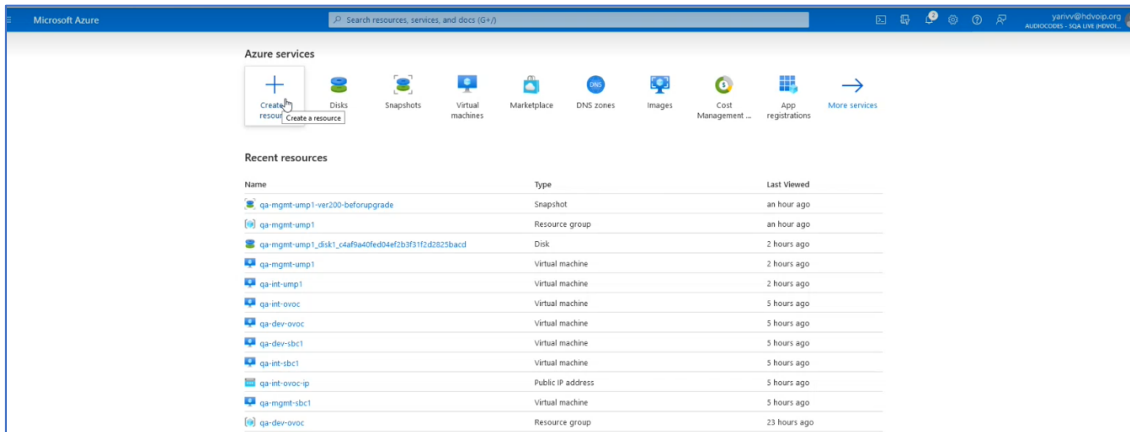
19 UMP Backup– Disk Snapshot

This section describes how to create a snapshot of the UMP Virtual Machine. This procedure should be performed prior to running the upgrade and then rolled back once the upgrade is complete.

Do the following:

1. Open the Azure portal, type “Create a Resource” and then click **Create a Resource**.

Figure 19-1: Create a Resource



2. In the Search field, type “Snapshot” and then click **Create**.

Figure 19-2: Create Snapshot

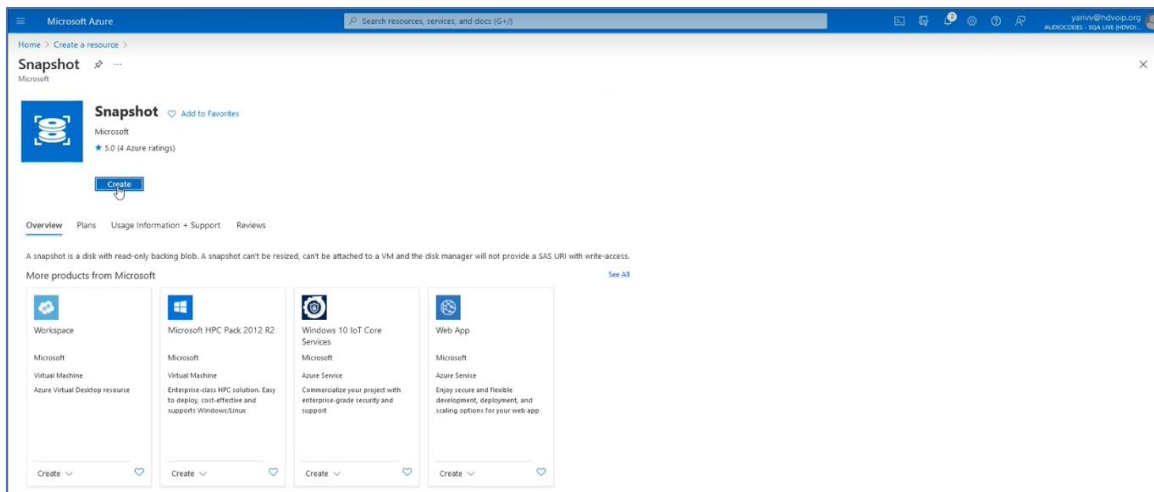


Figure 19-3: Snapshot Details

Microsoft Azure

Home > Create a resource > Snapshot >

Create snapshot

Basics Encryption Networking Tags Review + create

A snapshot is a read-only copy of a virtual hard drive (VHD). You can take a snapshot of an OS or data disk VHD to use as a backup, or to troubleshoot virtual machine (VM) issues. [Learn more about snapshots in Azure](#)

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *

Resource group * [Create new](#)

Instance details

Name *

Region *

Snapshot type * Full - make a complete read-only copy of the selected disk.
 Incremental - save on storage costs by making a partial copy of the disk based on the difference between the last snapshot.

Source subscription

Source disk *

Storage type *

[Review + create](#) [< Previous](#) [Next : Encryption >](#)

3. In the Resource group field select your working Resource Group.
4. Enter the desired name of the snapshot.
5. In the Source disk field drop-down list choose the name of the disk that you wish to backup.
6. In the Storage type field drop-down list choose the type of disk that you wish to backup e.g. Standard HDD.
7. Select the **Tags** tab to optionally define tags for the snapshot and then click **Review + create**.

Figure 19-4: Define Snapshot Tags

Microsoft Azure

Search resources, services, and docs (G+)

Home > Create a resource > Snapshot >

Create snapshot

Basics Encryption Networking **Tags** Review + create

Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups. [Learn more about tags](#)

Note that if you create tags and then change resource settings on other tabs, your tags will be automatically updated.

Name	Value	Resource
LiveCloudEnv	qa-mgmt	2 selected
		2 selected

Review + create < Previous Next : Review + create >

8. Review the details of the snapshot and then click **Create**.

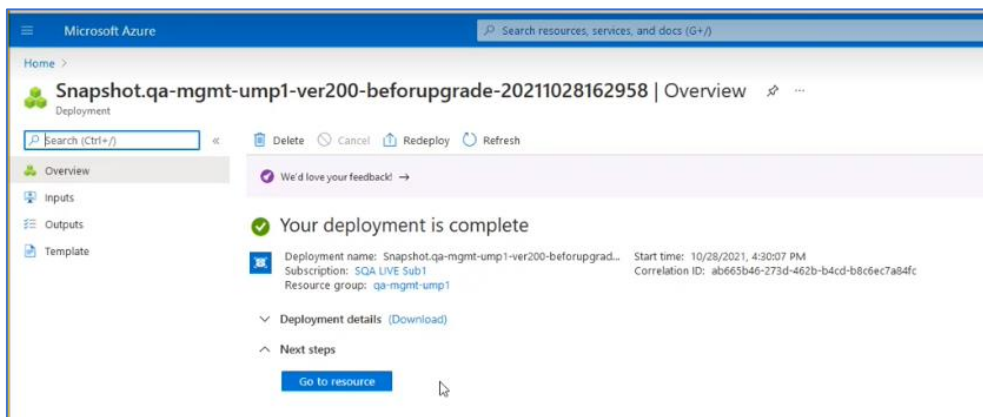
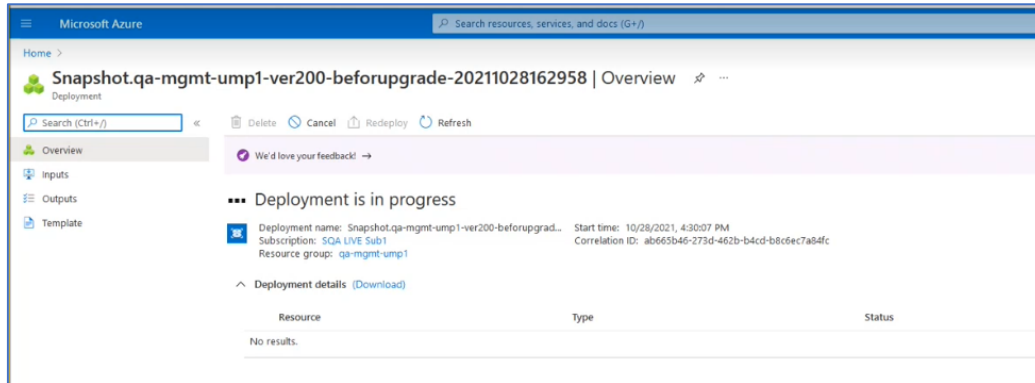
Figure 19-5: Review Snapshot Details

The screenshot shows the Microsoft Azure portal interface for creating a snapshot. The breadcrumb navigation is 'Home > Create a resource > Snapshot >'. The main heading is 'Create snapshot ...'. A green banner indicates 'Validation passed'. The 'Review + create' tab is selected, showing configuration details for Basics, Encryption, Networking, and Tags. At the bottom, the 'Create' button is highlighted with a mouse cursor, along with navigation buttons for '< Previous', 'Next >', and a link to 'Download a template for automation'.

Section	Property	Value
Basics	Subscription	SQA LIVE Sub1
	Resource group	qa-mgmt-ump1
	Region	West Europe
	Name	qa-mgmt-ump1-ver200-beforupgrade
	Source subscription	SQA LIVE Sub1
	Source disk	qa-mgmt-ump1_disk1_c4af9a40fed04ef2b3f31f2d2825bacd
	Storage type	Standard_LRS
	Snapshot type	Full
Encryption	Encryption type	Platform-managed key
Networking	Connectivity method	AllowAll
Tags	LiveCloudEnv	qa-mgmt
	LiveCloudEnv	qa-mgmt

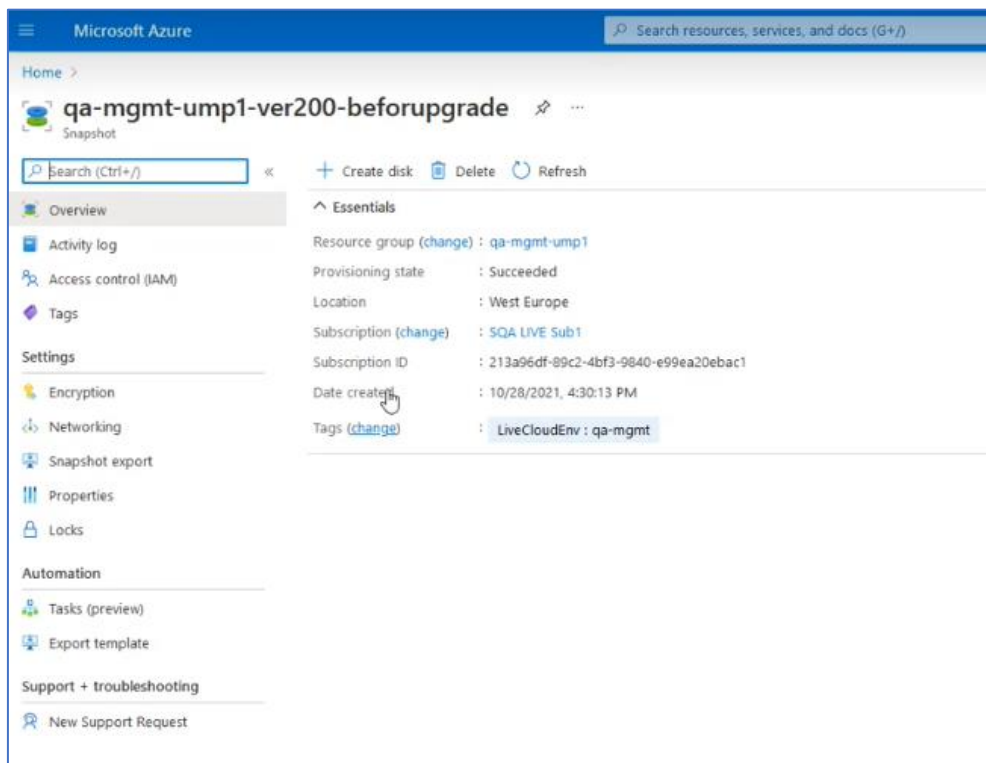
The snapshot is created. The following progress messages are displayed:

Figure 19-6: Progress of Snapshot Deployment



9. Click **Go to Resource** to view details of the snapshot.

Figure 19-7: Snapshot Details



10. Proceed to Chapter 20.

20 Upgrade using Wyupdate

This chapter describes how to install patch updates and version updates using the Wyupdate tool which does the following:

- Validates whether new patch updates are available for installation and if so, downloads and installs them.
- Validates whether the UMP-365 version requires a version upgrade e.g. from Version 8.0.100 to version 8.0.200



Before proceeding with the upgrade, ensure that the SBC and OVOC versions are compatible with the UMP-365 version. See [Release Notes](#) for more information.

20.1 Prerequisites

- Install SSL certificates on the UMP Windows server for securing the HTTPS connection with Microsoft Azure (see Chapter 3).
- When using a backend SQL server create the following directory on the SQL server:

```
c:/acs/dbbackup/
```



UMP requires a direct connection to Internet. If you are using a reverse proxy make sure to enable Web Socket. If the connection fails, first test it on the server with a direct connection without a reverse proxy before creating a support ticket.

20.2 Run Wyupdate Tool

This step describes how to run the patch update/version upgrade scripts on the Main UMP tenant and for each customer tenant.



Run the Wyupdate as administrator using the UMP service admin account that was created in Section 6.3.

20.2.1 Main UMP Tenant Update

This step describes how to run the scripts on the Main UMP Tenant.

Do the following:

1. In the Windows Services Manager, stop all **sysadmin** services, or enter the following PowerShell command to start all UMP sysadmin services:

```
stop-service sysadmin*
```

2. Enter the following command to start all www services/internet IIS services

```
stop-service w3svc
```

3. To verify whether the services have been started, specify the following commands:

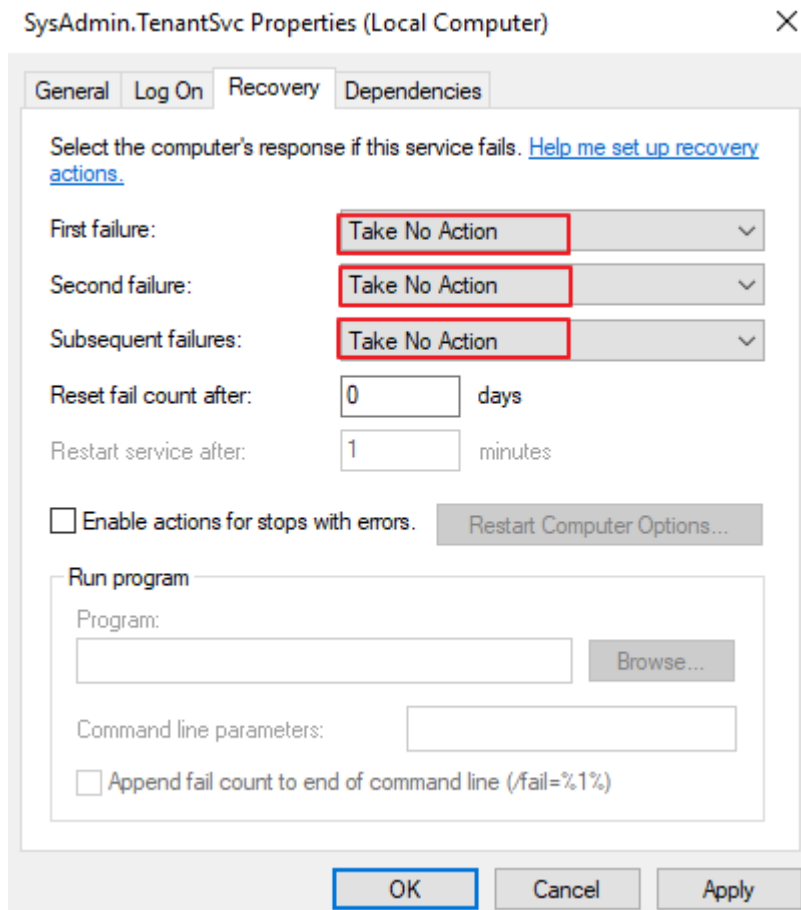
```
get-service w3svc
```

```
Get-service sysadmin*
```

If one of the above services has not been started, open the Services App, select the service and then right-click **Start**.

4. Set the properties of the service SysAdmin.TenantSvc to **Take No Action**.

Figure 20-1: Take No Action



5. Open RDP to the UMP, navigate to c:\acs folder and run wyupdate.exe from the ..:\acs root directory as shown in the screen below.

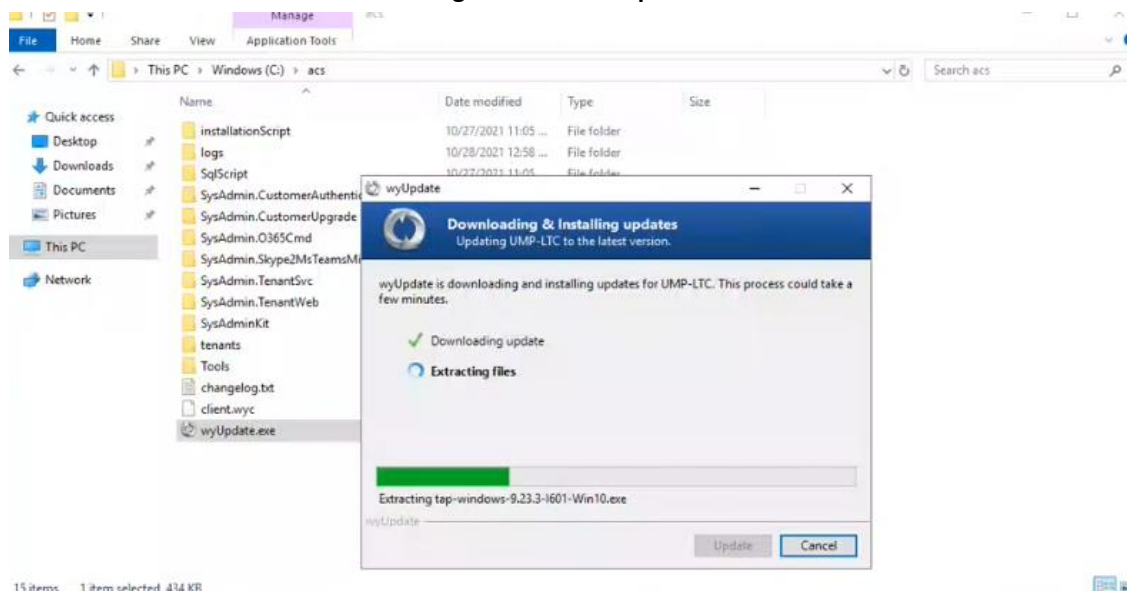
Figure 20-2: Main Upgrade File

Windows (C:) > acs >

Name	Date modified	Type	Size
dbbackup	6/16/2021 8:05 AM	File folder	
installationScript	6/9/2021 7:17 PM	File folder	
Logs	8/11/2021 7:13 AM	File folder	
SqlScript	6/9/2021 7:17 PM	File folder	
SysAdmin.CustomerAuthentication	8/11/2021 7:00 AM	File folder	
SysAdmin.CustomerUpgrade	6/9/2021 7:17 PM	File folder	
SysAdmin.O365Cmd	8/11/2021 7:00 AM	File folder	
SysAdmin.Skype2MsTeamsMigrator	6/9/2021 7:17 PM	File folder	
SysAdmin.TenantSvc	6/9/2021 7:17 PM	File folder	
SysAdmin.TenantWeb	6/24/2021 7:37 AM	File folder	
SysAdminKit	5/19/2021 4:18 PM	File folder	
tenants	8/11/2021 7:07 AM	File folder	
Tools	6/16/2021 7:56 AM	File folder	
changelog.txt	8/9/2021 11:06 AM	Text Document	3 KB
client.wyc	8/11/2021 7:03 AM	WYC File	56 KB
SysAdmin.AdalCache.8.0.200.355.nupkg	6/8/2021 6:56 AM	NUPKG File	8 KB
SysAdmin.AdalCache.8.0.200.359.nupkg	8/8/2021 5:47 AM	NUPKG File	8 KB
<input checked="" type="checkbox"/> wyUpdate.exe	3/31/2021 12:18 PM	Application	435 KB

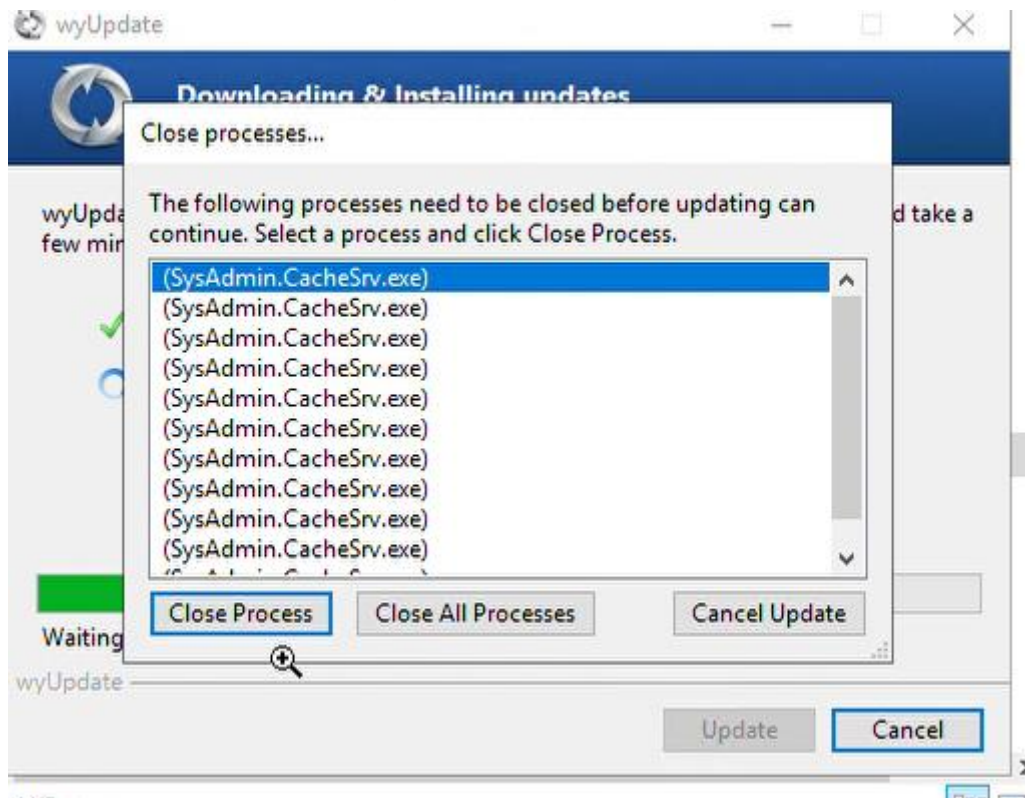
- Run **wyUpdate.exe**.
- In the Updated dialog, click **Update**. The wyUpdate tool validates the installed version to determine whether updates are available or an upgrade is required.

Figure 20-3: Run Update



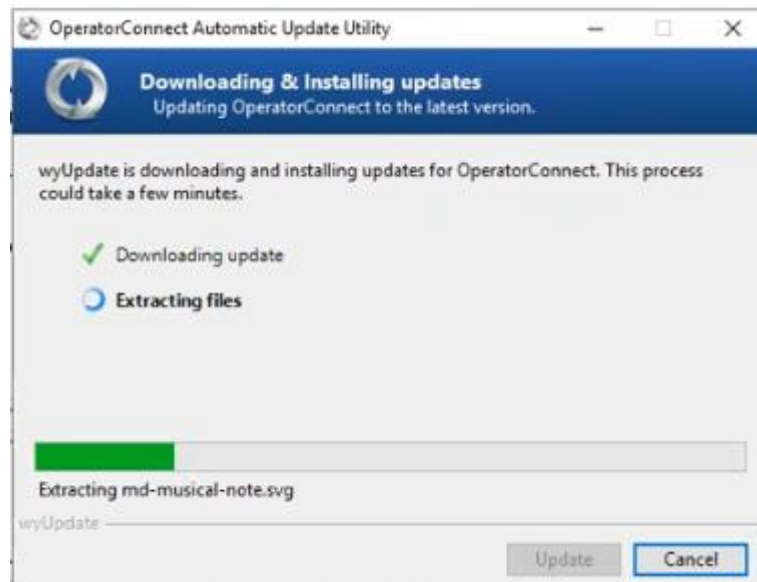
- During the update you are prompted to “close All Processes” services. Confirm this action. This confirmation enforces the upgrade and kills the running processes.

Figure 20-4: Close Processes



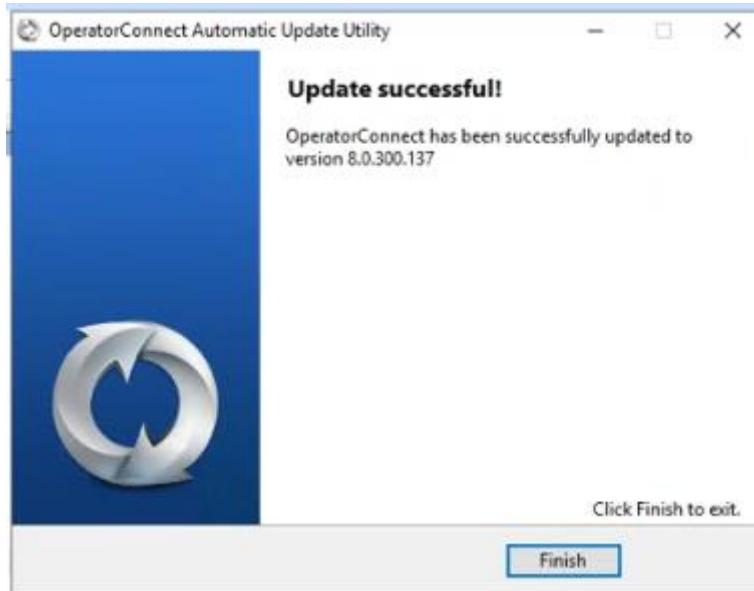
The available updates or version upgrade package is downloaded and the files are installed.

Figure 20-5: Downloading & Installing updates



2. Click **Finish**.

Figure 20-6: Update successful



3. In the Command shell, press enter to continue.

Figure 20-7: Command Shell

```
-----  
DO NOT FORGET TO RUN CUSTOMERUPGRADE IN ADMINISTRATIVE MODE  
AFTER WYUPDATE FINISHES SUCCESSFULLY  
-----  
Press any key to continue . . .
```

20.2.2 Services Updates for each Tenant

This step describes how to run the Services updates separately for each M365 customer tenant.



Run the WyUpdate as administrator using the UMP service admin account that was created in Section 6.3.

Do the following:

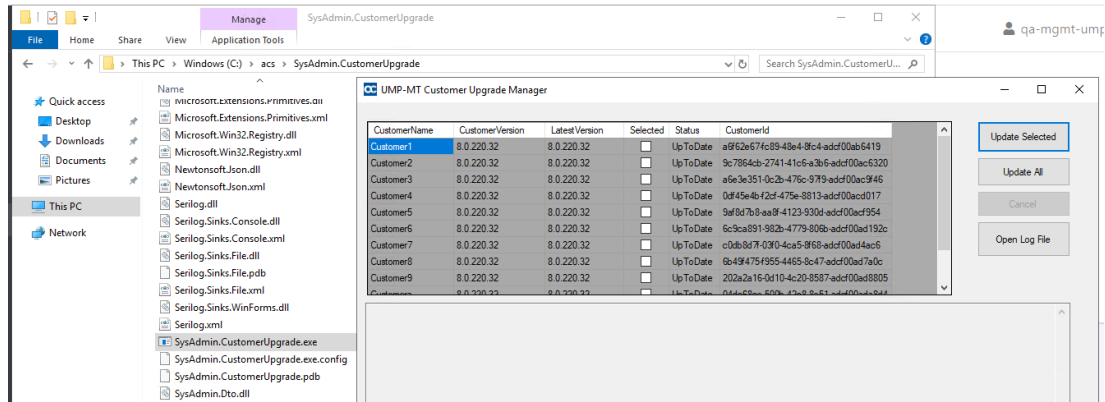
1. Run the file Sysadmin.CustomerUpgrade.exe from directory ...\\acs\SysAdmin.CustomerUpgrade.

Figure 20-8: Run CustomerUpgrade Exe

Name	Date modified	Type	Size
Dapper.dll	8/8/2021 5:54 AM	Application extens...	188 KB
Dapper.xml	8/8/2021 5:54 AM	XML Document	166 KB
DapperExtensions.dll	8/8/2021 5:54 AM	Application extens...	96 KB
DapperExtensions.pdb	8/8/2021 5:54 AM	PDB File	192 KB
Ensure.That.dll	8/8/2021 5:54 AM	Application extens...	63 KB
Ensure.That.xml	8/8/2021 5:54 AM	XML Document	18 KB
Flurl.dll	8/8/2021 5:54 AM	Application extens...	24 KB
Flurl.Http.dll	8/8/2021 5:54 AM	Application extens...	67 KB
Flurl.Http.xml	8/8/2021 5:54 AM	XML Document	160 KB
Flurl.xml	8/8/2021 5:54 AM	XML Document	29 KB
Microsoft.Extensions.Logging.Abstrac...	8/8/2021 5:54 AM	Application extens...	48 KB
Microsoft.Extensions.Logging.Abstrac...	8/8/2021 5:54 AM	XML Document	58 KB
Newtonsoft.Json.dll	8/8/2021 5:54 AM	Application extens...	684 KB
Newtonsoft.Json.xml	8/8/2021 5:54 AM	XML Document	692 KB
Serilog.dll	8/8/2021 5:54 AM	Application extens...	124 KB
Serilog.Sinks.Console.dll	8/8/2021 5:54 AM	Application extens...	32 KB
Serilog.Sinks.Console.xml	8/8/2021 5:54 AM	XML Document	15 KB
Serilog.Sinks.File.dll	8/8/2021 5:54 AM	Application extens...	28 KB
Serilog.Sinks.File.pdb	8/8/2021 5:54 AM	PDB File	7 KB
Serilog.Sinks.File.xml	8/8/2021 5:54 AM	XML Document	33 KB
Serilog.Sinks.WinForms.dll	8/8/2021 5:54 AM	Application extens...	15 KB
Serilog.xml	8/8/2021 5:54 AM	XML Document	284 KB
SysAdmin.CustomerUpgrade.exe	8/8/2021 5:54 AM	Application	46 KB
SysAdmin.CustomerUpgrade.exe.config	8/8/2021 5:54 AM	CONFIG File	2 KB
SysAdmin.CustomerUpgrade.pdb	8/8/2021 5:54 AM	PDB File	80 KB
SysAdmin.Dto.dll	8/8/2021 5:54 AM	Application extens...	255 KB
SysAdmin.TenantLib.dll	8/8/2021 5:54 AM	Application extens...	182 KB
SysAdmin.TenantLib.pdb	8/8/2021 5:54 AM	PDB File	55 KB
System.ComponentModel.Annotation...	8/8/2021 5:54 AM	Application extens...	43 KB
System.Data.SqlClient.dll	8/8/2021 5:54 AM	Application extens...	218 KB
System.Data.SqlClient.xml	8/8/2021 5:54 AM	XML Document	433 KB

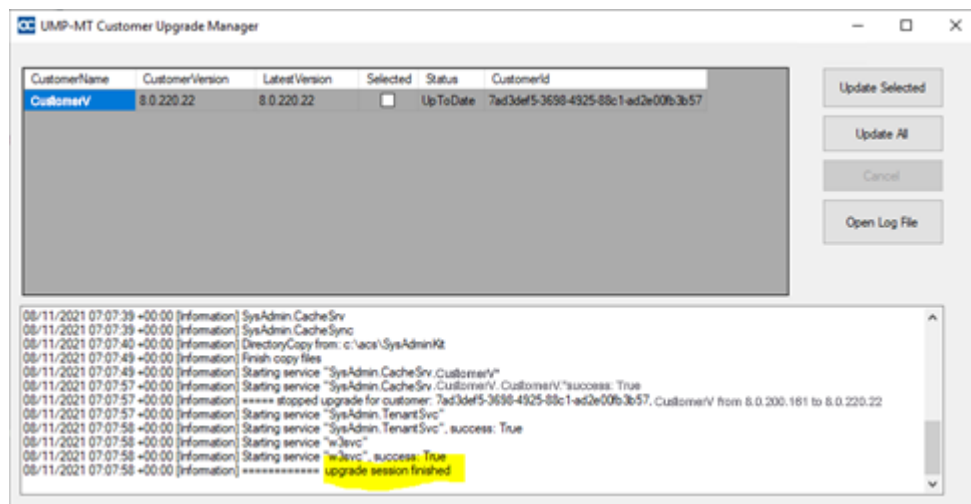
2. In the Customer Upgrade Manager select the customers for which you wish to upgrade and then click **Update Selected**.

Figure 20-9: Choose Customer



- At the end of the process, verify in the log that the upgrade session has been successfully completed.

Figure 20-10: Upgrade Session Finished



- In the Windows Services Manager, start all **sysadmin** services, or in PowerShell, type the following commands:

```
Start-Service sysadmin*
start-service w3svc
```

- In the Main UMP tenant interface, open the License page (**System > License**) and verify that the new version is displayed.

Figure 20-11: Verify UMP Version

MachineId: d3334061-e81b-4ad7-acbb-ef1d3d49e375
 Product Key:
 MultiTenant User License Count: 10000
 MultiTenant Tenant License Count: 25
 MultiTenant Version: 8.0.300.138
 Expiration Date: 2050-12-31

Insert License key

License:

Save license

Copyright © 2020 AudioCodes. All rights reserved.

- In the Multitenant portal, open the Tenants page and verify that the upgraded version is displayed.

Figure 20-12: Verify Upgraded Version

Available Users: 9875, Available Customers: 19
 SysadminKit Version: 8.0.300.138

Show 10 entries

Customer Name	State	SysAdmin Info	Licensing (licensed users)	Queued commands status
essentials	Deployed	version: 8.0.300.138 replication: 2022.03.27.18.25.31 SysAdmin	M365 - EssentialPlus (10)	Queued commands: 0 Executing commands: 0 Replication in progress: no
M365x202362	Deployed	version: 8.0.300.138 replication: 2022.03.27.18.24.48 SysAdmin	M365 - Pro (30)	Queued commands: 0 Executing commands: 0 Replication in progress: no
M365x35102214	Deployed	version: 8.0.300.138 replication: 2022.03.27.18.24.48 SysAdmin	M365 - Pro (25)	Queued commands: 0 Executing commands: 0 Replication in progress: no
M365x45661692	Deployed	version: 8.0.300.138 replication: 2022.03.27.18.25.29 SysAdmin	M365 - Pro (25)	Queued commands: 0 Executing commands: 0 Replication in progress: no
M365x78596656	Deployed	version: 8.0.300.138 replication: 2022.03.27.18.26.02 SysAdmin	M365 - Pro (25)	Queued commands: 0 Executing commands: 0

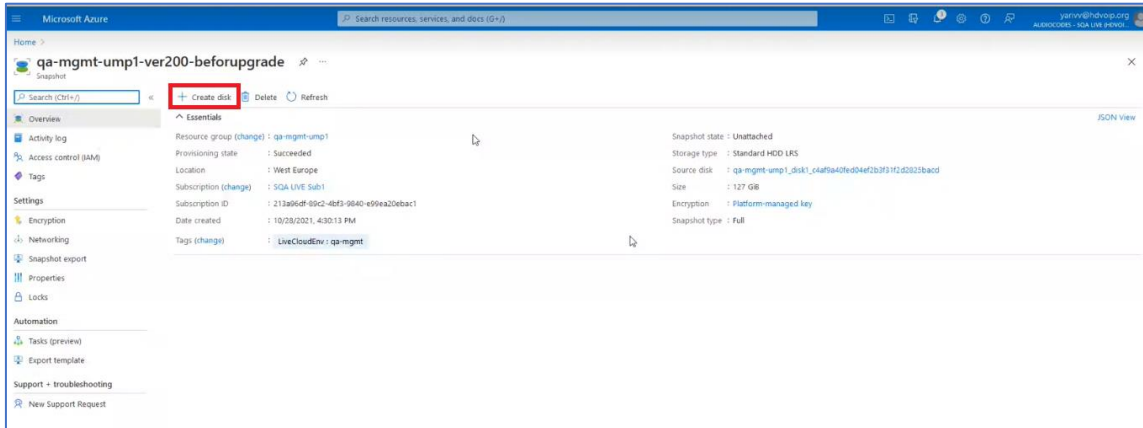
21 UMP Snapshot Restore

This section describes how to create a new disk on the UMP VM and to restore the snapshot image created in Chapter 19 to this disk (create a new VHD image for this disk).

Do the following:

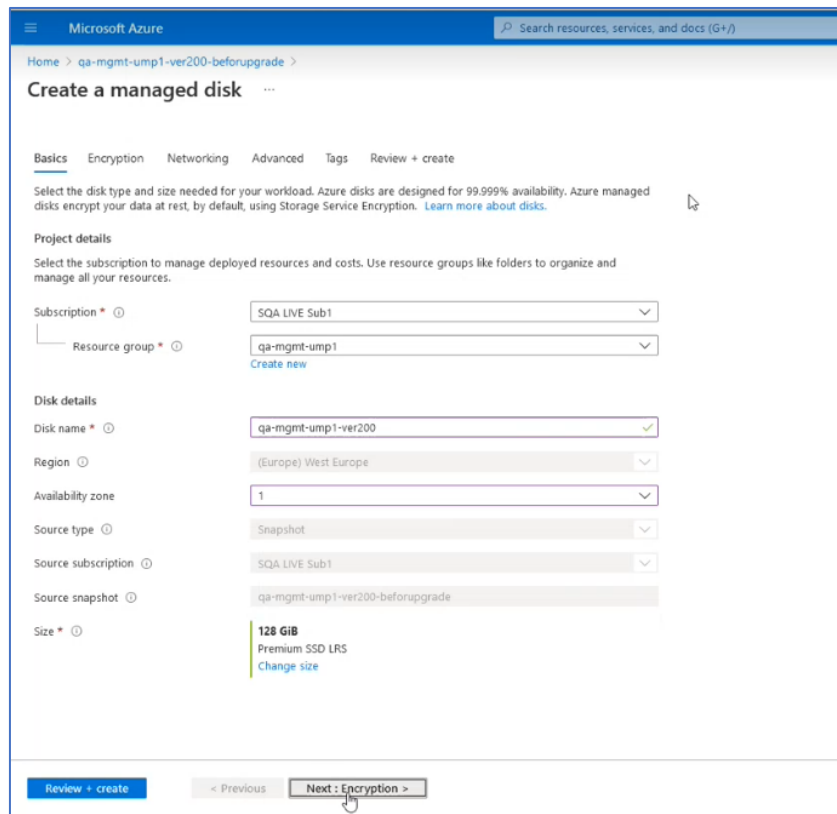
1. Open the new snapshot that you created in Chapter 19 and click **Create Disk**.

Figure 21-1: Create Disk



2. Enter the details of the disk to create a new VHD image.

Figure 21-2: Managed Disk Details



3. Select the **Tags** tab to optionally defined tags for the new disk.

Figure 21-3: Define Tags for the New Disk

Microsoft Azure

Home > qa-mgmt-ump1-ver200-beforupgrade >

Create a managed disk

Basics Encryption Networking Advanced **Tags** Review + create

Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups. [Learn more about tags](#)

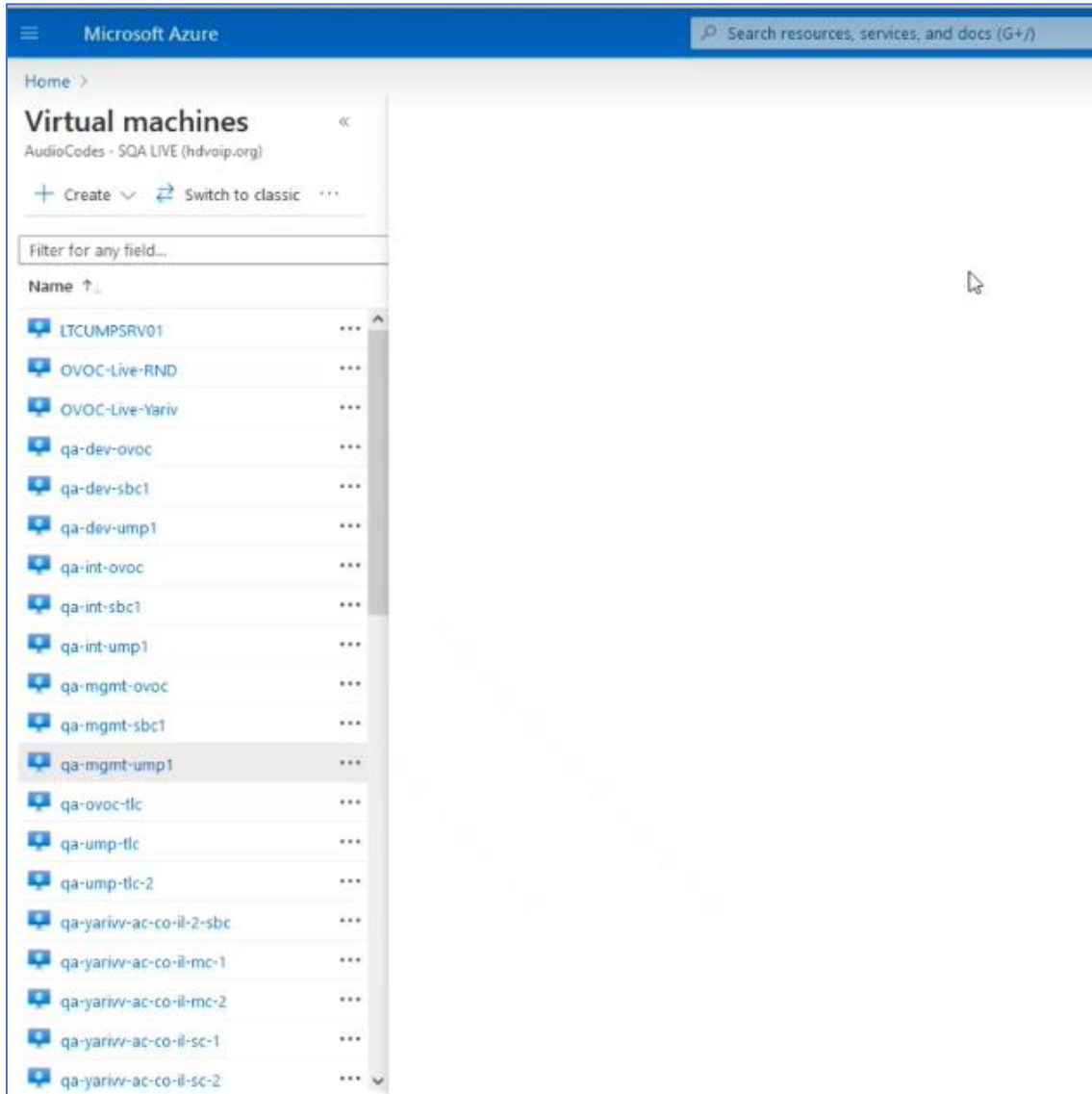
Note that if you create tags and then change resource settings on other tabs, your tags will be automatically updated.

Name	Value	Resource
LiveCloudEnv		2 selected
	qa-dev qa-int qa-mgmt	2 selected

Review + create < Previous Next: Review + create >

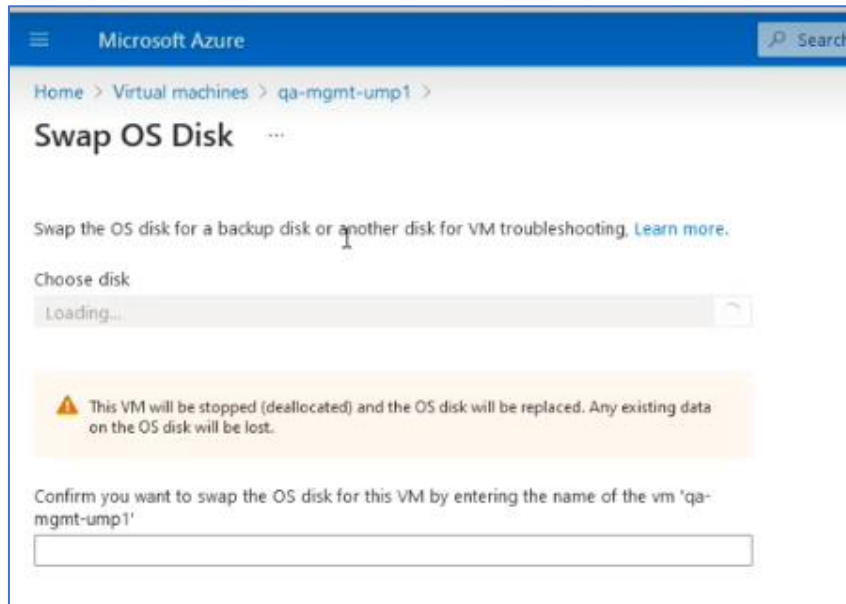
4. Click Review + create.
5. Navigate to the UMP Virtual Machine.

Figure 21-4: UMP Virtual Machine



6. In the portal search field, type **Swap OS Disk**.

Figure 21-5: Swap OS Disk



7. From the Choose Disk drop-down list, choose the snapshot that you created in Chapter 19 (in this example “qa-mgmt-ump1-ver200”).

Figure 21-6: Choose Existing Disk



8. Enter the UMP VM name (in this example “qa-mgmt-ump1”).
9. When the Swap Disk action completes, open the UMP interface and check that all customer data is displayed.

22 UMP Upgrade Testing Checklist

Use the following checklist to verify that all the configuration components of the upgrade have been successfully updated.

Interface	Menu Navigation Path	Check	Configuration Action
OVOC	Network > Device > Manage	<input type="checkbox"/>	Verify the UMP Status is "Green" in the Devices table
		<input type="checkbox"/>	Open the Managed Device page, select device , click Show and verify that "UMP Management" displays "Connected"
OVOC	Open Device Page for UMP Tenant	<input type="checkbox"/>	Verify Customers Deployment State is "Deployed"
		<input type="checkbox"/>	Verify for each customer that the SysAdminKit version is 8.0.300.138
UMP	System > License	<input type="checkbox"/>	Verify "MultiTenant Version: 8.0. 300.138"
		<input type="checkbox"/>	Verify available license is not missing
	System > Invitation Settings	<input type="checkbox"/>	Verify Customer Authentication Portal Url is set to: https://<UMP_FQDN>/authenticate
	Security > Auth Tokens	<input type="checkbox"/>	Verify that the Client ID and Secret ID are provided by the UMP app registration (check PMP site).
		<input type="checkbox"/>	Verify that the Redirect Url is set to: https://<UMP_FQDN>/authenticate/OAuth2Callback Note: Verify that the same redirect Uri is configured for the UMP app registration.
SBC List	<input type="checkbox"/>	Verify that the SBC exists.	
OVOC	Network > Customers	<input type="checkbox"/>	Verify the Customers Status and Deployment status is "Green" in the Devices table
		<input type="checkbox"/>	Verify "Enabled" is checked

Interface	Menu Navigation Path	Check	Configuration Action
		<input type="checkbox"/>	Verify the "total number of DIDs" and "users count" is displayed.
		<input type="checkbox"/>	Verify Azure Tenant ID exists.
		<input type="checkbox"/>	Navigate to "Provider side" and Verify the "Users Count" is displayed
	Customer Actions Menu > Edit Customer	<input type="checkbox"/>	<p>Edit User and change a parameter (e.g. Department) and the verify that the change has been implemented in OVOC / Teams.</p> <ul style="list-style-type: none"> ■ To enforce the Teams update, in the UMP interface, navigate to Queue Changes -> Process All <ul style="list-style-type: none"> ● To verify users in OVOC: Open OVOC -> Users -> User details ● To Verify users in Microsoft Teams: Open https://admin.Teams.microsoft.com
UMP Self-service portal	Site Locations	<input type="checkbox"/>	Verify that the SBC is in "Deployed" status. Click "Add/Edit SBC Prefix".
		<input type="checkbox"/>	Verify that the DID exists.
		<input type="checkbox"/>	Add a DID and verify that its successfully added on the SBC.

23 Post Upgrade Actions

This section describes the actions to perform following the upgrade.

23.1.1 Remove Token Registration Permissions

This version includes an enhanced token mechanism that eliminates the need to configure API permissions for the UMP Background Registration application registration (see Chapter 10). This procedure describes how to remove these permissions from your app registration.

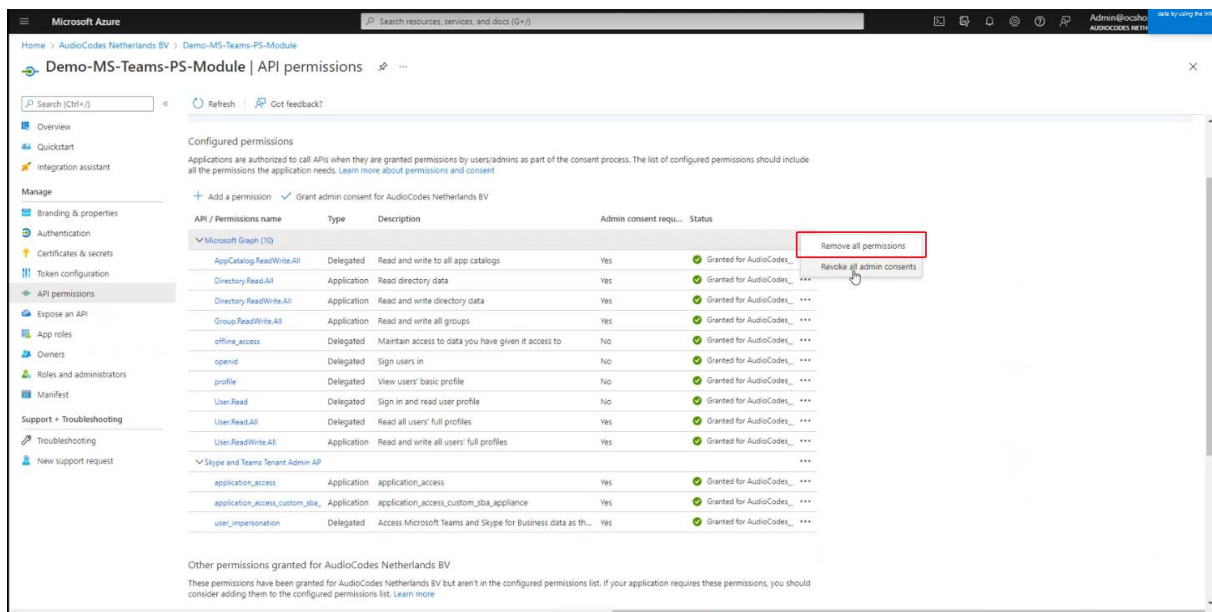


This procedure is relevant for UMP upgrades from Versions 8.0.200 and 8.0.220.

To remove configured permissions:

1. Open the API Permissions screen for the UMP Background Replication registration.

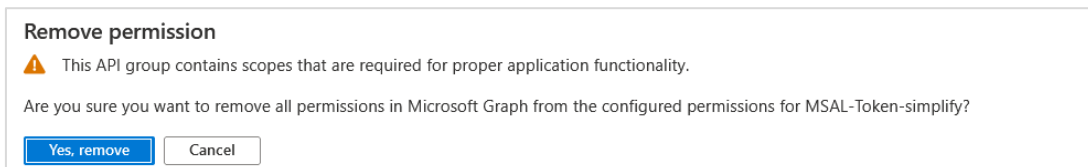
Figure 23-1: API permissions



2. At the top right-hand corner of the Microsoft Graph table for the Configured permissions, click and select **Remove all permissions**.

The following confirmation is displayed:

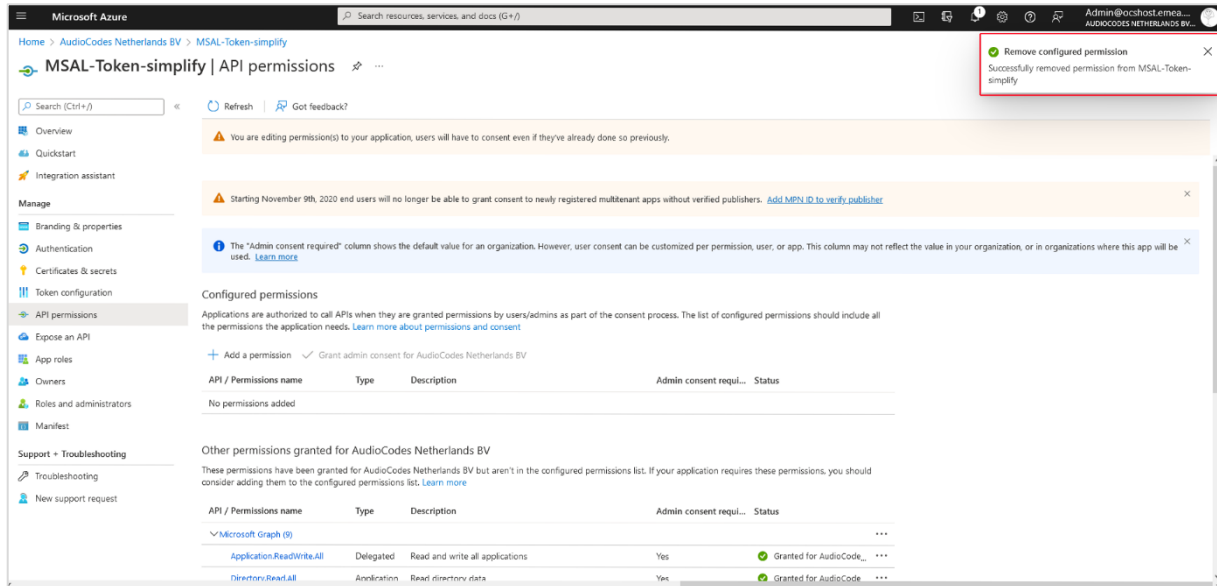
Figure 23-2: Remove permission



3. Click **Yes, remove**.

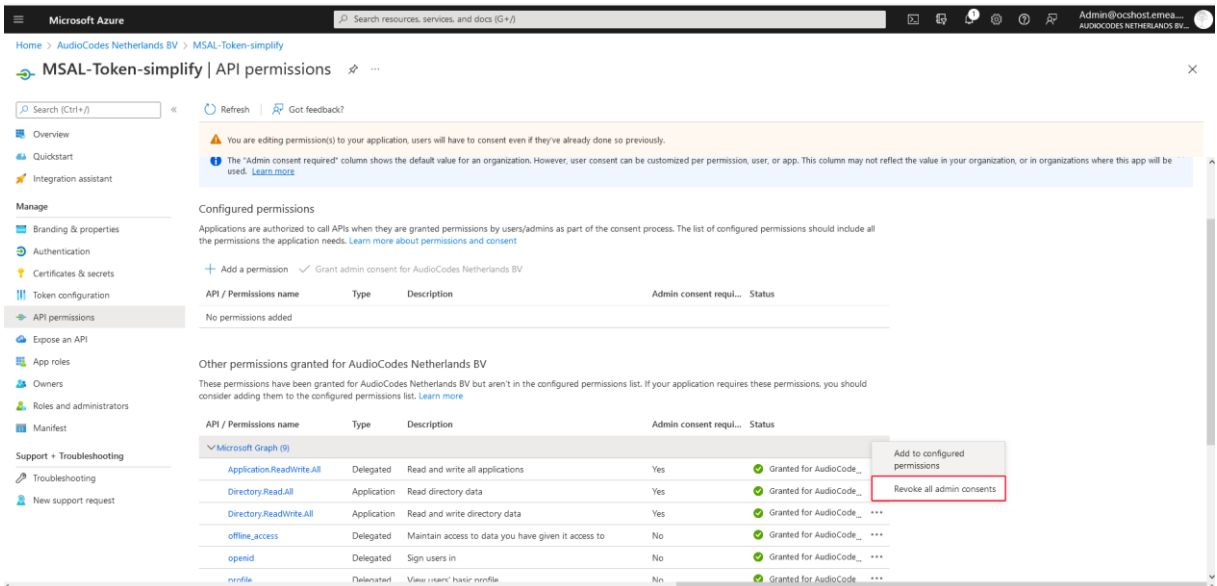
The configured permissions are removed.

Figure 23-3: Configured Permissions Removed



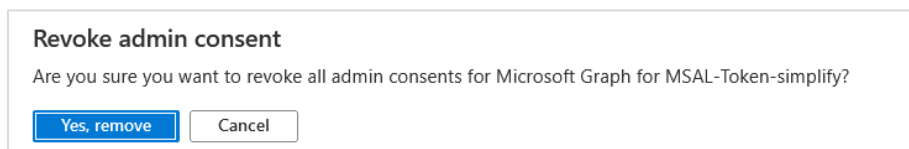
- At the top right-hand corner of the Microsoft Graph table for the Other permissions granted for the <UMP tenant>, click ...and then select **Revoke all admin consents**.

Figure 23-4: Remove other permissions



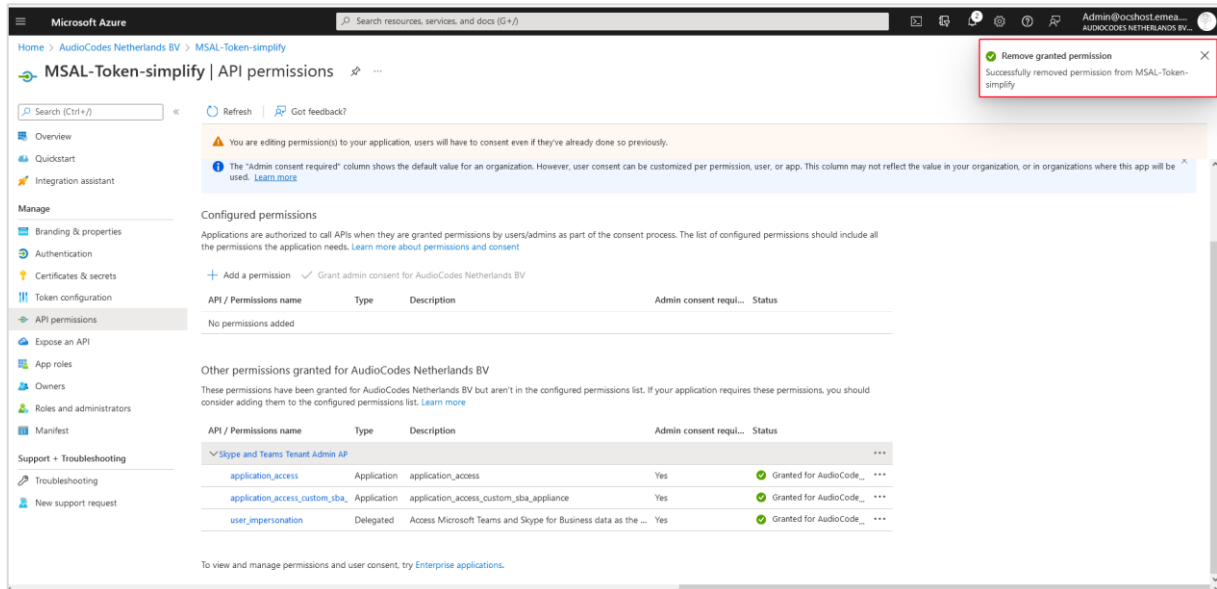
The following confirmation is displayed:

Figure 23-5: Revoke admin consent



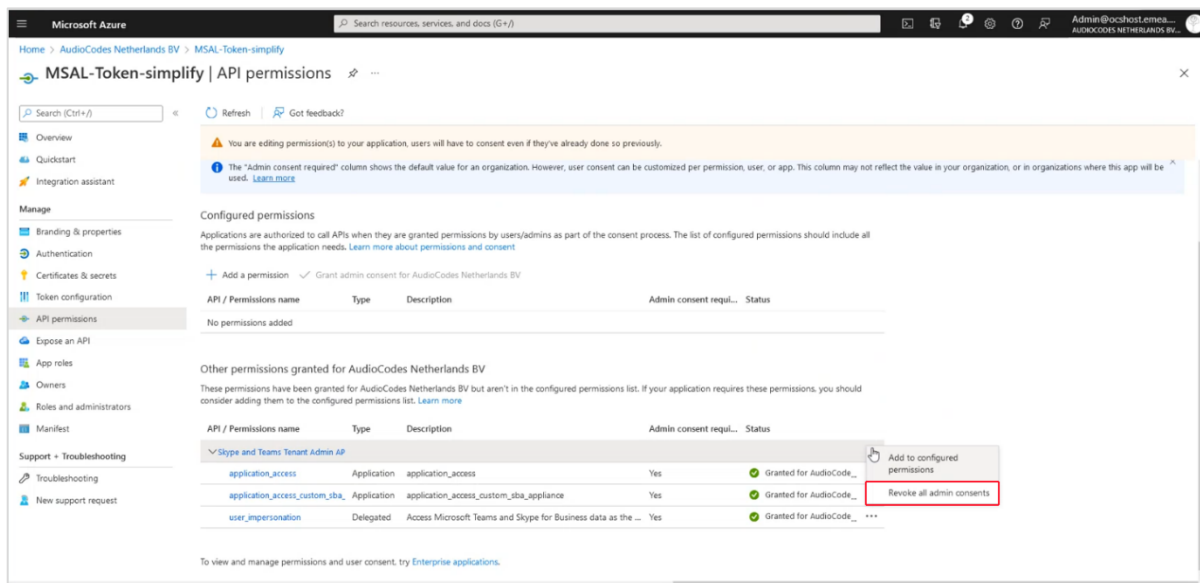
- Click **Yes, remove**.

Figure 23-6: Granted Permissions Removed



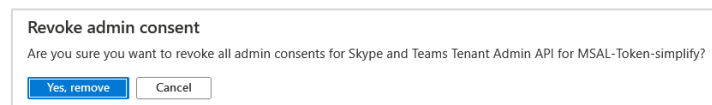
- At the top right-hand corner of the Microsoft Graph table for the Skype and Teams Tenant Admin AP permissions granted for the <UMP tenant>, click ...and then select **Revoke all admin consents**.

Figure 23-7: Revoke Skype and Teams Tenant Admin AP



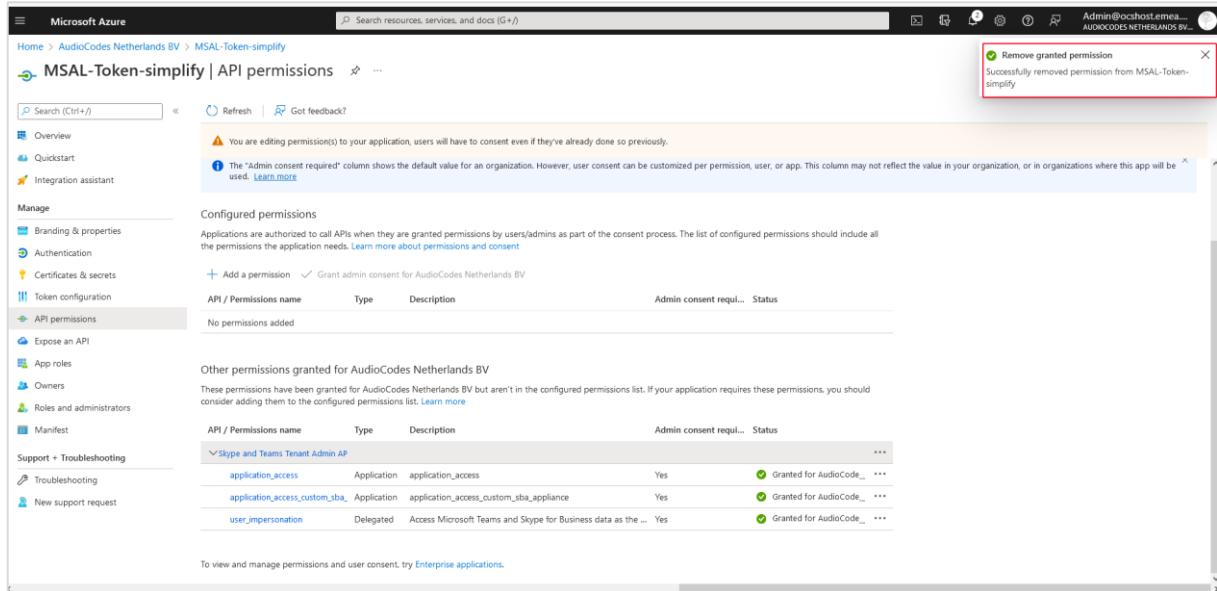
The following confirmation is displayed:

Figure 23-8: Revoke admin consent



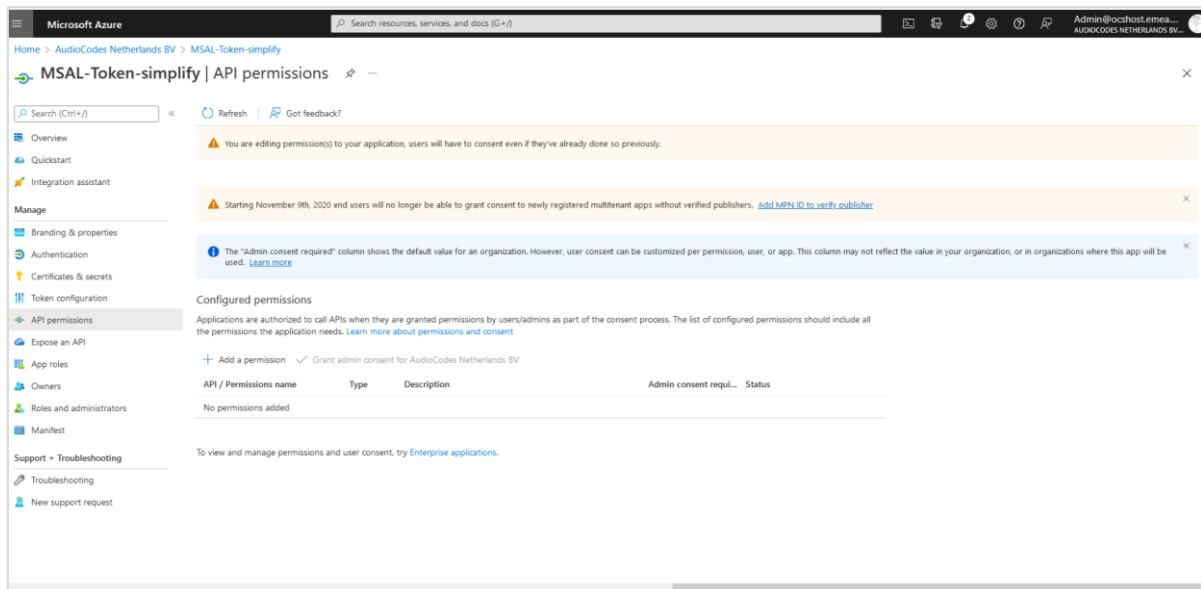
- Click **Yes, remove**.

Figure 23-9: Remove granted permission



The following screen is displayed with all permissions removed.

Figure 23-10: Removed Permissions



23.1.2 Update Scripts

The template scenario scripts have been updated in version 8.0.300, therefore existing scripts are overwritten and must be updated to the correct notation (see Section 24.5.2).

Part IV

Service Provider Management

24 SBC and M365 Onboarding Script Templates

The Onboarding wizard enables you to apply template deployment scripts for both the SBC and Microsoft 365 configuration. AudioCodes Professional Services provides a library of templates scripts that are based on common customer scenarios. The SBC Onboarding wizard applies the SBC Onboarding CLI scripts to the SBC device during the deployment process. Likewise it applies the Microsoft 365 scripts to the Azure platform. The scripts can be tailored to Service Provider requirements globally or for specific M365 tenants.



Warning: Editing the script, can damage the onboarding process and the SBC configuration. It is highly recommended that scripts should be changed only by AudioCodes Professional services.



Before Onboarding new customers SBC device CLI script files should be preconfigured according to M365 tenant site requirements. Consult with AudioCodes Professional Services.

The scripts contain several elements:

- Preconfigured SBC CLI script parameters according to the deployment type e.g. SIP Trunk, BYOC or IP-PBX
- Common Parameters for all the Tenants per SBC include:
 - Carrier Side:
 - ◆ Proxy set = Per Carrier
 - ◆ IP Profile Name = Per Carrier
 - ◆ N x (Proxy set = IP Profile Name)
 - Teams Side:
 - ◆ Proxy set = Teams
 - ◆ SIP Interface = Teams
 - ◆ IP Profile Name = Teams
 - Dial Plan Name = CustDialPlan
- Unique Parameters per Tenant include:
 - IP Group name
 - ◆ Carrier Side = “customer Name”-C’
 - ◆ Teams Side = “customer Name”-T’
- Custom Variables (see below)

24.1 SBC Template Scenarios

The following table describes the template scenario scripts that are provided in the UMP-365. These scripts are saved in the SQL database in the dbo.SbcScriptTemplate file.

Table 24-1: Scenario Scripts

ID	Scenario Script	Description
7	sbc-scenario7	performs basic configuration of SBC when provider side is configured with SIP Trunk.
700	sbc-scenario7cleanup	Removes sbc-scenario7 script configuration.
100	sbc-add-prefix	Adds dial plan prefix when the provider side is configured as either an IP-PBX or a SIP Trunk.
101	sbc-remove-prefix	Removes dial plan prefix when the provider side is configured as either an IP-PBX or a SIP Trunk.
103	add-ipx-user	Adds an IP-PBX registered user when provider side is configured as an IP-PBX.

Figure 24-1: dbo.SbcScriptTemplate

Id	Script	Description	FriendlyName	ScriptType	CustomerName
7	configure voip	NULL	sbc-scenario7	1	NULL
700	configure voip	NULL	sbc-scenario7C...	2	NULL
100	configure voip	NULL	sbc-add-prefix	NULL	NULL
101	configure voip	NULL	sbc-remove-pr...	NULL	NULL
103	# Registration...	NULL	add-ip-pbx-user	NULL	NULL
5000	configure voip	NULL	sbc-add-vo-...	NULL	NULL
5001	configure voip...	NULL	sbc-remove-ec...	NULL	NULL
800	NULL	NULL	NULL	NULL	NULL
NULL	NULL	NULL	NULL	NULL	NULL

24.1.1 sbc-scenario7

The following example displays the **sbc-scenario7** script for basic SBC configuration. Onboarding wizard defined variables are highlighted in **blue**.

```
configure voip
ip-group new
name "{{CustomerId}}-c"
proxy-set-name "{{SBC.CarrierID}}"
ip-profile-name "{{SBC.CarrierID}}"
tags "Trunk={{SBC.OnlinePstnGateway}}"
classify-by-proxy-set disable
call-setup-rules-set-id 1
activate
exit
ip-group new
```

```

name "{{CustomerId}}-t"
proxy-set-name "Teams"
ip-profile-name "Teams"
local-host-name "{{SBC.OnlinePstnGateway}}"
always-use-source-addr enable
tags "Tenant={{SBC.OnlinePstnGateway}}"
classify-by-proxy-set disable
call-setup-rules-set-id 0
{{#if SBC.EnableCAC}}
  cac-profile "{{SBC.CacProfile}}"
{{/if }}
activate
exit

{{#if SBC.FlagCarrierRegistration}}
sip-definition account new
  account-name "{{CustomerId}}"
  served-ip-group-name "{{CustomerId}}-t"
  serving-ip-group-name "{{CustomerId}}-c"
  user-name "{{SBC.CarrierUserName}}"
  password "{{SBC.CarrierPassword}}"
  host-name "{{SBC.CarrierHostName}}"
  contact-user "{{SBC.CarrierMainLine}}"
  register reg
  application-type sbc
  activate
  exit
{{/if }}

{{#each SBC.DialPlanPrefixes}}
sbc dial-plan where name "{{this.DialPlanName}}"
  {{#each this.Rules}}
  dial-plan-rule new
    name "{{this.Name}}"
    prefix "{{this.Prefix}}"
    tag "{{this.Tag}}"
  exit
  {{/each}}
  activate
  exit
  {{/each}}

do write

```

For each rule (for each number prefix added in the Onboarding wizard), add the prefix for customer ID (this.name) and apply it to the PSTN gateway tag (this.Tag).

The following shows an example script:

Figure 24-2: Example Script

```

configure voip
ip-group new

```

```

name "SIPTrunkPlus-c"
proxy-set-name "SIPTrunk"
ip-profile-name "SIPTrunk"
tags "Trunk=audio0code.onmicrosoft.com"
classify-by-proxy-set disable
call-setup-rules-set-id 1
activate
exit
ip-group new
name "SIPTrunkPlus-t"
proxy-set-name "Teams"
ip-profile-name "Teams"
local-host-name "audio0code.onmicrosoft.com"
always-use-source-addr enable
tags "Tenant=audio0code.onmicrosoft.com"
classify-by-proxy-set disable
call-setup-rules-set-id 0
activate
exit

sbc dial-plan where name "CustDialPlan"
dial-plan-rule new
  name "SIPTrunkPlus"
  prefix "+9723976400"
  tag "audio0code.onmicrosoft.com"
exit
dial-plan-rule new
  name "SIPTrunkPlus"
  prefix "+6138884445"
  tag "audio0code.onmicrosoft.com"
exit
dial-plan-rule new
  name "SIPTrunkPlus"
  prefix "+0139123345689"
  tag "audio0code.onmicrosoft.com"
exit
activate
exit
do write

```

24.1.2 sbc-scenario7Cleanup

This **sbc-scenario7Cleanup** script removes every dial plan rule that matches the customer ID.

```

configure voip
  no ip-group where name "{{CustomerId}}-c"
  no ip-group where name "{{CustomerId}}-t"
  no sip-definition account where account-name "{{CustomerId}}"
  sbc dial-plan where name "CustDialPlan"
  no dial-plan-rule where name "{{CustomerId}}"
activate

```

```
exit
do write
```

24.1.3 add-ipx-user

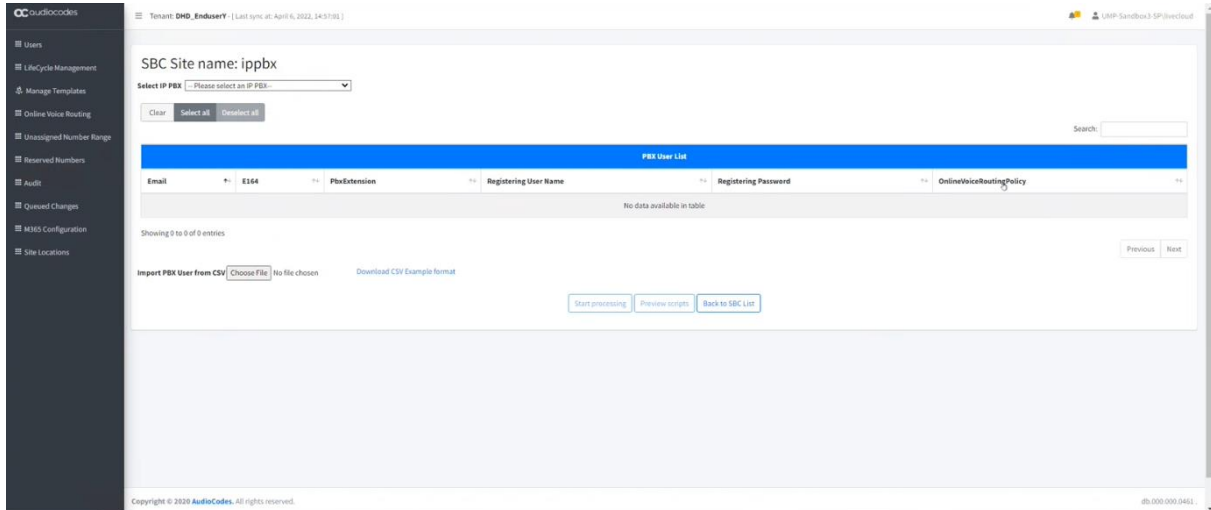
The **add-ipx-user** script adds a registered IP-PBX user and extensions to specific site and configures connection to specific SBC. Onboarding wizard defined variables are highlighted in blue. Note that this script includes a unique Dial Plan name **RegisteredUsers**.

```
# Registration
configure voip
sbc dial-plan where name "CustDialPlan"
dial-plan-rule new
name "{{SBC.SbcSiteName}}"
prefix "{{sbcEscape PbxUser.PbxExtension}}"
tag "{{SBC.OnlinePstnGateway}}"
exit
dial-plan-rule new
name "{{SBC.SbcSiteName}}"
prefix "+{{sbcEscape PbxUser.E164}}"
tag "{{SBC.OnlinePstnGateway}}"
exit
activate
exit
sip-definition proxy-and-registration
user-info sbc-user-info new
  local-user "{{PbxUser.LocalUserName}}"
    username "{{PbxUser.RegisteringUserName}}"
    password {{PbxUser.RegisteringPassword}}
    ip-group-name "{{SBC.SbcSiteName}}-t"

  activate
  exit
exit
sbc dial-plan where name "RegisteredUsers"
  dial-plan-rule new
  name "{{SBC.SbcSiteName}}"
  prefix "+{{sbcEscape PbxUser.E164}}"
  tag "{{PbxUser.PbxExtension}}"
  activate
  exit
  dial-plan-rule new
  name "{{SBC.SbcSiteName}}"
  prefix "{{sbcEscape PbxUser.PbxExtension}}"
  tag "{{PbxUser.E164}}"
  activate
  exit
exit
do write
```

The figure below shows an example of an SBC site for an IP-PBX customer.

Figure 24-3: IP-PBX Customer



24.1.4 sbc-add-prefix

The **sbc-add-prefix** script adds phone prefixes to a specific site for a specific customer. Onboarding wizard defined variables are highlighted in **blue**.

```
configure voip
  sbc dial-plan where name "{{DialPlanName}}"
  {{#each CmdData.DialPlanRules.ToAdd}}
  dial-plan-rule new
  name "{{../SBC.SbcSiteName}}"
  prefix "{{this.Prefix}}"
  tag "{{this.Tag}}"
  exit
  {{/each}}
  activate
exit
do write
```

For example in the figure below, four different prefixes are defined. The first one is defined on the **fixedmobileuc.com** SBC and the other three are defined on a different SBC with a different dial plan assigned for each prefix. For each rule, the script substitutes the variables with the appropriate values. Note that this script includes a unique Dial Plan name **Teams**.

Figure 24-4: Add Prefixes

SBC: 22 - Location: CustomerId

Add additional prefixes / number ranges

Select Dial Plan: Teams Tag / PSTN Gateway: M365x25175153.onmicrosoft.com

Telephone Number Prefix: New Number prefix

Upload from single file: Choose file Browse

Current prefixes

Prefixes shown below are from cache. Press **Reload** to refresh them from SBC.

Dial Plan Name	Prefix	Tag
<input type="checkbox"/> CustDialPlan	+312355561	CustomerId.sbc-tobi.customers.fixedmobileuc.com
<input type="checkbox"/> CustDialPlan	+97239764000	M365x25175153.onmicrosoft.com
<input type="checkbox"/> RegisteredUsers	+013614456789	M365x25175153.onmicrosoft.com
<input type="checkbox"/> Teams	+019123854567	M365x25175153.onmicrosoft.com

1 - 4 of 4 items

Save

```

configure voip
sbc dial-plan where name "{{CustDialPlan}}"
{{#each CmdData.DialPlanRules.ToAdd}}
dial-plan-rule new
name "{{./CustomerId}}"
prefix "{{+31255561}}"
tag "{{CustomerId.sbc-tobi.fixedmobileuc.com}}"
exit
{{/each}}
activate

exit
do write

```

```

configure voip
sbc dial-plan where name "{{CustDialPlan}}"
{{#each CmdData.DialPlanRules.ToAdd}}
dial-plan-rule new
name "{{./CustomerId}}"
prefix "{{+97239764000}}"
tag "{{M365x25175153.onmicrosoft.com}}"
exit
{{/each}}
activate

exit
do write

```

```

configure voip
sbc dial-plan where name "{{RegisteredUsers}}"
{{#each CmdData.DialPlanRules.ToAdd}}
dial-plan-rule new
name "{{./CustomerId}}"
prefix "{{+013614456789}}"

```

```

tag "{{M365x25175153.onmicrosoft.com}}"
exit
{{/each}}
activate
exit
do write

```

```

configure voip
  sbc dial-plan where name "{{Teams}}"
  {{#each CmdData.DialPlanRules.ToAdd}}
  dial-plan-rule new
  name "{{../CustomerId}}"
  prefix "{{+019123854567}}"
  tag "{{M365x25175153.onmicrosoft.com}}"
  exit
  {{/each}}
  activate
exit
do write

```

24.1.5 sbc-remove-prefix

The **sbc-remove-prefix** script removes all configured phone prefixes from the CustDialPlan (applied globally for all customers).

```

configure voip
  sbc dial-plan where name "CustDialPlan"
  {{#each ToRemove}}
  no dial-plan-rule "{{this.Index}}"
  {{/each}}
  activate
exit
do write

```

24.2 M365 Template Scenarios

The default M365 Onboarding scripts are embedded in the UMP-365 software; however, are not included in the database. These scripts are shown in the sections below. When you wish to create your own scripts, they must be added to the database in a similar manner to SBC scripts (with script type "3" assigned for onboarding a customer and script type "4" for cleanup / removal of a customer). See Section 24.4.

Figure 24-5: M365 Scripts

Id	Script	Description	FriendlyName	ScriptType	CustomerVariables
7	configure voip ip-group new name "{{CustomerId}}...	NULL	sbcs-scenario7	1	NULL
700	configure voip no ip-group where name "{{Custome...	NULL	sbcs-scenario7Cleanup	2	NULL
100	configure voip sbc dial-plan where name "{{DialPl...	NULL	sbcs-add-prefix	1	NULL
101	configure voip sbc dial-plan where name "{{DialPl...	NULL	sbcs-remove-prefix	2	NULL
5000	configure voip sbc dial-plan where name "{{DialPla...	NULL	sbcs-add-oc-numbers	1	NULL
5001	configure voip sbc dial-plan where name "{{DialPla...	NULL	sbcs-remove-oc-numbers	2	NULL
8	Set-CsOnlinePstnUsage -Identity Global -Usage @{{A...	Custom M365 script	M365-onboarding	3	NULL
800	Get-CsOnlineVoiceRoute Where-Object {\$_.Online...	Customer M365 cleanup	M365-cleanup	4	NULL
103	# Registration configure voip sbc dial-plan where...	NULL	add-ip-pbx-user	NULL	NULL


Table 24-2: M365 Script Scenarios

ID	Script Type	Scenario Script	Description
8	3	Custom M365 script	Custom M365 Onboarding script.
800	4	Custom M365 Cleanup	Custom M365 Onboarding cleanup script.

24.2.1 Default M365 Tenant Onboarding Script

The default M365 Onboarding script is shown below. This script is hardcoded and is not included in the SQL database.


```
Set-CsOnlinePstnUsage -Identity Global -Usage
@{Add='Unrestricted'} -ErrorAction ignore;
New-CsOnlineVoiceRoute -Identity 'Unrestricted' -NumberPattern
'.*' -OnlinePstnGatewayList '{{SBC.OnlinePstnGateway}}' -Priority
1 -OnlinePstnUsages 'Unrestricted' -ErrorAction ignore;
New-CsOnlineVoiceRoutingPolicy -Identity 'Unrestricted' -
OnlinePstnUsages 'Unrestricted' -ErrorAction ignore;# end
script;";
```

 Custom variables can be applied to this script in a similar manner to the SBC scripts.

24.2.2 Default M365 Tenant Cleanup Script

The default M365 Tenant Cleanup script is shown below. This script is hardcoded and is not included in the SQL database.

```
Get-CsOnlineVoiceRoute | Where-Object {$_.OnlinePstnGatewayList -
like '{{SBC.OnlinePstnGateway}}'} | Remove-CsOnlineVoiceRoute"
```

 Custom variables can be applied to this script in a similar manner to the SBC scripts.

24.3 Onboarding Wizard Defined Variables

The following table describes the list of variables that are configured in the Onboarding wizard and are applied in the CLI script runtime.

Table 24-3: Predefined Variables

Variable	Description
{{CustomerId}}	The Short Customer Name.
{{CustomerId}}-t	served-ip-group-name
{{CustomerId}}-c	serving-ip-group-name
{{SBC.CarrierID}}	proxy-set-name and ip-profile-name.
{SBC.OnlinePstnGateway}}	The Known FQDN of the SBC device.
{{SBC.EnableCAC}}	Indicates whether Call Admission Control is enabled.
{{SBC.CacProfile}}	When {{SBC.EnableCAC}} is enabled, the name of the CAC Profile.
{{ SBC.FlagCarrierRegistration}}	Indicates whether the SBC is connected to a SIP trunk or BYOC. The following SIP definitions are created by the script: <ul style="list-style-type: none"> ■ account-name-CustomerID ■ served-ip-group-name- CustomerID -t ■ serving-ip-group-name- CustomerID -c
{{SBC.CarrierUserName}}	When {{ SBC.FlagCarrierRegistration}} is enabled, the username used to connect to the SIP trunk or BYOC provider.
{{SBC.CarrierPassword}}	When {{ SBC.FlagCarrierRegistration}} is enabled, the password used to connect to the SIP trunk or BYOC provider.
{{SBC.CarrierHostName}}	When {{ SBC.FlagCarrierRegistration}} is enabled, the host-name of the SIP trunk or BYOC provider.
{{SBC.CarrierMainLine}}	When {{ SBC.FlagCarrierRegistration}} is enabled, the contact-user of the SIP trunk or BYOC provider.
{{this.DialPlanName}}	Default hard-coded value: CustDialPlan
{{SBC.DialPlanPrefixes}}	SBC dial plan prefixes.

Variable	Description
{{this.Name}}	Used to indicate the customer’s shortname in the dial plan rule.
{{this.Prefix}}	The prefixes configured in the dial plan rule.
{{this.Tag}}	Used to indicate the Known FQDN of the SBC device (PSTN Gateway) to match with {{this.Prefix}} in the Dial Plan Rule.
{{sbcEscape PbxUser.E164}}	The PBX Username used to connect to an IP-PBX provider.
{{PbxUser.PbxExtension}}	The PBX User extension used to connect to an IP-PBX provider.
{{PbxUser.E164}}	The PBX E164 username used to connect to an IP-PBX provider.

24.4 Custom Variables

Custom variables can be defined either in the template scenario scripts or in custom scripts. They must be configured in the Custom/Variables column for the script in the dbo.SbcScriptTemplate table. Its recommended to define them with proper names such as “localhostname” and not simply variable1, variable2 etc.

Figure 24-6: Custom Script

The figure consists of two screenshots of a SQL Server Enterprise Manager interface showing the 'dbo.SbcScriptTemplate' table. The top screenshot shows a table with columns: Id, Script, Description, FriendlyName, ScriptType, and CustomerVariables. Row 800 is highlighted with a red box, showing 'custom script' in the Script column, 'customscript' in the FriendlyName column, and 'variable1,variable2' in the CustomerVariables column. The bottom screenshot shows the same table, but row 800 now has 'localhostname' in the CustomerVariables column.

In the script itself, the custom variable must be defined with the notation “{{CustomVar.xxx}}”. In the script example below, the defined customer variables are local host name=variable1 and tenant ID=variable2. These variables then appear as fields the Onboarding wizard when the script is selected.

Figure 24-7: Custom Variables

```

SQLQuery6.sql - U...1-c\umpadmin (97)*  UMP-training1-c\SbcScriptTemplate  SQLQuery4.sql - U...1-c\umpadmin (80)  SQLQuery3.sql - U...1-c\umpadmin (59)
ip_profile_name "Teams"
local_host_name "{{CustomVar.Variable1}}"
always-use-source-add-enable-y
tags "tenant={{CustomVar.Variable2}}"
classify-by-proxy-set-disable
call-setup-rules-set-id @
{{if SBC.EnableCAC}}
cac-profile "{{SBC.CacProfile}}"
{{/if }}
activate
exit

{{if SBC.FlagCarrierRegistration}}
sip-definition account new
account-name "{{CustomerId}}"
served-ip-group-name "{{CustomerId}}-t"
serving-ip-group-name "{{CustomerId}}-c"
user-name "{{SBC.CarrierUserName}}"
password "{{SBC.CarrierPassword}}"
host-name "{{SBC.CarrierHostName}}"
contact-user "{{SBC.CarrierMainLine}}"
register reg
application-type sbc
activate
exit
{{/if }}

{{each SBC.DialPlanPrefixes}}
sbc dial-plan where name "{{this.DialPlanName}}"
{{each this.Rules}}
dial-plan-rule new
name "{{this.Name}}"
prefix "{{this.Prefix}}"
tag "{{this.Tag}}"
exit
{{/each}}
activate
exit
{{/each}}
do write

```

100 %
 Connected (1/1) UMP-training1-c\SQLSYSADMIN... UMP-training1-c\umpadm... SysAdminTenant 00:00:00

In the screen below, custom variables are defined for the IP-PBX.

Figure 24-8: Custom Variables for IP-PBX

Id	Script	Description	FriendlyName	Script Type	CustomerVariables	
1	1031	configure voip sbc dial-plan where name "CustDia...	NULL	SIP Trunk Registration Cleanup	2	NULL
2	10700	configure voip no ip-group where name "{{Custo...	NULL	old_sbc-scenario7Cleanup	2	NULL
3	10100	configure voip sbc dial-plan where name "CustDi...	NULL	old_sbc-add-prefix	NULL	NULL
4	10101	configure voip sbc dial-plan where name "CustDi...	NULL	old_sbc-remove-prefix	NULL	NULL
5	7	configure voip ip-group new name "{{CustomerI...	NULL	sbc-scenario7	1	NULL
6	1010	# definitions of PBX connectivity # # customer ...	NULL	IP PBX	1	IPIPPBX-proxyaddress,IPPBX-proxyaddress-SIPPort...
7	1011	# definitions of IPPBX cleanup configure voip sp-...	NULL	IP PBX Cleanup	2	NULL
8	1021	configure voip no ip-group where name "{{Custo...	NULL	Add SIP Trunk Cleanup	2	NULL
9	10103	# Registration configure voip sbc dial-plan wher...	NULL	old_add-ip-pbx-user	NULL	NULL
10	1020	configure voip ip-group new name "{{CustomerI...	NULL	Add SIP Trunk Basic	1	OnlinePatrnGateway,CustomerName
11	700	configure voip no ip-group where name "{{Custo...	NULL	sbc-scenario7Cleanup	2	NULL
12	100	configure voip sbc dial-plan where name "{{Dial...	NULL	sbc-add-prefix	NULL	NULL
13	101	configure voip sbc dial-plan where name "{{Dial...	NULL	sbc-remove-prefix	NULL	NULL
14	5000	configure voip sbc dial-plan where name "{{Dial...	NULL	sbc-add-oc-numbers	NULL	NULL
15	10007	configure voip ip-group new name "{{CustomerI...	NULL	old_sbc-scenario7	1	NULL

In Figure 24-9, the IP PBX is configured with Custom Variables defined above.

Figure 24-9: Customer Variables

The screenshot shows a configuration interface for Customer Variables. At the top, there are three tabs: "1 M365 Tenant", "2 M365", and "3 Voice Route". Below the tabs, there are two dropdown menus: "Onboarding Script" (set to "IP PBX") and "Cleanup Script" (set to "IP PBX Cleanup"). Below these is a table with two columns: "Customer Variables" and "Value". The table contains three rows: "IPPBX-proxyaddress", "IPPBX-proxyaddress-SIPPort", and "SIP-Hostname", each with an empty input field. At the bottom right, there are "Back" and "Submit" buttons.

In cases where it's not clear which type of value must be entered for the custom variable, then this must be verified with the SBC INI file. For example, for the Custom Variable shown below "IP-PBX-proxy address", it's not clear whether to enter an FQDN or IP address. In this case, the Message Manipulation User-defined string defined in the Outbound Message Manipulation rule must be verified on the SBC.

Figure 24-10: Outbound Message Manipulation Rule

```

SQLQuery17.sql - U...SP\livecloud (221)*  SQLQuery16.sql - U...SP\livecloud (222)  SQLQuery15.sql - U...SP\livecloud (D12)*  SQLQuery14.sql - U...SP\livecloud (334)  SQLQuery13.sql - U...SP\livecloud (343)
proxy enable keep-alive using options
sbcip4 sip-int-name "PBXSIP"
activate
proxy-ip 0
proxy-address "{{(CustomVar.IPPBX-proxyaddress)}}:{{(CustomVar.IPPBX-proxyaddress-SIPPort)}}"
transport-type udp
activate
exit
ip-group new
name "{{(CustomerId)}-c"
proxy-set-name "{{(CustomerId)}-c"
media-real-name "HSUAM"
ip-profile-name "PBX"
sip-group-name "{{(CustomVar.SIP-Hostname)}}"
outbound-msg-manipulation-set 17
authentication-mode sbc-as-client
msg-man-user-defined-string1 "{{(CustomVar.IPPBX-proxyaddress)}}"
tags "Trunk={{(SBC.OnlinePstnGateway)}}"
proxy-keepalive-use-ipg enable
call-setup-rules-set-id 4
classify-by-proxy-set disable
activate
exit
ip-group new
name "{{(CustomerId)}-t"
type user
proxy-set-name "Teams"
ip-profile-name "Teams"
local-host-name "{{(SBC.OnlinePstnGateway)}}"
always-use-source-addr enable
tags "Tenant={{(SBC.OnlinePstnGateway)}}"
classify-by-proxy-set disable
call-setup-rules-set-id 0
registration-mode sbs-initiates
authentication-mode sbc-as-client
{{if SBC.EnableCAC}}
cac-profile "{{(SBC.CacProfile)}}"
{{/if}}
activate
exit

```

In a similar way, the custom variable SIP-Hostname is configured on the SBC as the sip-group-name. It's necessary to verify on the SBC whether the value for this parameter is an IP-address or FQDN and whether configured for a gateway or SBC call.

Figure 24-11: SIP Group Name

```

SQLQuery17.sql - U...SP\livecloud (221)*  SQLQuery16.sql - U...SP\livecloud (222)  SQLQuery15.sql - U...SP\livecloud (512)*  SQLQuery14.sql - U...SP\livecloud (334)  SQLQuery13.sql - U...SP\livecloud (343)
proxy enable keep-alive using options
sbcpv4-sip-int name "PBXSIP"
activate
proxy ip 0
proxy address "{{CustomVar.IPPBX-proxyaddress}}:{{CustomVar.IPPBX-proxyaddress-SIPPort}}"
transport-type udp
activate
exit
ip-group new
name "{{CustomerId}}-c"
proxy-set-name "{{CustomerId}}-c"
media-real-name "PBXM"
ip-profile-name "PBX"
sip-group-name "{{CustomVar.SIP-Hqstname}}"
outbound-msg-manipulation-set 17
authentication-mode sbc-as-client
msg-man-user-defined-string1 "{{CustomVar.IPPBX-proxyaddress}}"
tags "Trunk-{{SBC.OnlinePstnGateway}}"
proxy-keepalive-use-igmp enable
call-setup-rules-set-id 4
classify-by-proxy-set disable
activate
exit
ip-group new
name "{{CustomerId}}-t"
type user
proxy-set-name "Teams"
ip-profile-name "Teams"
local-host-name "{{SBC.OnlinePstnGateway}}"
always-use-source-addr enable
tags "Tenant-{{SBC.OnlinePstnGateway}}"
classify-by-proxy-set disable
call-setup-rules-set-id 0
registration-mode sbs-initiates
authentication-mode sbc-as-client
{{#if SBC.EnableCAC}}
cac-profile "{{SBC.CacProfile}}"
{{/if}}
activate
exit

```

100 %
Connected: (1/1) UMP-Sandbox3-SP-SQLSYSADMIN... UMP-Sandbox3-SP\livecloud... SysAdminTenant: 00:00:00 0 rows

24.4.1.1 Custom Script

New scripts should be added to the SQL database in the `dbo.SbcScriptTemplate` table. A random number can be assigned to the script. The following shows an example of a custom script for SBC configuration with defined custom variables highlighted in green. In this script includes the creation of a media and control network interface for the customer tenant and SIP interfaces for the customer tenant and for Microsoft Teams.

```

configure network
network-dev new
vlan-id "{{CustomVar.vlan-id}}"
underlying-if "GROUP_4"
name "{{CustomerId}}"
tagging tagged
    activate
    exit
interface network-if new
    application-type media-control
    ip-address "{{CustomVar.IP address}}"
    prefix-length "{{CustomVar.Prefix}}"
    gateway "{{CustomVar.gateway address}}"
    name "{{CustomerId}}"
    underlying-dev "{{CustomerId}}"
    activate
    exit
exit

configure voip
realm new
    name "MR_{{CustomerId}}"
    ipv4if "{{CustomerId}}"
    udp-port-range-start 6000
    session-leg 240
    activate

```

```
exit
sip-interface new
  interface-name "SI_{{CustomerId}}"
  network-interface "{{CustomerId}}"
  tcp-port 0
  tls-port 0
  media-realm-name "MR_{{CustomerId}}"
  activate
exit
proxy-set new
  proxy-name "PS_{{CustomerId}}"
  proxy-enable-keep-alive using-options
  sbcipv4-sip-int-name "SI_{{CustomerId}}"
  activate
  proxy-ip 0
  proxy-address "{{CustomVar.SIP-
proxyaddress}}:{{CustomVar.SIP-SIPPort}}"
  transport-type udp
  activate
  exit
exit
ip-group new
  name "IPG_Teams_{{CustomerId}}"
  proxy-set-name "PS_Microsoft Teams"
  media-realm-name "MR_Teams"
  classify-by-proxy-set disable
  ip-profile-name "IPP_Microsoft Teams"
  outbound-mesg-manipulation-set 11
  local-host-name "{{SBC.OnlinePstnGateway}}"
  qoe-profile "QOE"
  always-use-source-addr enable
  dtls-context "Microsoft Teams"
  sbc-operation-mode b2bua
  topology-location up
  tags "Tenant={{SBC.OnlinePstnGateway}}"
  sbc-alt-route-reasons-set "Microsoft Teams"
  teams-direct-routing-mode enable
  activate
  exit
ip-group new
  name "IPG_{{CustomerId}}"
  proxy-set-name "PS_{{CustomerId}}"
  media-realm-name "MR_{{CustomerId}}"
  ip-profile-name "IPP_Customers"
  outbound-mesg-manipulation-set 12
  sbc-operation-mode b2bua
  activate
  exit
exit
do write
```

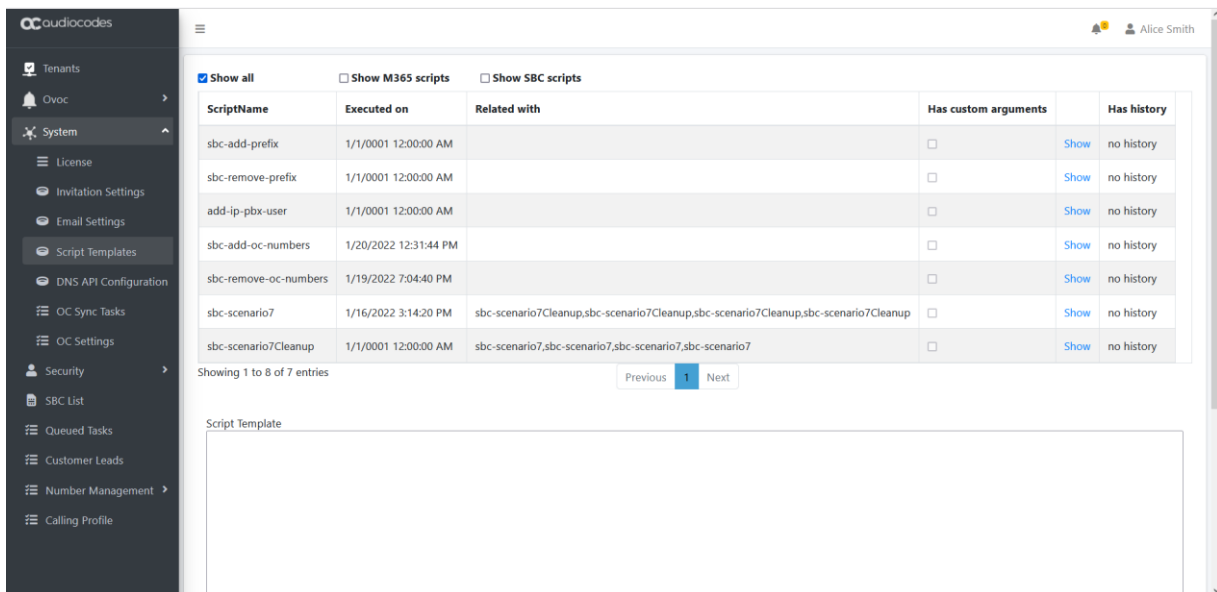
24.5 Scenario Scripts Templates Page

Scripts templates can be viewed and managed in the Scripts Templates page.

To manage scripts:

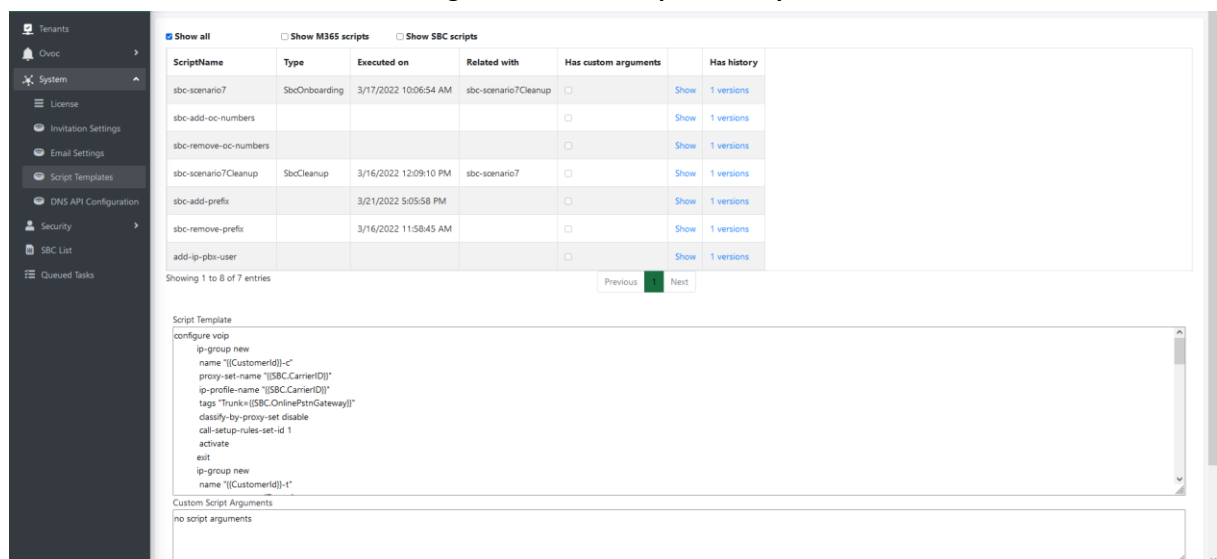
- In the UMP SP Main Tenant Main Page, open the Scripts Templates page (**System > Script Templates**).
 - Select the **Show M365 scripts** checkbox to display only M365 scripts
 - Select **Show SBC scripts** to display only SBC scripts

Figure 24-12: Show Scripts



- To display the contents of a specific script, select an entry and then click **Show**.

Figure 24-13: Show Specific Script



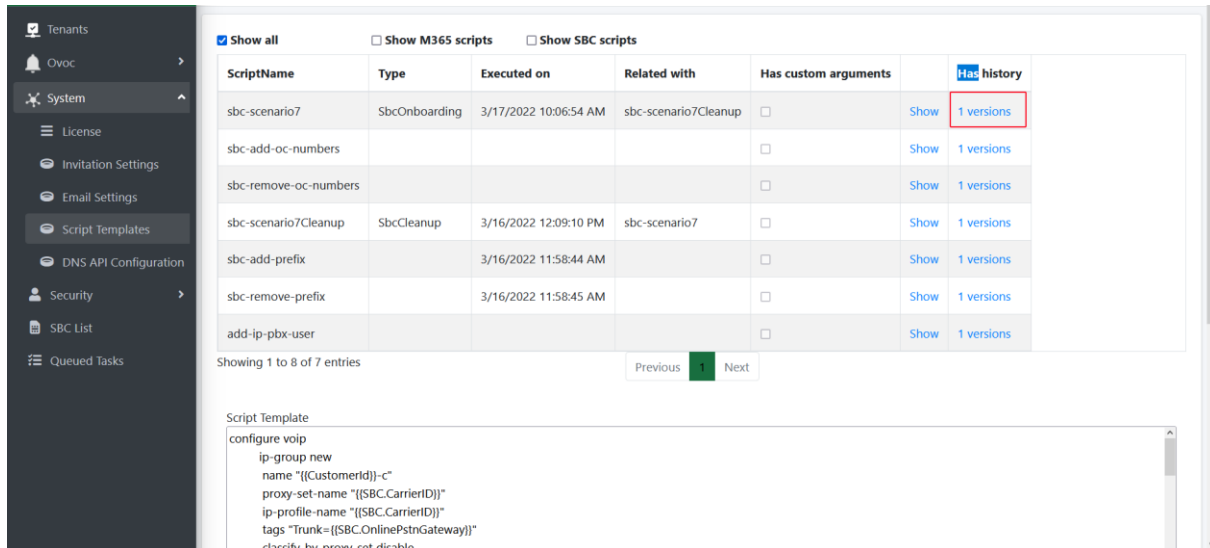
24.5.1 Script Scenario Comparison

This version includes updates to the template script scenarios. You can use the compare tool in the Script Templates page to view the differences between versions.

To compare scripts:

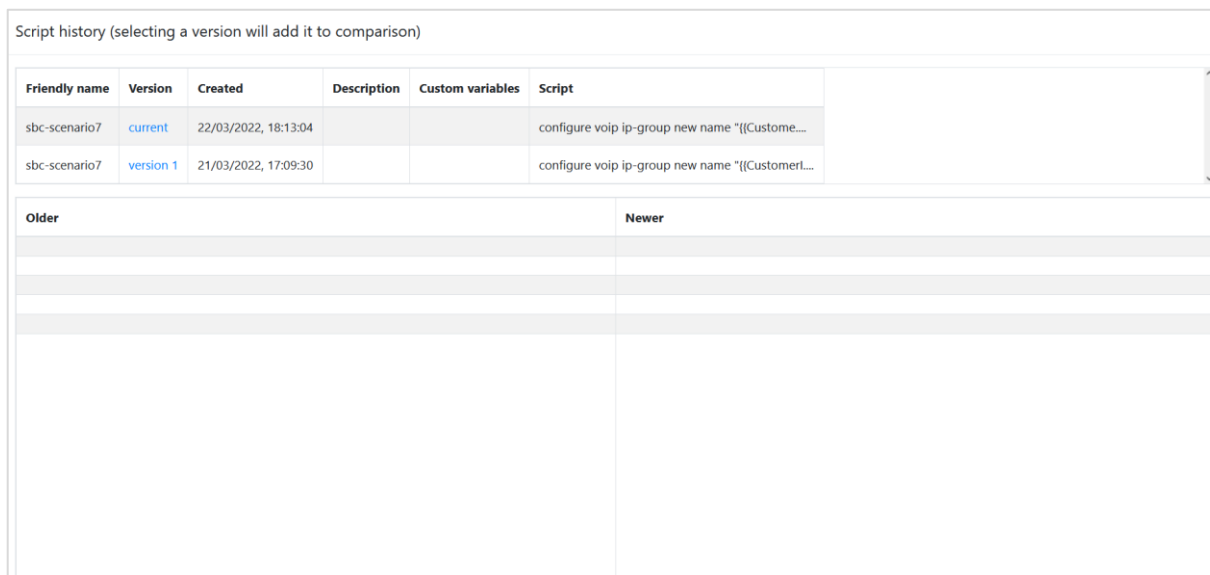
1. Click the **1 versions** link for the sbc-scenario7 script.

Figure 24-14: sbc-scenario7



The screen displays two entries, the first entry for the current script and the second entry for the upgraded script.

Figure 24-15: Script History



2. Click the **current** entry; the script content is displayed in the left “Older” pane. Click the **version 1** entry; the latest script is displayed in the right “Newer” pane.

Figure 24-16: Scripts Compare

21/03/2022, 17:09:30	21/03/2022, 18:19:40
<pre>sbc-scenario7 configure voip ip-group new name "{{CustomerId}}-c" proxy-set-name "{{SBC.CarrierID}}" ip-profile-name "{{SBC.CarrierID}}" tags "Trunk={{SBC.OnlinePstnGateway}}" classify-by-proxy-set disable call-setup-rules-set-id 1 activate exit ip-group new name "{{CustomerId}}-t" proxy-set-name "Teams" ip-profile-name "Teams" local-host-name "{{SBC.OnlinePstnGateway}}" always-use-source-addr enable tags "Tenant={{SBC.OnlinePstnGateway}}" classify-by-proxy-set disable call-setup-rules-set-id 0 {{#if SBC.EnableCAC}} cac-profile "{{SBC.CacProfile}}" {{/if }} activate exit {{#if SBC.FlagCarrierRegistration}}</pre>	<pre>sbc-scenario7 configure voip ip-group new name "{{CustomerId}}-c" proxy-set-name "{{SBC.CarrierID}}" ip-profile-name "{{SBC.CarrierID}}" tags "Trunk={{SBC.OnlinePstnGateway}}" classify-by-proxy-set disable call-setup-rules-set-id 1 activate exit ip-group new name "{{CustomerId}}-t" proxy-set-name "Teams" ip-profile-name "Teams" local-host-name "{{SBC.OnlinePstnGateway}}" always-use-source-addr enable tags "Tenant={{SBC.OnlinePstnGateway}}" classify-by-proxy-set disable call-setup-rules-set-id 0 {{#if SBC.EnableCAC}} cac-profile "{{SBC.CacProfile}}" {{/if }} activate exit {{#if SBC.FlagCarrierRegistration}}</pre>

3. Scroll down to review the differences.

Figure 24-17: View Script Differences

<pre>sip-destination account new account-name "{{CustomerId}}" served-ip-group-name "{{CustomerId}}-t" serving-ip-group-name "{{CustomerId}}-c" user-name "{{SBC.CarrierUserName}}" password "{{SBC.CarrierPassword}}" host-name "{{SBC.CarrierHostName}}" contact-user "{{SBC.CarrierMainLine}}" register reg application-type sbc activate exit {{/if }} sbc dial-plan where name "DialPlan" {{#each es}} dial-plan-rule new name "{{ }}" prefix "{{this}}" tag "{{this }}" exit {{/each}} activate exit do write</pre>	<pre>sip-destination account new account-name "{{CustomerId}}" served-ip-group-name "{{CustomerId}}-t" serving-ip-group-name "{{CustomerId}}-c" user-name "{{SBC.CarrierUserName}}" password "{{SBC.CarrierPassword}}" host-name "{{SBC.CarrierHostName}}" contact-user "{{SBC.CarrierMainLine}}" register reg application-type sbc activate exit {{/if }} {{#each SBC.DialPlanPrefixes}} sbc dial-plan where name "{{this.CustDialPlanName}}" {{#each this.RuSBCPhones}} dial-plan-rule new name "{{this.Name}}/CustomerID" prefix "{{this.Prefix}}" tag "{{this.Tag}}/SBC.OnlinePstnGateway" exit {{/each}} activate exit {{/each}} do write</pre>
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

The following screen shows the differences for the **sbc-scenario7** cleanup script.

Figure 24-18: sbc-scenario7cleanup script

Script history (selecting a version will add it to comparison)

Friendly name	Version	Created	Description	Custom variables	Script
sbc-scenario7Cleanup	current	22/03/2022, 18:46:16			configure voip no ip-group where name "{{Custom...
sbc-scenario7Cleanup	version 1	21/03/2022, 17:09:30			configure voip no ip-group where name "{{Custom...

Older

version 1

21/03/2022, 17:09:30

sbc-scenario7Cleanup

```

configure voip
no ip-group where name "{{Customerid}}-c"
no ip-group where name "{{Customerid}}-t"
no sip-definition account where account-name "{{Customerid}}"
sbc dial-plan where name "DialPlan"
no dial-plan-rule where name "{{Customerid}}"
activate
exit
do write
            
```

Clear Left

Newer

current

22/03/2022, 18:46:16

sbc-scenario7Cleanup

```

configure voip
no ip-group where name "{{Customerid}}-c"
no ip-group where name "{{Customerid}}-t"
no sip-definition account where account-name "{{Customerid}}"
{{each SBC-DialPlanPrefixes}}
sbc dial-plan where name "{{this.CustDialPlanName}}"
no dial-plan-rule where name "{{Customerid}}"
activate
exit
{{/each}}
do write
            
```

Clear right

The following screen shows the differences for the **sbc-remove-prefix** script.

Figure 24-19: sbc-remove-prefix script

Script history (selecting a version will add it to comparison)

Friendly name	Version	Created	Description	Custom variables	Script
sbc-remove-prefix	current	22/03/2022, 18:52:48			configure voip sbc dial-plan where name "CustD....
sbc-remove-prefix	version 1	21/03/2022, 17:09:30			configure voip sbc dial-plan where name "{{Di...

Older

version 1

21/03/2022, 17:09:30

sbc-remove-prefix

```

configure voip
sbc dial-plan where name "DialPlan"
{{each ToRemove}}
no dial-plan-rule "{{this.Index}}"
{{/each}}
activate
exit
do write
            
```

Clear Left

Newer

current

22/03/2022, 18:52:48

sbc-remove-prefix

```

configure voip
sbc dial-plan where name "CustDialPlanName"
{{each ToRemove}}
no dial-plan-rule "{{this.Index}}"
{{/each}}
activate
exit
do write
            
```

Clear right

4. Click Clear Left and Clear Right to clear the scripts display.

24.5.2 Script Templates Updates

This section describes the updates to the template scripts for version 8.0.300. After upgrading to this version, the following actions must be performed:

- Replace the attribute `SysAdmin.O365OnlinePSTNGateway` to `SBC.OnlinePstnGateway`
- Update scripts with the new syntax as shown in the sections below:
 - **Red** indicates the syntax to remove
 - **Green** indicates the syntax to add

24.5.2.1 sbc-scenario7

```
configure voip

ip-group new

  name "{{CustomerId}}-c"

  proxy-set-name "{{SBC.CarrierID}}"

  ip-profile-name "{{SBC.CarrierID}}"

  tags "Trunk={{SysAdmin.O365OnlinePSTNGateway
SBC.OnlinePstnGateway}}"

  classify-by-proxy-set disable

  call-setup-rules-set-id 1

  activate

exit

ip-group new

  name "{{CustomerId}}-t"

  proxy-set-name "Teams"

  ip-profile-name "Teams"

  local-host-name "{{SysAdmin.O365OnlinePSTNGateway
SBC.OnlinePstnGateway}}"

  always-use-source-addr enable

  tags "Tenant={{SBC.OnlinePstnGateway
SysAdmin.O365OnlinePSTNGateway}}"

  classify-by-proxy-set disable
```

```
call-setup-rules-set-id 0

{{#if SBC.EnableCAC}}

  cac-profile "{{SBC.CacProfile}}"

{{/if }}

activate

exit

{{#if SBC.FlagCarrierRegistration}}

sip-definition account new

  account-name "{{CustomerId}}"

  served-ip-group-name "{{CustomerId}}-t"

  serving-ip-group-name "{{CustomerId}}-c"

  user-name "{{SBC.CarrierUserName}}"

  password "{{SBC.CarrierPassword}}"

  host-name "{{SBC.CarrierHostName}}"

  contact-user "{{SBC.CarrierMainLine}}"

  register reg

  application-type sbc

  activate

  exit

{{/if }}

{{#each SBC.DialPlanPrefixes}}

sbc dial-plan where name "{{this.CustDialPlanName}}"

{{#each this.RulSBC-Phones}}

  dial-plan-rule new
```



```

    name "{{this.Name../CustomerId}}"

    prefix "{{this.Prefix}}"

    tag "{{-SysAdmin.O365OnlinePSTNGatewaythis.Tag}}"

    exit

  {{/each}}

  activate

  exit

{{/each}}

do write

```

24.5.2.2 sbc-scenario7Cleanup

```

configure voip

no ip-group where name "{{CustomerId}}-c"

no ip-group where name "{{CustomerId}}-t"

no sip-definition account where account-name "{{CustomerId}}"

{{#each SBC.DialPlanPrefixes}}

  sbc dial-plan where name "{{this.CustDialPlanName}}"

  no dial-plan-rule where name "{{../CustomerId}}"

  activate

  exit

{{/each}}

do write

```

24.5.2.3 sbc-add-prefix

```

configure voip

  sbc dial-plan where name "{{CustDialPlanName}}"

```

```
    {{#each CmdData.DialPlanRules.ToAdd}}

    dial-plan-rule new

    name "{{../SBC.SbcSiteName}}"

    prefix "{{this.Prefix}}"

    tag "{{SysAdmin.0365OnlinePSTNGatewaythis.Tag}}"

    exit

    {{/each}}

    activate

exit

do write
```

24.5.2.4 sbc-remove-prefix

```
configure voip

    sbc dial-plan where name "{{CustDialPlanName}}"

    {{#each ToRemove}}

    no dial-plan-rule "{{this.Index}}"

    {{/each}}

    activate

exit

do write
```

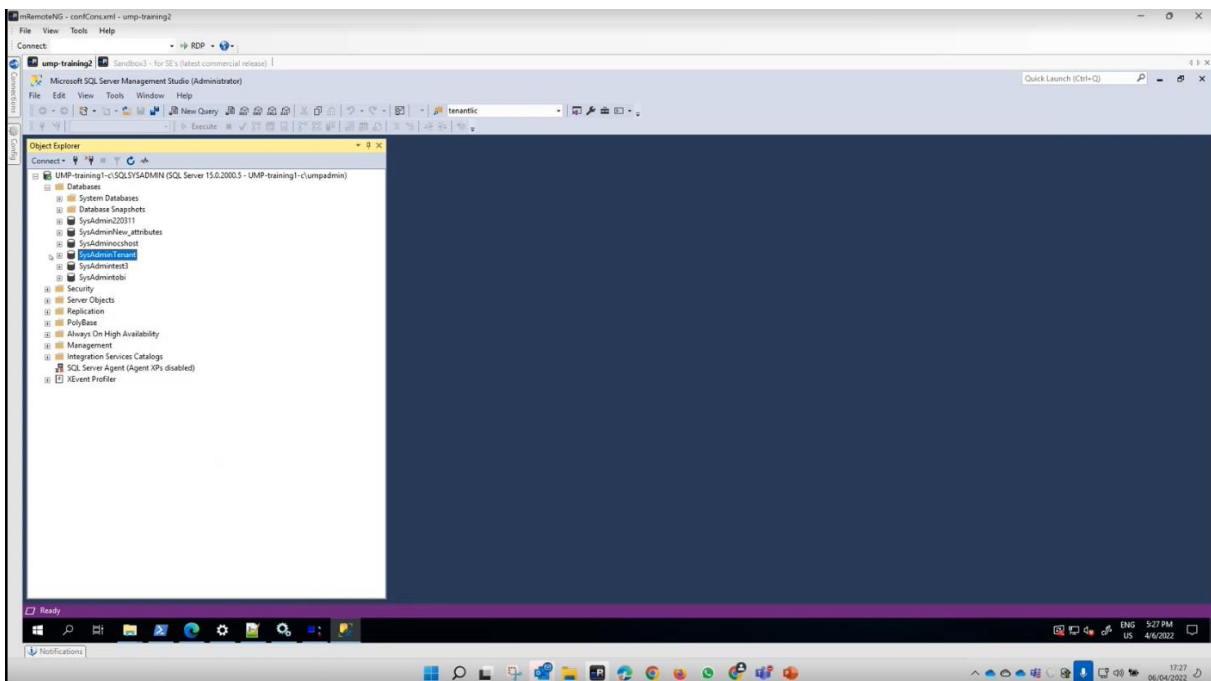
24.6 SQL DBA Script Pairing

Each execution script has an equivalent cleanup script for use in circumstances where you wish to undo the changes executed by the execution script. These two scripts must be paired in the `dbo.SBCScriptTemplate` table.

To pair SQL DBA scripts:

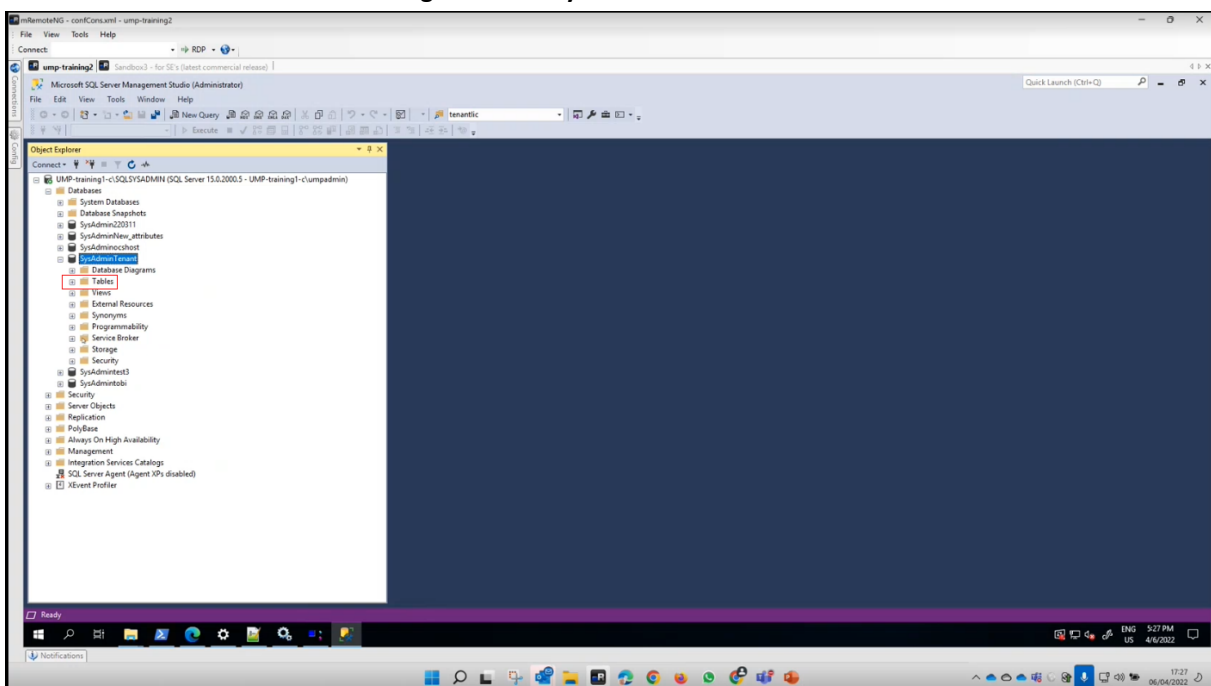
1. Open the SQL database Object Explorer.

Figure 24-20: SQL DBA Object Explorer



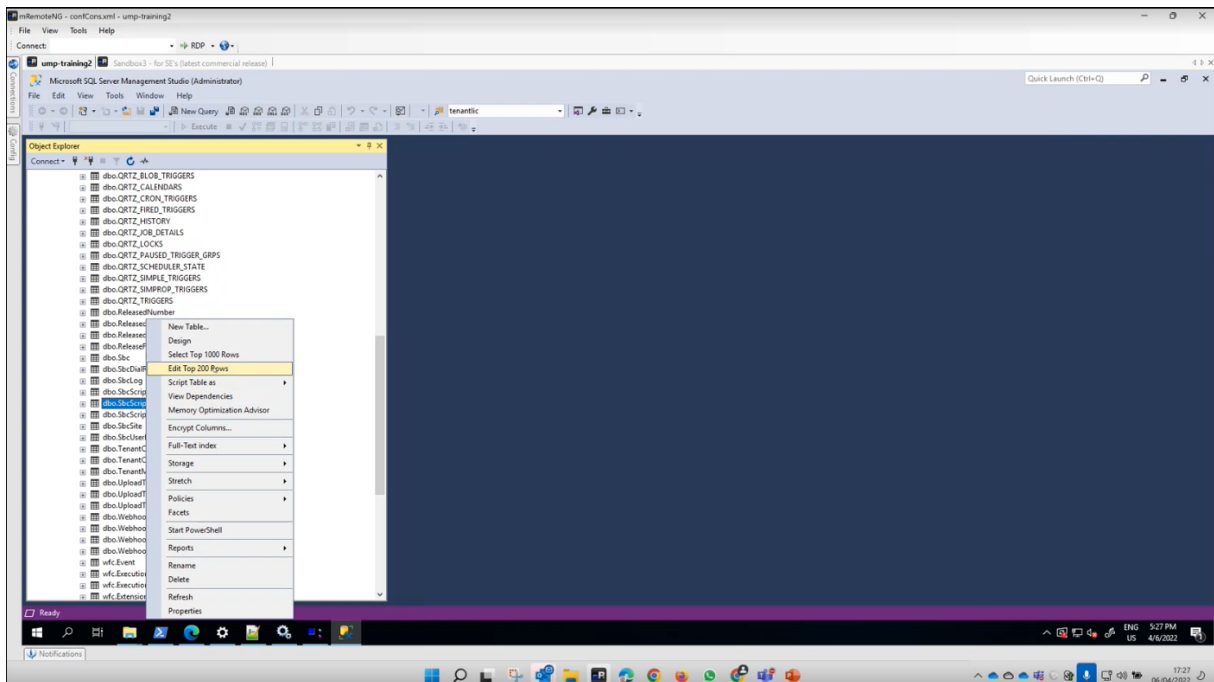
2. Select **SysAdminTenant** database.

Figure 24-21: SysAdminTenant-Tables



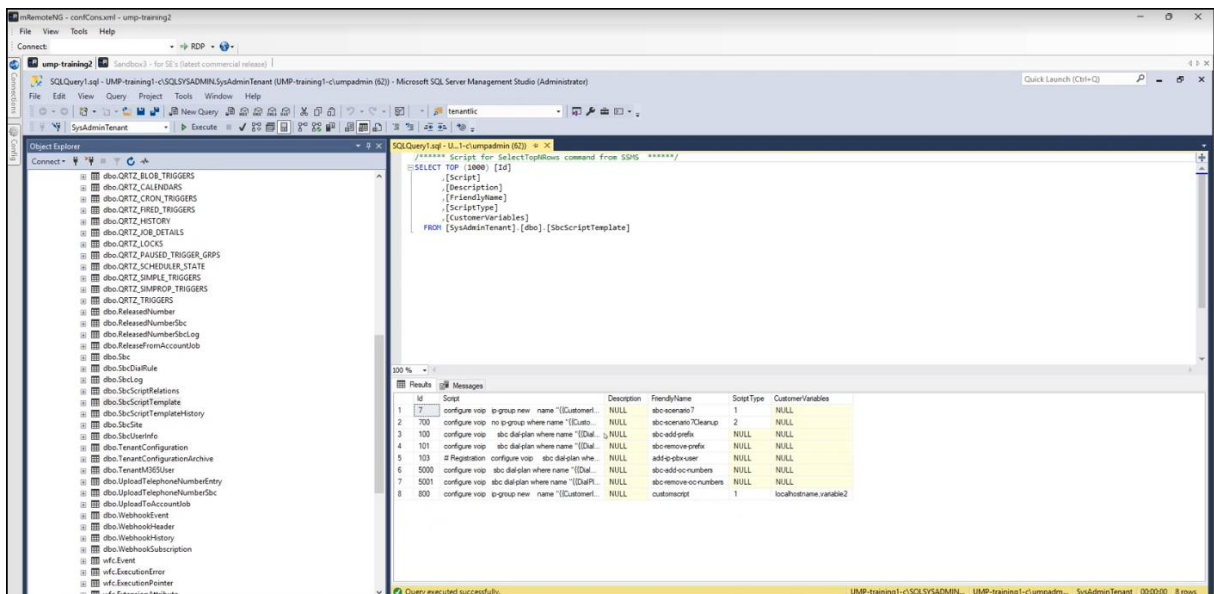
- Expand the Tables folder.

Figure 24-22: Edit Top 200 Rows



- Select the `dbo.SBCScriptTemplate` table, right-click and select **Edit Top 200 Rows**.

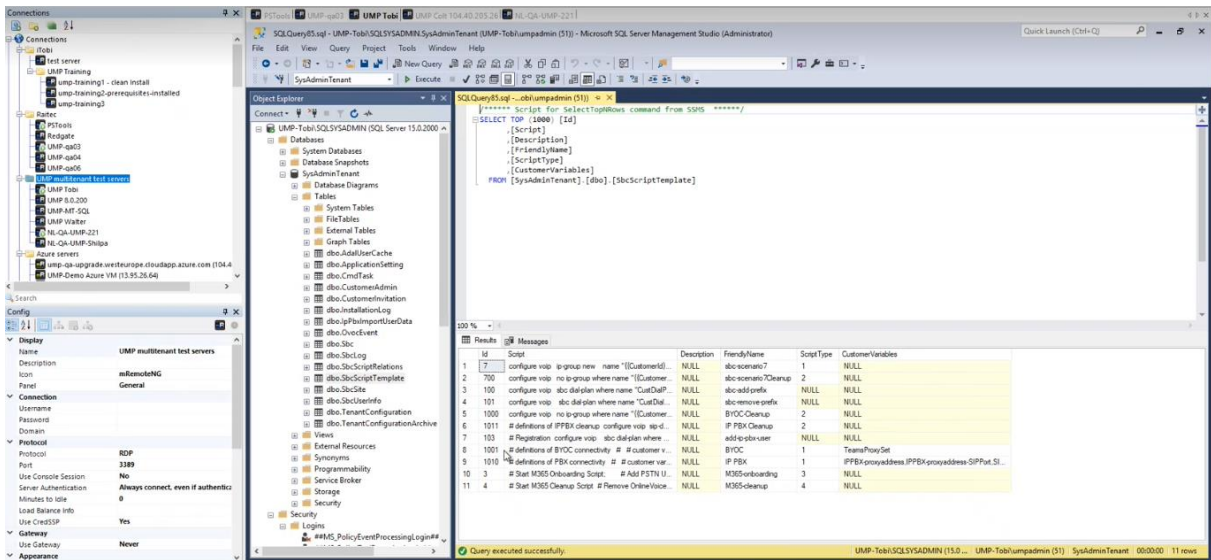
Figure 24-23: SBC Script Template



The template scenario scripts are displayed.

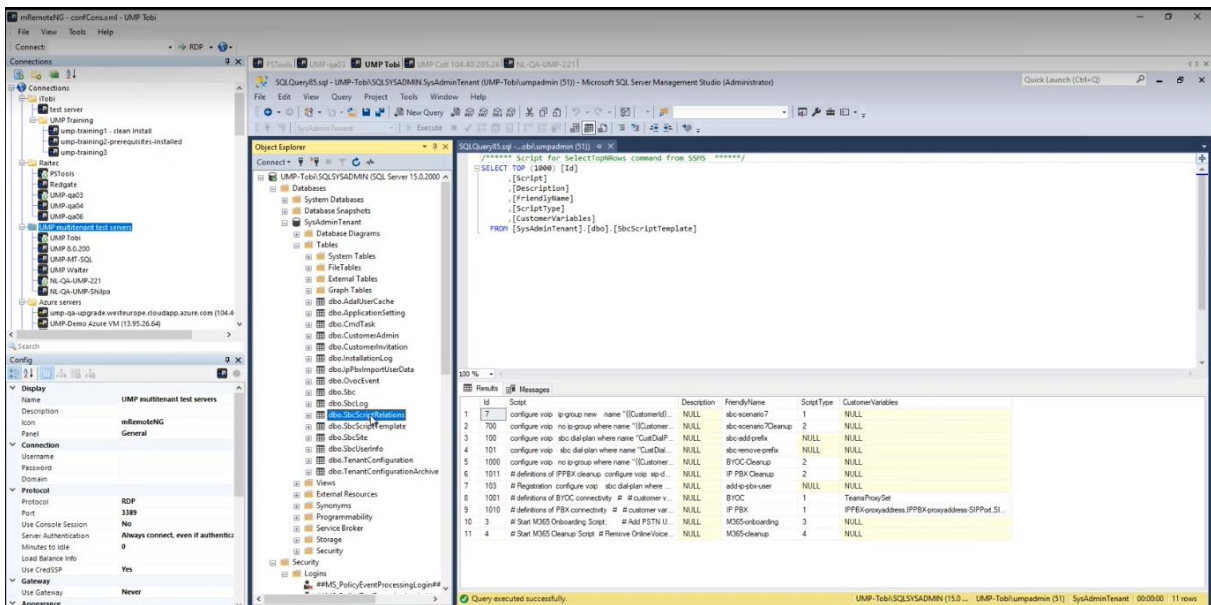
- To pair scripts, do the following:
 - In the `dbo.SBCScriptTemplate` table, note the scripts that you wish to pair.

Figure 24-24: dbo.SbcScriptTemplate



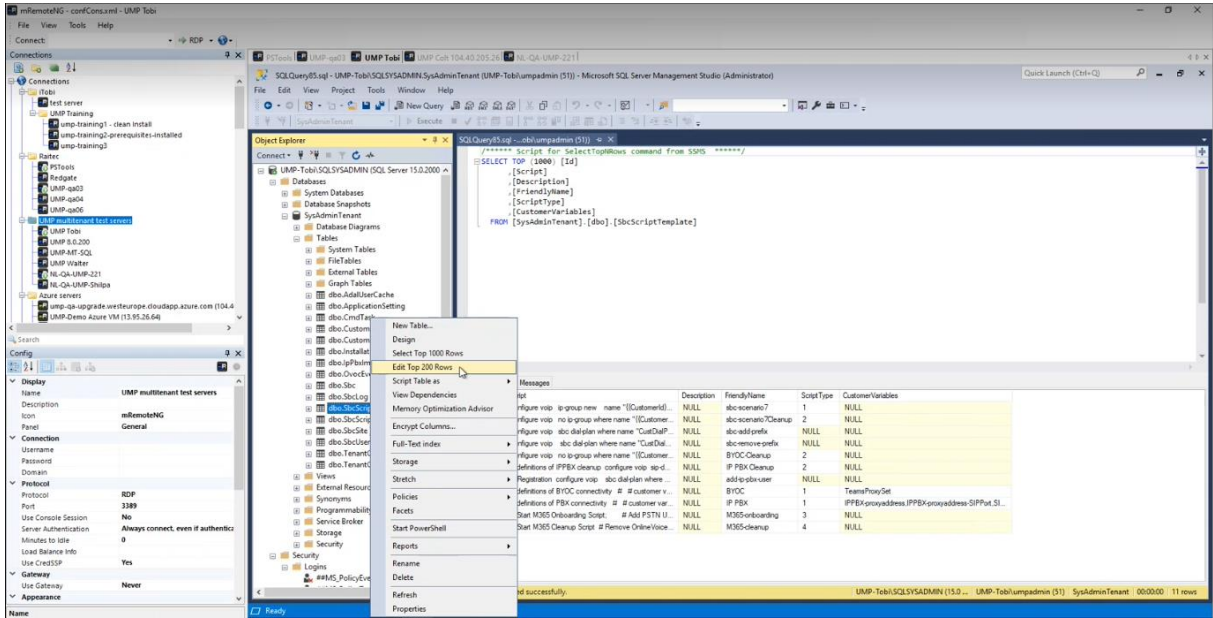
b. Right-click the dbo.SbcScriptRelations table.

Figure 24-25: dbo.SbcScriptRelations



c. Choose Edit Top 200 Rows.

Figure 24-26: Edit Top 200 Rows



- d. Create a new row and enter the matching Ids for the corresponding Onboarding and Cleanup scripts.

Figure 24-27: Create a New Row

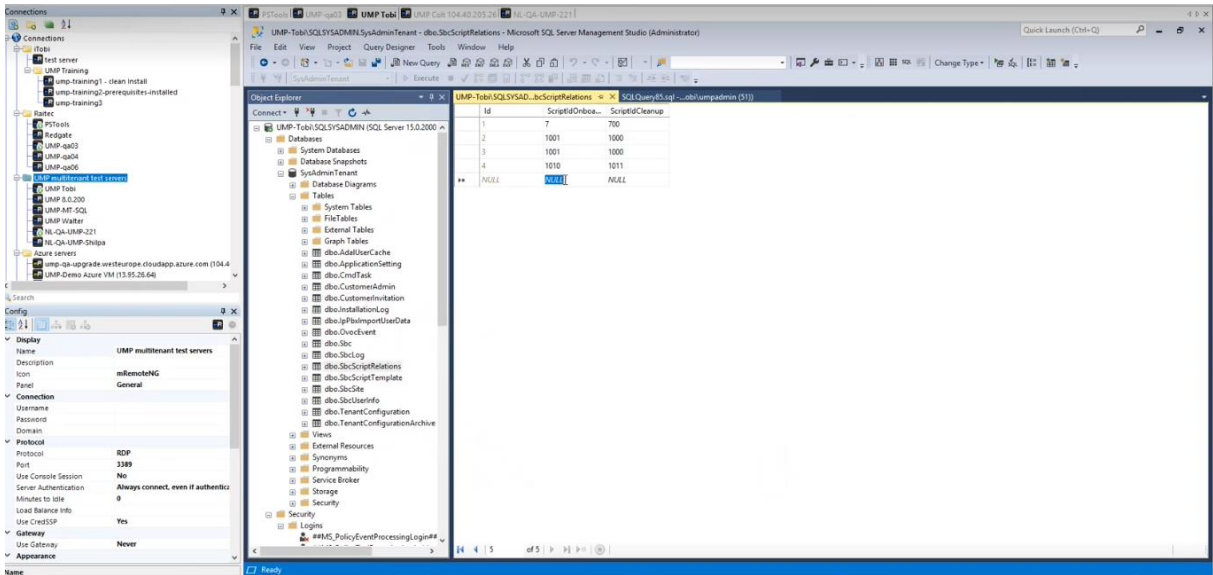
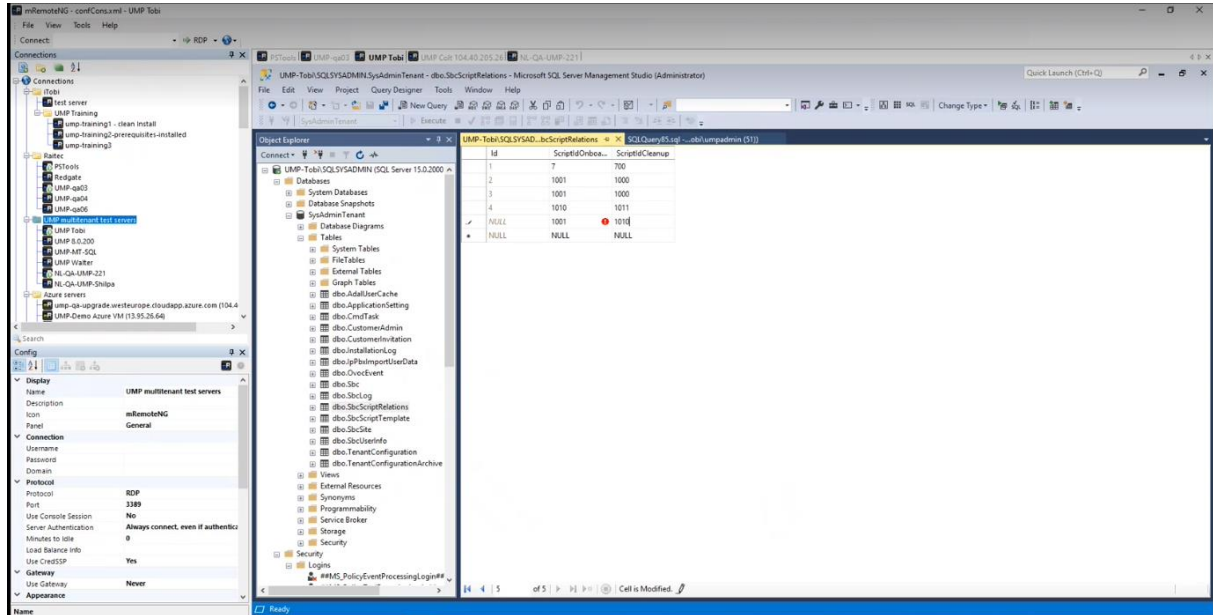


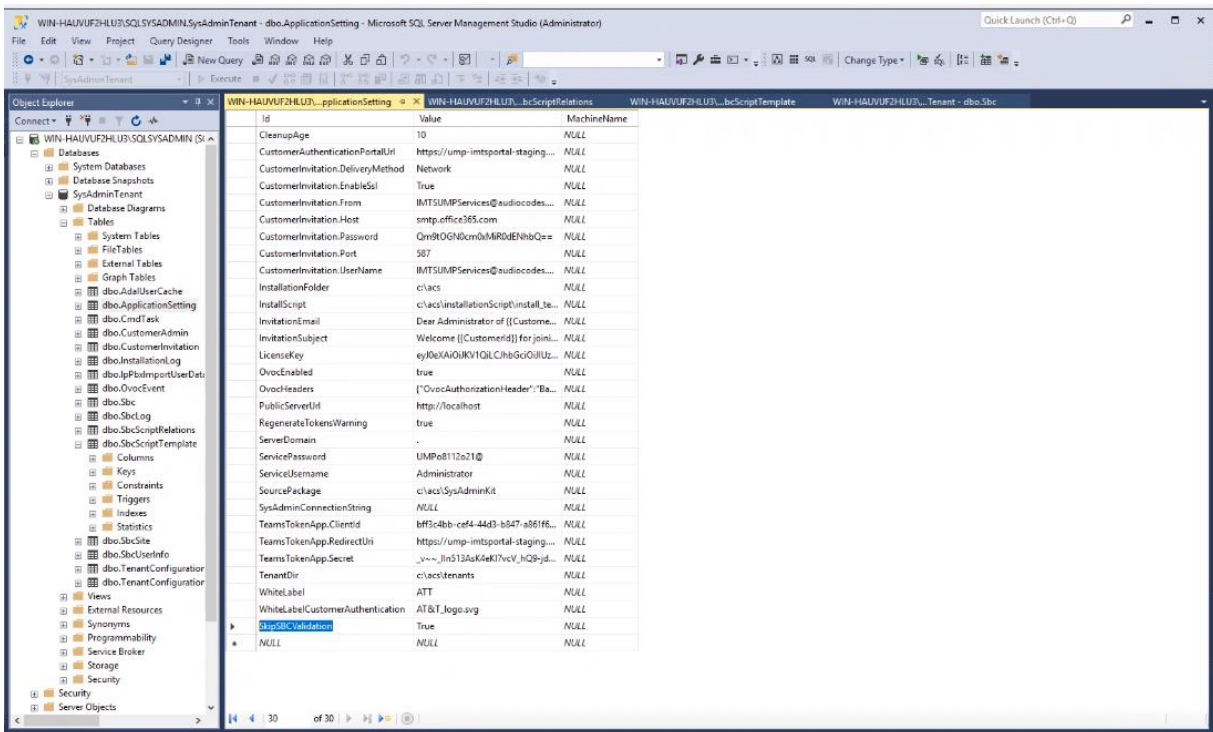
Figure 24-28: New Row Added



- To disable SBC validation, open the **dbo.ApplicationSettings** table and set **SkipSBCValidation** to **True**.

When disabled, the Onboarding script does not check for pre-existing SIP core entities configured on the SBC.

Figure 24-29: SBC Script Template



25 Security Settings

This section describes the following security settings:

- Customer Admins (see Section 25.1)
- Auth Tokens (see Section 25.2)
- Customer Invitations (see Section 25.2)

25.1 Customer Admins

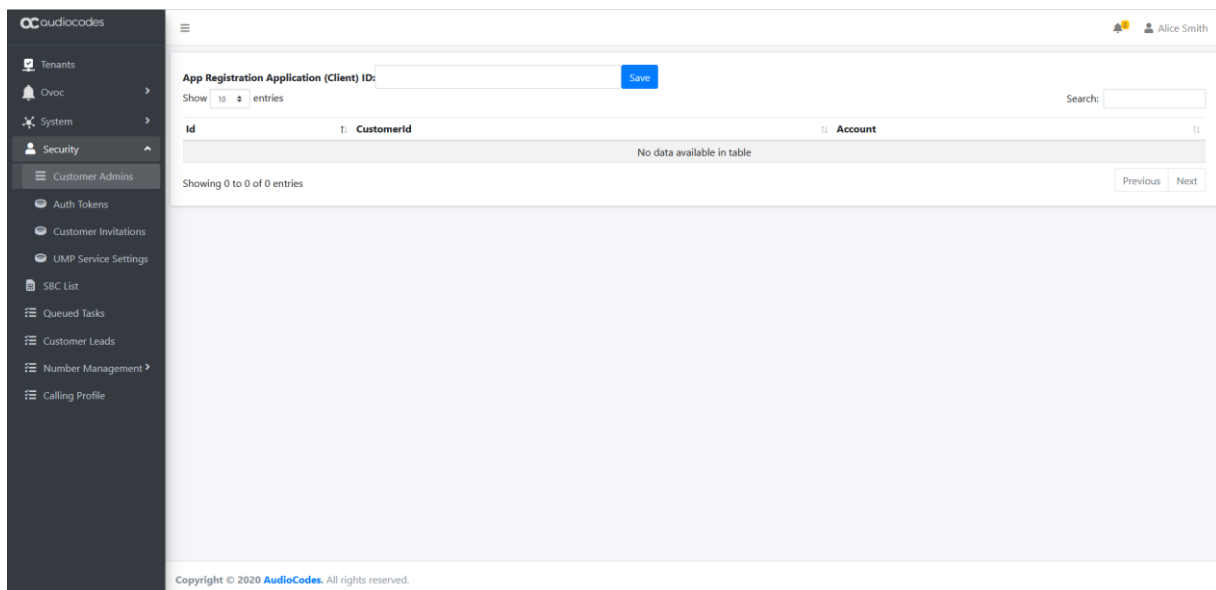
The Customer Admins screen allows you to manage a list of Client IDs for registered applications as described in Chapter 14. Once the Application Client ID is added, the logged in operator can view this customer in the UMP Multitenant.

To view Customer Admins:

1. In the UMP Main Tenant Navigation pane, open the **Customer Admins** page (**Security > Customer Admins**).

A list of Application (Client) IDs are displayed.

Figure 25-1: Customer Admins



25.2 Customer Invitations

The Customer Invitations page allows you to monitor the status of the Invitation emails that are sent from the Service Provider IT administrator to the customer IT administrator for requesting consent to connect to their Microsoft Office 365 platform. This connection is required for the Background Replication process, for which an App Registration on Azure is required (see Chapter 10). The invitation email includes a token authentication link, details of which are displayed in the Auth Tokens screen (see Section 25.30).

To monitor customer invitations:

1. In the UMP Main Tenant Navigation pane, open the **Customer Invitations** page (**Security > Customer Invitations**).

A list of Invitation emails sent by the System administrator to the customer are displayed.

Figure 25-2: Customer Invitations

ID	Full Name	Invitation Email	M365 Admin Email	Email Sent	Email Invitation Sent Count	Created at	Expires at	Device Authenticated	Tenant Installed	Actions
TrunkTest	TrunkTest	Test@gmail.com		true	1	2022-03-31	2022-04-05		No	Send Reminder Revoke Request Auth URL

Showing 1 to 1 of 1 entries

Previous 1 Next

Copyright © 2020 AudioCodes. All rights reserved.

This screen includes the following parameters:

Table 25-1: Customer Invitations

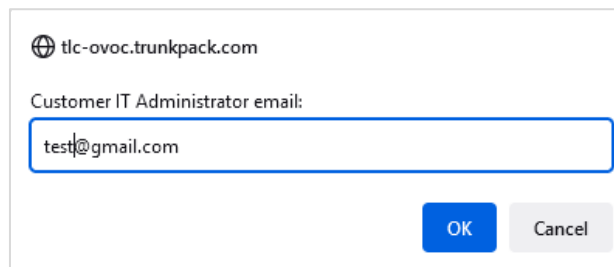
Parameter	Description
ID	Customer Shortname defined in the Onboarding wizard.
Full Name	Full Customer name defined in the Onboarding wizard.
Invitation Email	Email address of the customer IT administrator sent in the token authentication link from the Microsoft 365 Settings screen in the Multitenant portal using option “Switch to auth” (see Section 33.12)
M365 Admin Email	Email address of the M365 Admin account for which to request consent to allow UMP-365 to connect.
Email Sent	Indicates whether an email has been sent to the IT customer administrator.
Email Invitation Sent Count	<p>The number of retries for UMP to send the invitation email to the customer (the retry occurs per minute).</p> <p>The failure could be the result of the SMTP setup or due to network issues.</p>
Created at	The date that the invitation was sent.
Expires at	The expiry date of the invitation.
Device Authenticated	<ul style="list-style-type: none"> ■ No: Authentication has been processed; however the customer is still pending in the wizard. ■ Yes: The wizard runs again and the Service Provider approves the pending request and the tenant is created in UMP.
Tenant Installed	Indicates whether the customer IT administrator has completed the authentication process (Yes). You can then go ahead and add the customer.

Actions	See below.
---------	------------

The following actions can be performed:

- **Send Reminder:** Send a reminder to the customer IT administrator

Figure 25-3: Send Reminder



tlc-ovoc.trunkpack.com

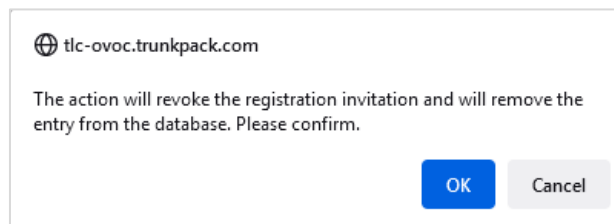
Customer IT Administrator email:

test@gmail.com

OK Cancel

- **Revoke Request:** Revokes the request sent to the Customer IT Administrator

Figure 25-4: Revoke Request



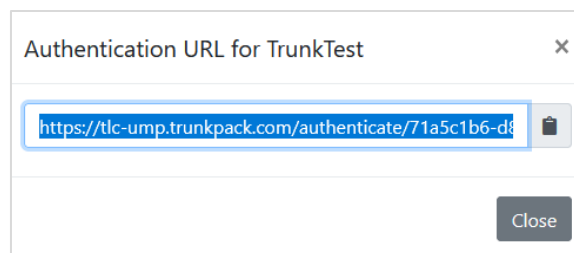
tlc-ovoc.trunkpack.com

The action will revoke the registration invitation and will remove the entry from the database. Please confirm.

OK Cancel

- **Auth URL:** Displays the tenant URL link to connect to the Multitenant portal that is sent to the customer IT administrator in the following format:
https://Customer_SubDomain/authenticate/uniqueInvitationID
 e.g. <https://tlc-ump.trunkpack.com/authenticate/71a5c1b6>

Figure 25-5: Authentication URL for Tenant



Authentication URL for TrunkTest

<https://tlc-ump.trunkpack.com/authenticate/71a5c1b6-d8>

Close



You can paste the above value in a Web browser to test the authentication.

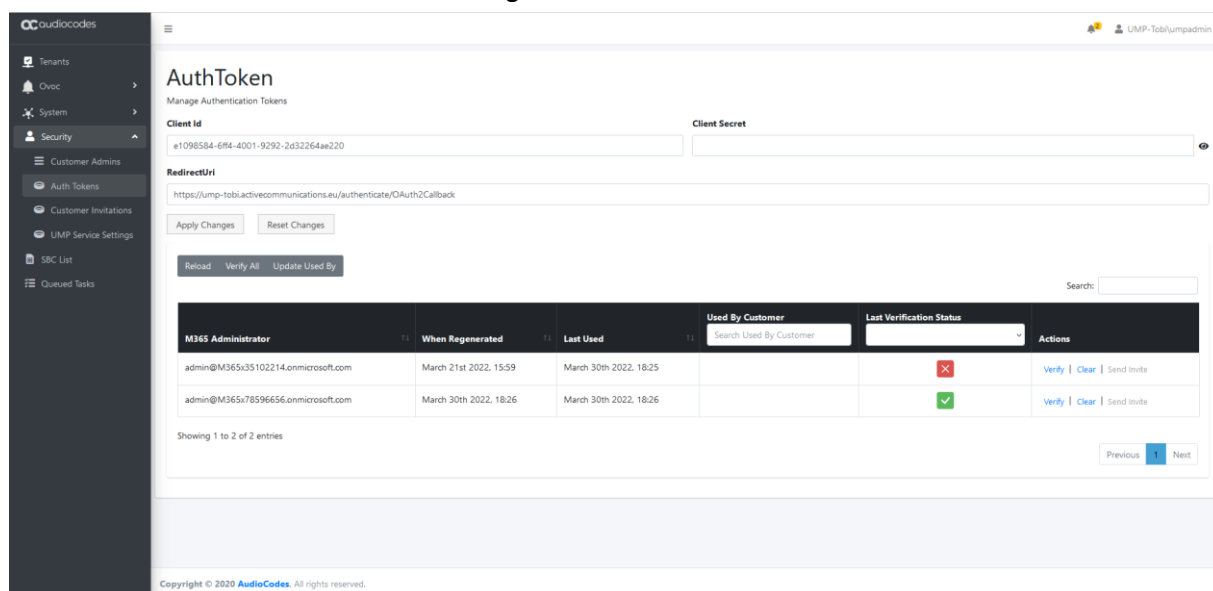
25.3 Auth Tokens

The Auth Tokens page configures the Client IDs and redirect URIs used by the Token Invitation mechanism for securing UMP-365 access to the customer tenant’s Microsoft Office 365 platform used for managing the Background Replication process (see Chapter 10). In the Onboarding wizard (for Hosted Essentials + and Hosted Pro customers), an option to connect to the Microsoft 365 platform by sending a consent link to customer IT administrator is provided (see Section 30.5). Once the Service Provider IT administrator performing the onboarding, choses this option and sends an email containing the consent request to the IT administrator, an entry is displayed in this screen.

To manage Authorization tokens:

1. In the UMP Main Tenant Navigation pane, open the **Auth Tokens** page (**Security > Auth Tokens**).


Figure 25-6: AuthToken



2. Enter the Client ID.
3. Enter the Redirect URL which consists of the IP address of the Service Provider portal. For example:
<https://finebak.domain.com/authenticate/OAuth2Callback>

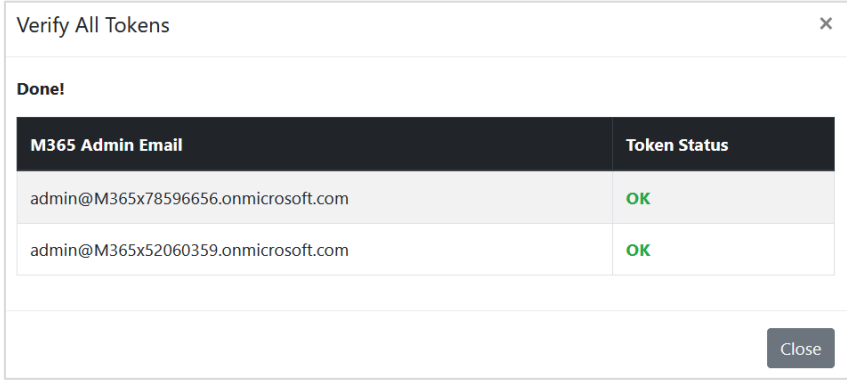
Table 25-2: Auth Token

Parameter	Description
M365 Administrator	The Microsoft Office 365 administrator to whom the consent request was sent.
When Regenerated	The last time the token is regenerated.
Last Used	The last time the token is used by the synchronization process with M365 performed every hour, upon manual sync through PowerShell or when Queued tasks are executed.
Used by Customer	Free search field to search for customer.

Parameter	Description
Last Verification Status	<p>Indicates one of the following verification statuses:</p> <ul style="list-style-type: none"> Never Performed Successful Failed Token not generated
Actions	<p>One of the following actions can be performed:</p> <ul style="list-style-type: none"> Verify: click to verify the token. Once verified,  is displayed in the Last Verification Status column. Clear- Removes the token authentication token. Send Invite – Manually send an invitation token to the customer IT administrator Reload-Reloads all active tokens Verify All-Verifies all active tokens Update Used By- Indicates which administrators use which tokens.

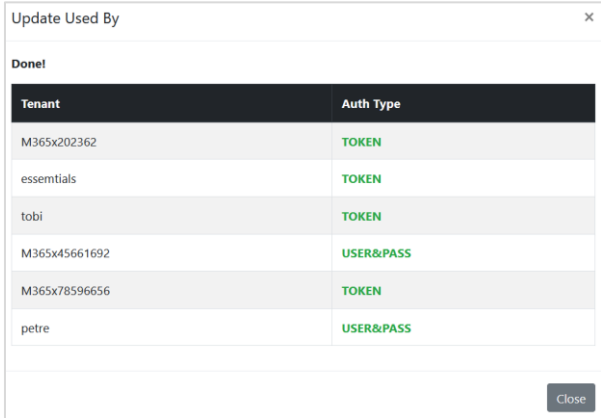
4. Click **Apply Changes** or click **Reset Changes** to reconfigure.

Figure 25-7: Verify All Tokens



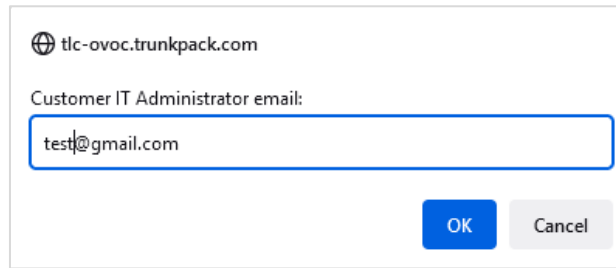
M365 Admin Email	Token Status
admin@M365x78596656.onmicrosoft.com	OK
admin@M365x52060359.onmicrosoft.com	OK

Figure 25-8: Update Used By



Tenant	Auth Type
M365x202362	TOKEN
essentials	TOKEN
tobi	TOKEN
M365x45661692	USER&PASS
M365x78596656	TOKEN
petre	USER&PASS

Figure 25-9: Sent Invite



tlc-ovoc.trunkpack.com

Customer IT Administrator email:

test@gmail.com

OK Cancel

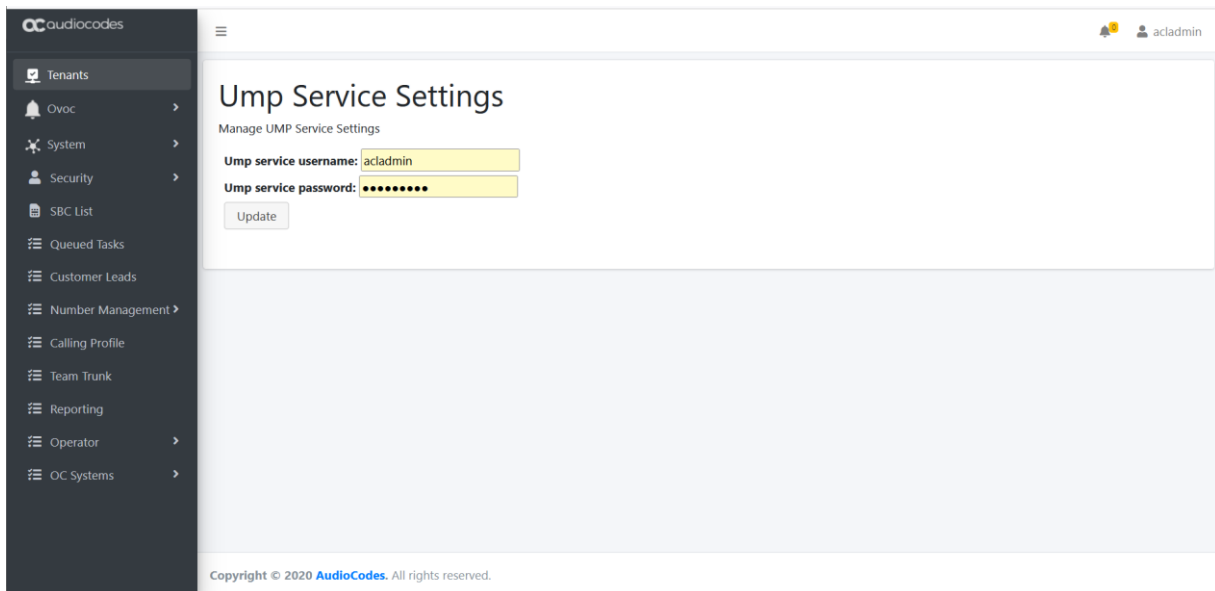
25.4 UMP Service Settings

The UMP Service Settings for Windows server displays the SysAdmin Windows Services credentials used to install the UMP-365 (see Section 6.3).

To configure UMP Service Settings:

1. In the UMP Main Tenant Navigation pane, open the **UMP Service Settings** page (**Security >. UMP Service Settings**).

Figure 25-10: UMP Service Settings



The screenshot shows the 'Ump Service Settings' page in the AudioCodes management console. The page title is 'Ump Service Settings' and the subtitle is 'Manage UMP Service Settings'. There are two input fields: 'Ump service username' with the value 'acladmin' and 'Ump service password' with masked characters. An 'Update' button is located below the password field. The left sidebar contains a navigation menu with items like Tenants, Ovoc, System, Security, SBC List, Queued Tasks, Customer Leads, Number Management, Calling Profile, Team Trunk, Reporting, Operator, and OC Systems. The top right corner shows a user profile for 'acladmin'. The footer contains the copyright notice: 'Copyright © 2020 AudioCodes. All rights reserved.'

2. Configure the **Ump Service username**.
3. Configure the **Ump service password**.
4. Click **Update** to apply changes.

26 Managing SBC Devices

The Known SBCs page displays a list of all connected SBC devices. You can perform the following actions:

- **Reload from OVOC:** reconnect to the Known SBCs through OVOC
- **Add new SBC:** add new SBC devices which can then later be configured for new customers and site locations when onboarding new customers in the Onboarding wizard.
- **Show Sites:** show a list of configured site locations that are connected to a specific SBC device.
- **Import customers:** not applicable for this release.
- **Show Prefixes:** Show a list of configured number prefixes for the SBC.

26.1 Add an SBC Device

This section describes how to add a new SBC device.

To add a new SBC device:

1. In the UMP Main Tenant Navigation pane, click **SBC List**. A list of Know SBCs is displayed.

Figure 26-1: Known SBCs

SBC List										
Id	Ovoc Sbc Id	Name	Ip Address	Device Fqdn	NAT Ip Addresses	Https	Gateway User	Status	Sip Users Count	Sites Count
2	2205	oc1.customers.audio-code.co.il [51.137.97.95]	169.254.4.66	oc1.customers.audio-code.co.il	51.137.97.95	False	acladmin	Connected	-N/A-	1
3	2224	oc2.customers.audio-code.co.il [52.178.43.85]	169.254.4.67	oc2.customers.audio-code.co.il	52.178.43.85	False	acladmin	Connected	-N/A-	1

The table below describes the fields in this screen.

Table 26-1: Known SBC Devices

Parameter	Description
Id	Id of the Known SBC entry.
OVOC SBC Id	Id of the OVOC SBC.
Name	Known FQDN of the SBC device/NAT IP address of SBC device.
NAT IP Address	NAT IP address of the SBC device.
Device FQDN	Known FQDN of the SBC device.

Parameter	Description
HTTPS	Indicates whether HTTPS is enabled for the device.
Gateway User	The name of the administrator user account of the SBC.
Status	The status of the connection between UMP-365 and the SBC.
SIP Users Count	The number of SIP users registered for the SBC.
Site Count	The number of site locations that are configured with the SBC.

- Click **Add New SBC** to connect to a new SBC device (the new connection is secured by default by HTTPS).

Figure 26-2: Add new SBC

The screenshot shows a dialog box titled "Add New SBC" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- Name:** A text input field with the placeholder text "SBC Name".
- Ip Address:** A text input field with the placeholder text "ex. 1.2.3.4". To its right is a checkbox labeled "Use https:" which is checked.
- Device Fqdn:** A text input field with the placeholder text "ex. sbc.contoso.com or contoso.com".
- Gateway User:** A text input field highlighted in yellow.
- Gateway Password:** A text input field highlighted in yellow.
- At the bottom right, there are two buttons: "Close" (grey) and "Save" (blue).

- Enter the name of the SBC device.
- Enter the IP address of the SBC device.
- Enter the Device FQDN.
- Enter the Gateway username and password.
- Click **Save** to apply the changes.

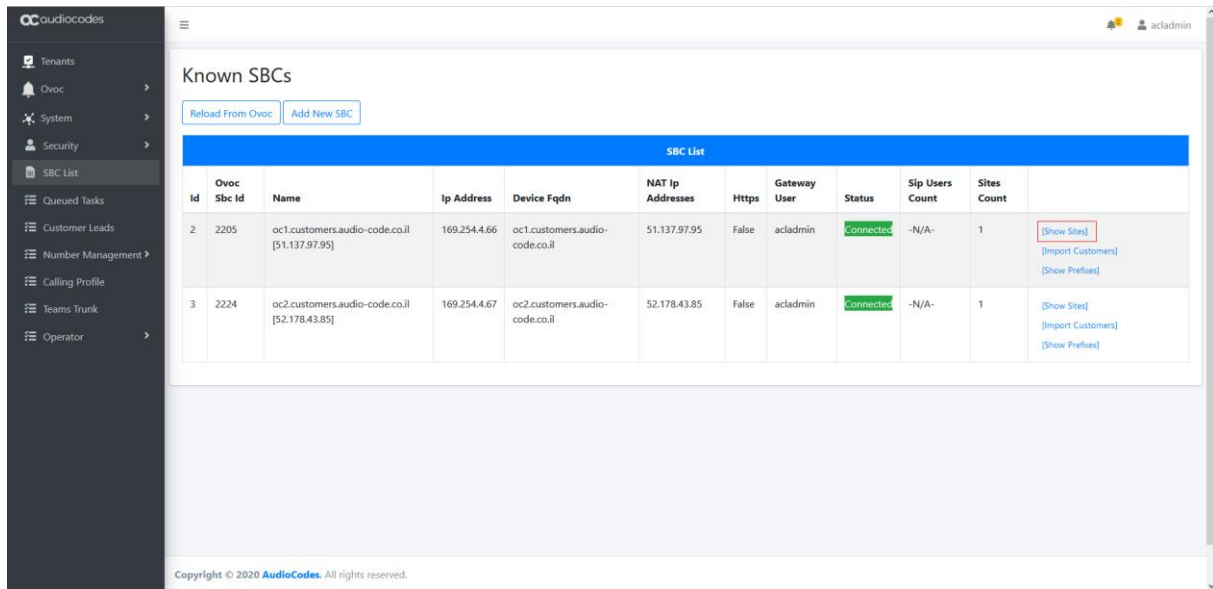
26.2 Show SBC Site Locations

A list of site locations that are provisioned with a specific SBC device can be displayed.

To show site locations:

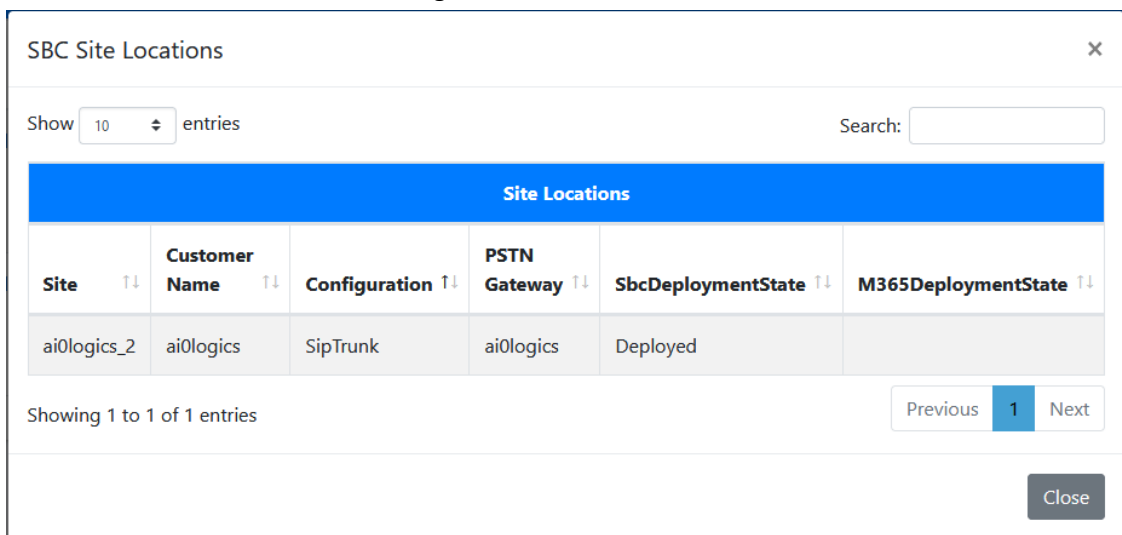
1. In the Known SBCs page, select an SBC device, and then click **Show Sites**.

Figure 26-3: Show Sites



A list of site locations that are provisioned with the selected SBC are displayed:

Figure 26-4: Show SBC Sites



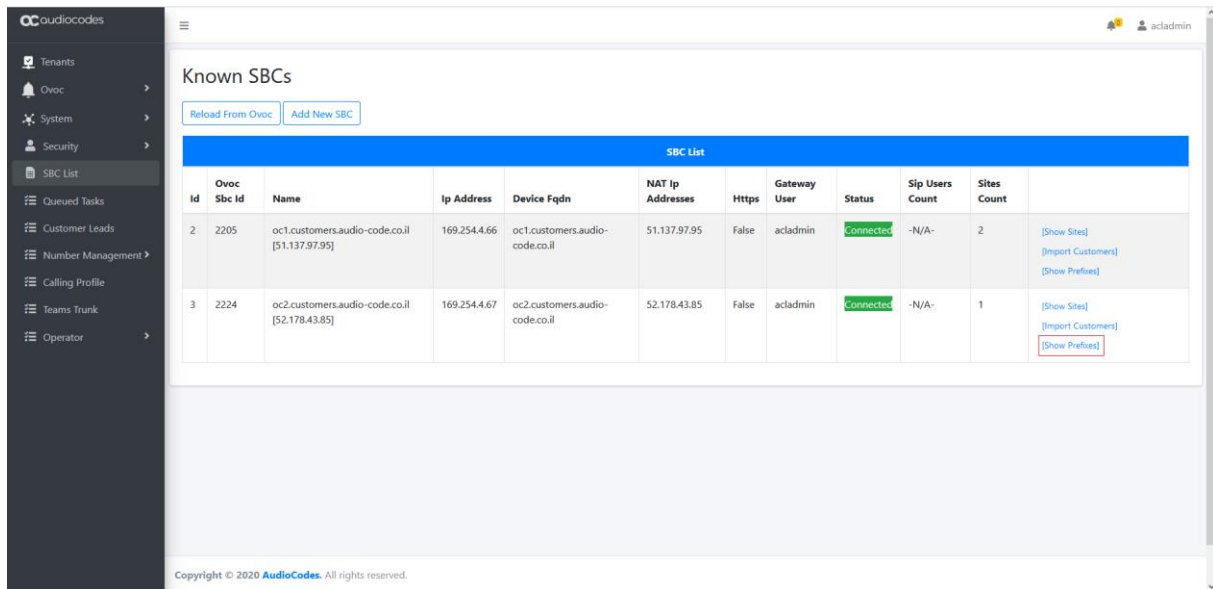
26.3 Show Prefixes

This option enables you to view a list of configured prefixes for a customer.

To show prefixes:

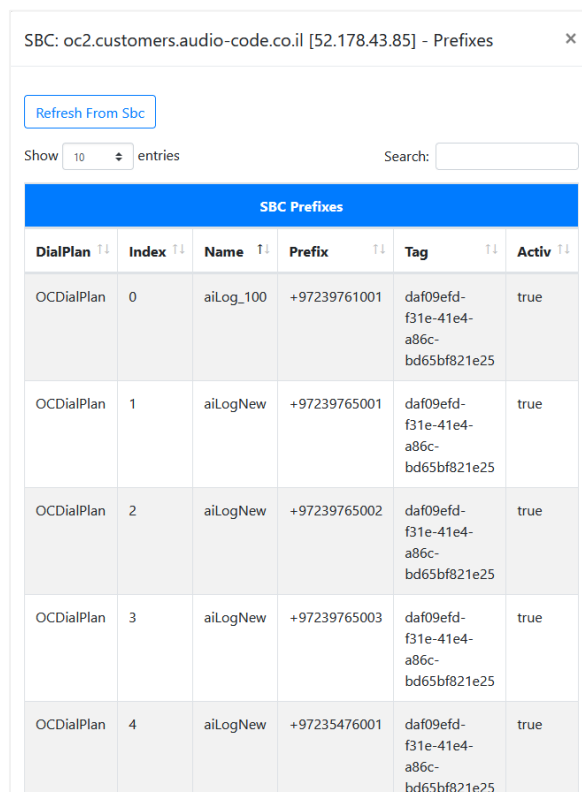
1. In the Known SBCs page, , select an SBC device, and then click **Show Prefixes**.

Figure 26-5: Show Prefixes



A list of configured prefixes for the selected SBC are displayed.

Figure 26-6: Configured SBC Prefixes



27 Queued Tasks

You can view a list of queued tasks that are pending execution.

To view a list of queued tasks:

1. In the UMP Main Tenant Navigation pane, click **Queued Tasks**.

Figure 27-1: Queued Tasks

Id	Customer	Cmd Type	State	Retries	When Executed	Execution Result	Next Execution Minutes	Was Successful	When Created
3865	BasicPack	TenantRemove	Executing	0			Now		16-01-2022, 12:23
3864	BasicConnect	TenantRemove	Executing	0			Now		16-01-2022, 12:23
3863	Test1	TenantRemove	Executing	0			Now		16-01-2022, 12:23
3862	BasicPack	TenantRemove	Executing	1			Now		16-01-2022, 12:23
3861	BasicConnect	TenantRemove	Executing	1			Now		16-01-2022, 12:23
3860	Test1	TenantRemove	Executing	1			Now		16-01-2022, 12:23
3859	BasicPack	TenantRemove	Executing	2			Now		16-01-2022, 12:23
3858	BasicConnect	TenantRemove	Executing	2			Now		16-01-2022, 12:23
3857	Test1	TenantRemove	Executing	2			Now		16-01-2022, 12:23

The following details are displayed for each task:

Table 27-1: Queued Tasks

Parameter	Description
Customer	Indicates the name of the customer.
Cmd Type	Indicates the name of the script that has been applied to a customer. For example, Cleanup SBC or tenant remove.
State	One of the following: <ul style="list-style-type: none"> ■ Queued ■ Reserved ■ Executing ■ FinishSuccess ■ FinishFailure
Retries	Indicates the number of retry attempts.
When Executed	Indicates when the task was executed.
Execution Result	Indicates the execution result.
Next Execution Minutes	Indicates the next execution time in minutes.
Was Successful	Indicates whether the task was executed successfully.
When Created	Indicates when the task was created.

Part V

Onboarding a New Tenant Customer

28 Introduction

This section describes how to add the new Customer Microsoft 365 (M365) Tenant in the AudioCodes UMP 365 SP Edition application. When a new Customer M365 Tenant is added, a new end-to-end service is created between Microsoft Teams to the Provider SIP interface and full replication of the customer M365 Tenant to the management system is performed.

29 Onboarding Prerequisites

- All customer users must be preconfigured with User Type “Teams Only” and with “Enterprise voice” enabled.
- The customer should have at least one Teams phone system free as part of Direct Routing requirements.
- Verify with the customer Tenant that Voice Routing Policy ‘Unrestricted’ isn’t in use.



- For further information, see Microsoft’s guidelines “Register a subdomain name in a M365 Tenant”: [https://docs.microsoft.com/en-us/microsoftteams/direct-routing-sbc-multiple-tenants#register-a-subdomain-name-in-a-M365 Tenant-tenant](https://docs.microsoft.com/en-us/microsoftteams/direct-routing-sbc-multiple-tenants#register-a-subdomain-name-in-a-M365-Tenant-tenant).

30 Onboarding Teams Direct Routing Customers

This section describes how to onboard a new customer. New customers can be onboarded for the following license types:

- Hosted Essentials (see Section 30.1)
- Hosted Essentials + (see Section 30.2)
- Hosted Pro (see Section 30.3)

30.1 Hosted Essentials

This section describes how to onboard new customers with “Hosted Essentials” licenses.

To onboard a new “Hosted Essentials” customer:


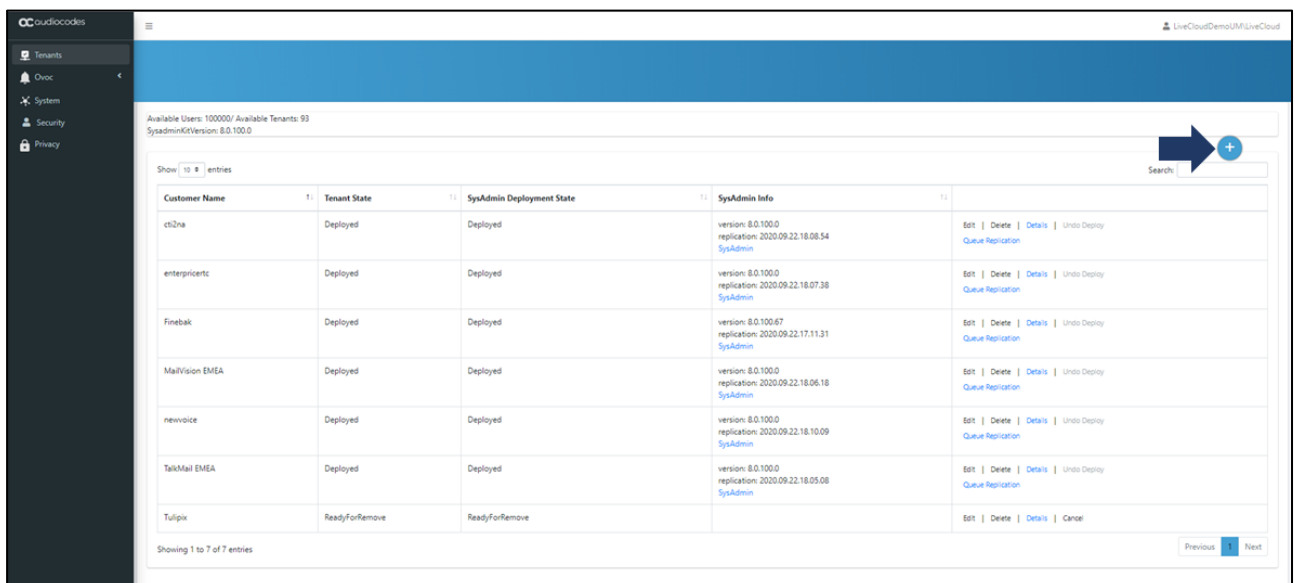
1. From the Main Provider Dashboard / Tenant view, select **Actions** .

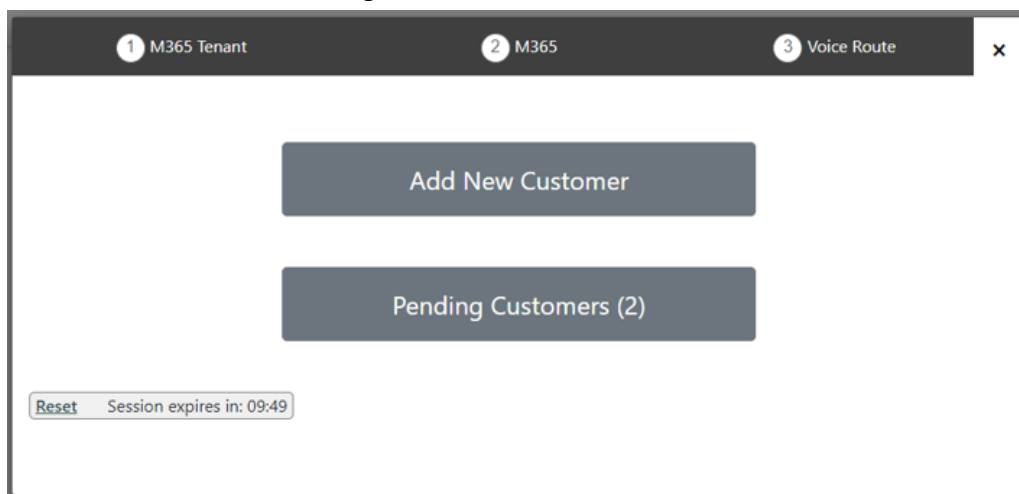
Figure 30-1: M365 Tenants



Customer Name	Tenant State	SysAdmin Deployment State	SysAdmin Info	
ct32na	Deployed	Deployed	version: 8.0.100.0 replication: 2020.09.22.18.08.54 SysAdmin	Edit Delete Details Undo Deploy Queue Replication
enterpricentc	Deployed	Deployed	version: 8.0.100.0 replication: 2020.09.22.18.07.38 SysAdmin	Edit Delete Details Undo Deploy Queue Replication
Finelbak	Deployed	Deployed	version: 8.0.100.67 replication: 2020.09.22.17.11.31 SysAdmin	Edit Delete Details Undo Deploy Queue Replication
MailVision EMEA	Deployed	Deployed	version: 8.0.100.0 replication: 2020.09.22.18.06.18 SysAdmin	Edit Delete Details Undo Deploy Queue Replication
newvoicce	Deployed	Deployed	version: 8.0.100.0 replication: 2020.09.22.18.10.09 SysAdmin	Edit Delete Details Undo Deploy Queue Replication
TalkMail EMEA	Deployed	Deployed	version: 8.0.100.0 replication: 2020.09.22.18.05.08 SysAdmin	Edit Delete Details Undo Deploy Queue Replication
Tulpix	ReadyForRemove	ReadyForRemove		Edit Delete Details Cancel

The Onboarding interface opens.

Figure 30-2: Add New Customer



2. Click **Add New Customer**.

Figure 30-3: Add New Customer

1 M365 Tenant 2 M365 3 Voice Route

Full Customer Name
BasicPackage

Short Customer Name
BasicPCK

License Type
 Hosted Essential
 Hosted Essentials+
 Hosted Pro

Back Next

3. Select the **Hosted Essential** License Type.

Figure 30-4: Configure SBC

1 M365 Tenant 2 M365 3 Voice Route

Customer: BasicPCK

Configure SBC

Sbc Site Name BasicPCK

Online PSTN Gateway Online PstnGateway

Sbc Configuration: Sip Trunk BYOC

Region Select an SBC from list

Carrier Select a Carrier from list

Carrier Registration

Enable Cac

Back Next

Carrier	Select a Carrier from list <input type="button" value="v"/>	
<input checked="" type="checkbox"/> Carrier Registration	<input type="text" value="Username"/>	<input type="text" value="Password"/>
	<input type="text" value="MainLine"/>	<input type="text" value="Hostname"/>
<input checked="" type="checkbox"/> Enable Cac	Select CAC Profile <input type="button" value="v"/>	
	<input type="button" value="Back"/>	<input type="button" value="Next"/>

4. Configure SBC parameters according to the table below and then click **Next**.

Table 30-1: SBC Parameters

O365 Setting	Description
Configure SBC	Select check box if you wish to configure the SBC.
SBC Site Name	Name of the SBC site location.
Online PSTN Gateway	<p>Unique subdomain name per M365 Tenant (CSOnlinePSTNGateway –FQDN) which represents the desired host name added for the carrier trunk.</p> <p>This name must be preconfigured on the M365 Tenant Domain or via DNS provisioning (see Chapter 9).</p>
SBC Configuration	<p>Select one of the following SBC configuration modes:</p> <ul style="list-style-type: none"> ■ SIP Trunk ■ BYOC
Region	Select the required SBC device according to site location IP address.
Carrier	<p>This option is available If you selected SIP Trunk or BYOC for SBC Configuration above. The selected carrier binds to the configured SIP Interface, Proxy Set and IP Profile on the SBC (where the same name is configured for all three entities on the SBC).</p>
Carrier Registration	<p>Select this option to perform SIP Account Registration for the Carrier trunk:</p> <ul style="list-style-type: none"> ■ Username: Defines the digest MD5 Authentication username. The valid value is a string of up to 60 characters. By default, no value is defined. ■ Password: Defines the digest MD5 Authentication password. The valid value is a string of up to 50 characters. Note: The password cannot be configured with wide characters. ■ MainLine (Contact User): Defines the AOR username. This appears in REGISTER From/To headers as ContactUser@HostName ■ Host Name: Defines the Address of Record (AOR) host name. The host name appears in SIP REGISTER From/To headers as ContactUser@HostName.
Enable CAC	Enable Call Admission Control (CAC). From the drop-down list, select the desired CAC Profile including the desired number of call sessions.

Figure 30-5: SBC Number Prefixes

5. Define a prefix number range by either by uploading a CSV file or by entering specific number prefixes.

Table 30-2: Define Prefixes

Setting	Description
Update from CSV	Browse to load a CSV file containing a range of telephone prefixes.
Telephone Number Prefix	Enter a specific telephone number prefix.

Figure 30-6: Load CSV Prefix File

Figure 30-7: Add Individual Prefixes





A Dial file xxxname must be preconfigured on the SBC or IP-PBX for applying this configuration.

Figure 30-8: SBC Scripts

Customer Variables	Value

6. Configure SBC scripts:

- Click the  to edit the SBC Onboarding Script file. This is a Preconfigured script that is prepared by AudioCodes Professional services and that can be customized by setting Custom Variables.
- Click the  to edit the SBC Cleanup Script file. Each SBC Onboarding script file has a corresponding Cleanup script file to restore the configuration to their original settings. This is a Preconfigured script that is prepared by AudioCodes Professional services and that can be customized by setting Custom Variables.
- Script variables can be customized and loaded to the SBC Onboarding and Cleanup scripts above.

See Section 24.4.


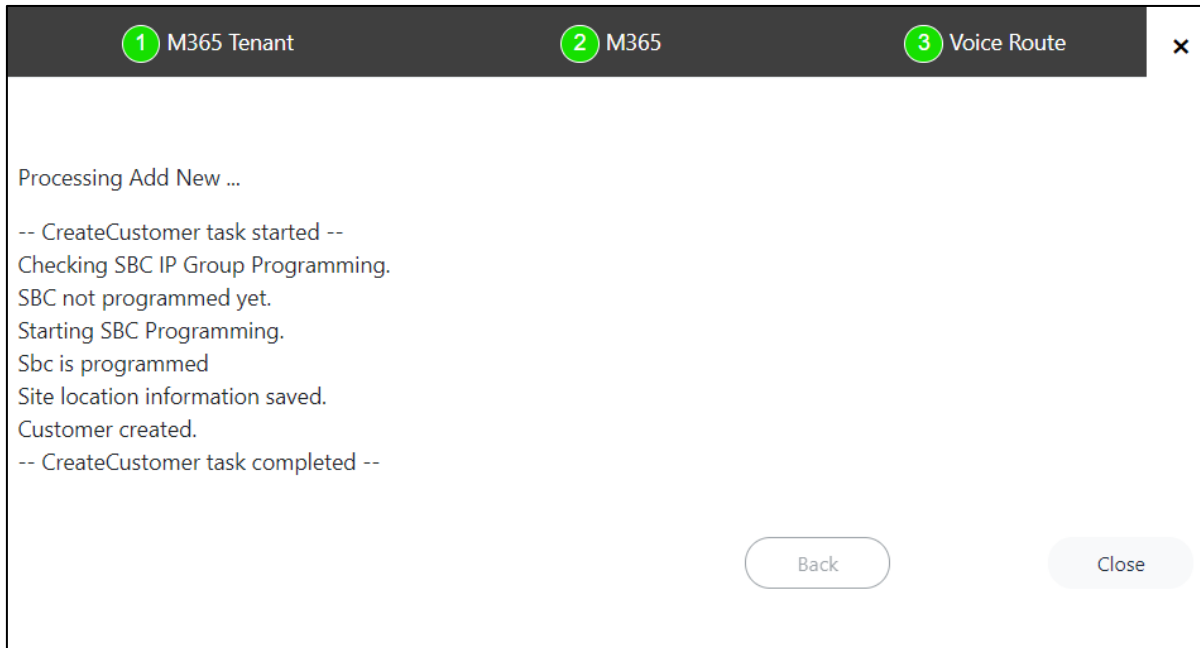
- When you have completed the configuration, click  .
The following screen is displayed:

Figure 30-9: Configuration Complete



30.2 Hosted Essentials +

This section describes how to onboard new “Hosted Essentials +” customers.

To onboard a new Hosted Essentials + customer:


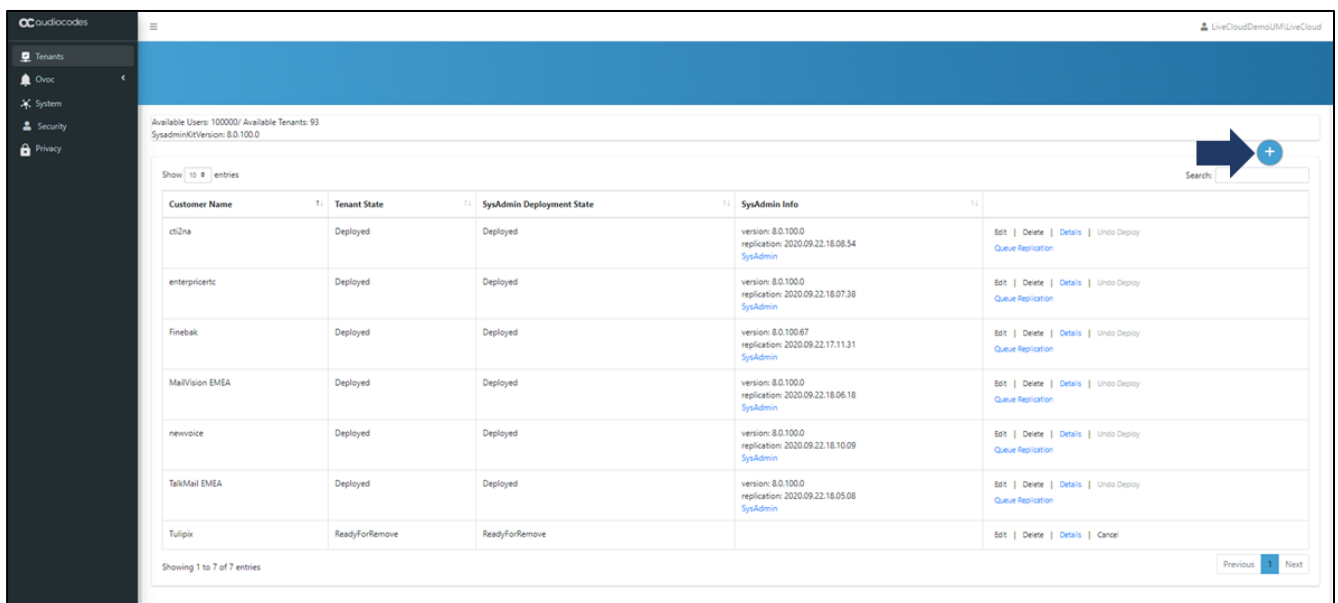
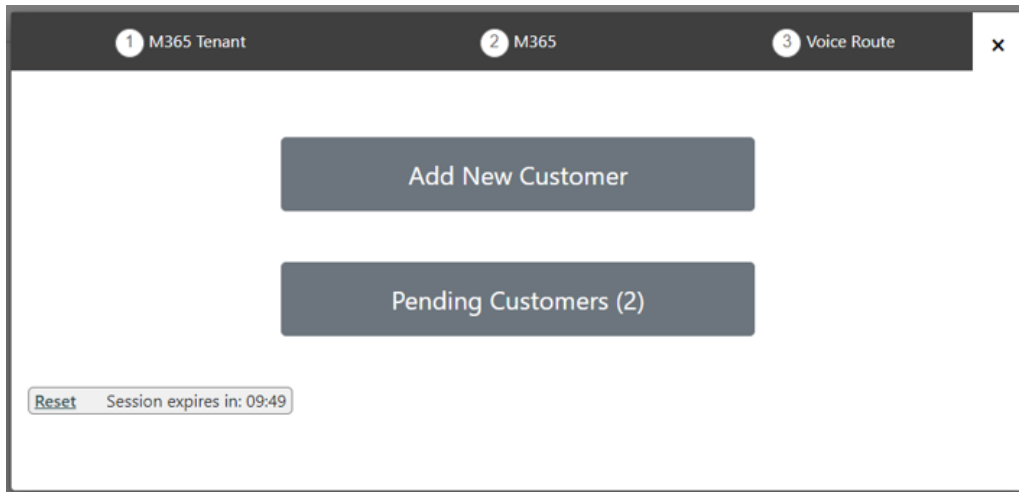
- From the Main Provider Dashboard / Tenant view, select **Actions**  .

Figure 30-10: Add Customer Button



The Onboarding interface opens.

Figure 30-11: Add New Customer



2. Click **Add New Customer**.

Figure 30-12: Add New Customer

3. Full Customer M365 Tenant Name – Free Text.
4. Unique new Customer M365 Tenant Name - Define a unique name for the new M365 Tenant.
Note the following rules:
 - The string should be 3-15 characters long
 - The following characters cannot be used: \ / : * ? " < > | audit
 - Can contain letters (lower/UPPER case), Numbers and special characters are allowed, however cannot contain the dot (.) or blank spaces.
 - Unique name per M365 Tenant M365 Tenant Name

5. Select the **Hosted Essentials+** license Type.
6. Select the number of licensed users. A maximum of 500 users can be configured per customer.
7. Select one of the following options and then click **Next**:
 - Enter the M365admin user account name and password (credentials are validated; see figure below).
 - Send link to customer IT administrator for authentication (see Section 30.3 below).

Figure 30-13: Validating Credentials

1 M365 Tenant 2 M365 3 Voice Route

Validating credentials, please wait! On successful authentication the wizard will continue.

Back Next

Once you have established a secure connection to Microsoft 365, the following screen is displayed.

Figure 30-14: Microsoft 365 Settings

1 M365 Tenant 2 M365 3 Voice Route

Customer **BasicPlus**

Override Admin Domain:

Tenant ID:

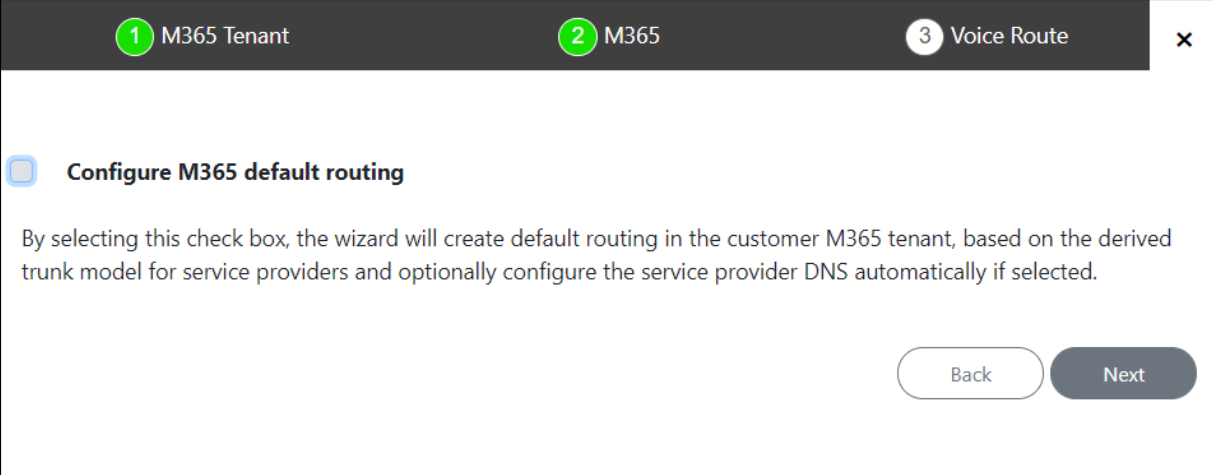
Grant Admin Access to:

Back Next

8. Define Microsoft 365 settings and then click **Next**.

Table 30-3: Microsoft 365 Settings

M365 Setting	Description
M365 Domain (Override Admin Domain)	Customer Tenant original Microsoft 365 domain prior to applying vanity domain names (“example.onmicrosoft.com”).
Tenant ID	The customer Tenant ID. This field is automatically filled; the Tenant ID of the M365 authenticated user for this Onboarding wizard process.
Grant Admin Access to	This option provides multi-tier support for third-party administrators such as Channel or Customer administrators to perform actions in Live Cloud for Teams Channel/Customer Portal (Optional). When this option is used, Single Sign-on support with the customer Azure AD is provided.

Figure 30-15: Configure Default Routing


1 M365 Tenant 2 M365 3 Voice Route

Configure M365 default routing

By selecting this check box, the wizard will create default routing in the customer M365 tenant, based on the derived trunk model for service providers and optionally configure the service provider DNS automatically if selected.

Back Next

9. Do one of the following:
 - Select **Configure M365 default routing** checkbox; the wizard creates default routing in the customer tenant based on the derived trunk model for service providers. In addition, you can optionally configure the DNS server. See Section 30.2.1.
 - Click **Next** and proceed to Section 30.2.20.

30.2.1 Configure Default Routing

If option **Configure M365 default routing** is selected, the following screen is displayed:

Figure 30-16: Configure M365 Default Routing

1 M365 Tenant **2** M365 **3** Voice Route

Configure M365 default routing

Click [[Here](#)] to Provision M365 Domain and DNS Automatically

Online PSTN Gateway audio0code.onmicrosoft.com

M365 Onboarding Script Default Script



M365 Cleanup Script Default Script

Customer Variables	Value
--------------------	-------

Back Next

1. Configure parameters as described in the table below and then click **Next**.

Table 30-4: M365 Default Routing

O365 Setting	Description
Click here to Provision M365 Domain and DNS Automatically	Support for automatic and semi-automatic DNS provisioning (see Sections 9.1 and 09.2 respectively).
Region/Country	The customer SBC region subdomain name configured in Section 9.1.1.4.
IP Address	Preconfigured IP address of the region SBC.
SBC	Preconfigured FQDN of the region SBC.
Domain Name	Preconfigured domain name of the DNS (A-record).
SBC Site Name	The Customer Shortname configured at the start of the wizard.
License Plan	Preconfigured license plan including all phone system licenses not only E5. The customer should have at least one Teams phone system free as part of Direct Routing requirements.
Other Configuration	
Online PSTN Gateway	Unique subdomain name per M365 Tenant (CSOnlinePSTNGateway –FQDN) which represents the desired host name added for the carrier trunk. This name must be preconfigured on the M365 Tenant Domain or via DNS provisioning (see Chapter 9).
M365 Onboarding Script	Preconfigured script that is prepared by AudioCodes Professional services and that can be customized by setting Customer Variables. Click the  to edit the Onboarding script file. For example, when a service provider needs a separate registration per customer tenant. See Section 24.2.1.
M365 Cleanup Script	Preconfigured script that is prepared by AudioCodes Professional services and that can be customized by setting Customer Variables. Click the  to edit the Cleanup script file. See Section 24.2.2.
Customer Variables	Script variables can be customized and loaded to the M365 Onboarding and Cleanup scripts. See Section 24.4.

The following screens are displayed:

Figure 30-17: Configure SBC (Default Routing)-Hosted Essentials+ with SIP Trunk/BYOC

1 M365 Tenant
 2 M365
 3 Voice Route
 ✕

Customer: HostedPlus

Configure SBC

Sbc Site Name

Online PSTN Gateway

Sbc Configuration: Sip Trunk IP PBX BYOC

Region

Carrier

Carrier Registration

Enable Cac

Sbc Configuration: Sip Trunk IP PBX BYOC

Region

Carrier

Carrier Registration

Enable Cac

Figure 30-18: Configure SBC (Default Routing)-Hosted Essentials+ with IP PBX

The screenshot shows a configuration wizard with three steps: 1. M365 Tenant, 2. M365, and 3. Voice Route. The current step is 'M365'. The configuration is for a 'HostedPlus' customer. The 'Configure SBC' checkbox is checked. The 'Sbc Site Name' is 'HostedPlus'. The 'Online PSTN Gateway' is 'audio0code.onmicrosoft.com'. The 'Sbc Configuration' is set to 'IP PBX'. The 'Region' is a dropdown menu with the text 'Select an SBC from list'. There are 'Back' and 'Next' buttons at the bottom right.

Customer: HostedPlus

Configure SBC

Sbc Site Name

Online PSTN Gateway

Sbc Configuration: Sip Trunk IP PBX BYOC

Region

2. Configure SBC parameters according to the table below and then click **Next**.

Table 30-5: SBC Parameters

O365 Setting	Description
Configure SBC	Select check box if you wish to configure the SBC.
SBC Site Name	Name of the SBC site location.
Online PSTN Gateway	<p>Unique subdomain name per M365 Tenant (CSOnlinePSTNGateway –FQDN) which represents the desired host name added for the carrier trunk.</p> <p>This name must be preconfigured on the M365 Tenant Domain or via DNS provisioning (see Chapter 9).</p> <p>Note: If Default Routing is configured, then this field is automatically filled.</p>
SBC Configuration	<p>Select one of the following SBC configuration modes:</p> <ul style="list-style-type: none"> ■ SIP Trunk ■ IP-PBX ■ BYOC
Region	Select the required SBC device according to site location IP address.
<p>Carrier: (this option is only relevant if SIP Trunk and BYOC were selected above). This option is available if you selected SIP Trunk or BYOC for SBC Configuration above. The selected carrier binds to the configured SIP Interface, Proxy Set and IP Profile on the SBC (where the same name is configured for all three entities on the SBC).</p>	
Carrier Registration	<p>Select this option to perform SIP Account Registration for the Carrier trunk:</p> <ul style="list-style-type: none"> ■ Username: Defines the digest MD5 Authentication username. The valid value is a string of up to 60 characters. By default, no value is defined. ■ Password: Defines the digest MD5 Authentication password. The valid value is a string of up to 50 characters. Note: The password cannot be configured with wide characters. ■ MainLine (Contact User): Defines the AOR username. This appears in REGISTER From/To headers as ContactUser@HostName ■ Host Name: Defines the Address of Record (AOR) host name. The host name appears in SIP REGISTER From/To headers as ContactUser@HostName.
Enable CAC	Enable Call Admission Control (CAC). From the drop-down list, select the desired CAC Profile including the desired number of call sessions.

Figure 30-19: Enable CAC

1 M365 Tenant **2** M365 **3** Voice Route ✕

Customer: EPC

Configure SBC

Sbc Site Name EPC

Online PSTN Gateway OS365 Trunk

Sbc Configuration: Sip Trunk BYOC

Region 52.143.14.26_SBC

Carrier SIPTrunk

Carrier Registration

SIP Trunk ddswwdsds

SIPMain O365Host

Enable Cac

1 session

1 session

5 sessions

10 sessions

20 sessions

1000 sessions

thisisthemaxallowednumberofcharsincactem

Back Next

30.2.2 Configure without Default Routing

If the **Configure M365 Default Routing** option was not selected, then the following screens are displayed:

Figure 30-20: Configure SBC with IP PBX

1 M365 Tenant **2** M365 **3** Voice Route

Customer: HostedPlus

Configure SBC

Sbc Site Name HostedPlus

Online PSTN Gateway audio0code.onmicrosoft.com

Sbc Configuration: Sip Trunk IP PBX BYOC

Region Select an SBC from list

Back Next

Figure 30-21: Configure SBC with SIP Trunk/BYOC

1 M365 Tenant **2** M365 **3** Voice Route

Customer: HostedPlus

Configure SBC

Sbc Site Name HostedPlus

Online PSTN Gateway audio0code.onmicrosoft.com

Sbc Configuration: Sip Trunk IP PBX BYOC

Region Select an SBC from list

Carrier Select a Carrier from list

Carrier Registration

Enable Cac

Back Next

Sbc Configuration: Sip Trunk IP PBX BYOC

Region customers.audio-code.co.il [51.137.97.95] ▼

Carrier Select a Carrier from list ▼

Carrier Registration

Username Password

MainLine Hostname

Enable Cac Select an CAC Profile ▼

Back Next

1. Configure SBC parameters according to Table 30-5, click **Next**, and then proceed to Section 30.3.3.

30.2.3 Configure SBC Number Prefixes and Scripts

The Wizard continues with the configuration of the SBC Number Prefixes.

Figure 30-22: SBC Number Prefixes

1 M365 Tenant 2 M365 3 Voice Route ×

SBC number prefixes Choose File No file chosen

+97239760000 +

Back Next

2. Define a prefix number range by either by uploading a CSV file or by entering specific number prefixes.

Table 30-6: Define Prefixes

Setting	Description
Update from CSV	Browse to load a CSV file containing a range of telephone prefixes.
Telephone Number Prefix	Enter a specific telephone number prefix.

Figure 30-23: Load CSV Prefix File

Figure 30-24: Add Individual Prefixes



A Dial file xxxname must be preconfigured on the SBC or IP-PBX for applying this configuration.

Figure 30-25: SBC Scripts

1 M365 Tenant 2 M365 3 Voice Route



SBC Onboarding Script: sbc-scenario7

SBC Cleanup Script: sbc-scenario7Cleanup

Customer Variables	Value

Back Submit

3. Configure SBC scripts:

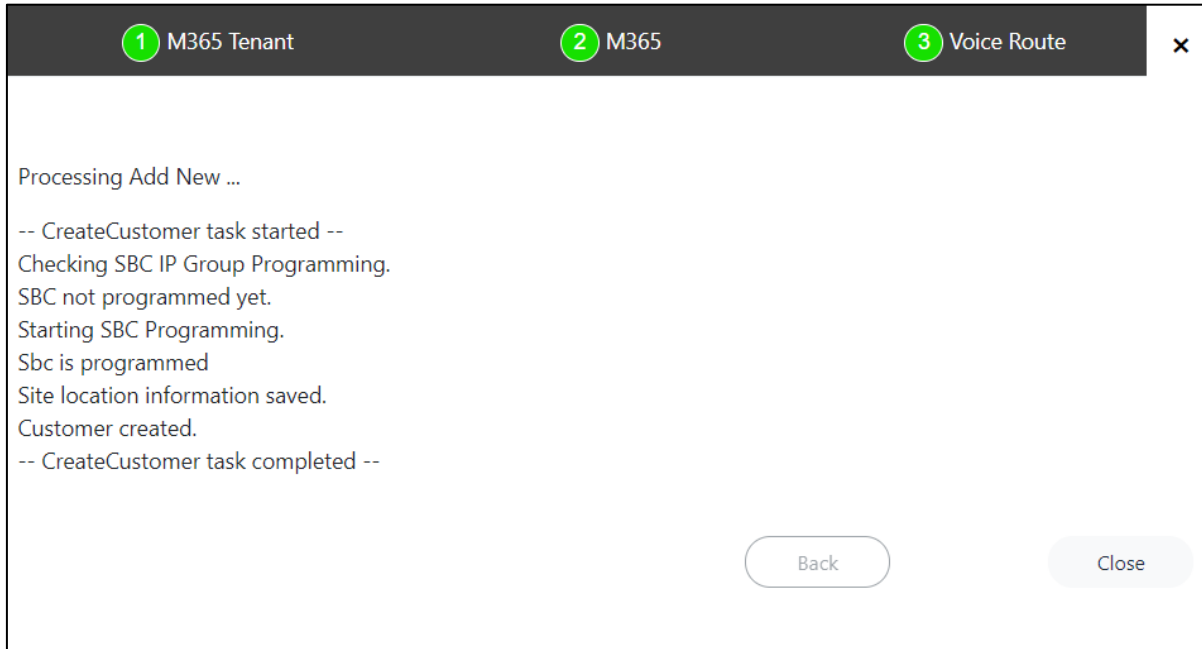
- Click the  to edit the SBC Onboarding Script file. This is a Preconfigured script that is prepared by AudioCodes Professional services and that can be customized by setting Custom Variables.
- Click the  to edit the SBC Cleanup Script file. Each SBC Onboarding script file has a corresponding Cleanup script file to restore the configuration to their original settings. This is a Preconfigured script that is prepared by AudioCodes Professional services and that can be customized by setting Custom Variables.
- Script variables can be customized and loaded to the SBC Onboarding and Cleanup scripts above.

See Section 24.4.

4. When you have completed the configuration, click  .

The following screen is displayed:

Figure 30-26: Configuration Complete



30.3 Hosted Pro

This section describes how to onboard new “ Hosted Pro” customers.

To onboard a new Hosted Essentials + customer:


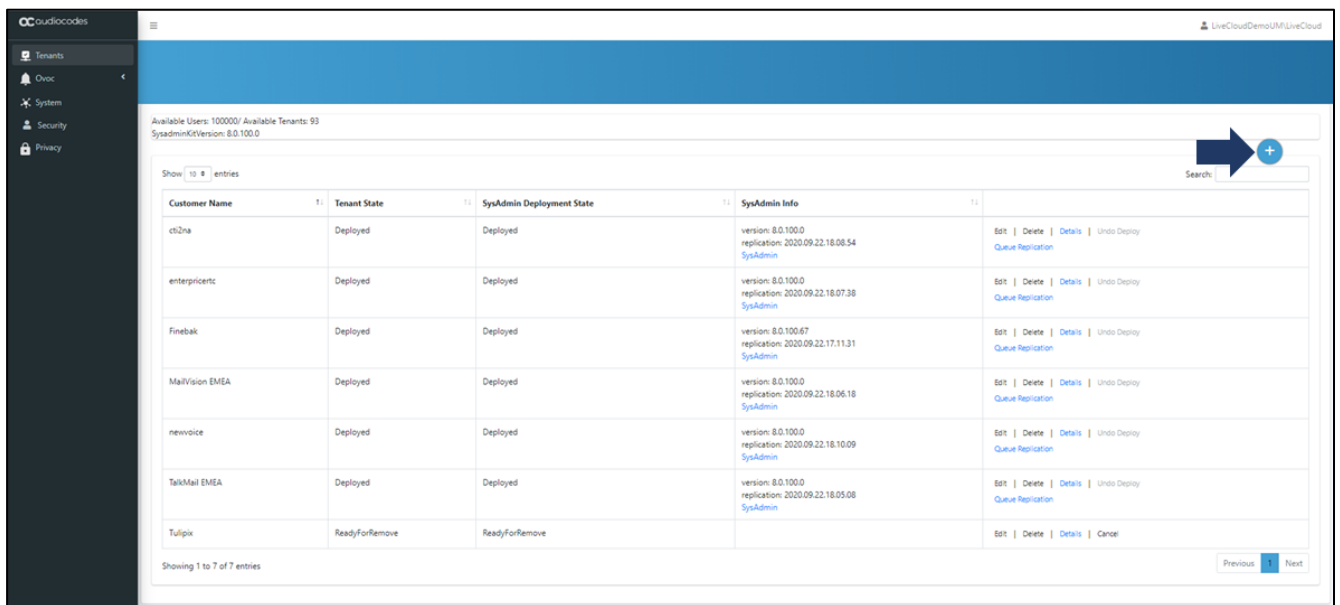
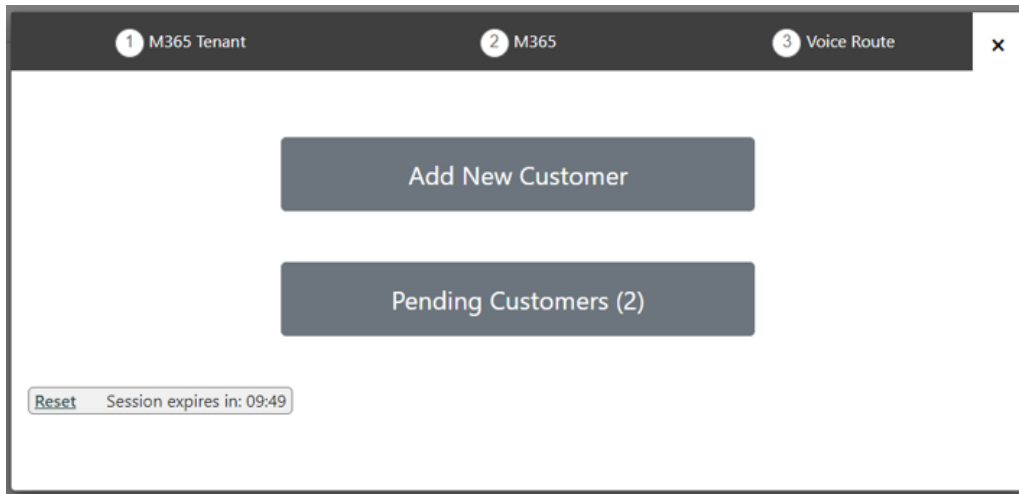
1. From the Main Provider Dashboard / Tenant view, select **Actions** .

Figure 30-27: Add Customer Button



The Onboarding interface opens.

Figure 30-28: Add New Customer



2. Click **Add New Customer**.

Figure 30-29: Add New Customer

3. Full Customer M365 Tenant Name – Free Text.
4. Unique new Customer M365 Tenant Name - Define a unique name for the new M365 Tenant.
Note the following rules:
 - The string should be 3-15 characters long
 - The following characters cannot be used: \ / : * ? " < > | audit
 - Can contain letters (lower/UPPER case), Numbers and special characters are allowed, however cannot contain the dot (.) or blank spaces.
 - Unique name per M365 Tenant M365 Tenant Name

5. Select the **Hosted Pro** license Type.
6. Select the number of licensed users. A maximum of 500 users can be configured per customer.
7. Select one of the following options and then click **Next**:
 - Enter the M365admin user account name and password (credentials are validated; see figure below).
 - Send link to customer IT administrator for authentication (see Section 30.3 below).

Figure 30-30: Validating Credentials

1 M365 Tenant 2 M365 3 Voice Route

Validating credentials, please wait! On succesfull authentication the wizard will continue.

Back Next

Once you have established a secure connection to Microsoft 365, the following screen is displayed.

Figure 30-31: Microsoft 365 Settings

1 M365 Tenant 2 M365 3 Voice Route

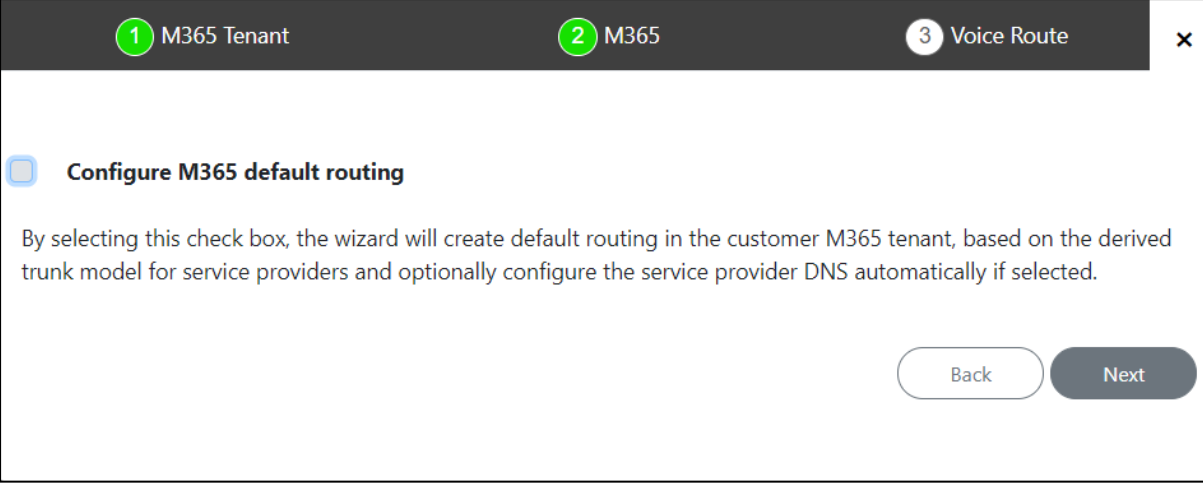
Customer	ProTrunk
Override Admin Domain:	audio0code.onmicrosoft.com
Tenant ID:	bb8950c6-9262-4757-92eb-212e113ec24c
Grant Admin Access to:	Administrator user principal name

Back Next

8. Define Microsoft 365 settings and then click **Next**.

Table 30-7: Microsoft 365 Settings

M365 Setting	Description
M365 Domain (Override Admin Domain)	Customer Tenant original Microsoft 365 domain prior to applying vanity domain names (“example.onmicrosoft.com”).
Tenant ID	The customer Tenant ID. This field is automatically filled; the Tenant ID of the M365 authenticated user for this Onboarding wizard process.
Grant Admin Access to	This option provides multi-tier support for third-party administrators such as Channel or Customer administrators to perform actions in Live Cloud for Teams Channel/Customer Portal (Optional). When this option is used, Single Sign-on support with the customer Azure AD is provided.

Figure 30-32: Configure Default Routing


1 M365 Tenant **2** M365 **3** Voice Route

Configure M365 default routing

By selecting this check box, the wizard will create default routing in the customer M365 tenant, based on the derived trunk model for service providers and optionally configure the service provider DNS automatically if selected.

Back Next

9. Do one of the following:
 - Select **Configure M365 default routing** checkbox; the wizard creates default routing in the customer tenant based on the derived trunk model for service providers. In addition, you can optionally configure the DNS server. Proceed to Section 10.
 - Click **Next** and proceed to Section 10.

30.3.1 Configure Default Routing

If option **Configure M365 default routing** is selected, the following screen is displayed:

Figure 30-33: Configure M365 Default Routing

1 M365 Tenant **2** M365 **3** Voice Route

Configure M365 default routing

Click [[Here](#)] to Provision M365 Domain and DNS Automatically

Online PSTN Gateway: audio0code.onmicrosoft.com

M365 Onboarding Script: Default Script

M365 Cleanup Script: Default Script



Customer Variables	Value

Back Next

1. Configure parameters as described in the table below and then click **Next**.

Table 30-8: M365 Default Routing

O365 Setting	Description
Click here to Provision M365 Domain and DNS Automatically	Support for automatic and semi-automatic DNS provisioning (refer to Sections 9.1 and 9.20 respectively).
Region/Country	The customer SBC region subdomain name configured in Section 9.1.1.4.
IP Address	Preconfigured IP address of the region SBC.
SBC	Preconfigured FQDN of the region SBC.
Domain Name	Preconfigured domain name of the DNS (A-record).
SBC Site Name	The Customer Shortname configured at the start of the wizard.

O365 Setting	Description
License Plan	Preconfigured license plan including all phone system licenses not only E5. The customer should have at least one Teams phone system free as part of Direct Routing requirements.
Other Configuration	
Online PSTN Gateway	Unique subdomain name per M365 Tenant (CSOnlinePSTNGateway –FQDN) which represents the desired host name added for the carrier trunk. This name must be preconfigured on the M365 Tenant Domain or via DNS provisioning (see Chapter 9).
M365 Onboarding Script	Preconfigured script that is prepared by AudioCodes Professional services and that can be customized by setting Customer Variables. Click the  to edit the Onboarding script file. For example, when a service provider needs a separate registration per customer tenant. See Section 24.2.1.
M365 Cleanup Script	Preconfigured script that is prepared by AudioCodes Professional services and that can be customized by setting Customer Variables. Click the  to edit the Cleanup script file. See Section 24.2.2.
Customer Variables	Script variables can be customized and loaded to the M365 Onboarding and Cleanup scripts. See Section 24.4.

The following screens are displayed:

Figure 30-34: Configure SBC with Default Routing-Hosted Pro with IP PBX

The screenshot shows a configuration window with a dark header bar containing three steps: 1 M365 Tenant, 2 M365, and 3 Voice Route. The main content area is white and contains the following fields and options:

- Customer:** ProTrunk
- Configure SBC**
- Sbc Site Name:** TestPro
- Online PSTN Gateway:** audio0code.onmicrosoft.com
- Sbc Configuration:** Sip Trunk IP PBX BYOC
- Region:** Select an SBC from list

At the bottom right, there are two buttons: "Back" and "Next".

Figure 30-35: Configure SBC with Default Routing -Hosted Pro with SIP Trunk/BYOC

The screenshot shows a configuration window with a dark header bar containing three steps: 1 M365 Tenant, 2 M365, and 3 Voice Route. The main content area is white and contains the following fields and options:

- Customer:** ProTrunk
- Configure SBC**
- Sbc Site Name:** TestPro
- Online PSTN Gateway:** audio0code.onmicrosoft.com
- Sbc Configuration:** Sip Trunk IP PBX BYOC
- Region:** Select an SBC from list
- Carrier:** Select a Carrier from list
- Carrier Registration**
- Enable Cac**

At the bottom right, there are two buttons: "Back" and "Next".

Sbc Configuration: Sip Trunk IP PBX BYOC

Region customers.audio-code.co.il [51.137.97.95] ▾

Carrier Select a Carrier from list ▾

Carrier Registration

 Username Password

 MainLine Hostname

Enable Cac Select an CAC Profile ▾

2. Configure SBC parameters according to the table below and then click **Next**.

Table 30-9: SBC Parameters

O365 Setting	Description
Configure SBC	Select check box if you wish to configure the SBC.
SBC Site Name	Name of the SBC site location.
Online PSTN Gateway	If Default Routing was selected, then this field is automatically filled.
SBC Configuration	Select one of the following SBC configuration modes: <ul style="list-style-type: none"> ■ SIP Trunk ■ IP-PBX ■ BYOC
Region	Select the required SBC device according to site location IP address.
Carrier: (this option is only relevant if SIP Trunk and BYOC were selected above). This option is available if you selected SIP Trunk or BYOC for SBC Configuration above. The selected carrier binds to the configured SIP Interface, Proxy Set and IP Profile on the SBC (where the same name is configured for all three entities on the SBC).	
Carrier Registration	Select this option to perform SIP Account Registration for the Carrier trunk: <ul style="list-style-type: none"> ■ Username: Defines the digest MD5 Authentication username. The valid value is a string of up to 60 characters. By default, no value is defined. ■ Password: Defines the digest MD5 Authentication password. The valid value is a string of up to 50 characters. Note: The password cannot be configured with wide characters. ■ MainLine (Contact User): Defines the AOR username. This appears in REGISTER From/To headers as ContactUser@HostName ■ Host Name: Defines the Address of Record (AOR) host name. The host name appears in SIP REGISTER From/To headers as ContactUser@HostName.
Enable CAC	Enable Call Admission Control (CAC). From the drop-down list, select the desired CAC Profile including the desired number of call sessions.

Figure 30-36: Select Region

1 M365 Tenant 2 M365 3 Voice Route x

Customer: EPC

Configure SBC

Sbc Site Name

Online PSTN Gateway

Sbc Configuration: Sip Trunk BYOC

Region ▼

Carrier

Carrier Registration

Enable Cac ▼

Figure 30-37: Select Carrier

The screenshot displays a configuration window with a dark header containing three steps: 1 M365 Tenant, 2 M365, and 3 Voice Route. The main content area includes the following fields and options:

- Customer:** EPC
- Configure SBC**
- Sbc Site Name:** EPC
- Online PSTN Gateway:** OS365 Trunk
- Sbc Configuration:** Sip Trunk BYOC
- Region:** 52.143.14.26_SBC
- Carrier:** Select a Carrier from list (dropdown menu open with options: ProxySet_0, SIPTrunk, SIPTrunk1, this is a very long name deliberately_12)
- Carrier Registration**
- Enable Cac**: Select an CAC Profile

At the bottom right, there are two buttons: "Back" and "Next".

Figure 30-38: Enable CAC

1 M365 Tenant **2** M365 **3** Voice Route ✕

Customer: EPC

Configure SBC

Sbc Site Name EPC

Online PSTN Gateway OS365 Trunk

Sbc Configuration: Sip Trunk BYOC

Region 52.143.14.26_SBC

Carrier SIPTrunk

Carrier Registration

SIP Trunk ddswwdsds

SIPMain O365Host

Enable Cac

1 session

1 session

5 sessions

10 sessions

20 sessions

1000 sessions

thisisthemaxallowednumberofcharsincactem

Back Next

30.3.2 Configure without Default Routing

If the **Configure M365 Default Routing** option was not selected, then the following screens are displayed:

Figure 30-39: Configure SBC with IP PBX

1 M365 Tenant **2** M365 **3** Voice Route

Customer: ProTrunk

Configure SBC

Sbc Site Name TestPro

Online PSTN Gateway -- Please select --

Sbc Configuration: Sip Trunk IP PBX BYOC

Region Select an SBC from list

Back Next

Figure 30-40: Configure SBC with SIP Trunk/BYOC

1 M365 Tenant **2** M365 **3** Voice Route

Customer: ProTrunk

Configure SBC

Sbc Site Name TestPro

Online PSTN Gateway -- Please select --

Sbc Configuration: Sip Trunk IP PBX BYOC

Region Select an SBC from list

Carrier Select a Carrier from list

Carrier Registration

Enable Cac

Back Next

Sbc Configuration: Sip Trunk IP PBX BYOC

Region customers.audio-code.co.il [51.137.97.95] ▾

Carrier Select a Carrier from list ▾

Carrier Registration

Username Password

MainLine Hostname

Enable Cac Select an CAC Profile ▾

Back Next

1. Configure SBC parameters according to Table 30-5, click **Next**, and then proceed to Section 30.3.3.

30.3.3 Configure SBC Number Prefixes and Scripts

The Wizard continues with the configuration of the SBC Number Prefixes.

Figure 30-41: SBC Number Prefixes

1 M365 Tenant 2 M365 3 Voice Route ×

SBC number prefixes Choose File No file chosen

+97239760000 +

Back Next

1. Define a prefix number range by either by uploading a CSV file or by entering specific number prefixes.

Table 30-10: Define Prefixes

Setting	Description
Update from CSV	Browse to load a CSV file containing a range of telephone prefixes.
Telephone Number Prefix	Enter a specific telephone number prefix.

Figure 30-42: Load CSV Prefix File

Figure 30-43: Add Individual Prefixes





A Dial file xxxname must be preconfigured on the SBC or IP-PBX for applying this configuration.

Figure 30-44: SBC Scripts

The screenshot shows a configuration interface for SBC Scripts. At the top, there is a dark navigation bar with three tabs: '1 M365 Tenant', '2 M365', and '3 Voice Route'. Below this, the 'SBC Onboarding Script' is set to 'sbc-scenario7' and the 'SBC Cleanup Script' is set to 'sbc-scenario7Cleanup'. Each script selection has a small icon with a code symbol. Below the script selections is a table with a dark header 'Customer Variables' and 'Value'. At the bottom right, there are two buttons: 'Back' and 'Submit'.

2. Configure SBC scripts:

- Click the  to edit the SBC Onboarding Script file. This is a Preconfigured script that is prepared by AudioCodes Professional services and that can be customized by setting Custom Variables.
- Click the  to edit the SBC Cleanup Script file. Each SBC Onboarding script file has a corresponding Cleanup script file to restore the configuration to their original settings. This is a Preconfigured script that is prepared by AudioCodes Professional services and that can be customized by setting Custom Variables.
- Script variables can be customized and loaded to the SBC Onboarding and Cleanup scripts above.

See Section 24.4.

3. When you have completed the configuration, click  .

The following screen is displayed:

Figure 30-45: Configuration Complete

1 M365 Tenant 2 M365 3 Voice Route

Processing Add New ...

-- CreateCustomer task started --
 Checking SBC IP Group Programming.
 SBC not programmed yet.
 Starting SBC Programming.
 Sbc is programmed
 Site location information saved.
 Customer created.
 -- CreateCustomer task completed --

Back Close

30.4 Provision M365 Domain and DNS Server Automatically

The provisioning of DNS requires the pre-configuration of the DNS regions on Azure (see Chapter 9).

To provision M365 domain and DNS:

1. Click [Here](#) to provision M365 Domain and DNS Automatically.

Figure 30-46: Provision Domain and DNS

1 M365 Tenant 2 M365 3 Voice Route

Dns Region

Sbc

Domain Name

Sbc Site Name Note: You won't be able to change the sbc site name after adding the PSTN Gateway!

License Plan

Back Next

2. Configure parameters as described in the table below.

Table 30-11: DNS Parameters

Setting	Description
DNS Region	The name of the DNS region.
SBC	The SBC device name.
Domain Name	The Domain name
SBC Site Name	The wizard uses the customer ID, for example customers.finebak.com to provision a new service provider subdomain to be used as the voice routing domain for the customer.
License Plan.	One of the following license plans: <ul style="list-style-type: none">■ Hosted Essentials■ Hosted Essentials +

30.5 Running Token Authentication Invitation Wizard

This procedure describes how to authenticate operators using the Token Authentication Invitation wizard for onboarding new customers. This procedure requests consent from the Service Provider IT administrator to the customer tenant IT administrator to allow UMP-365 to connect to their Microsoft 365 platform for the purpose of background replication processing.

When the token authentication requests are sent to the customer IT administrator from the Service Provider administrator, the details of the email Invitation are displayed in the Customer Invitations screen (see Section 25.2) and the details of the authentication token are displayed in the Auth Tokens screen (see Section 25.30).



The customer tenant requires the following UC admin roles (see Section 11.1):

- Teams Admin
- Skype For Business Admin
- Application Administrator

To run the Token Authentication wizard:

1. In the UMP Interface, open the Tenants page to add a new customer.

Figure 30-47: Add New Customer-UMP 365

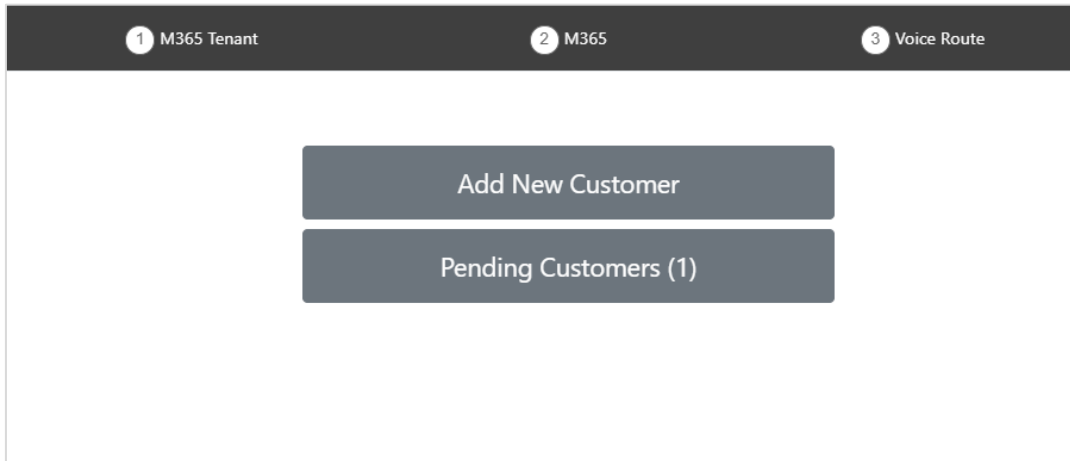
The screenshot shows the UMP interface with a sidebar on the left containing navigation items: Tenants, Ovoc, System, Security, SBC List, and Queued Tasks. The main content area displays a table of customers. At the top right of the main content area, there is a blue circular button with a white plus sign, which is highlighted with a red box. Below this button, there is a search bar containing the text 'finebak'. The table below has the following data:

Customer Name	State	SysAdmin Info	Licensing (licensed users)	Queued commands status
Finebak	Deployed	version: 8.0.220.27 replication: 2021.08.26.14.14.02 SysAdmin	M365 - EssentialPlus (10)	Queued commands: 0 Executing commands: 1 Replication in progress: no

At the bottom of the table, it says 'Showing 1 to 1 of 1 entries (filtered from 12 total entries)'. There are also 'Previous', '1', and 'Next' navigation buttons.

2. Click Add New Customer.

Figure 30-48: Add New Customer



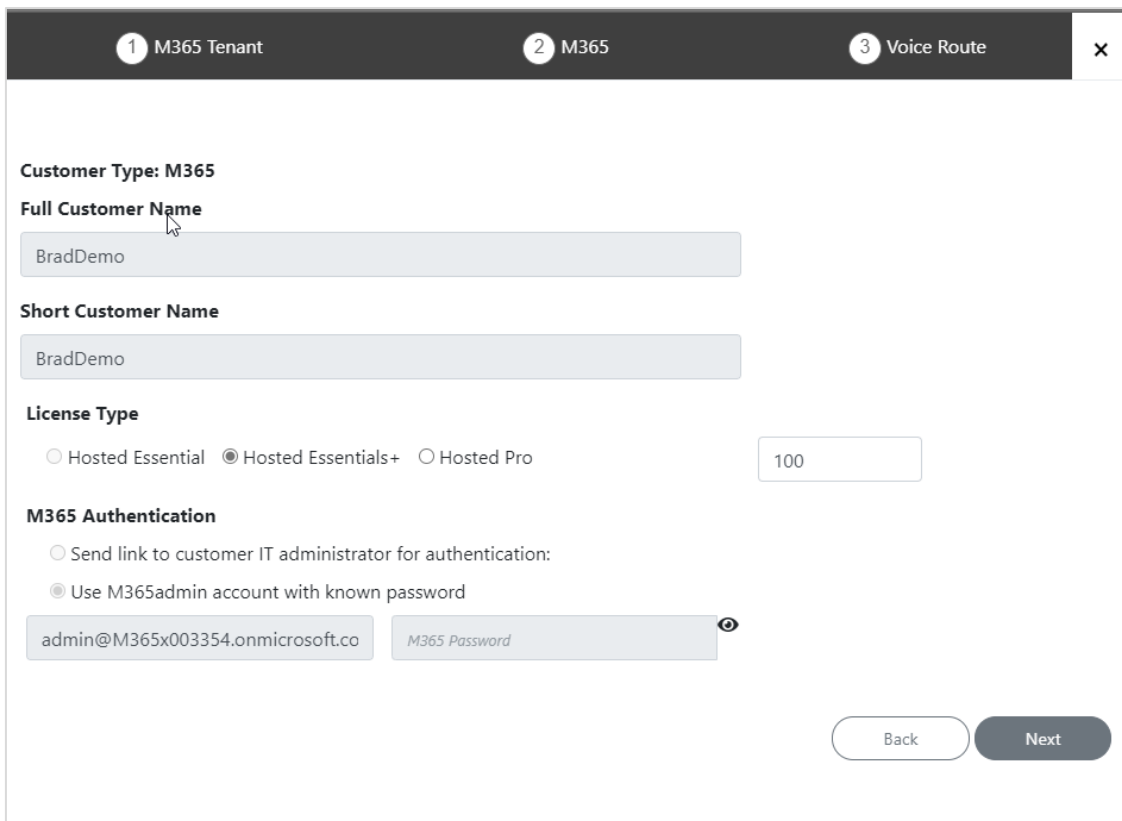
1 M365 Tenant 2 M365 3 Voice Route

Add New Customer

Pending Customers (1)

3. Enter full customer name and short customer name.

Figure 30-49: Enter Customer Names



1 M365 Tenant 2 M365 3 Voice Route

Customer Type: M365

Full Customer Name

BradDemo

Short Customer Name

BradDemo

License Type

Hosted Essential Hosted Essentials+ Hosted Pro

100

M365 Authentication

Send link to customer IT administrator for authentication:

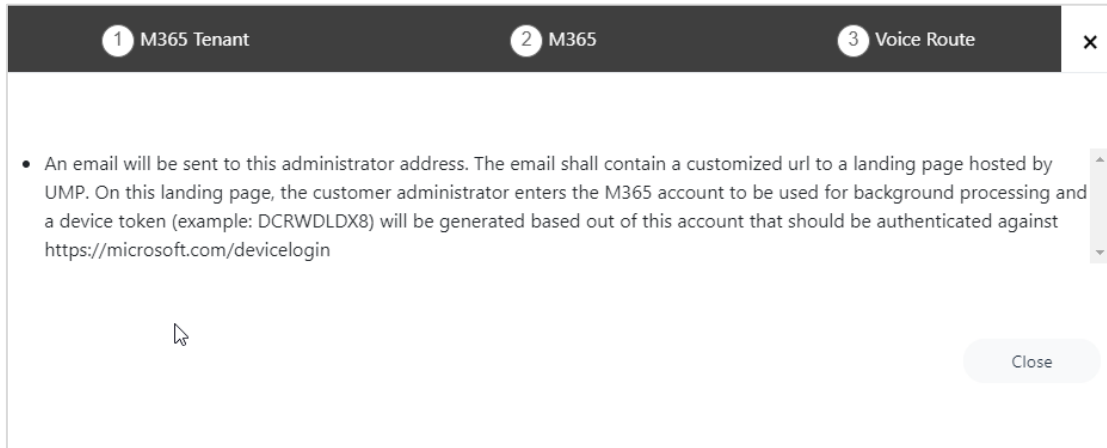
Use M365admin account with known password

admin@M365x003354.onmicrosoft.co M365 Password

Back Next

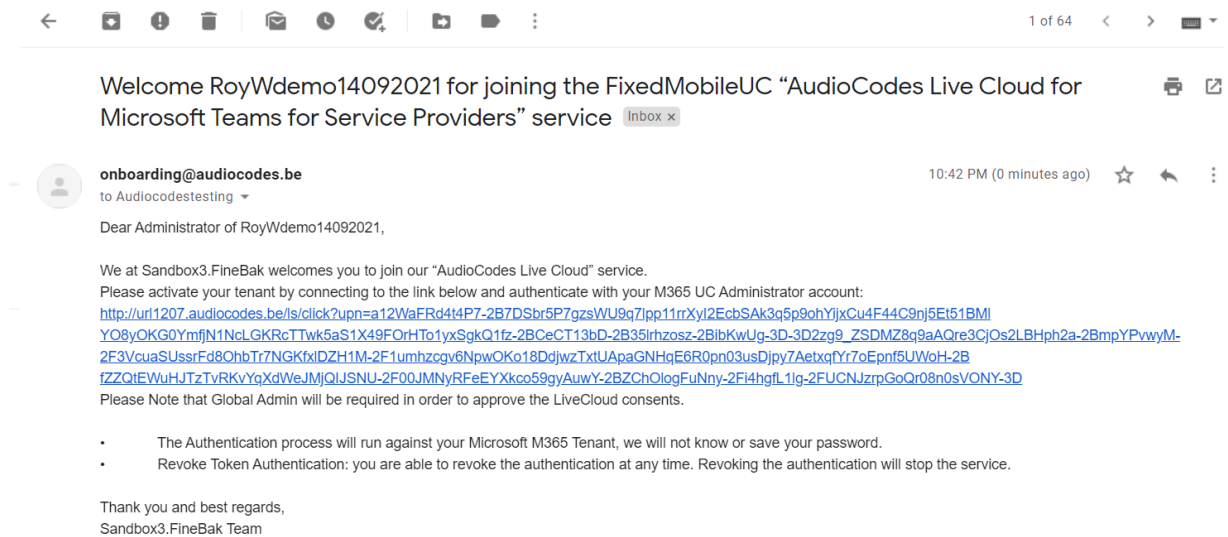
4. Select option Send link to customer IT administrator for authentication.

Figure 30-50: Email Notification



This procedure describes how to authenticate operators using the Token Authentication Invitation wizard. An email message similar to the following is sent to your IT administrator:

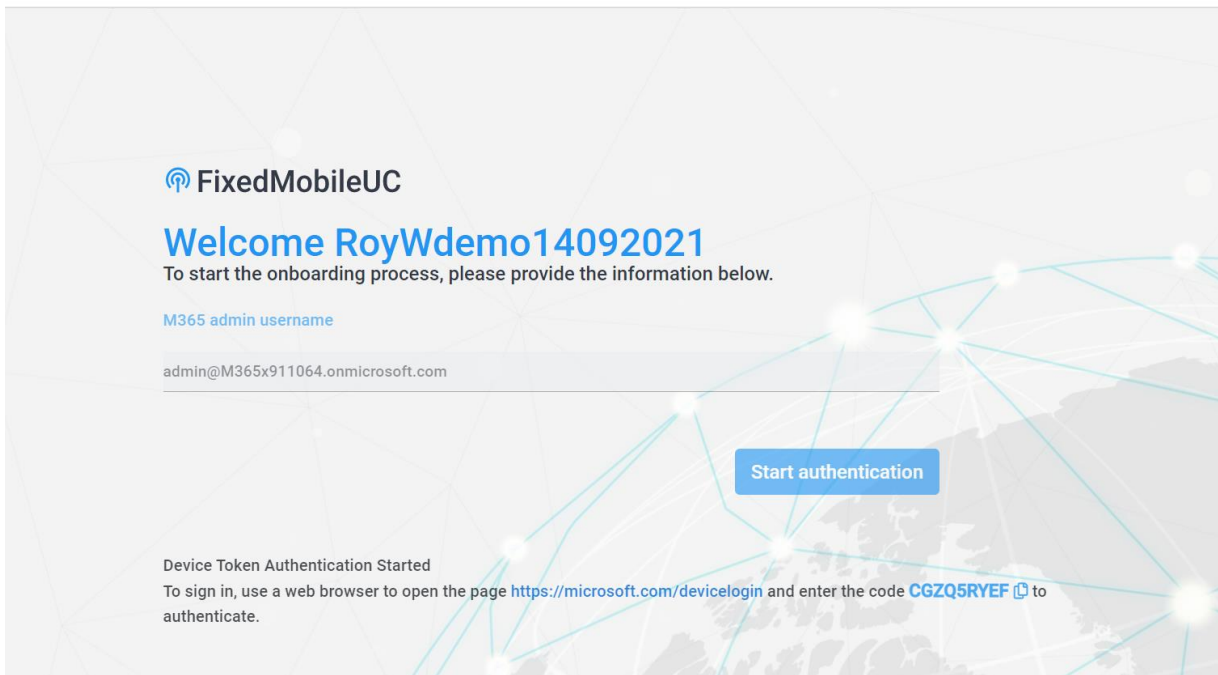
Figure 30-51: Email Notification



Do the following:

1. Click the link sent in the mail; the Token Invitation Wizard Welcome screen is displayed.

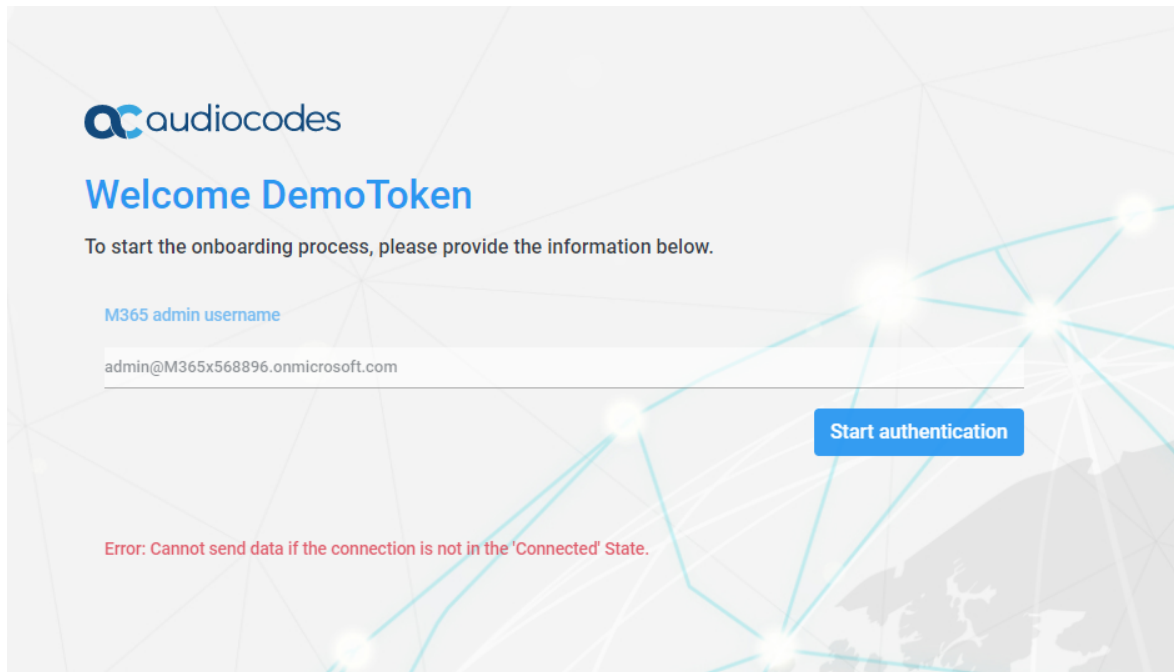
Figure 30-52: Token Authentication Wizard Welcome Screen



2. Enter the credentials of the logged in tenant administrator and then click **Start authentication**.

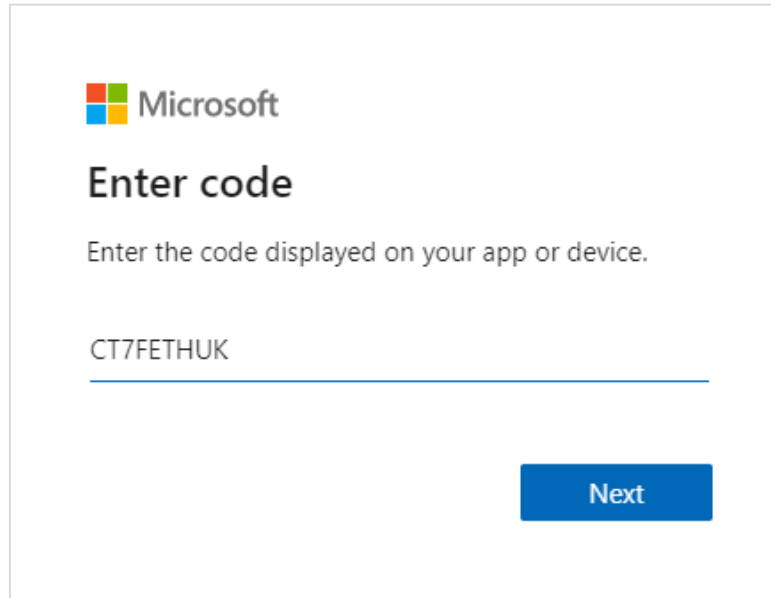
The following error may appear if there is no connection between Azure and the UMP Virtual Machine.

Figure 30-53: Connection Error



- Verify that an inbound firewall rule has been created for port 443 on the Virtual Machine
 - Verify that the connection is secured over HTTPS with Trusted Root CA certificate.
3. Copy the code appearing on the bottom of the screen and then click **Next**.

Figure 30-54: Copy Code



Microsoft

Enter code

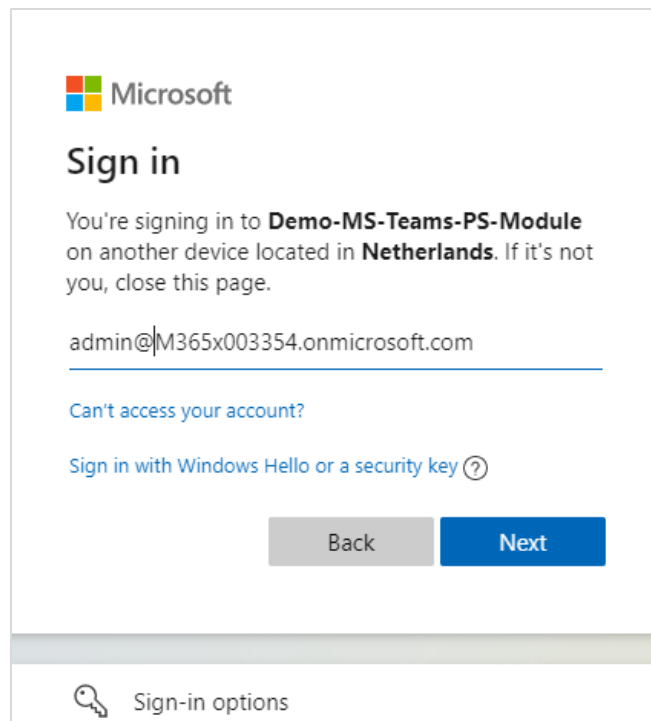
Enter the code displayed on your app or device.

CT7FETHUK

Next

4. Enter the code.

Figure 30-55: Enter Code



Microsoft

Sign in


You're signing in to **Demo-MS-Teams-PS-Module** on another device located in **Netherlands**. If it's not you, close this page.

admin@M365x003354.onmicrosoft.com

[Can't access your account?](#)

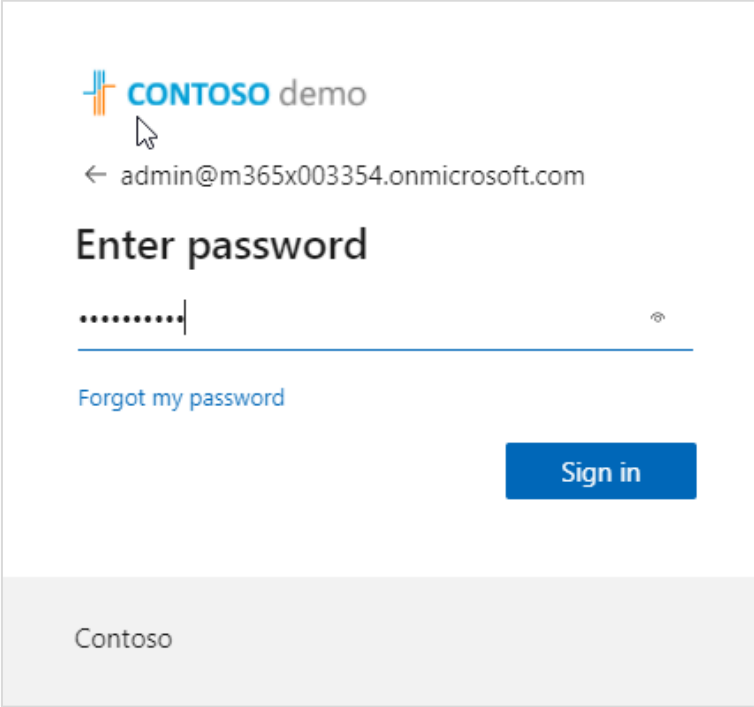
[Sign in with Windows Hello or a security key](#) ?

Back Next

 Sign-in options

5. Enter the domain administrator username and then click **Next**.

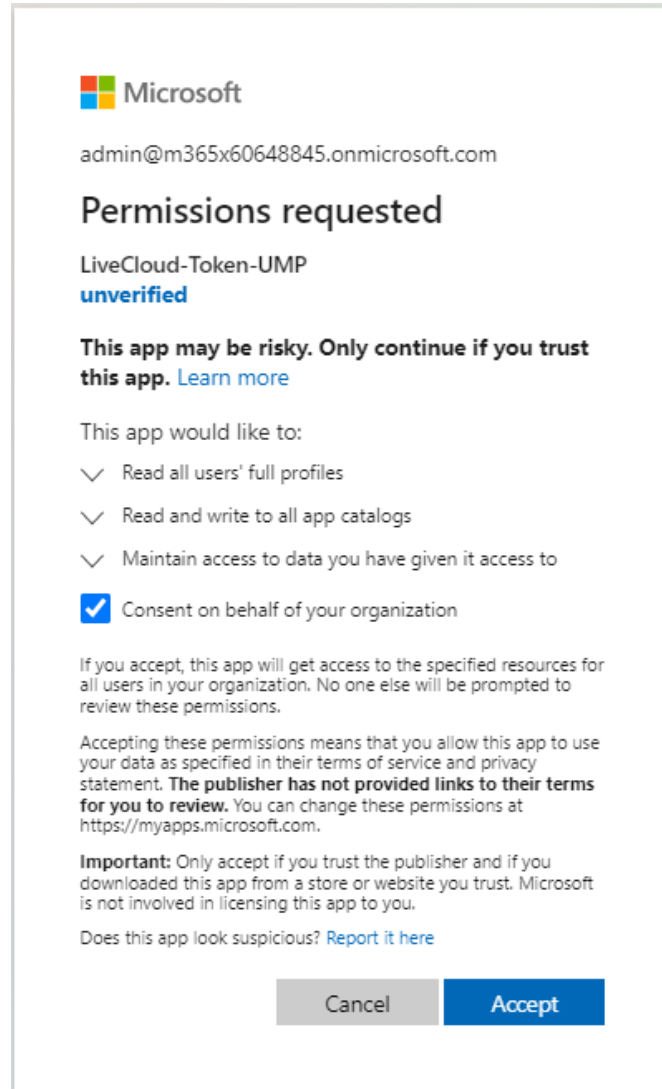
Figure 30-56: Enter Password



The screenshot shows a login interface for a 'CONTOSO demo' environment. At the top left is the Contoso logo. Below it, the email address 'admin@m365x003354.onmicrosoft.com' is displayed with a back arrow. The main heading is 'Enter password'. Below this is a password input field with a masked password '.....' and a visibility toggle icon. A blue link 'Forgot my password' is positioned below the input field. A blue 'Sign in' button is located to the right of the input field. At the bottom of the page, the word 'Contoso' is displayed in a light gray footer area.

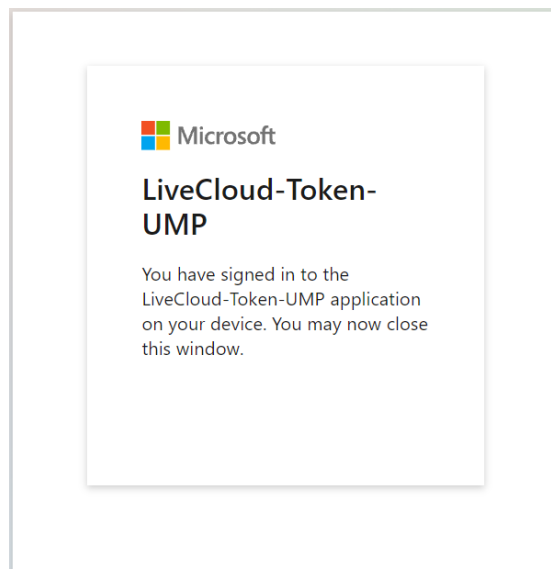
6. Enter the domain administrator password and then click **Sign in**.

Figure 30-57: Permissions Requested



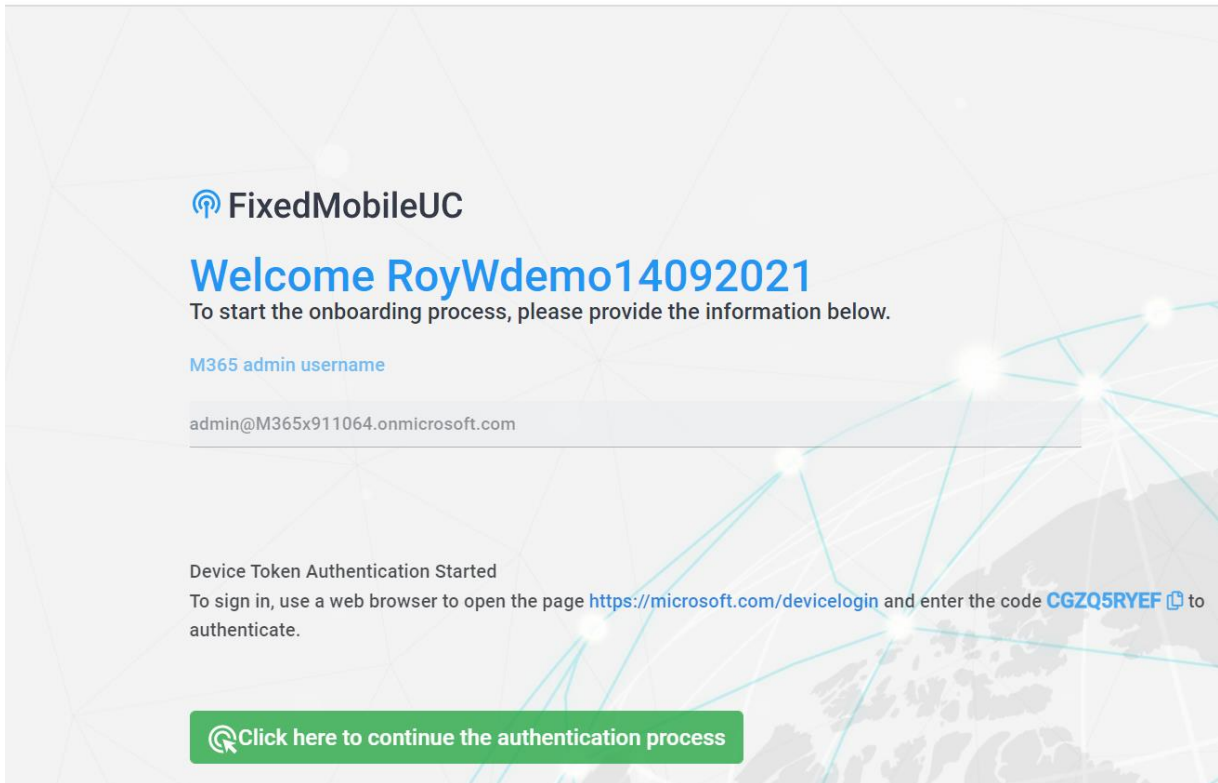
7. Select **Consent on behalf of your organization** check box and then click **Accept**.

Figure 30-58: Application Sign In



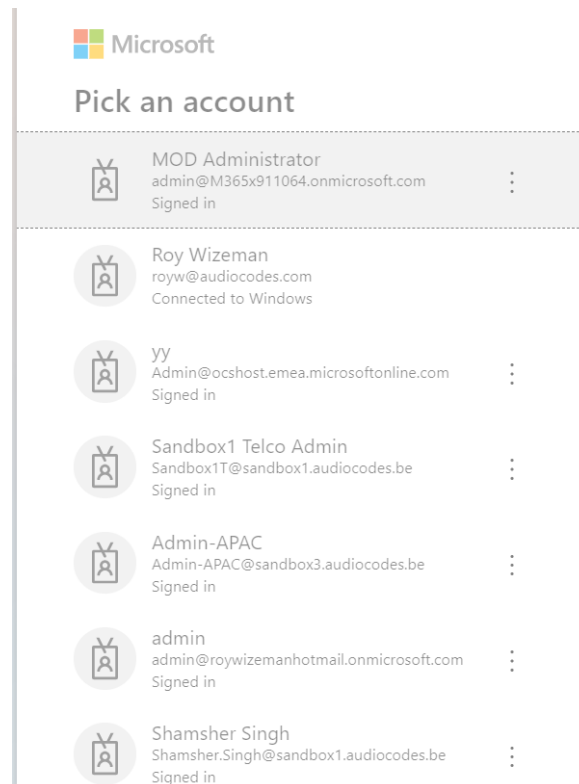
8. Close the Information window.

Figure 30-59: Welcome



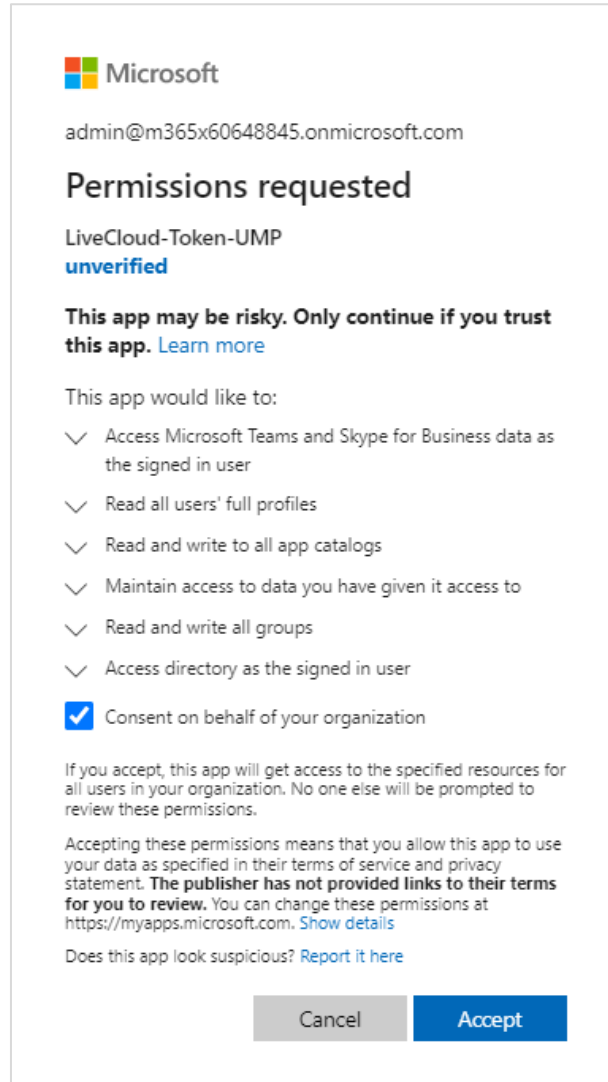
9. Click **Click here to continue the authentication process** link.

Figure 30-60: Pick an account



10. Re-login with the M365 Admin.

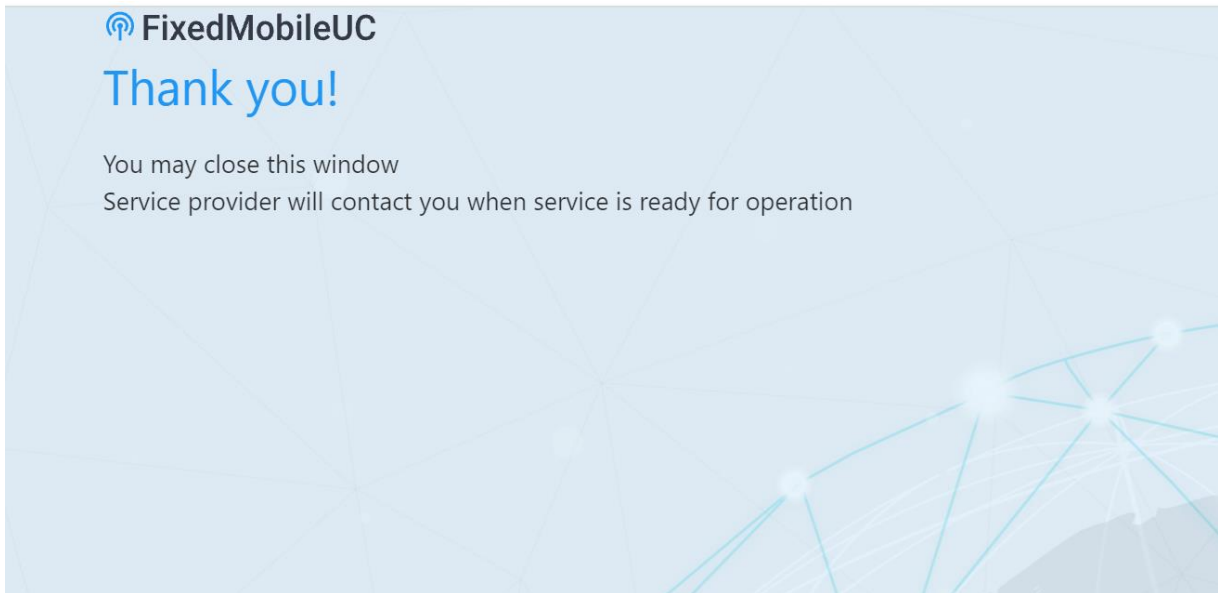
Figure 30-61: Permission requested



11. Select the **Consent on behalf of your organization** check box and then click **Accept**.

At the end of the process, the following screen is displayed informing the service provider domain administrator that AudioCodes Professional Services will complete the process.

Figure 30-62: Wizard Complete

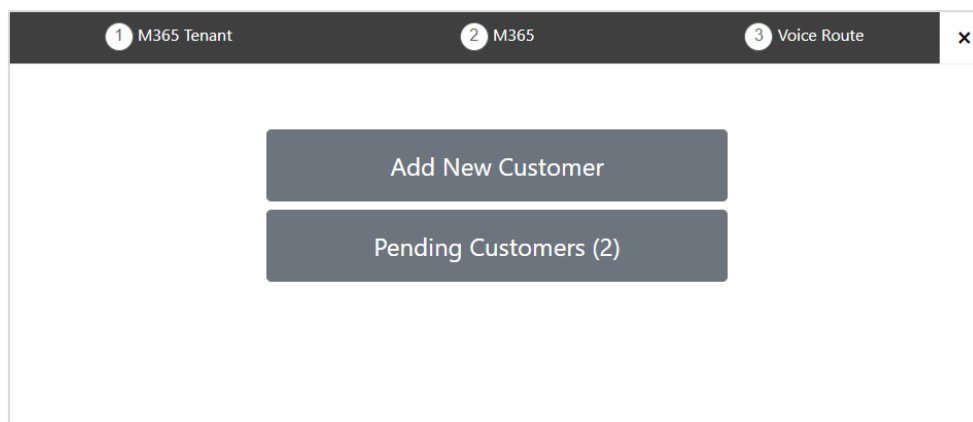


12. Click **Pending Customers** to monitor the process of the request. Once status “Authentication Complete” is displayed, you can proceed with the Add New Customer process (see Section 30.5.130).

Figure 30-63: Pending Customers

Customer ID	Status	Actions
BradDemo	Authentication Complete	Add Customer Revoke Request

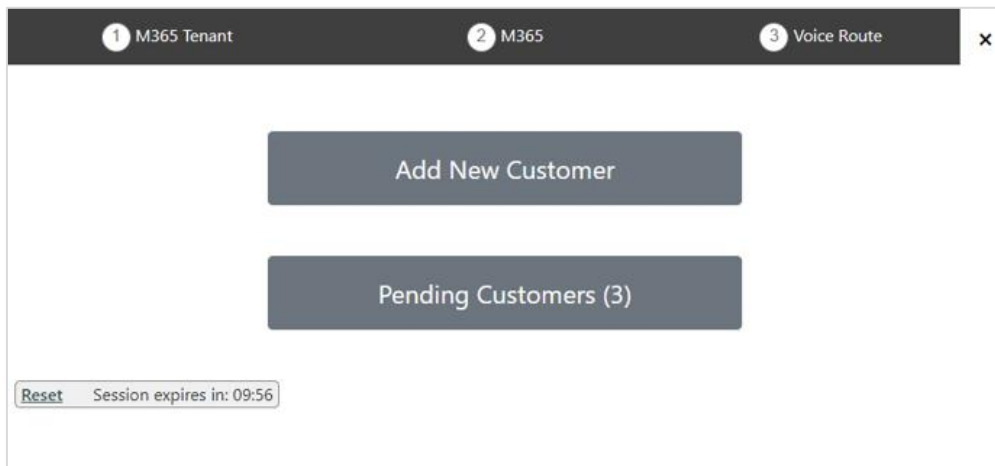
Figure 30-64: Add New Customer



30.5.1 Pending Requests

You can monitor the status of Pending Requests by clicking **Pending Customers**.

Figure 30-65: Pending Customers



A list of pending authentication requests is displayed:

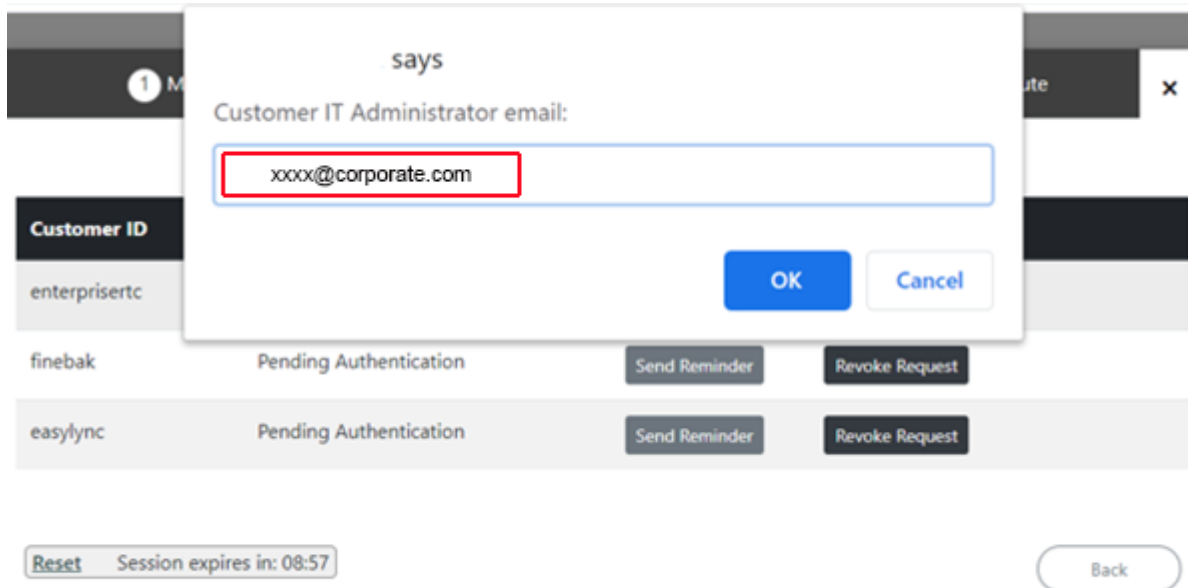
Figure 30-66: List of Pending Customers

Customer ID	Status	Actions
enterprisertc	Pending Authentication	Send Reminder Revoke Request
finebak	Pending Authentication	Send Reminder Revoke Request
easylnc	Pending Authentication	Send Reminder Revoke Request

You can perform one of the following actions:

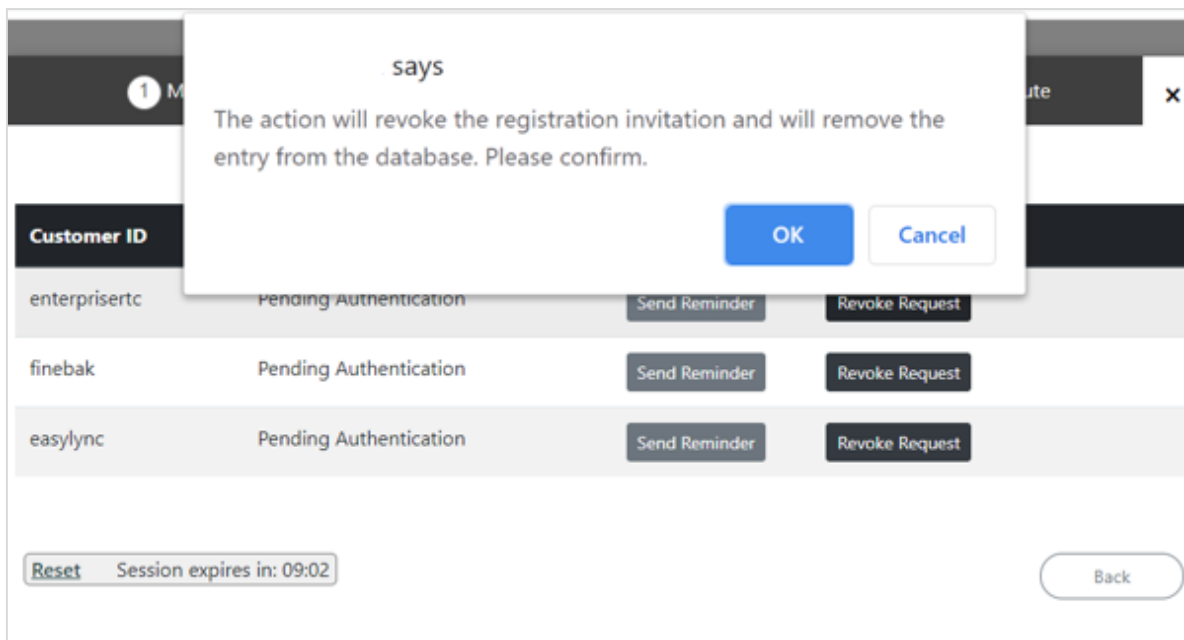
- **Send Reminder:** send a reminder to the customer IT administrator to approve the request. The windows will pop up with the email sent with the original request. The administrator can change the email address.

Figure 30-67: Send Customer Email



- **Revoke Request:** revoke the request sent to the customer IT administrator

Figure 30-68: Revoke Request



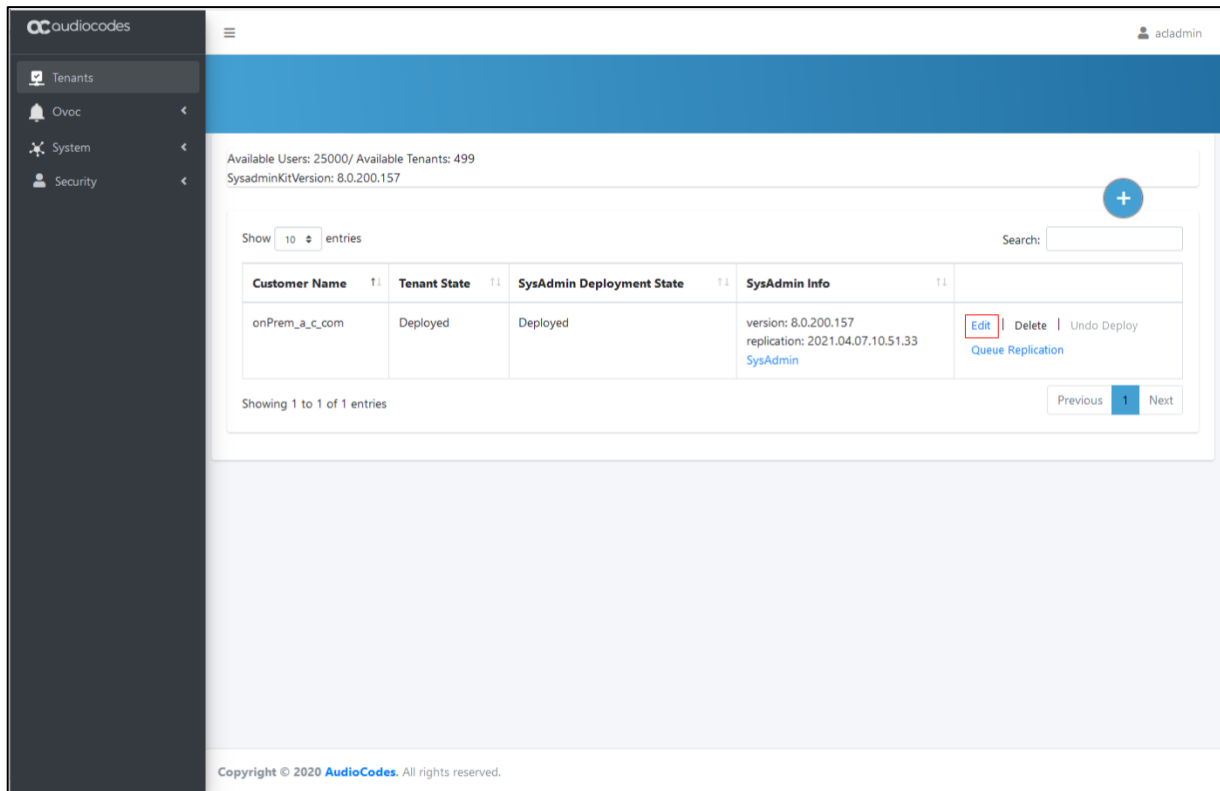
31 Managing Licensed Users

After a new customer is deployed, the number of licensed users to an SBC can be changed.

To manage the number of licensed users:

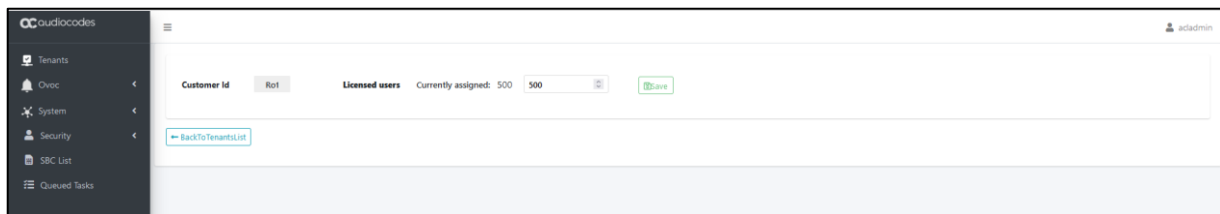
1. In the Main Tenant page Navigation page, select **Tenants**.


Figure 31-1: Tenant Details



2. Click **Edit** to edit customer details.
A page loads where these changes can be made.

Figure 31-2: Example Customer Edit



3. Set the desired number of licensed users.
4. Click  to apply changes.

Part VI

2nd Day Operations

32 Introduction

This section describes how to edit the M365 Tenant's configuration for second-day management. This interface allows you to do perform the following actions:

- Search for users
- Edit User MACD
- Assign Phone Number
- Users LifeCycle Management configuration
- Configure Online Routing
- Reserve M365 Tenant Phone Numbers
- Audit activities
- View queue for tasks status and results
- Update the Microsoft 365 Setting

The figure below displays the Provider Portal home page.

Figure 32-1: UMP 365 Home page - Provider Portal

User Type	Full Name	SIP Address	Line URI	Template	Department	Online Voice Ro...	Usage Locati...	enterprise vo...
TeamsOnly	qa	sipqa@ente...				Unrestricted	IL	No
TeamsOnly	Bogota	sipBogota@...	tel:+972397...	Sales		Unrestricted	IL	Yes
TeamsOnly	Rio De Janeiro	sipRio@ACL...	tel:+972397...	Executive		Unrestricted	IL	Yes
TeamsOnly	test	siptest@AC...				Unrestricted	IL	No
TeamsOnly	David Edri	sipdavid@...	tel:+972397...	ALL		Unrestricted	IL	No
TeamsOnly	Gadi Holdenbreger	sipadmin@...				Unrestricted	IL	No
TeamsOnly	admin demo	sipadmin@...				Unrestricted	IL	No

33 Provider Self-Service Portal

This chapter describes how to manage customers and users in the Providers portal. Access this portal by clicking the **SysAdmin** link under the desired tenant in the Tenants page.

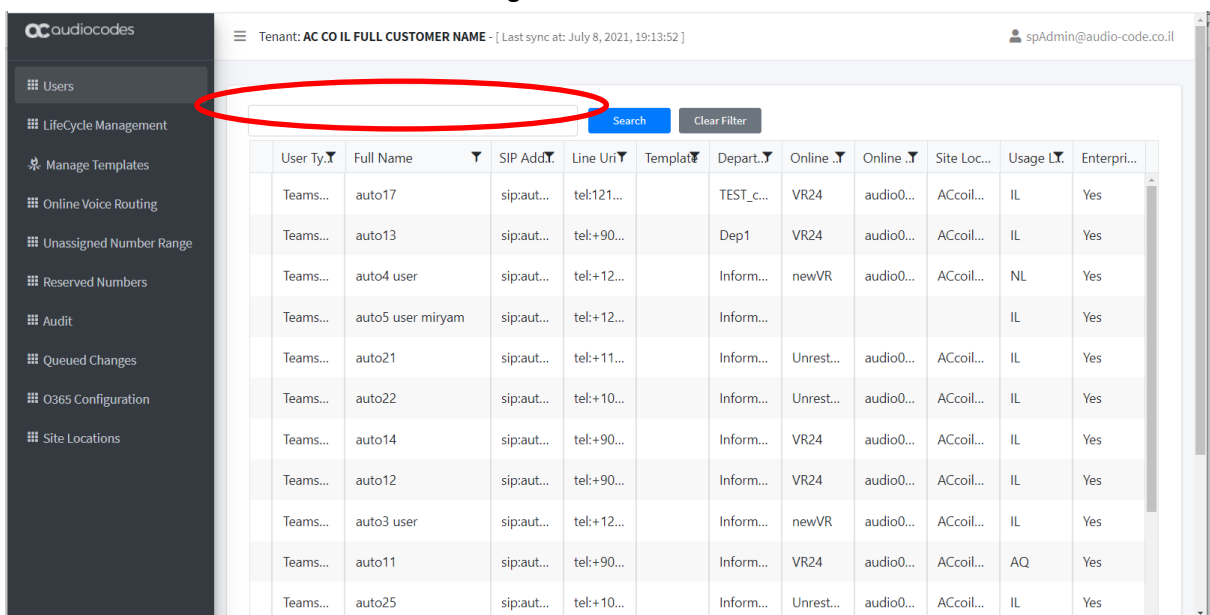
33.1 Editing User Policies

You can search for specific users to display their details in the screen and edit the assigned policies as part of Second day management. For example, change the assigned number range for the user or assign a different Online Voicerouting Policy. When a new customer is onboarded, a default Online Voicerouting Policy “Unrestricted” is created, you can later assign custom routing policies to users according to their site location (see Section 33.8.2).

To search for a user, do the following:

1. In the Home page (Users page) search field, select the user name or # of characters to search for a specific user.

Figure 33-1: Users List



The screenshot shows the 'Users List' page in the Provider Self-Service Portal. The page header includes the tenant name 'AC CO IL FULL CUSTOMER NAME' and the user 'spAdmin@audio-code.co.il'. A search bar is located at the top of the table, with a red oval highlighting it. The table contains the following data:

User Ty.	Full Name	SIP Add.	Line Uri	Templat	Depart.	Online	Online	Site Loc...	Usage L.	Enterpri...
Teams...	auto17	sip:aut...	tel:121...		TEST_c...	VR24	audio0...	ACcoil...	IL	Yes
Teams...	auto13	sip:aut...	tel:+90...		Dep1	VR24	audio0...	ACcoil...	IL	Yes
Teams...	auto4 user	sip:aut...	tel:+12...		Inform...	newVR	audio0...	ACcoil...	NL	Yes
Teams...	auto5 user miryam	sip:aut...	tel:+12...		Inform...				IL	Yes
Teams...	auto21	sip:aut...	tel:+11...		Inform...	Unrest...	audio0...	ACcoil...	IL	Yes
Teams...	auto22	sip:aut...	tel:+10...		Inform...	Unrest...	audio0...	ACcoil...	IL	Yes
Teams...	auto14	sip:aut...	tel:+90...		Inform...	VR24	audio0...	ACcoil...	IL	Yes
Teams...	auto12	sip:aut...	tel:+90...		Inform...	VR24	audio0...	ACcoil...	IL	Yes
Teams...	auto3 user	sip:aut...	tel:+12...		Inform...	newVR	audio0...	ACcoil...	IL	Yes
Teams...	auto11	sip:aut...	tel:+90...		Inform...	VR24	audio0...	ACcoil...	AQ	Yes
Teams...	auto25	sip:aut...	tel:+10...		Inform...	Unrest...	audio0...	ACcoil...	IL	Yes

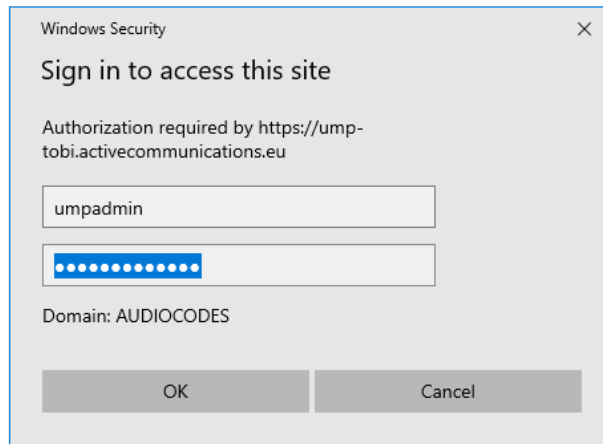
33.2 Grant Admin Permissions to Service Provider IT Administrator User

Once you have registered the application, you must grant permissions to a Service Provider IT administrator user to login to the Multitenant interface. The initial login should be performed by the local administrator of the server with the service account for this server. Once logged in, navigate to the relevant Service Provider tenant and choose any user to grant permissions as an administrator. This user administrator is then able to login to the tenant portal for this tenant.

To grant permissions to a user:

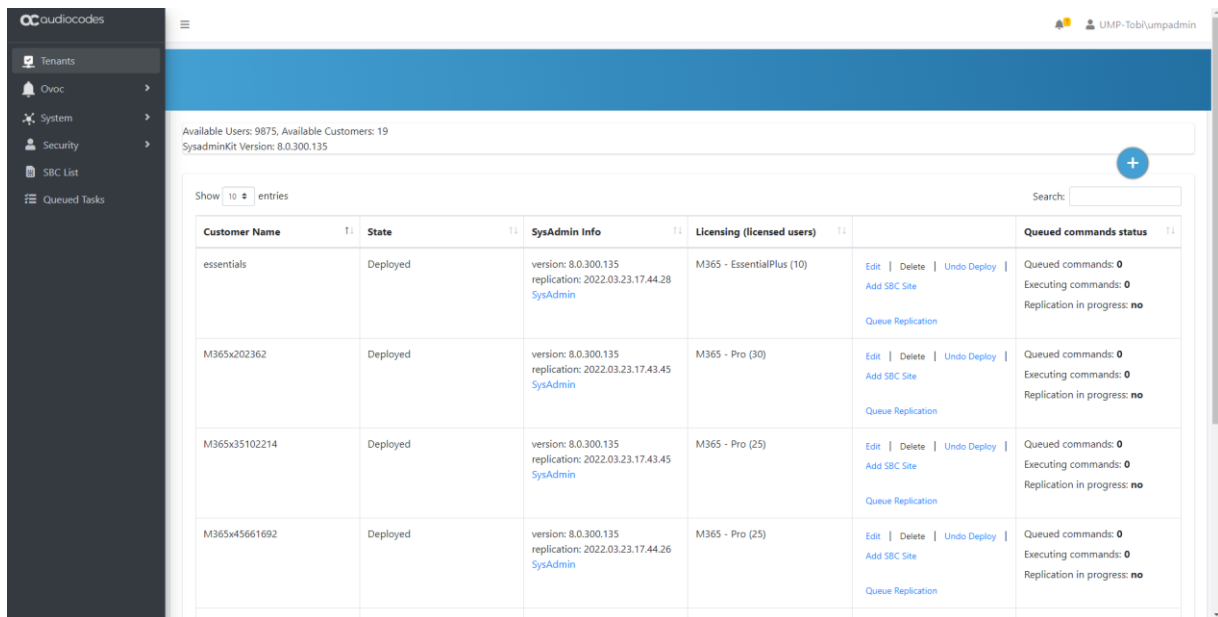
1. Login to the Multitenant portal with a Windows User account.

Figure 33-2: Multi-Tenant Access (Provider Only)



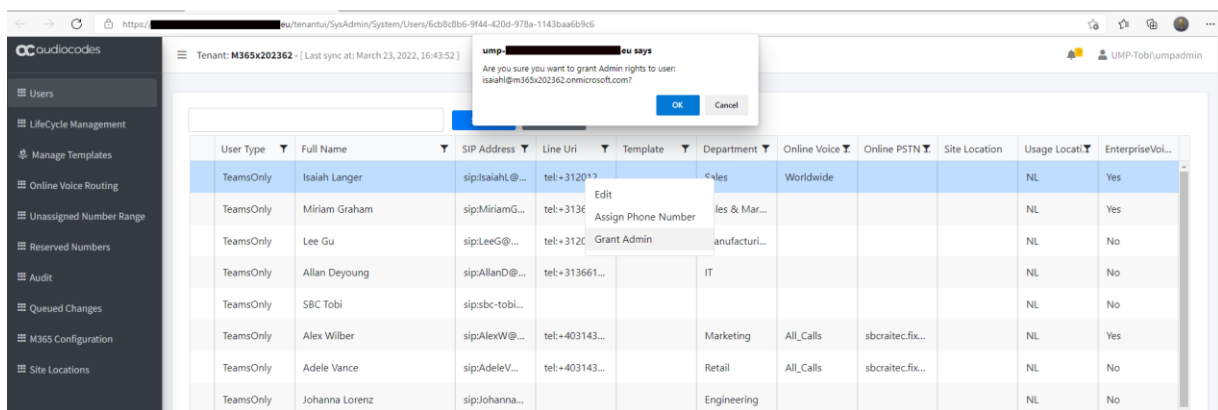
- In the Tenants screen, select the relevant customer.

Figure 33-3: Select Customer



- Select the desired user, right-click, select **Grant Admin**, and then click **OK**.

Figure 33-4: Grant Admin



A confirmation message is displayed.

Figure 33-5: Admin Rights Granted to User

User Type	Full Name	SIP Address	Line Uri	Template	Department	Online Voice	Online PSTN	Site Location	Usage Locati	EnterpriseVoL...
TeamsOnly	Isaiah Langer	sip:isaiahL@...	tel:+312012...		Sales	Worldwide			NL	Yes
TeamsOnly	Miriam Graham	sip:MiriamG@...	tel:+313661...		Sales & Mar...				NL	Yes
TeamsOnly	Lee Gu	sip:LeeG@...	tel:+312063...		Manufacturi...				NL	No
TeamsOnly	Allan Deyoung	sip:AllanD@...	tel:+313661...		IT				NL	No
TeamsOnly	SBC Tobl	sip:stbc-tobl...							NL	No
TeamsOnly	Alex Wilber	sip:AlexW@...	tel:+403143...		Marketing	All_Calls	sbcrattec.fix...		NL	Yes
TeamsOnly	Adele Vance	sip:AdeleV@...	tel:+403143...		Retail	All_Calls	sbcrattec.fix...		NL	No
TeamsOnly	Johanna Lorenz	sip:Johanna...			Engineering				NL	No
TeamsOnly	Nestor Wilke	sip:NestorW...	tel:+1000		Operations				NL	No
TeamsOnly	Debra Berger	sip:DebraB...	tel:+313661...		Executive M...				NL	No
TeamsOnly	Megan Bowen	sip:MeganB...	tel:+1002		Marketing				NL	No
TeamsOnly	MOD Administrator	sip:admin@...	tel:+313661...						NL	No

4. Open the Multitenant portal Customer Admins page (**Security > Customer Admins**). Notice the user to whom you granted Admin permissions is added to the list.

Figure 33-6: Customer Admins

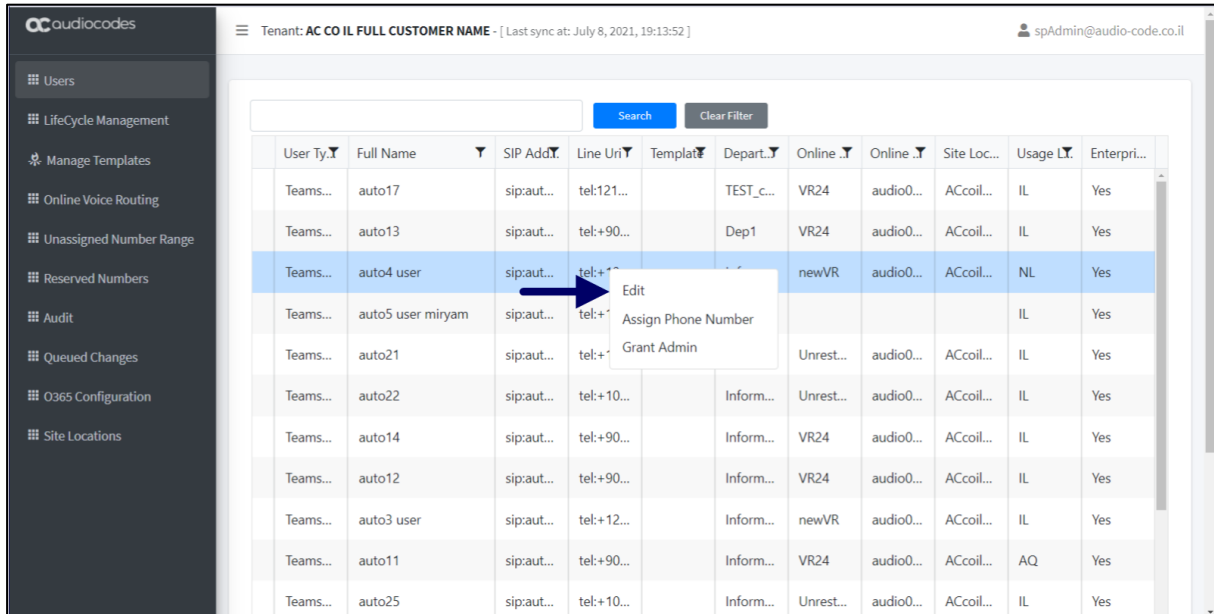
Id	Customerid	Account
64	M365x202362	AlexW@M365x202362.OnMicrosoft.com
66	essentials	admin@ocshost.emea.microsoftonline.com
67	M365x202362	isaiah@m365x202362.onmicrosoft.com

Showing 1 to 3 of 3 entries

33.3 Edit Users

1. You can select a user and right-click **Edit** to edit User Policies.

Figure 33-7: Edit a User



The figure below shows an example user policy.

Figure 33-8: Example User Policy

Edit sip:B1_User@ai-logics.com

General Pending changes Audit

Display name B1_User Enabled

First name B1_User

Last name Dirsync enabled

SIP address sip:B1_User@ai-logics.com

Manager Last sync timestamp 2021-11-03T13:40:35

Interpreted user type PureOnlineTeamsOnlyUser

Location City aaaaa Company bbbb

Policies Department 2222 Office cccc1

Telephony Postal code ffffff State or Province dddddd

Teams Street address gggggggg Usage location IL

Update Cancel


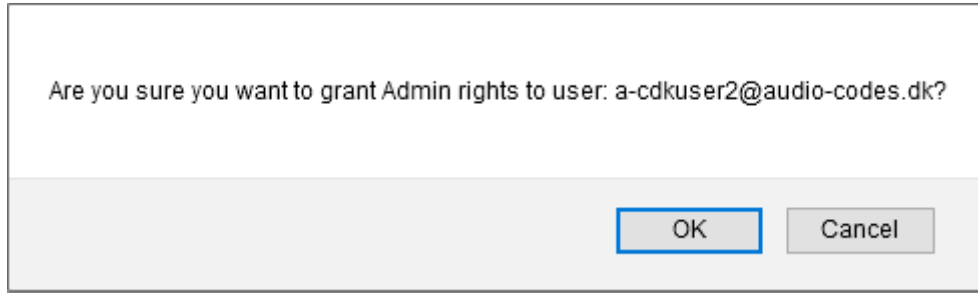
- Edit properties and click .
- Right-click and choose **Assign Phone Number** (see Section 'Assigning Phone Numbers' below).
- Right-click and choose **Grant/revoke Admin rights** to enable user as a third-party administrator (for multi-tier support).

Figure 33-9: Grant Admin Rights



33.4 Assigning Phone Numbers

You can manually assign phone numbers that you do not wish to be automatically assigned.

To assign a phone number:

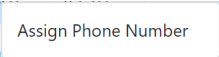
1. On the User view page, select a user and right click  to assign a phone number.

Figure 33-10: Assign Phone to Subscriber

2. Enter the phone number that you wish to assign to the user, and then click **OK**.
 - Phone number format – [tel:+xxxxxxx](#)
3. Set the OnlineVoiceRouting Policy (default: Unrestricted).

The Onboarding script creates the default policy “unrestricted”. You can assign a custom policy for the site location as described in Section 33.8.

Figure 33-11: Assign Phone Numbers

User	Full Name	SIP A	Line URI	Temp	Depa	Onlin	Onlin	Site L	Usag	Enter
Tea...	auto17	sip:a...	tel:1...		TEST...	VR24	audi...	ACc...	IL	Yes
Tea...	auto13	sip:a...	tel:+...		Dep1	VR24	audi...	ACc...	IL	Yes
Tea...	auto4 user	sip:a...	tel:+...		Infor...	new...	audi...	ACc...	NL	Yes
Tea...	auto5 user miry...	sip:a...	tel:+...		Infor...				IL	Yes
Tea...	auto21	sip:a...	tel:+...		Infor...	Unre...	audi...	ACc...	IL	Yes
Tea...	auto22	sip:a...	tel:+...		Infor...	Unre...	audi...	ACc...	IL	Yes
Tea...	auto14	sip:a...	tel:+...		Infor...	VR24	audi...	ACc...	IL	Yes
Tea...	auto12	sip:a...	tel:+...		Infor...	VR24	audi...	ACc...	IL	Yes
Tea...	auto3 user	sip:a...	tel:+...		Infor...	new...	audi...	ACc...	IL	Yes

33.5 Lifecycle Management

Lifecycle Management is a key element in the management of the M365 Tenants users. It allows automated user management based on Azure Active Directory Microsoft 365 security group membership. Users added to a security group will automatically be enabled for Microsoft Teams and will have policies and telephony settings like numbers applied based on the defined “persona” templates. Azure AD Security Group may represent a group of users on the M365 Tenants, as Site Members (HQ, Branch A unit or department where the template is tailored for the specific needs of the department or unit).

The lifecycle management feature is built upon three components, where it is critical to configure the components in the following order, because the completion of the configuration for each component is dependent on the previous one:

1. Configure unassigned number ranges, so numbers can be assigned to a template
2. Configure templates, holding policies and telephony settings
3. Configure lifecycle management and bind templates to security groups

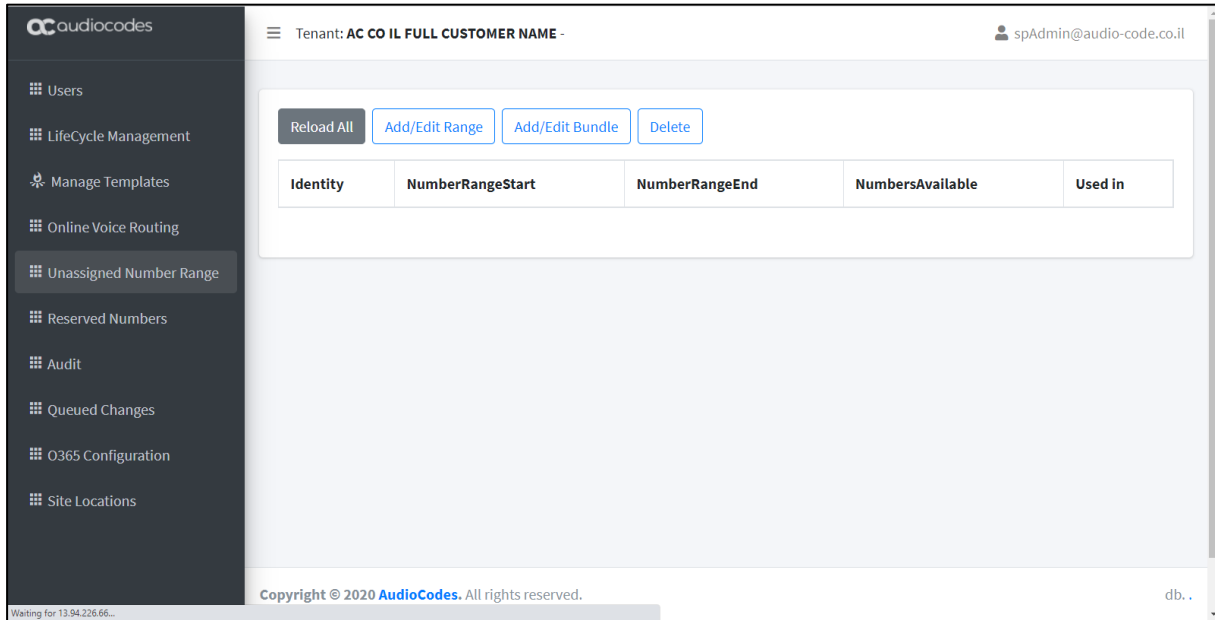
33.6 Managing Unassigned Number Ranges

The Unassigned Number Range allows a provider administrator to define ranges with numbers that belong to their Customer M365 Tenant and should be configured under **Unassigned Number Ranges**. Unassigned Number Ranges can be used in Lifecycle Management to automatically assign telephone numbers upon user creation. You can configure a range of phone numbers to be automatically assigned to a new user.

To configure an unassigned number range, do the following:

1. In the Navigation pane, select **Unassigned Number Range**.

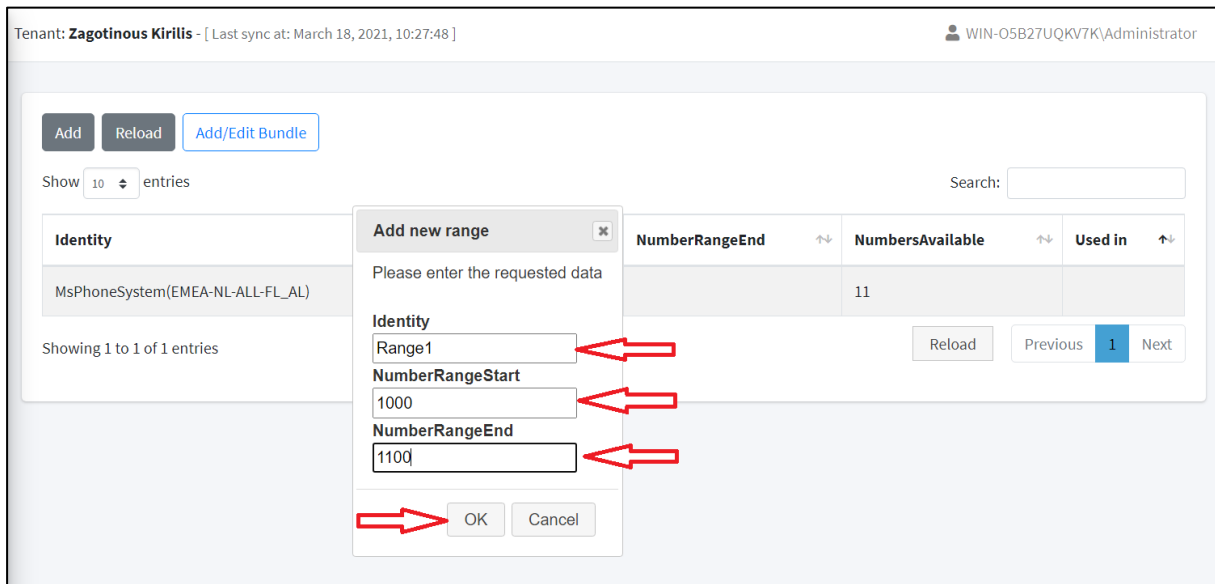
Figure 33-12: Unassigned Number Range



A dialog appears from where you can provide a number range name as well as set a limit of the desired phone numbers.

2. Click to add a new number range.

Figure 33-13: Number Range



3. Select the Identity Name and the DID Range.
 4. Click **OK**.
- The newly created number range should appear in the table below.

Figure 33-14: New Number Range

Tenant: **Zagotinous Kirilis** - [Last sync at: March 18, 2021, 10:27:48] WIN-O5B27UQKV7K\Administrator

Buttons: Add, Reload, Add/Edit Bundle

Show 10 entries Search:

Identity	NumberRangeStart	NumberRangeEnd	NumbersAvailable	Used in
MsPhoneSystem(EMEA-NL-ALL-FL_AL)			11	
Range1	1000	1100	101	

Showing 1 to 2 of 2 entries Reload Previous 1 Next

- Repeat the steps for creating another number range, fill required fields in popup with different values. At this point a bundle can be created whose content should be new created number ranges.

33.6.1 Creating a Bundle

To create a **Bundle** it is necessary to execute another action before creating it (the bundle), because a bundle cannot be created without content. Therefore the step that must be performed beforehand is the creation of **number ranges** that will represent the actual content of the bundle that we will create later. A bundle can contain one or more number ranges.

Figure 33-15: Add/Edit Bundle

Tenant: **Zagotinous Kirilis** - [Last sync at: March 18, 2021, 10:27:48] WIN-O5B27UQKV7K\Administrator

Buttons: Add, Reload, Add/Edit Bundle

Show 10 entries Search:

Identity	NumberRangeStart	NumberRangeEnd	NumbersAvailable	Used in
MsPhoneSystem(EMEA-NL-ALL-FL_AL)			11	
Range1	1000	1100	101	
Range2	1101	1200	100	

Showing 1 to 3 of 3 entries Reload Previous 1 Next

A new popup window will open from which it is necessary to fill in the **BundleName** field.



If you want the new **NumberRanges** to be part of a previously created bundle, it can be selected from the **SelectBundle** droplist – right side.

Figure 33-16: Select Bundle

The screenshot shows a form titled "Add/Edit DID Bundle". At the top, there is a "Bundle Name:" label followed by a text input field containing "Bundle One" and a dropdown menu with "select bundle" selected. A red box highlights the dropdown menu, and a red arrow points to the "Bundle Name:" label. Below this, the instruction "Select below the number ranges to combine" is displayed. There are two list boxes: "Available Ranges" containing "Range1" and "Range2", and "Selected Ranges" which is currently empty. Between these list boxes are two arrow buttons: a right-pointing arrow and a left-pointing arrow. At the bottom right of the form are "Save" and "Cancel" buttons.

Number ranges will already be displayed in the lower left in AvailableRanges window. Select the desired number range then click the right arrow button to move it to the Selected Ranges window. A number range cannot be moved if it is not selected first, also multiple selected ranges cannot be moved at the same time.

Figure 33-17: Add/Edit DID Bundle

This screenshot shows the same "Add/Edit DID Bundle" form. The "Bundle Name" field now contains "Bundle One". The "Available Ranges" list box has "Range1" highlighted in blue, with a red arrow pointing to it. The right-pointing arrow button between the list boxes is also highlighted with a red arrow. The "Selected Ranges" list box remains empty. The "Save" and "Cancel" buttons are still visible at the bottom right.

6. The selected number ranges should appear in **SelectedRanges** table in popup. Click **Save**.

Figure 33-18: Save Bundle

After clicking **Save** the window closes and the newly created bundle appears in the table on the **Unassigned Number Ranges** page. Notice that in the **Identity** column next to the bundle name, the number ranges names that are part of the new bundle are listed. Also the **NumbersAvailable** column in the table next to the new bundle is displayed including the total sum of the two number ranges that are part of the same bundle.

Figure 33-19: Bundle Details

Buttons: Add, Reload, Add/Edit Bundle

Show 10 entries Search:

Identity	NumberRangeStart	NumberRangeEnd	NumbersAvailable	Used in
Bundle One (Range1,Range2)			201	
MsPhoneSystem(EMEA-NL-ALL-FL_AL)			11	
Range1	1000	1100	101	
Range2	1101	1200	100	

Showing 1 to 4 of 4 entries

Buttons: Reload, Previous, 1, Next

Number list: tel:+1000, tel:+1001, tel:+1002, tel:+1003, tel:+1004, tel:+1005, tel:+1006, tel:+1007, tel:+1008, tel:+1009, tel:+1010, tel:+1011, tel:+1012, tel:+1013, tel:+1014, tel:+1015, tel:+1016, tel:+1017, tel:+1018, tel:+1019, tel:+1020, tel:+1021, tel:+1022, tel:+1023, tel:+1024



It is possible for one or more phone numbers to be part of both number ranges in the bundle. For example, if phone number counting of Number Range B starts from a phone number which is inside Number Range A. The bundle for which the two number ranges belong will still calculate the phone numbers as a sum of two number ranges. In this case, there is no phone number duplication; the bundle treats the phone number as if it exists in each number range even if the same phone number is common to both of these two number ranges (see example in figure below).

Figure 33-20: Number Overlap

Identity	NumberRangeStart	NumberRangeEnd	NumbersAvailable	Used in
Bundle One (Range1,Range2)			203	
MsPhoneSystem(EMEA-NL-ALL-FL_AL)			11	
Range1	1000	1100	101	
Range2	1099	1200	102	

Showing 1 to 4 of 4 entries

[tel:+1099](#) [tel:+1100](#) [tel:+1101](#) [tel:+1102](#) [tel:+1103](#) [tel:+1104](#) [tel:+1105](#)
[tel:+1106](#) [tel:+1107](#) [tel:+1108](#) [tel:+1109](#) [tel:+1110](#) [tel:+1111](#) [tel:+1112](#)
[tel:+1113](#) [tel:+1114](#) [tel:+1115](#) [tel:+1116](#) [tel:+1117](#) [tel:+1118](#) [tel:+1119](#)

33.6.2 Editing a Bundle

This section describes how to edit a bundle.

To edit a bundle:

1. In the table on the **Unassigned Number Ranges** page, select the desired bundle > right click > choose **Edit**.

A dialog similar to the one creating the bundle will open where you can add another number range, remove the number range from the bundle, change the name of the bundle. Complete the operation by clicking **Save**.

Figure 33-21: Editing a Bundle

Identity	NumberRangeStart	NumberRangeEnd	NumbersAvailable	Used in
Bundle One (Range1,Range2)			203	
MsPhoneSystem(EMEA-NL-ALL-FL_AL)			11	
Range1	1000	1100	101	
Range2	1099	1200	102	

Showing 1 to 4 of 4 entries 1 row selected

[tel:+1000](#) [tel:+1001](#) [tel:+1002](#) [tel:+1003](#) [tel:+1004](#) [tel:+1005](#) [tel:+1006](#) [tel:+1007](#)
[tel:+1008](#) [tel:+1009](#) [tel:+1010](#) [tel:+1011](#) [tel:+1012](#) [tel:+1013](#) [tel:+1014](#) [tel:+1015](#)
[tel:+1016](#) [tel:+1017](#) [tel:+1018](#) [tel:+1019](#) [tel:+1020](#) [tel:+1021](#) [tel:+1022](#) [tel:+1023](#)
[tel:+1024](#)

Figure 33-22: Bundle Edit Details

Add/Edit DID Bundle ✕

Bundle Name:

Select below the number ranges to combine

Available Ranges

→

←

Selected Ranges

Range1

Range2

Save Cancel

33.6.3 Deleting a Bundle

This section describes how to delete a bundle.

1. On the UnassignedNumberRanges page select the desired bundle > right click > choose Delete. A confirmation popup will open.
2. Click **OK** so that can be deleted or **Cancel** to abort the operation. After deleting the bundle it will no longer appear in the table on the **UnassignedNumberRanges** page.

Figure 33-23: Delete a Bundle

Add Reload Add/Edit Bundle

Search:

Show 10 entries

Identity	NumberRangeStart	NumberRangeEnd	NumbersAvailable	Used in
Bundle One (Range1,Range2)			203	
MsPhoneSystem(EMEA-NL-NL-FL-AL)			11	
Range1	1000	1100	101	
Range2	1099	1200	102	

Showing 1 to 4 of 4 entries 1 row selected

Reload Previous 1 Next

tel:+1000 tel:+1001 tel:+1002 tel:+1003 tel:+1004 tel:+1005 tel:+1006 tel:+1007

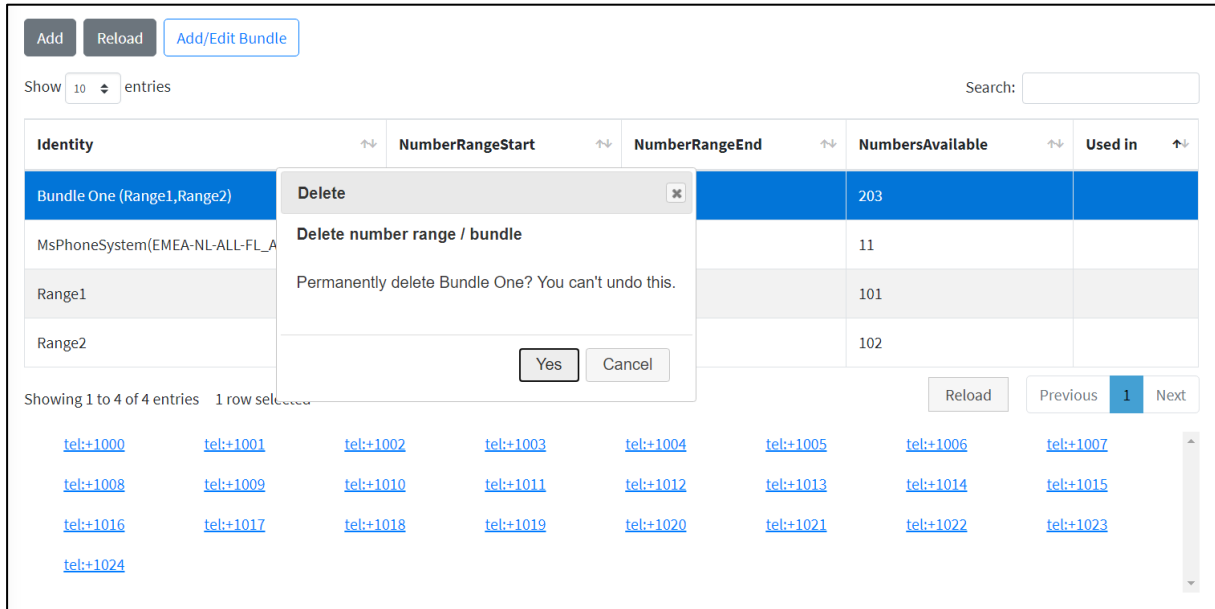
tel:+1008 tel:+1009 tel:+1010 tel:+1011 tel:+1012 tel:+1013 tel:+1014 tel:+1015

tel:+1016 tel:+1017 tel:+1018 tel:+1019 tel:+1020 tel:+1021 tel:+1022 tel:+1023

tel:+1024

3. You are prompted whether you wish to delete the number range/bundle.

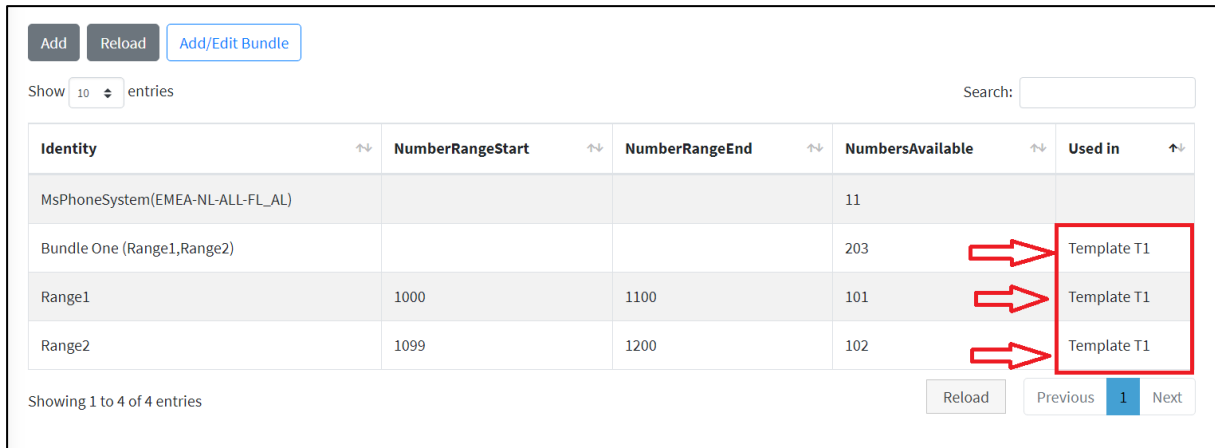
Figure 33-24: Delete the Number Range



33.6.3.1 Troubleshooting

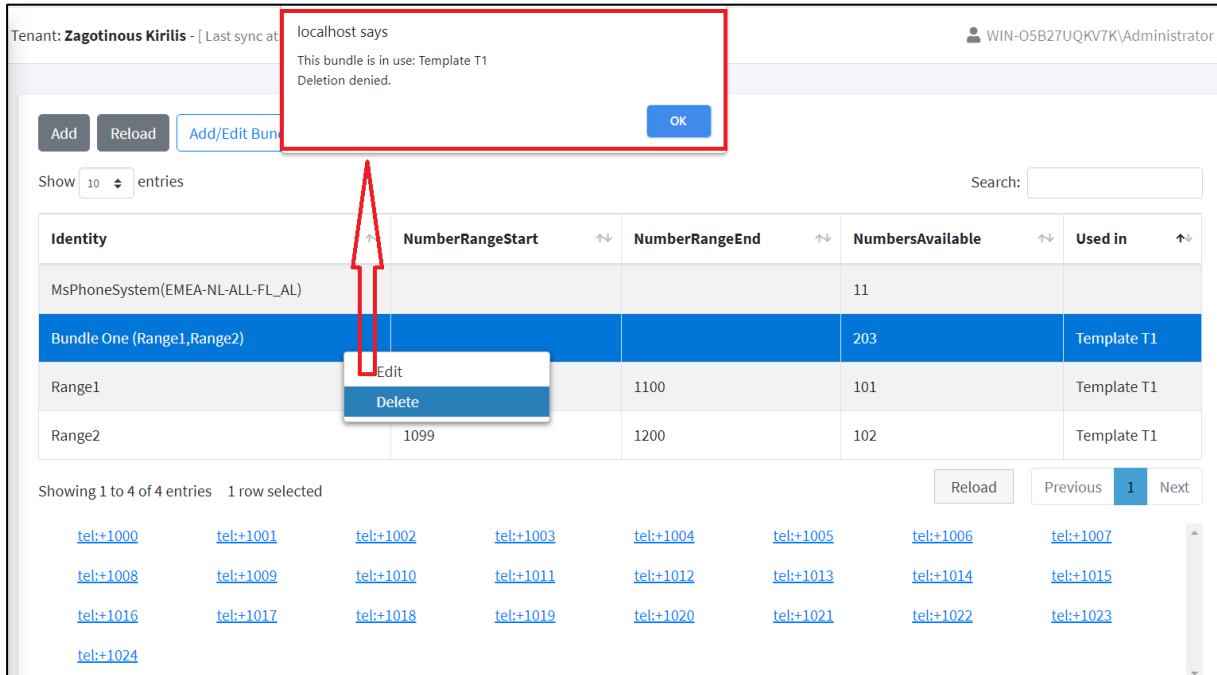
There is a possibility that a bundle is assigned a **Template** from the Template Manager and then automatically the same template is assigned to those number ranges that are part of that bundle. Assigned template appears in the table on the **UnsignedNumberRanges** page next to the bundle and the number ranges in **UsedIn** column.

Figure 33-25: Delete Warning Message



In this case a bundle cannot be deleted by the simple method mentioned above, a denial **warning message** will be displayed when attempting to delete.

Figure 33-26: Bundle is in Use – Deletion Denied



To resolve this issue, firstly its necessary to delete the template wich is assigned to the bundle from the Template Manager, then the bundle can be deleted as described above.

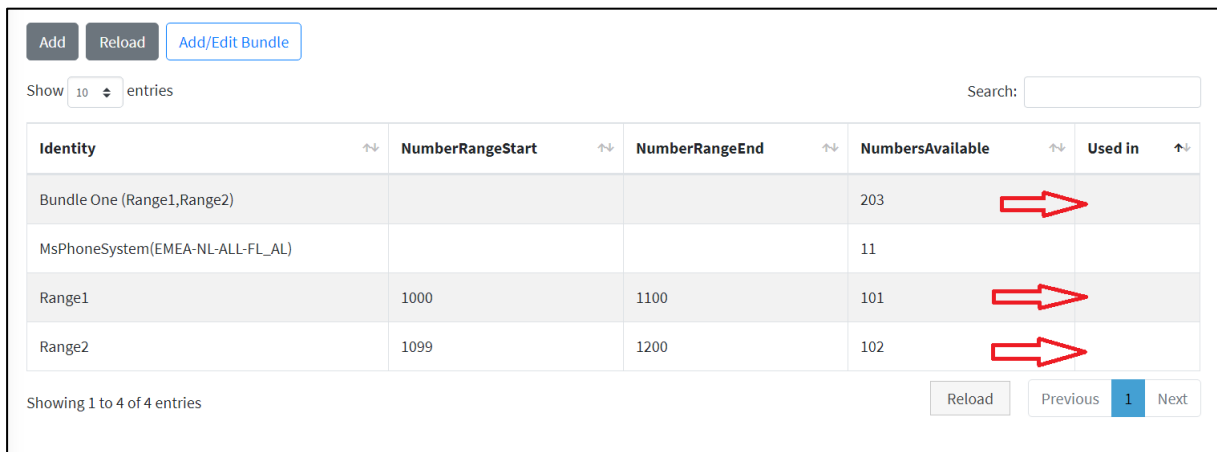
To delete the template assigned to a bundle:

- Click **ManageTemplate**, select the template name from the drop-down list > click **Delete** > click **Yes** in popup for confirmation.

Note that the “Used In” column indicates for which templates the bundles are assigned.

After deleting the template assigned to the bundle, the template name will no longer appear next to the bundle or number ranges in table from **UnassignedNumberRange** page.

Figure 33-27: Bundle Successfully Deleted



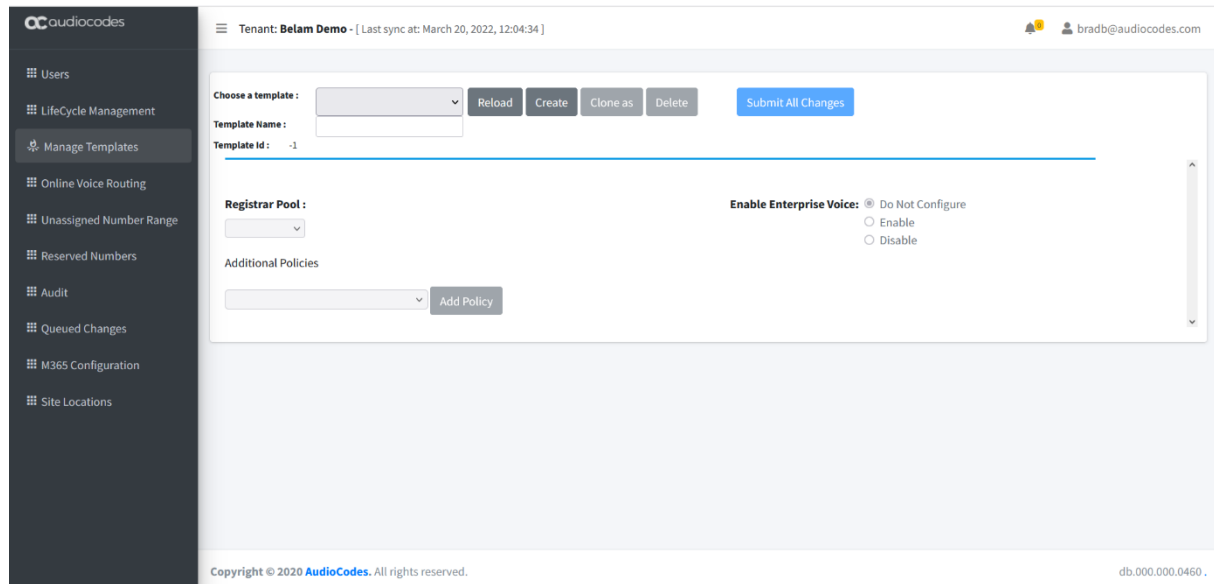
33.7 Managing Templates

Templates are created under **Manage Templates** and are assigned to Azure AD security groups in Lifecycle management to automate policies and number assignment for users.

To manage templates:

1. In the Navigation pane, select **Manage Templates**.

Figure 33-28: Manage Templates



To create a new template, do the following:

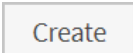
1. From the template drop-down list, select . A new template is created with a random number (like New-Template).
2. In the Selected Template box, enter the desired name.

Figure 33-29: New Template

The screenshot shows a dialog box titled 'Enter new data' with a close button (X). The text inside says 'Please enter the requested data'. Below this is a label 'Template Name' followed by an empty text input field. At the bottom of the dialog are two buttons: 'OK' and 'Cancel'.

3. Complete the Policy and Telephony settings section, and then select the policies you want to assign.
4. From the Additional Policies drop-down list, select the desired Teams Policies, and then click




Figure 33-30: Add Policy

The screenshot shows a list of policy templates in a scrollable area. The templates listed are: Cloudmeeting, Conferencing, Externalaccess, Externalusercommunication, Graph, Iphone, Mobility, Onlinedialinconferencing, Onlinevoicemail, Onlinevoiceroutingpolicy, Presence, Teamscalling, Teamsmeeting, Teamsmeetingbroadcast, Teamsmessaging, Teamsupgrade, and Teamsvideointeropservice. Below the list is an 'Add Policy' button. A date 't: April 25, 2020, 1' is visible in the top right corner of the interface.

5. Select the Policy Value for the selected policies.

Figure 33-31: Set Policy Value

The screenshot shows the 'Set Policy Value' configuration page. At the top, there is a 'Choose a template:' section with a dropdown menu set to 'All Users' and buttons for 'Reload', 'Create', 'Clone as', and 'Delete'. Below this, the 'Template Name:' is 'All Users' and the 'Template Id:' is '4'. The 'Registrar Pool:' is set to 'Office365'. Under 'Additional Policies', the 'Teamsmeeting Policy:' dropdown is open, showing a list of options: Choose, Global, AllOff, AllOn, Default, General, Kiosk, RestrictedAnonymousAccess, RestrictedAnonymousNoRecording, SalesMarketing, Tech support, and Training. A 'del' button is next to the selected policy value.

- Select Telephony setting template. You must select the **Enable Enterprise Voice** option to enable Phone System in Microsoft 365 voice services. When configuring the Customer M365 Tenant voice in a template, a telephone number can automatically be assigned on user creation; a choice can be made from a selection of source numbers as follows:

Figure 33-32: Set Telephony Setting

Enable Enterprise Voice :

DialPlan : Local ▼

Assign Number from : ▼

NumberRange : -- Select Number Source --

NumberRange details : Phone

Use Extensions : Home

Number Of Digits : Mobile

NumberRange

Ipphone

- When you have completed the configuration, click .



When **Phone** is selected as source, the Azure Active Directory Phone number will be applied. If this number is changed within Azure Active Directory, it will also be used as the new telephone number for Teams. Telephone numbers other than **Phone** are only assigned during the automatic creation of the user and unlike policies are not enforced / changed during the lifecycle scheduled policy replication.

For Additional Templates Management:

- Click to reload an existing template.
- Click to clone an existing template.
- Click to delete an existing template.

33.7.1 Importing Bulk Templates from a File

You can import a template list of user URI entries from an external CSV file.

To import a bulk template from a CSV file:

- From the template drop-down list, choose a template to import.

Figure 33-33: Choose Template

Tenant: **Belam Demo** - [Last sync at: March 20, 2022, 12:04:34] bradb@audiocodes.com

Choose a template: bulkupload Reload Create Clone as Delete Submit All Changes

Template Name: bulkupload

Template id: -1

Registrar Pool: Office365

Additional Policies: Add Policy

Enable Enterprise Voice: Do Not Configure Enable Disable

Copyright © 2020 AudioCodes. All rights reserved. db.000.000.0460.

Figure 33-34: Import File

Tenant: **Belam Demo** - [Last sync at: March 20, 2022, 12:04:34] bradb@audiocodes.com

Choose a template: bulkupload Reload Create Clone as Delete Submit All Changes Import File >

Template Name: bulkupload

Template id: 1

Registrar Pool: Office365

Additional Policies: Add Policy

Enable Enterprise Voice: Enable Do Not Configure Disable

Clear Line URI:

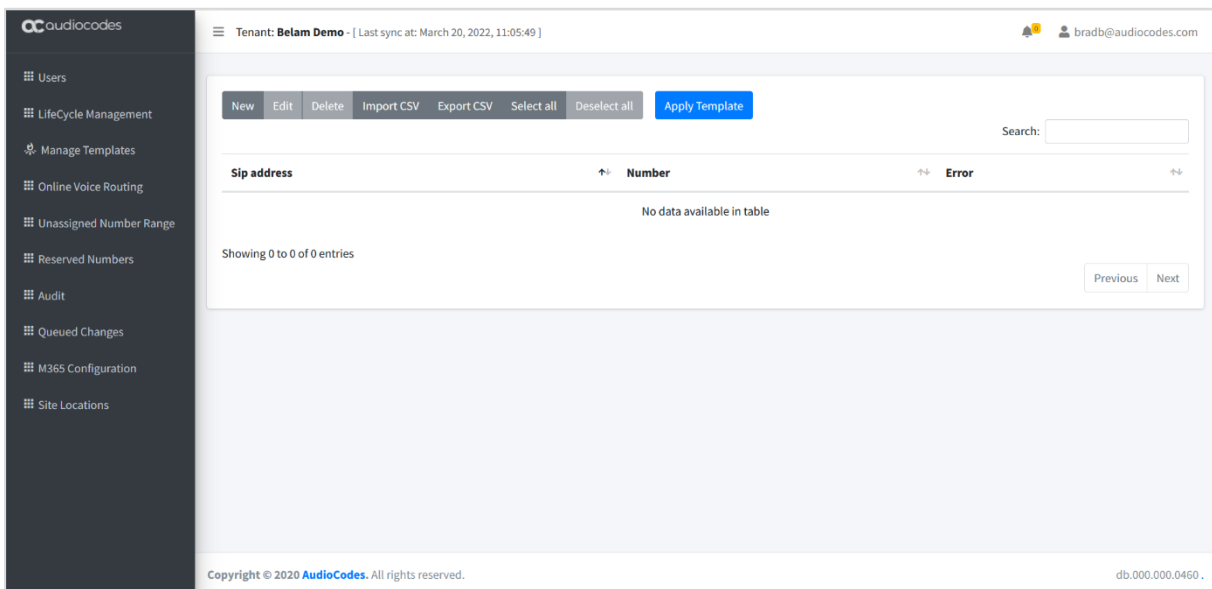
Assign Number from: File

Submit policy changes, then proceed to "Import File"

Copyright © 2020 AudioCodes. All rights reserved. db.000.000.0460.

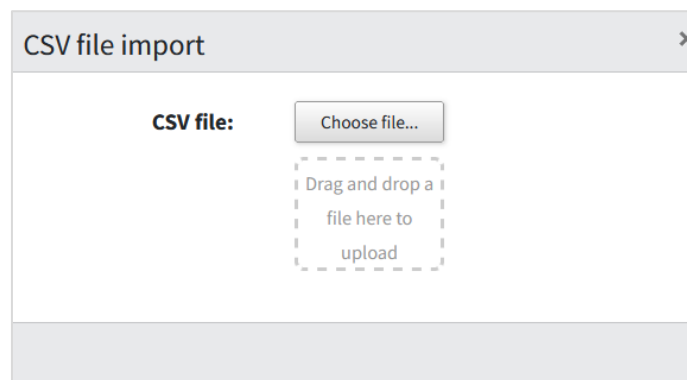
2. Click Import File > to import a template file.

Figure 33-35: Import File



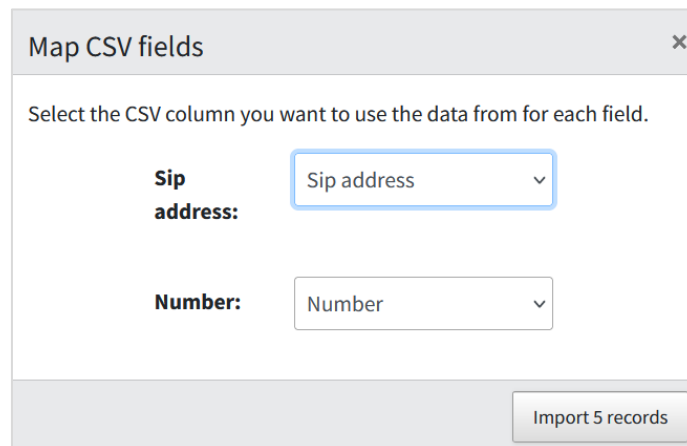
3. Click **Import CSV**. The Import file dialog is displayed.

Figure 33-36: CSV File import



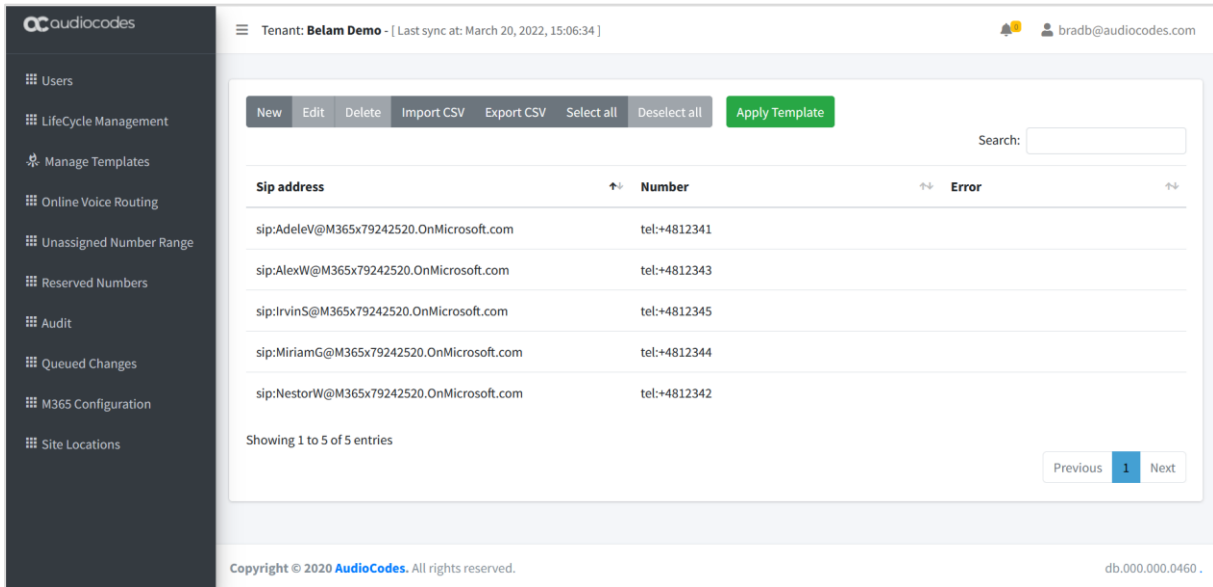
4. Choose a file to import.

Figure 33-37: Map CSV fields



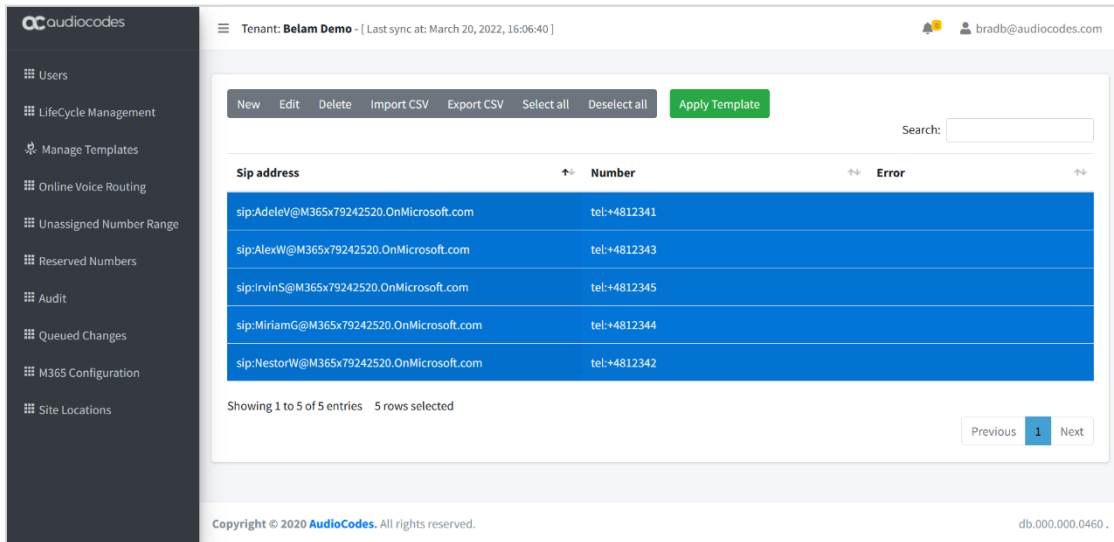
5. Optionally select the CSV column to apply to the SIP address and Number fields.
6. Select **Import <number of records> records**.

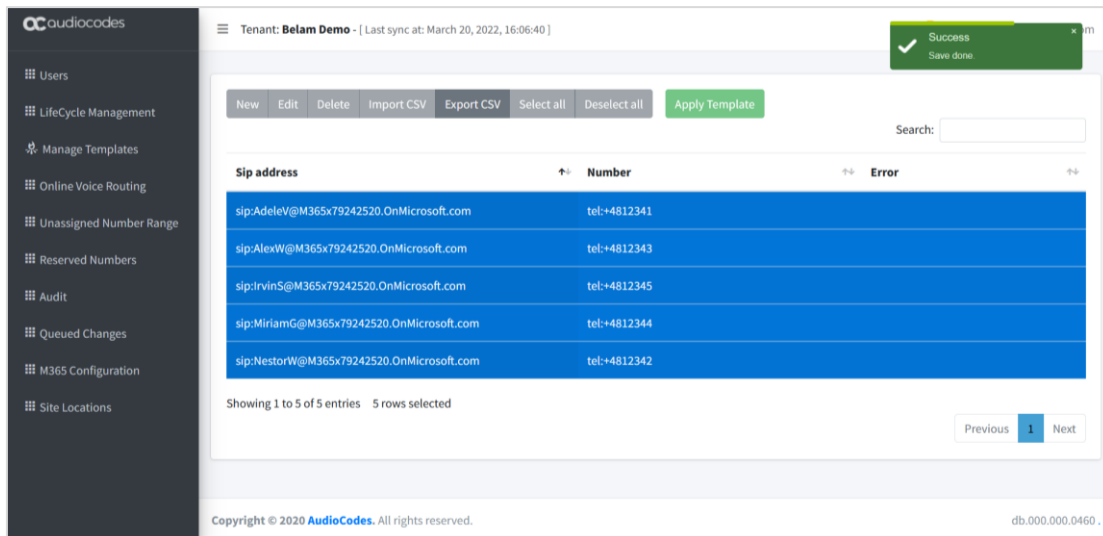
Figure 33-38: Imported Records



7. Select all records and then click **Apply Template**.

Figure 33-39: Selected Entries





The screenshot shows the AudioCodes Provider Self-Service Portal interface. The left sidebar contains navigation options: Users, LifeCycle Management, Manage Templates, Online Voice Routing, Unassigned Number Range, Reserved Numbers, Audit, Queued Changes, M365 Configuration, and Site Locations. The main content area displays a table of SIP entries for tenant 'Belam Demo' (last sync: March 20, 2022, 16:06:40). A success message 'Success Save done' is visible in the top right. The table has columns for 'Sip address', 'Number', and 'Error'. Five entries are listed, all selected. A search bar and pagination controls are also present.

Sip address	Number	Error
sip:AdeleV@M365x79242520.OnMicrosoft.com	tel:+4812341	
sip:AlexW@M365x79242520.OnMicrosoft.com	tel:+4812343	
sip:IrvinS@M365x79242520.OnMicrosoft.com	tel:+4812345	
sip:MiriamG@M365x79242520.OnMicrosoft.com	tel:+4812344	
sip:NestorW@M365x79242520.OnMicrosoft.com	tel:+4812342	

Showing 1 to 5 of 5 entries 5 rows selected

Copyright © 2020 AudioCodes. All rights reserved. db.000.000.0460.

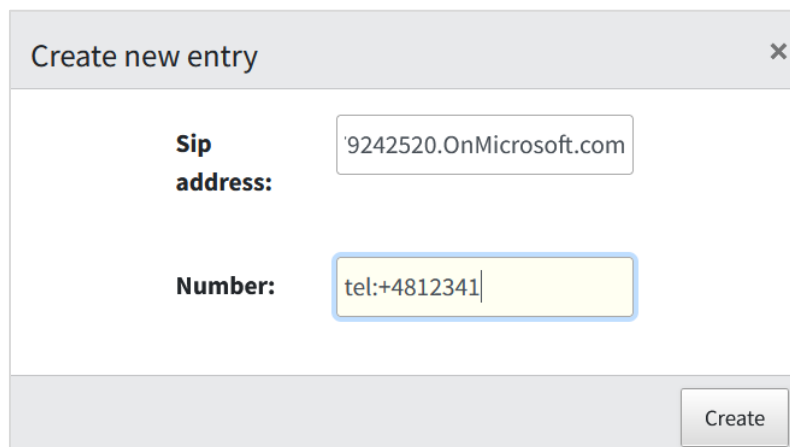
33.7.2 Create New Entry Manually

You can create a new template entry manually.

To create a new entry:

1. Click **New**.

Figure 33-40: Create new entry



The 'Create new entry' dialog box contains two input fields. The 'Sip address' field contains '9242520.OnMicrosoft.com' and the 'Number' field contains 'tel:+4812341'. A 'Create' button is located at the bottom right of the dialog.

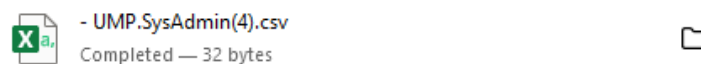
2. Enter the user SIP URI and telephone and then click **Create**.

33.7.3 Export CSV

You can export a CSV file containing a list of entries.

- Click **Export CSV**.

Figure 33-41: Export CSV



33.7.4 Binding Templates to Security Groups

This section describes how to assign templates to Security Groups.

To assign templates to security groups, do the following:

1. In the Navigation pane, select **Lifecycle Management**. A list of the assignments of templates to security groups is displayed.

Figure 33-42: Life Cycle Management

The screenshot shows the 'Life Cycle Management' interface for tenant 'ac_cloud'. It features a table with the following data:

Rank	Replication Template	Security Group	Error
1	TempleRun	SG_Auto11-20	
2	t1	SG_Auto11-20	
3	t2	user24_1	

Below the table, it indicates 'Showing 1 to 3 of 3 entries' and '1 row selected'. A note states: 'Templates are processed by priority, the lowest rank index has the highest priority.'

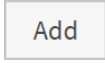
2. Click  to assign a Template to a Security Group.

Figure 33-43: Binding Template to AAD Security Group

The 'Add new' pop-up window contains the following fields and controls:

- Security Group (min 1 char):** A multi-select field containing 'group102', 'group103', 'group104', and 'group105'.
- Template:** A dropdown menu with 't1' selected.
- Buttons:** 'Close' and 'Save' buttons at the bottom right.

3. In the pop-up window, select one or more Security Groups and select a Security Template to be applied to them. If multiple Security Groups are selected, the template will only be assigned to group members that belong to all security groups (A logical AND function is performed on all groups specified).

4. Click .

Figure 33-44: New Binding

Tenant: **ac_cloud** - [Last sync at: April 4, 2021, 11:56:45] Alice Smith

Add

Show 10 entries Search:

Rank	Replication Template	Security Group	Error
1	TempleRun	SG_Auto11-20	
2	t1	SG_Auto11-20	
3	t2	user24_1	
4	t1	group102,group103,group104,group105	

Showing 1 to 4 of 4 entries
Templates are processed by priority, the lowest rank index has the highest priority.

Previous **1** Next

Copyright © 2020 AudioCodes. All rights reserved. db.000.000.0387

- The new binding with the replication template assigned to multiple security groups is assigned Rank “4” in the figure above. Select the new entry and then use the arrow key adjacent to ‘Rank’ to move the new binding to a higher rank.



If a user is a member of multiple security groups in the list, the template assigned to the group with the lowest rank (listed on top in the list) will prevail over the others.

33.8 Configuring Online Voice Routing

- In the Navigation pane, select **Online Voice Routing**.

Dial Plans **Normalization Rule Templates** PSTN Gateways PSTN Usage Voice Routes Voice Routing Policies

Add New Normalization Rule

Name	Description	Pattern	Translation	IsInternalExtension
test	test	^+31(653707180\d(-3\d+))\$	123\$1	false
test2	test2	^+3136123(\d(1\d+))\$	2222\$1	false

The Online Voice Routing screen allows a provider administrator to use a Web GUI interface to define their Customer M365 Tenant Voice Routing, including the following policies:

- PSTN Usage (see Section 33.8.1)

- Voice Routing Policies (see Section 33.8.2)
- Voice Route (see Section 33.8.3)
- PSTN Gateways (see Section 33.8.4)
- Normalization Rule Template (see Section 33.8.5)
- Dial Plan (see Section 33.8.5)



- A PSTN Gateway is not required on the customer tenant; instead, only the derived trunk FQDN must be added to the voice routing policies of the users.
- As part of the onboarding process of a customer M365 Tenant, the solution creates a new Online Voice Routing (Default name 'Unrestricted' however this can change per provider).

33.8.1 PSTN Usage

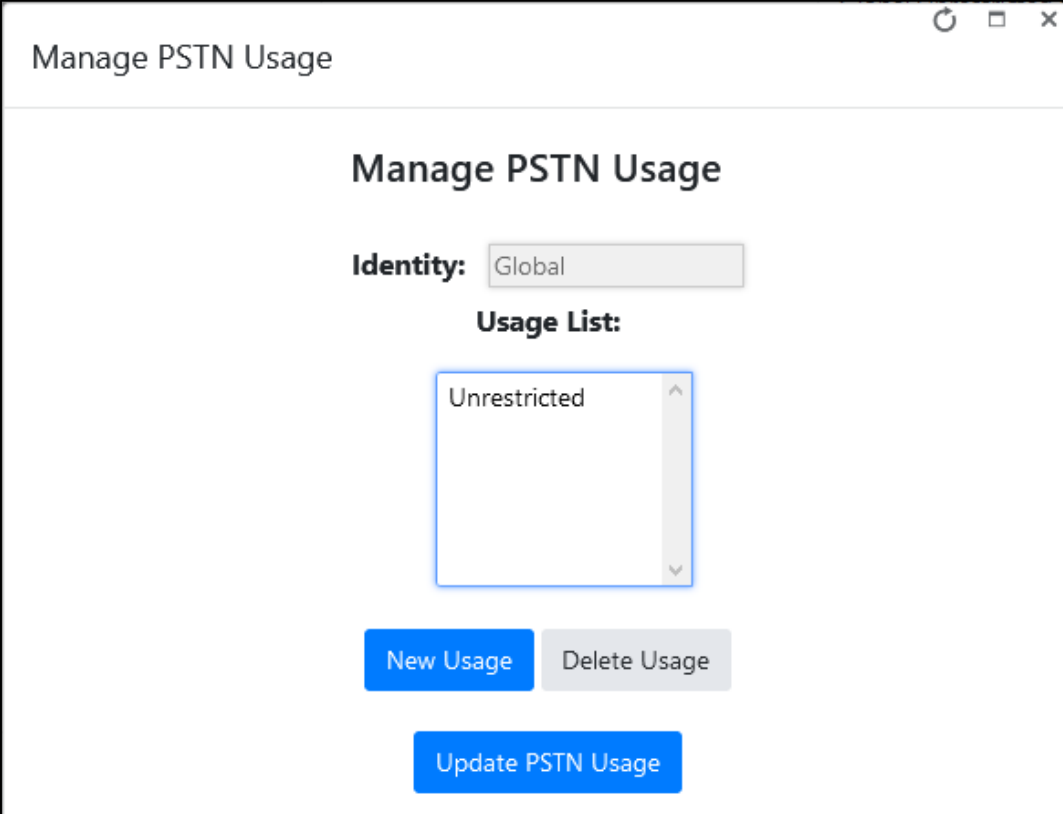
A container for voice routes and PSTN usages can be shared in different voice routing policies.

Figure 33-45: PSTN Usage

Identity	Routes	Policies	Last Replication
AT			
Unrestricted	Unrestricted		
TestUsage			

- Select the **Manage Pstn Usage** button to manage the PSTN Usage (Add/Edit/Delete).

Figure 33-46: PSTN Usage



Manage PSTN Usage

Identity: Global

Usage List:

- Unrestricted

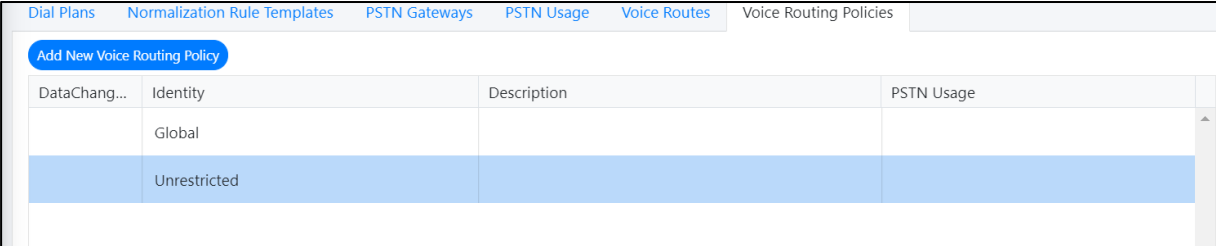
New Usage Delete Usage

Update PSTN Usage

33.8.2 Voice Routing Policy

A container for PSTN Usages can be assigned to a user or to multiple users.

Figure 33-47: Voice Routing Policy



DataChang...	Identity	Description	PSTN Usage
	Global		
	Unrestricted		

33.8.2.1 Adding Voice Routing Policy

- Select **Add New Voice Routing Policy** to add a New Voice Route.

Figure 33-48: Add New Voice Routing Policy

Add new Voice Routing Policy

Identity: **Description:**

[Save](#)

33.8.2.2 Editing Voice Routing Policy

This section shows how to edit a Voice Routing Policy.

To edit Voice Routing Policy, do the following:

1. Select a Voice Routing policy.
2. Right-click the selection
3. Select the Edit Voice Routing Policy option.

Figure 33-49: Edit Voice Routing Policy Step 1

Dial Plans Normalization Rule Templates PSTN Gateways PSTN Usage **Voice Routes** Voice Routing Policies

[Add New Voice Routing Policy](#)

DataChang...	Identity	Description	PSTN Usage
	Global		
	Unrestricted		

- Edit Voice Routing Policy
- Delete Voice Routing Policy
- Cancel changes

Figure 33-50: Edit Voice Routing Policy Step 2

33.8.2.3 Deleting/Canceling Voice Routing Policy

This section shows how to delete or cancel a Voice Routing policy.

To delete (or cancel) a Voice Routing Policy, do the following:

1. Select the Voice Routing policy.
2. Right-click on the selection.
3. Select the **Delete Voice Routing Policy** option, and then confirm in the pop-up prompt.

Figure 33-51: Delete Voice Routing Policy

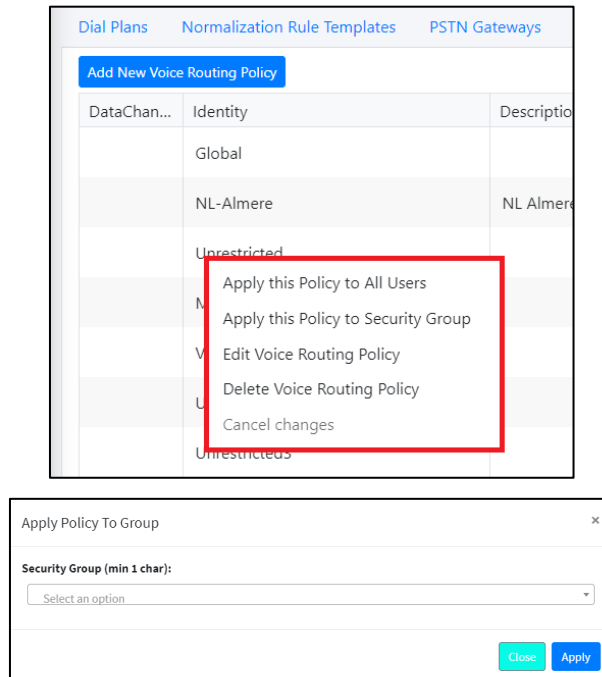
DataChang...	Identity	Description	PSTN Usage
	Global		
	Unrestricted		

Figure 33-52: Edit Voice Routing Policy - Step 2

33.8.2.4 Applying a Voice Routing Policy to a Group of Users

By right-clicking a Voice routing policy, the policy can be applied to all users within the Microsoft 365 environment or to a subset of users based on a security group membership:

Figure 33-53: Apply Voice Routing Policy to a Group of Users



33.8.3 Voice Route

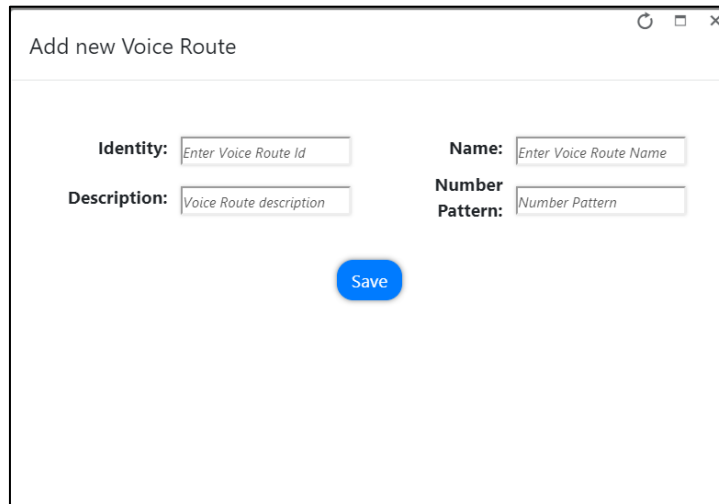
A voice route is a number pattern and set of online PSTN gateways to use for calls where the calling number matches the pattern.

Figure 33-54: Voice Routes

Dial Plans Normalization Rule Templates PSTN Gateways PSTN Usage Voice Routes Voice Routing Policies									
Add New Voice Route									
Dat...	Identity	P...	Pattern	Name	Description	Pattern	PSTN Gateway...	PSTN Usage	
	LocalRoute	0	^\{+1[0-9]{10}\}\$	LocalRoute		^\{+1[0-9]{10}\}\$			▼ ▲
	Unrestricted	1	.*	Unrestricted		.*	audiocodes-be.customers.audiocodes.be	Unrestricted	▼ ▲

To create a new Voice Route with a selection of assigned PSTN Usage records and assigned PSTN Gateway (Hosting solution - derived trunk FQDN), click **Add New Voice Route** to add a new Voice Route in the Voice.

Figure 33-55: Add New Voice Route



The screenshot shows a web form titled "Add new Voice Route". The form has a title bar with a refresh icon, a maximize icon, and a close icon. The form contains four input fields: "Identity" with placeholder text "Enter Voice Route Id", "Name" with placeholder text "Enter Voice Route Name", "Description" with placeholder text "Voice Route description", and "Number Pattern" with placeholder text "Number Pattern". A blue "Save" button is centered below the input fields.

The Voice Routing decisions are made top-down, so the table should be prioritized by using the green arrow buttons or drag and drop to make sure that a proper route is chosen if multiple routes to the same destination exist.

Voice Routing Policies will be assigned to subscribers, allowing them to reach certain destinations based on the PSTN Usage record that is assigned within the policy.

33.8.4 PSTN Gateways

A PSTN gateway is a pointer to an SBC that also stores the configuration that is applied when a call is placed through the SBC, such as forward P-Asserted-Identity (PAI) or Preferred Codecs. It can be added to voice routes. For the hosting model (Microsoft Super Trunk), only the carriers need to set up and manage a single trunk (carrier trunk in the carrier domain). For the customer tenant, the carrier needs to only add the derived trunk FQDN to the voice routing policies of the users. There is no need to create a new PSTN gateway for a customer trunk.

33.8.5 Dial Plan & Normalization Rules

A dial plan is a named set of normalization rules that translate phone numbers dialed by an individual user into an alternate format (typically E.164) for purposes of call authorization and call routing. Each dial plan consists of one or more normalization rules that define how phone numbers are expressed in various formats and are translated into an alternate format.

Normalization rules define how phone numbers expressed in various formats are to be translated. The same number string may be interpreted and translated differently, depending on the locale from which it is dialed. Normalization rules may be necessary if users need to be able to dial abbreviated internal or external numbers.



If Dial Plans have been created in Microsoft 365 using PowerShell before UMP SP has been installed, the normalization rules that are assigned to it will not be shown in the Normalization Rule Templates in this version. Only templates that are created using UMP SP are displayed.

Figure 33-56: Normalization Rules

Name	Description	Pattern	Translation	IsInternalExtension
------	-------------	---------	-------------	---------------------

To create a new normalization rule, do the following:

1. Click **Add New Normalization Rule** to add a new Normalization rule.
2. In the pop-up window, the following page appears. This page assists in the building of the required regular Pattern and Translation expressions.

Figure 33-57: Add New Normalization Rules

Add new Normalization Rule

Add new Normalization Rule

Name:

Description:

Starting digits:

Length:

Digits to remove:

Digits to add:

Pattern:

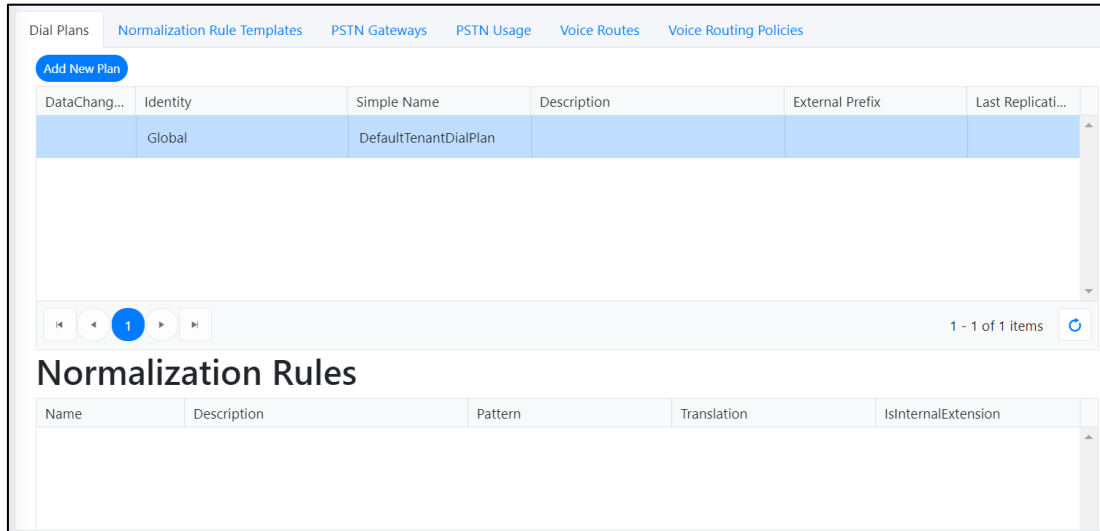
Translation:

IsInternalExtension:

Save Normalization Rule

Normalization Rule Templates can be assigned to new or existing Dial Plans by double-clicking the normalization rule from the Normalization Rules section in the New or Edit Dial Plan screens. If multiple rules exist, they can be ordered by either using the green arrow buttons or by dragging-and-dropping, by placing one rule above or below another.

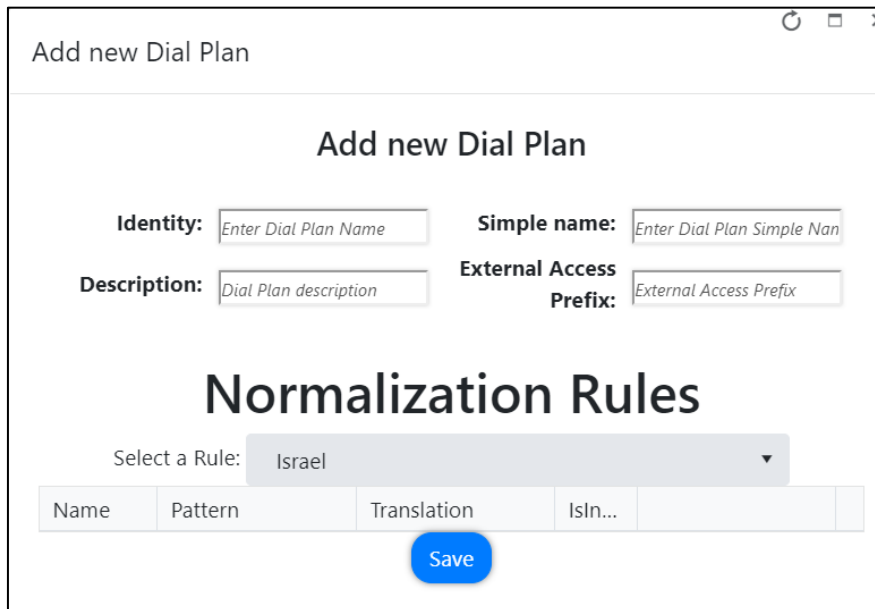
Figure 33-58: Dial Plan



To add Normalization Rules to a New Dial Plan, do the following:

- Click **Add New Plan** to add a new dial plan.

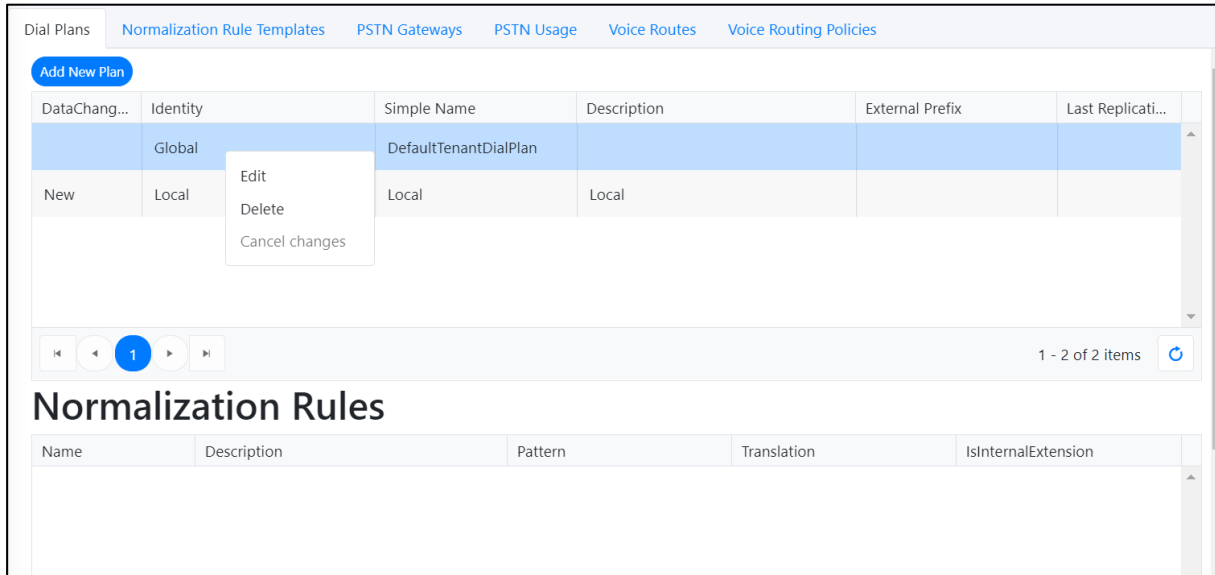
Figure 33-59: Add New Dial Plan



To add Normalization Rules to an existing Dial Plan, do the following:

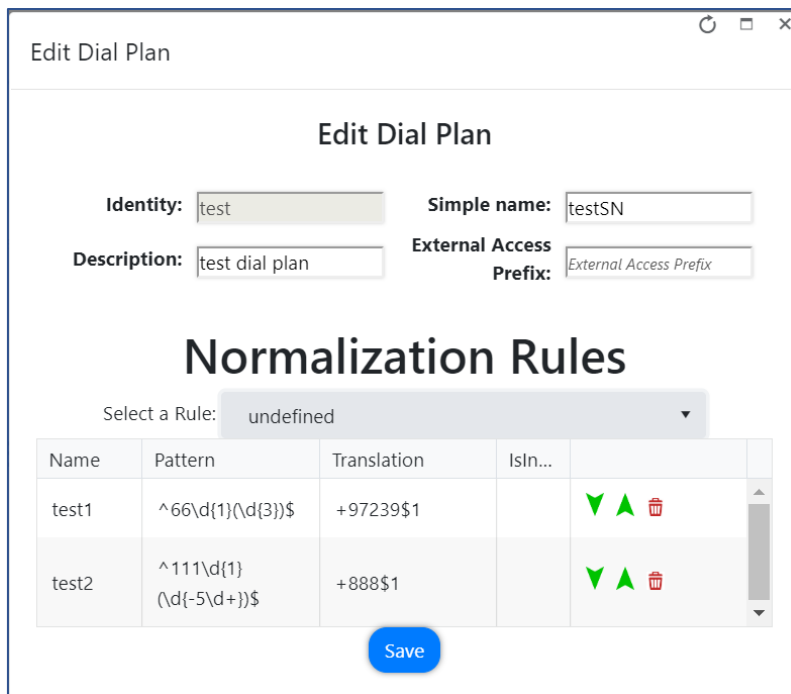
1. Select a Dial Plan.
2. Right-click the selection, and then select **Edit**.

Figure 33-60: Select Dial Plan



3. In the pop-up window, add Normalization Rules to the Dial Plan.

Figure 33-61: Edit Dial Plan



4. If multiple rules exist, they can be ordered by either using the green arrow buttons or by dragging and dropping, by placing a rule above or below another.

33.9 Reserving M365 Tenant Phone Numbers

You can reserve a phone number from the DID Range to assign to a specific user. When the phone number is reserved, it is not allocated in the automatic assignment.

To configure a reserved number range, do the following:

1. In the Main Tenant navigation pane, select **Reserved Numbers**. The reserved numbers are displayed.

Figure 33-62: Reserved Numbers

The screenshot shows the AudioCodes interface for managing reserved numbers. The left sidebar contains navigation options: Users, LifeCycle Management, Manage Templates, Online Voice Routing, Unassigned Number Range, Reserved Numbers (highlighted), Audit, Queued Changes, M365 Configuration, and Site Locations. The main content area displays a table of reserved numbers. The table has the following data:

LineUri	WhenAdded	WhenExpires	Reason	Comments		
+17326524656	03/25/2022	05/26/2022	Employee left comment	VP approval	Edit	Delete

The interface also includes a '+ Add new record' button, a pagination bar showing '1 - 1 of 1 items', and a footer with copyright information: 'Copyright © 2020 AudioCodes. All rights reserved.' and 'db.000.000.0461.'

2. Click **+ Add new record** to add a new record.
3. Add the required fields and click **Update** to add the new record.

Figure 33-63: Reserved Number

The screenshot shows the AudioCodes interface for managing reserved numbers. The left sidebar contains navigation options: Users, LifeCycle Management, Manage Templates, Online Voice Routing, Unassigned Number Range, Reserved Numbers (highlighted), Audit, Queued Changes, M365 Configuration, and Site Locations. The main content area displays a table of reserved numbers. The table has the following data:

LineUri	WhenAd...	WhenEx...	Reason	Comments		
Tel: + 9723976400 0	04/26/20 20	04/26/20 20	Reserved for IT	VP approval	Edit	Delete

The interface also includes a '+ Add new record' button, a pagination bar showing '1 - 1 of 1 items', and a footer with copyright information: 'Copyright © 2020 AudioCodes. All rights reserved.' and 'db.000.000.0461.'

33.10 Audit and Roll Back Historical Changes

UMP SP includes tracking for changes made by administrators. Under **Audit**, all changes performed are shown and can be reverted by right clicking a line. If multiple changes were performed in one action, a list is shown with the changes, where the appropriate change can be selected. Select the entry for the change that you wish to rollback and click **Update** to roll back to the previous value.

To view audit history and perform rollback, do the following:

1. In the Main Tenant navigation pane, select **Audit**. The Audit History is displayed.


Figure 33-64: Audit History

Date	Target	InitiatedBy	Status	WhenCompleted
13 Jan 2022 06:38:53	sip.MiriamG@M365x08167531.OnMicrosoft.com	Admin-EMEA@sandbox3.audiocodes.be	Processed	13 Jan 2022 06:58:31
13 Jan 2022 06:37:53	sip.MiriamG@M365x08167531.OnMicrosoft.com	Admin-EMEA@sandbox3.audiocodes.be	Processed	13 Jan 2022 06:58:31
03 Jan 2022 07:34:07	sip.MiriamG@M365x08167531.OnMicrosoft.com	Admin-EMEA@sandbox3.audiocodes.be	Processed	03 Jan 2022 08:00:53
03 Jan 2022 06:40:53	sip.MiriamG@M365x08167531.OnMicrosoft.com	Admin-EMEA@sandbox3.audiocodes.be	Processed	03 Jan 2022 07:02:10
29 Dec 2021 12:14:42	sip:AdeleV@M365x08167531.OnMicrosoft.com	Admin-EMEA@sandbox3.audiocodes.be	Processed	29 Dec 2021 12:51:03

2. Right-click an entry, and then click  to undo the policy update for the selected user.

Figure 33-65: Rollback

Field Name	Old Value	New Value
SipAddress	sip:pureonline@OCSHOST.onmicrosoft.com	sip:pureonline@OCSHOST.onmicrosoft.com
OnPremLineUri	null	tel:+123456
EnterpriseVoiceEnabled	False	True

3. Choose the specific fields that you want to rollback and then click .

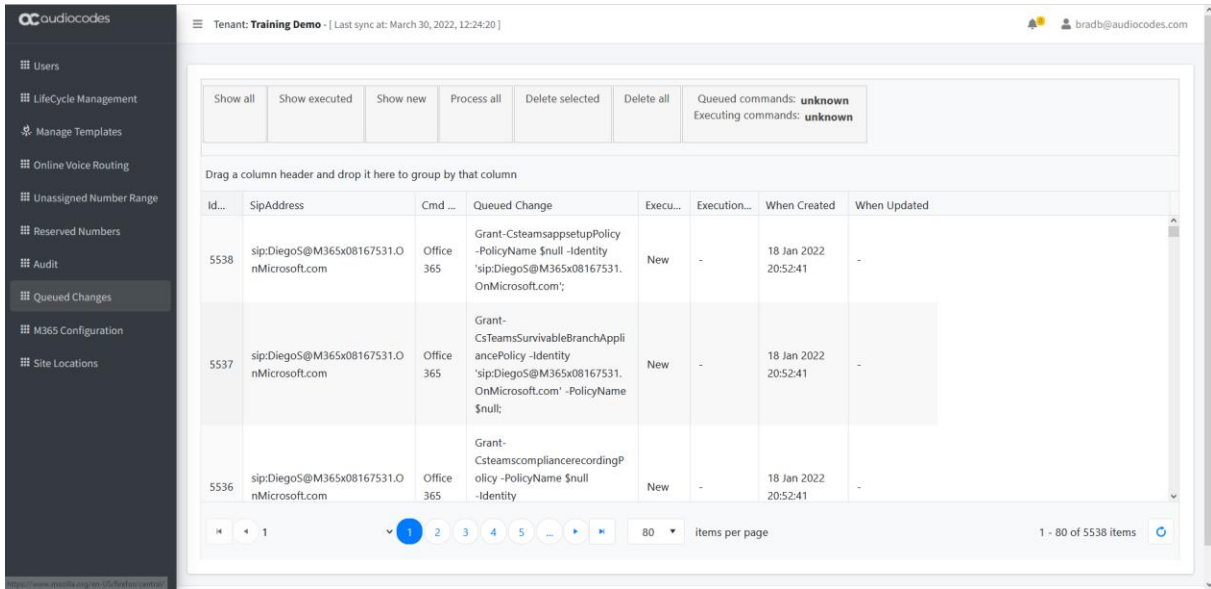
33.11 Queued Changes

You can view the queue for all actions including those that have been executed and those in waiting.

To view queued changes, do the following:

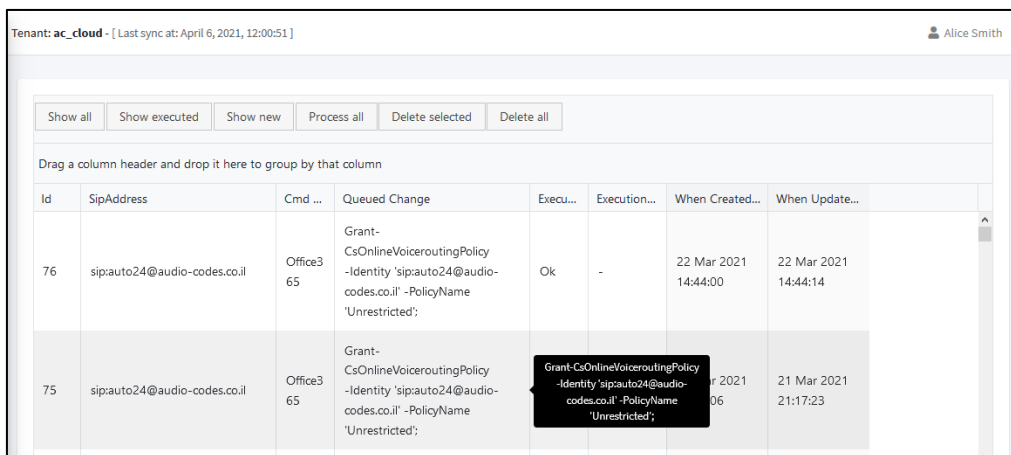
1. In the Main Tenant navigation pane, select **Queued Changes**. A list of updates are displayed.

Figure 33-66: Queued Changes



2. Hover over a specific column to view a callout of the text in the selection (this is useful when text is too detailed to be easily read in the initial view) as is shown in the example screen below. You can also drag-and-drop to group by a specific column.

Figure 33-67: Queued Changes Entry Tooltip



3. Use the table below as a guide to the actions available in this screen.

Figure 33-68: Queued Actions

Action	Description
Show all	Show all actions, including both executed and non-executed.
Show executed	Show all executed actions.

Action	Description
Show new	Show the latest actions.
Process all	Process all actions.
Delete selected	Delete selected actions.
Delete all	Delete all actions.

33.12 Microsoft 365 Settings

The Microsoft 365 Settings screen reflects the configuration of the Application Registration for the Background Synchronization from the customer Azure environment to UMP-365 as described in Chapter 10 . You can update Microsoft 365 connection credentials and also configure whether the user logs in to Microsoft 365 with Token authentication or with username/password.

To update Microsoft 365 connection credentials:

1. In the Main Tenant navigation pane, select **M365 Configuration**.

Figure 33-69: M365 Configuration

The screenshot displays the 'Microsoft 365 Settings' configuration page. On the left is a dark navigation sidebar with the AudioCodes logo and menu items: Users, LifeCycle Management, Manage Templates, Online Voice Routing, Unassigned Number Range, Reserved Numbers, Audit, Queued Changes, M365 Configuration (highlighted), and Site Locations. The main content area has a header with 'Tenant: Customer Id - [Last sync at: April 18, 2022, 11:43:28]' and a user profile 'UMP-TobiJumadmin'. The form includes:

- User Name:** admin@m365x25175153.onmicrosoft.com
- Password:** (empty field)
- Confirm password:** (empty field)
- Buttons: 'Switch to auth token' and 'Validate Authentication'
- Primary button: 'Save Microsoft365 settings'
- Footer: Copyright © 2020 AudioCodes. All rights reserved. db.000.000.0461.

2. Configuration the Microsoft 365 credentials as described in the table below:

Table 33-1: Microsoft 365 Settings

Parameter	Description
Username	Microsoft 365 UC Admin User that was configured for the Background Replication Processing (see Chapter 10)
Password	Microsoft 365 UC Admin Password.
Switch to auth token	Enables you to login by sending link to customer IT administrator for authentication (see Section 30.3).
Validate Authentication	Validates the user credentials.
Save Office 365 settings	Saves the settings updated in this screen.

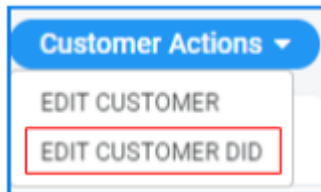
33.13 Manage Site Locations

This section describes how to manage multiple site locations. Once the onboarding wizard has added the M365 tenant and performed initial synchronization with Microsoft Teams, you can do the following:

- Onboard additional SBC devices for new sites (see Section 33.13.1 **Error! Reference source not found.**)
- Add and edit SBC prefixes (see Section 33.13.2)
- Import PBX users (see Section 33.13.3)

To manage site locations

1. In the Navigation pane, click **Site Locations**. You can also open this screen from AudioCodes Live Cloud for Teams Customer screen from the Customer Actions menu.



The table below describes the site location parameters.

Table 33-2: Site Locations

Parameter	Description
Site	FQDN of the site location.
SIP Address	IP address of the site location.
Configuration	Configuration type e.g. SIP Trunk (how is this field filled)
PSTN Gateway	PSTN Online Gateway
SbcDeploymentState	Indicates the SBC deployment state.
M365DeploymentState	Indicates the M365 deployment state.
Notes	Lists commands yet to be executed.
Actions	Describes the specific actions that can be performed in the location: <ul style="list-style-type: none"> ■ Add and edit SBC prefixes ■ Import PBX users

33.13.1 Add SBC Site Locations

You can add an SBC device to manage calls for a new site location. When selecting this option, you are redirected to the Onboarding wizard where customer credentials are automatically authenticated with Single Sign-on.

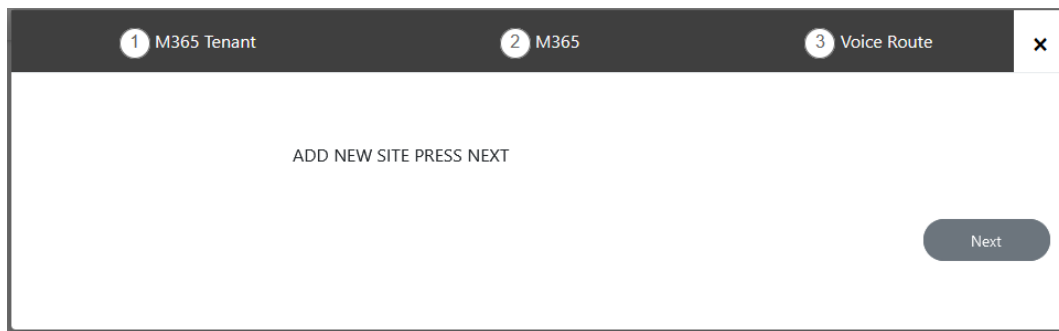
To onboard an SBC site:

1. Click **Add SBC Site** to connect an SBC device deployed in a specific site.

Figure 33-70: Add SBC Site-Hosted Pro

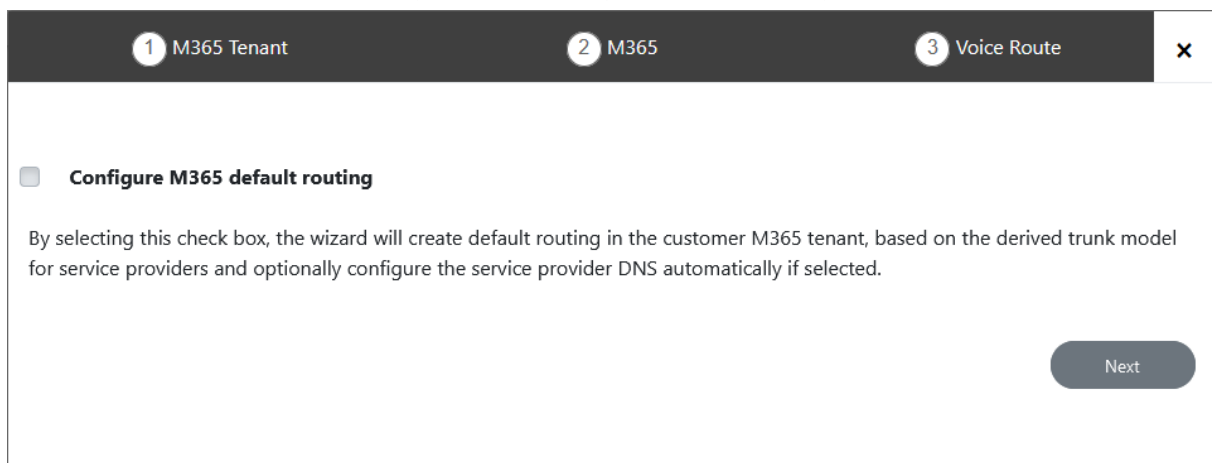
The screenshot shows the AudioCodes management console interface. On the left is a navigation menu with 'Site Locations' selected. The main content area displays a table of sites. A red box highlights the 'Add SBC Site' button at the top left of the table. The table has columns for Site, SIP Address, Configuration, PSTN Gateway, SbcDeploymentState, M365DeploymentState, Notes, and Actions. One site is listed with the name 'audc_at1_'. The Actions column for this site contains links for '[Uninstall]', 'Add / Edit Sbc Prefixes', and 'Import PBX users'.

Sites							
Site	SIP Address	Configuration	PSTN Gateway	SbcDeploymentState	M365DeploymentState	Notes	Actions
audc_at1_	169.254.0.145	SipTrunk	audio-codes.customers.fmcc.com	Deployed		Pending commands: 0	[Uninstall] Add / Edit Sbc Prefixes Import PBX users



2. Click **Next** to continue. Credentials are validated and the Onboarding wizard opens.

Figure 33-71: Configure Default Routing



3. Proceed to Chapter 30.

33.13.2 Configure SBC Prefixes

This section describes how to configure SBC prefixes for specific sites.

To configure SBC prefixes:

1. In the Navigation pane, click **Site Locations**.
4. Chose the site for which you wish to configure prefixes.

Figure 33-72: Add and Edit SBC Prefixes

Tenant: **audc_at1** - [Last sync at: July 15, 2021, 14:12:44]

operator@audio-codes.at

Add SBC Site

Sites							
Site	SIP Address	Configuration	PSTN Gateway	SbcDeploymentState	M365DeploymentState	Notes	Actions
audc_at1_	169.254.0.145	SipTrunk	audio-codes.customers.fmcuc.com	Deployed		Pending commands: 0	[Uninstall] Add / Edit Sbc Prefixes

Copyright © 2020 AudioCodes. All rights reserved. db.000.000.0404 .

5. Click **Add/Edit** SBC Prefixes.

Figure 33-73: SBC Prefixes

Tenant: **aiologics** - [Last sync at: December 26, 2021, 11:08:41]

spAdmin@audio-code.co.il

SBC: 2 - Location: aiologics

Add additional prefixes / number ranges

Select Dial Plan: -- Please select a dial plan -- Tag / PSTN Gateway: Enter tag

Telephone Number Prefix: New Number prefix

Upload from single file: Choose file Browse

Current prefixes

Prefixes shown below are from cache. Press **Reload** to refresh them from SBC.

Search: [] Delete UndoDelete

Drag a column header and drop it here to group by that column

Dial Plan Name	Prefix	Tag
No items to display		


10 data items per page

6. From the Select Dial Plan drop-down, select one of the following:
 - **CustDialPlan**: Default Dial Plan for the Direct Routing customers
 - **RegisteredUsers**: Dialplan used for managing IP-PBX users when an IP-PBX is configured in the Onboarding Wizard.

Figure 33-74: Customer Dial Plan

- In the Tag/PSTN Gateway field, enter the Derived Trunk FQDN of the site device to which to load the dial plan (there is no need to create a new PSTN gateway for a customer trunk).

Figure 33-75: PSTN Gateway

- Do one of the following:
 - Manually add telephone number prefixes and then click . The configured prefixes are displayed.
 - Browse to choose a prefix file to upload.

The new dialplan rule is displayed. Note that the dialplan rule does not have a unique name and instead inherits the name of the configured dialplan 'CustDialPlan'.

Figure 33-76: Customer Dial Plan

Dial Plan Name	Prefix	Tag
<input type="checkbox"/> CustDialPlan	+564654546	ai0logics.onmicrosoft.com
<input type="checkbox"/> CustDialPlan	+972	ai0logics.onmicrosoft.com


- Click  to apply configuration.
- Click **Reload** to refresh the list of prefixes with the SBC.

Figure 33-77: Reload

Current prefixes
 Prefixes shown below are from cache. Press **Reload** to refresh them from SBC.

33.13.3 Import PBX Users

This section describes how to import PBX users.

To import PBX users:

1. In the Navigation pane, click **Site Locations**.

Figure 33-78: Import PBX Users

Tenant: nl02 with channel - [Last sync at: June 7, 2021, 10:20:30]

Add SBC Site

Sites							
Site	SIP Address	Configuration	PSTN Gateway	SbcDeploymentState	M365DeploymentState	Notes	Actions
nl02	52.143.63.223	SipTrunk	M365x603711.onmicrosoft.com	Deployed		Pending commands: 0	[Uninstall] Add / Edit Sbc Prefixes
nl02_s1	52.143.63.223	IpPbx		Deployed		Pending commands: 0	[Uninstall] Import Pbx Users

Reload Select all Deselect all Delete

Search:

Pbx User Import Tasks									
Id	Import Progress	WhenCreated	WhenExecuted	NextExecution	Remaining retries	WasExecuted	WasSuccessful	State	
No data available in table									

Showing 0 to 0 of 0 entries

Previous Next

2. Click **Import Pbx Users**.

34 Multitier Admin Access

Providers can create an additional layer of support and grant access to the provider portal to specific channels including multiple customers. When the Channel Admin users sign-in to the Public Portal URL (Azure AD), they receive the list of customers that the provider has granted them access to manage.

Figure 34-1: Access to the Portal

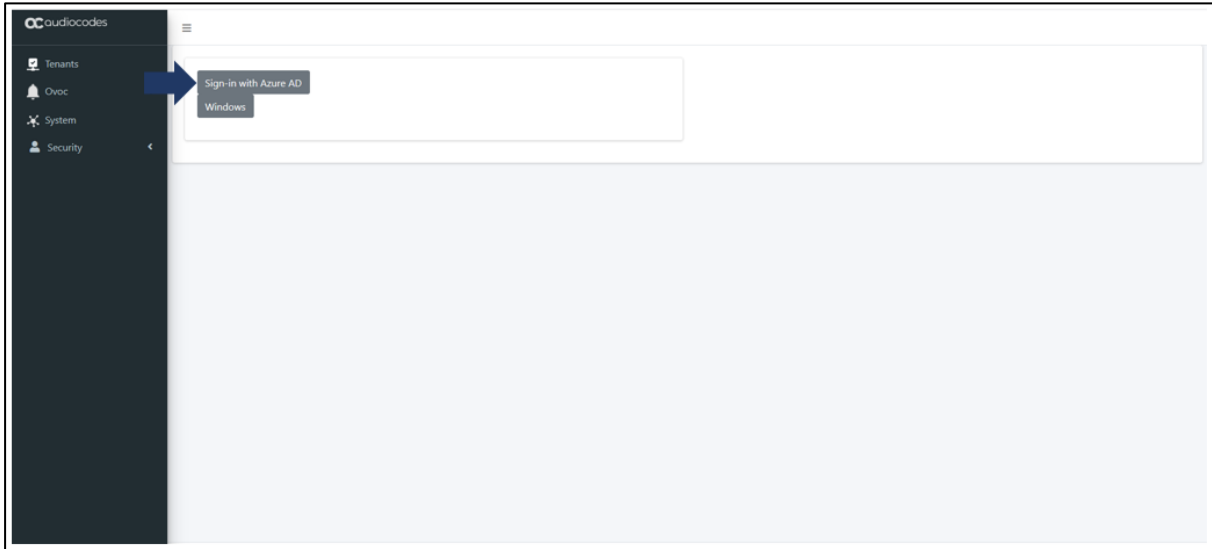


Figure 34-2: SSO with Azure Active Directory

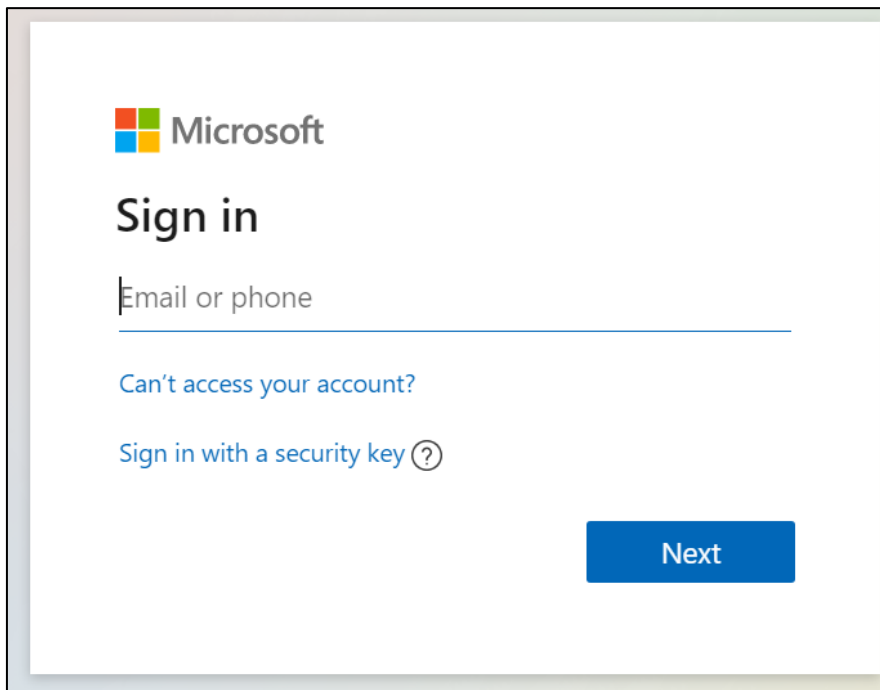


Figure 34-3: SSO with Azure Active Directory

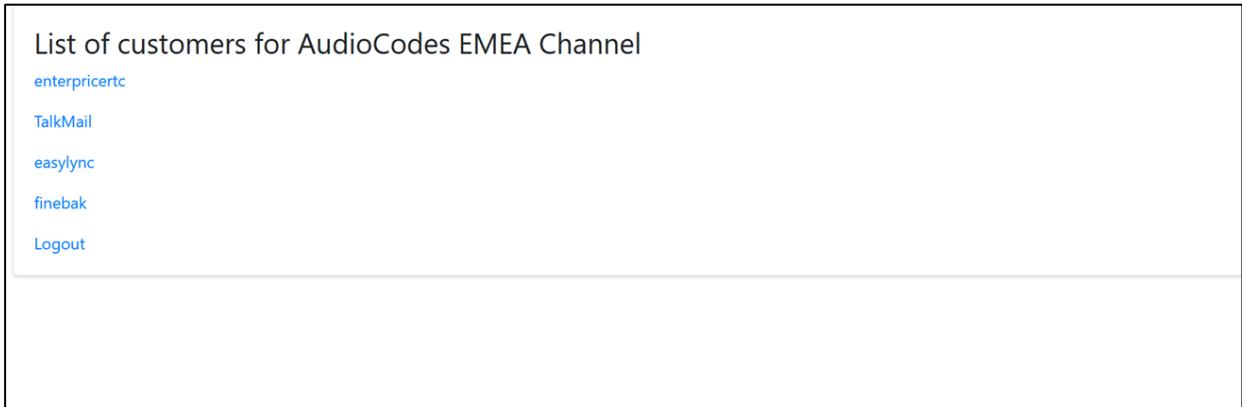
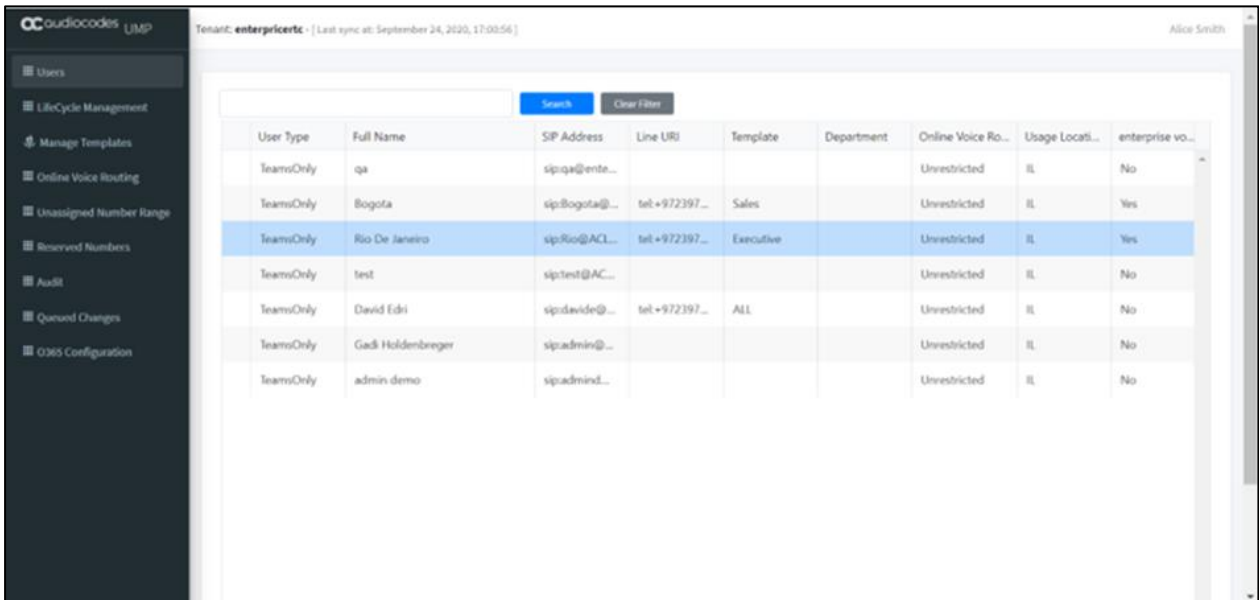


Figure 34-4: UMP 365 Customer Portal



Part VII

Appendix

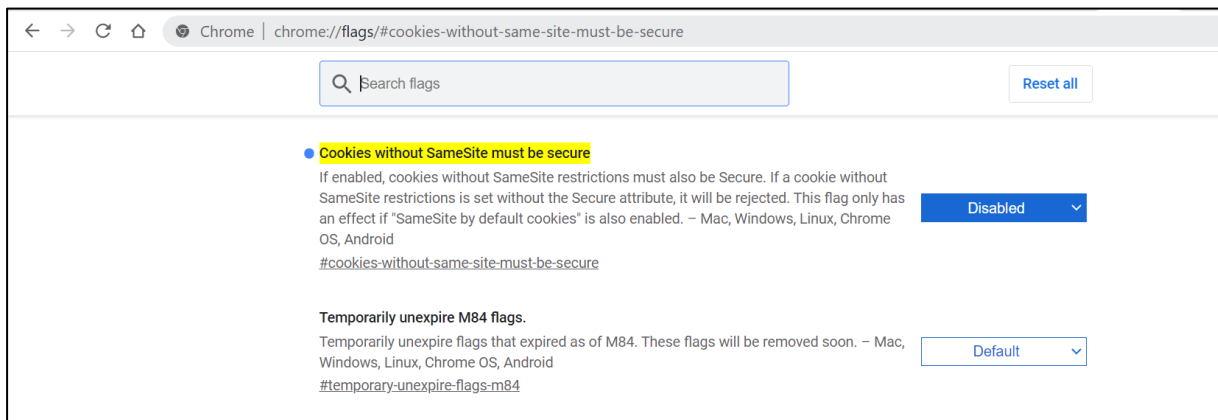
A Browser setting - IETF Same Site Cookie Attribute

The introduction of the IETF SameSite cookie attribute changed default behavior we are seeing issues with browsers addressing the UMP web pages using the http protocol, resulting in an access denied message. These problems do not occur when https is used and properly configured. A bypass for when http is absolutely required is to disable this new default behavior in the browser.

The following describes the steps required to prevent this occurrence of this issue for each respective browser:

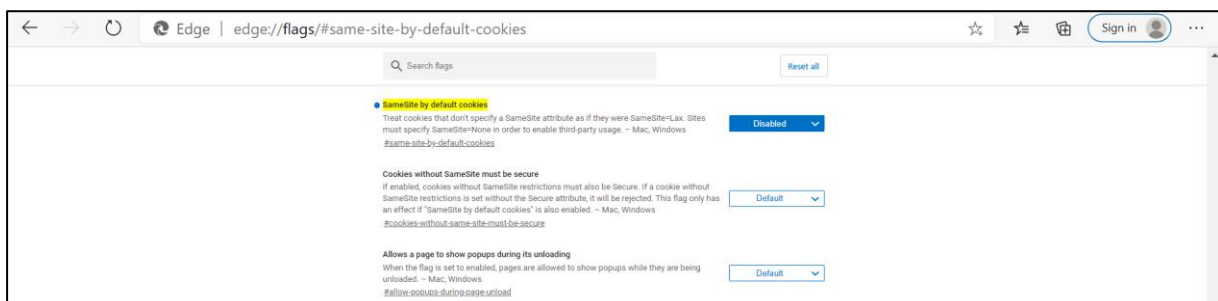
- **Chrome:**
 1. Go to: "chrome://flags/#cookies-without-same-site-must-be-secure"
 2. Disable option "Cookies without SameSite must be secure"
 3. Restart Chrome.

Figure A-1: Chrome Setting



- **Edge:**
 1. Go to: "edge://flags/#same-site-by-default-cookies"
 2. Disable option "SameSite by default cookies"
 3. Restart Edge.

Figure A-2: Edge Setting



- **Firefox: (works in any version past 75):**
 1. In the URL bar, navigate to **about:config**. (accept the warning prompt, if shown).
 2. Type **SameSite** into the "Search Preference Name" bar.
 3. Set `network.cookie.sameSite.laxByDefault` to **false** using the toggle icon.
 4. Set `network.cookie.sameSite.noneRequiresSecure` to **false** using the toggle icon.
 5. Restart Firefox.

Figure A-3: FireFOX Setting - about:config

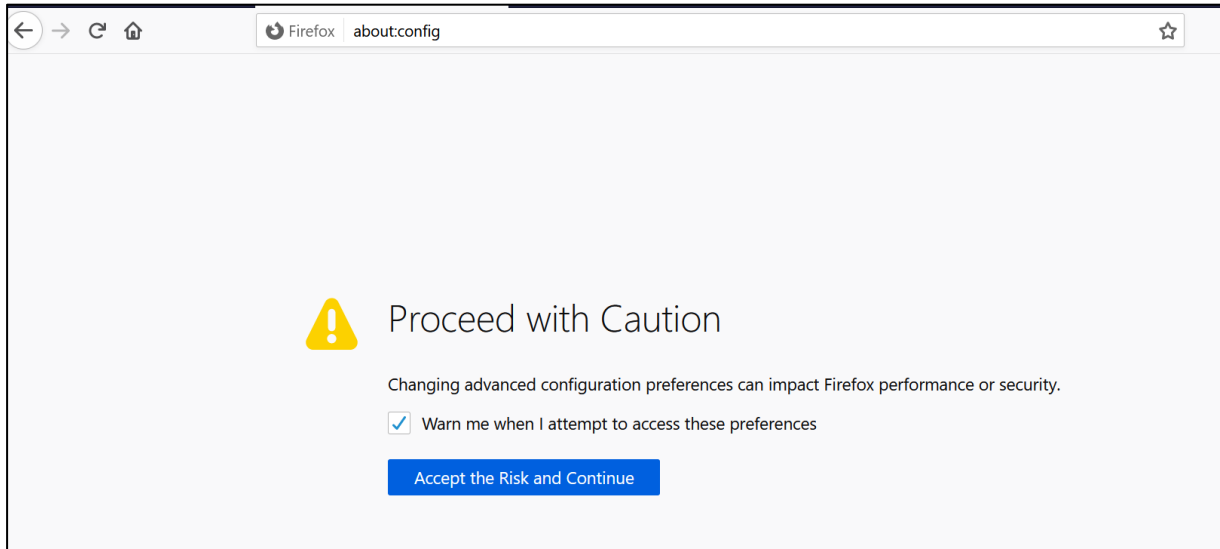
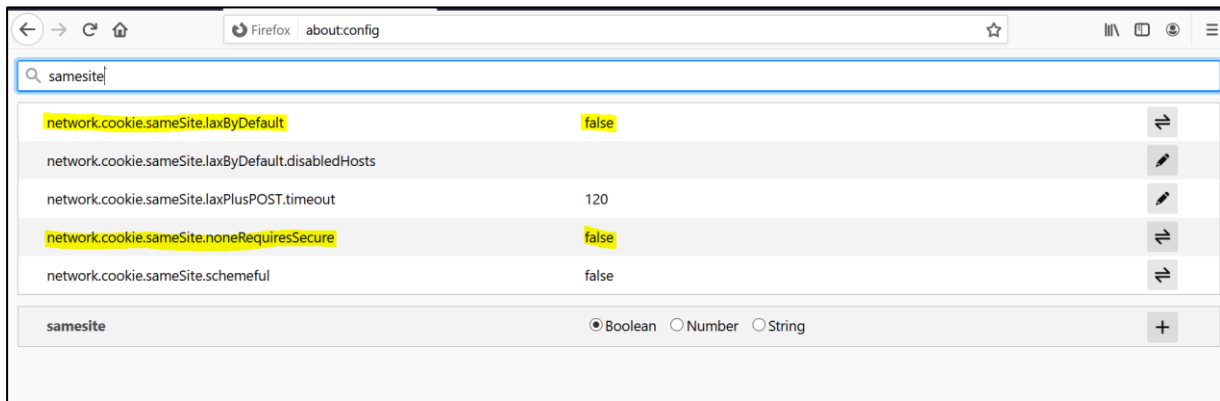


Figure A-4: FireFOX Setting



Public Customer/ Channel Url Portal requires a secure connection (HTTPS) as a default Mandatory requirement. Channel and Customer Admin do not need to edit the browser setting IETF SameSite cookie attribute.

B Backup and Restore Customer Tenant

This section describes how to Backup/Restore the customer tenant information.

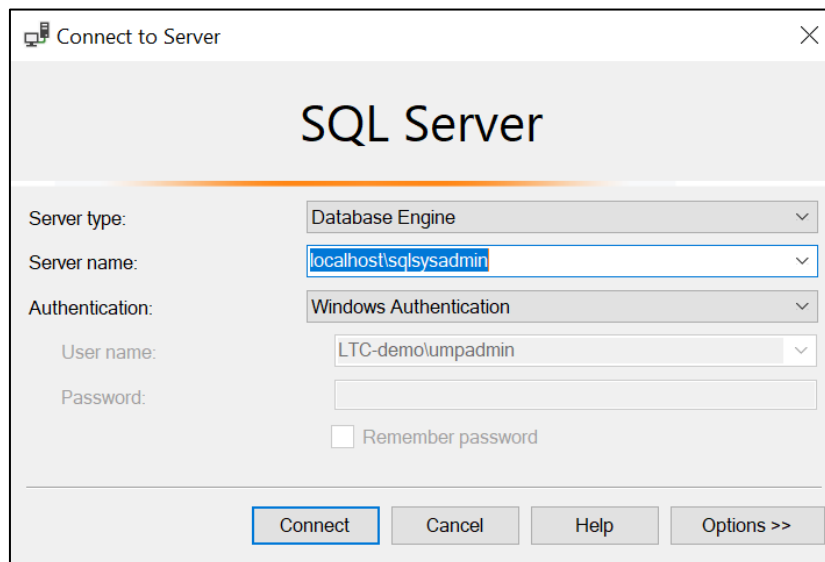
B.1 Backup the Customer Tenant Database

This section describes how to back up the customer tenant database.

To back up the customer tenant database, do the following:

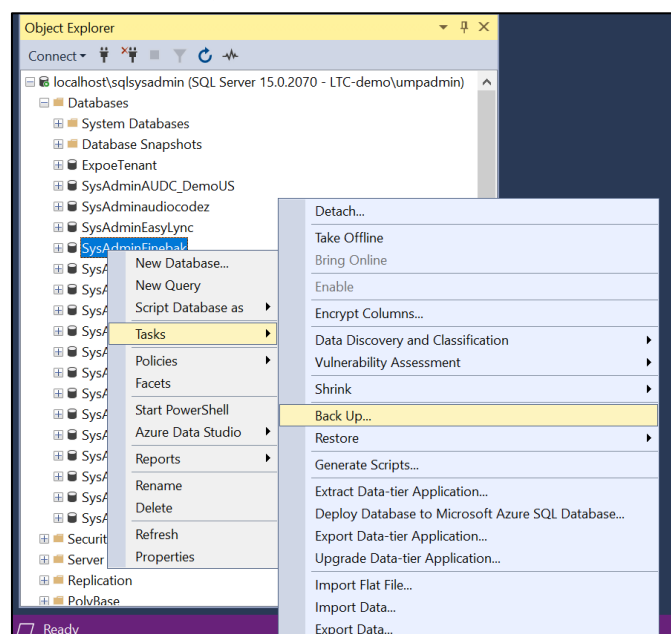
1. Start the Microsoft SQL Server Management Studio.

Figure B-1: SQL Server



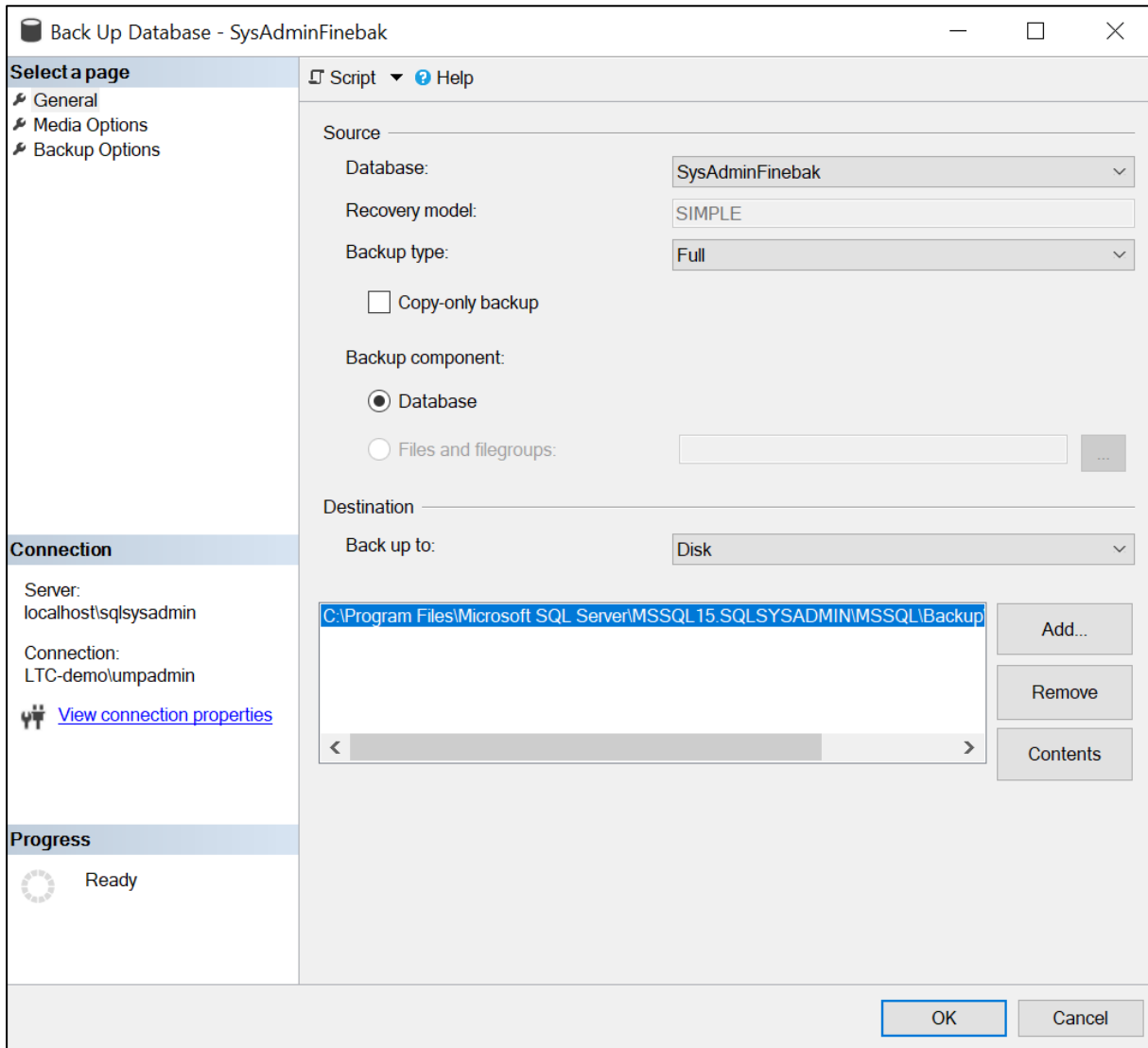
2. Apply **Connect** to the sysadmin database (localhost\sqlsysadmin).
3. Select the Customer Tenant that you would like to back up.
4. Right-click and select **Tasks/ Back Up**.

Figure B-2: Run Back Up Task



5. Right-click and select **the Destination**.

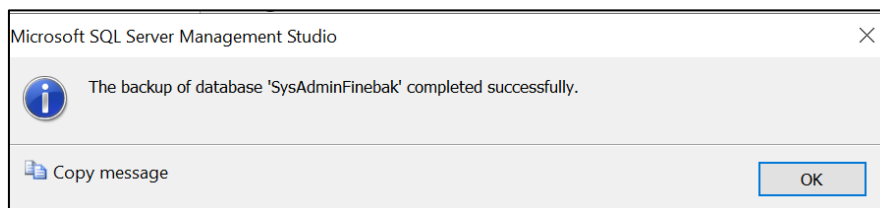
Figure B-3: Select the Database Destination



Don't save the backup on the same disk as the SQL database.

6. Select the 'Destination', and then click **OK**.

Figure B-4: Database Backup Completed Successfully



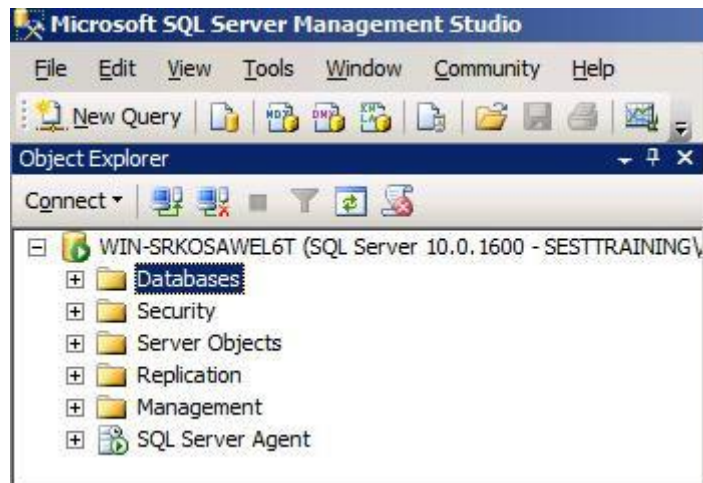
B.2 Restore the Customer Tenant Database

This section describes how to restore the customer tenant database.

To restore the database, do the following:

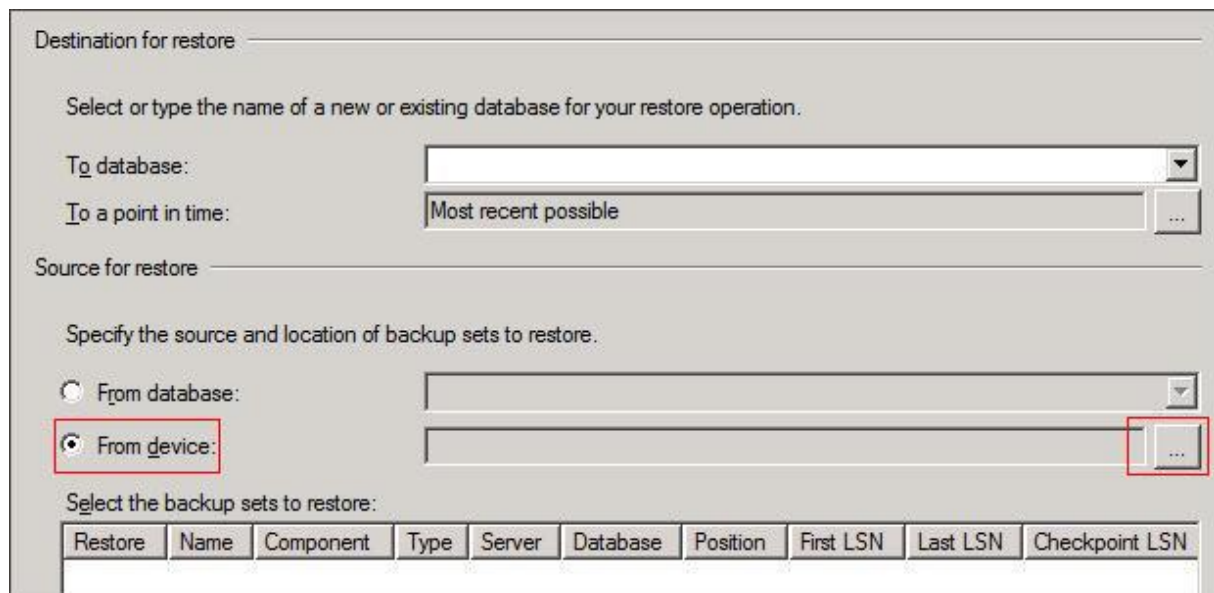
1. Open Microsoft SQL Server Management Studio and navigate to **Databases**:

Figure B-5: Select the Database resource



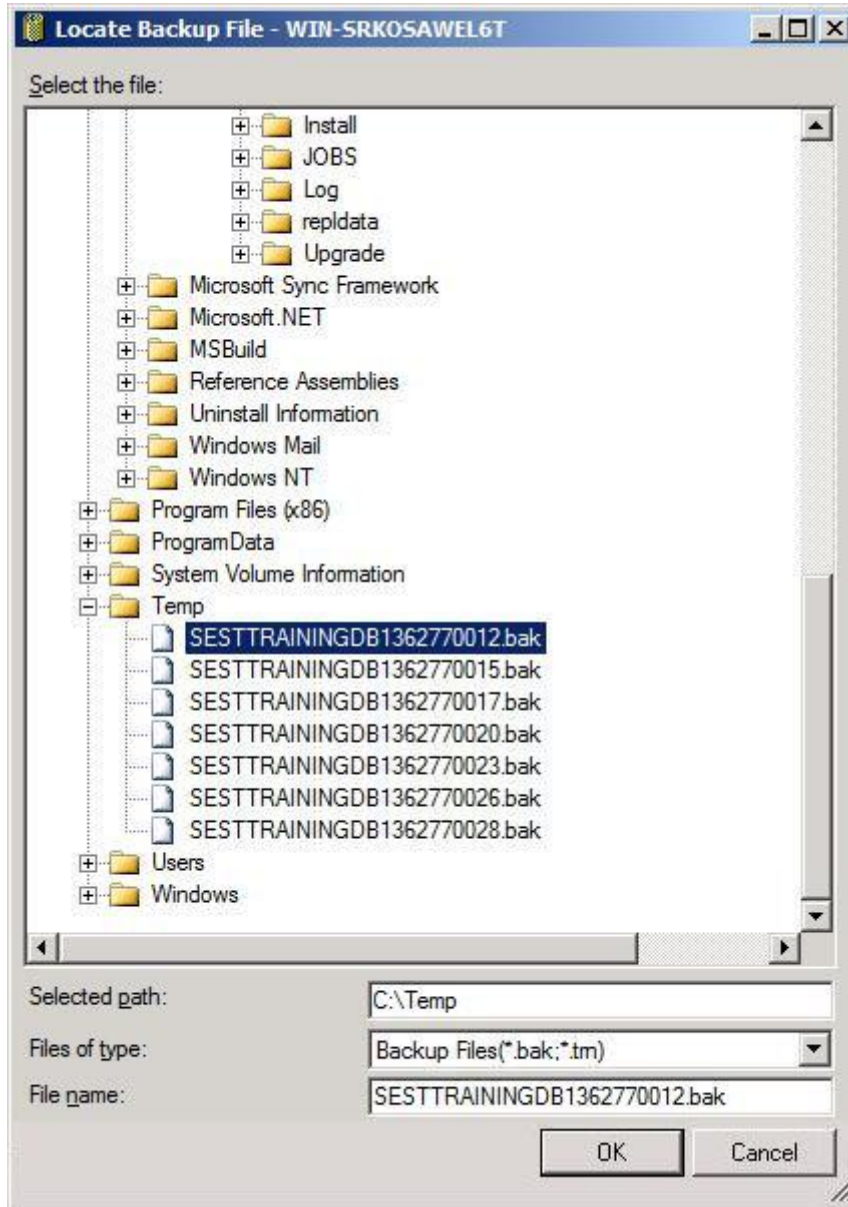
2. Right-click **Databases** and click **Restore Database**. In the screen section 'Source for restore', select **From Device** and then click the browse button:

Figure B-6: Select the Device



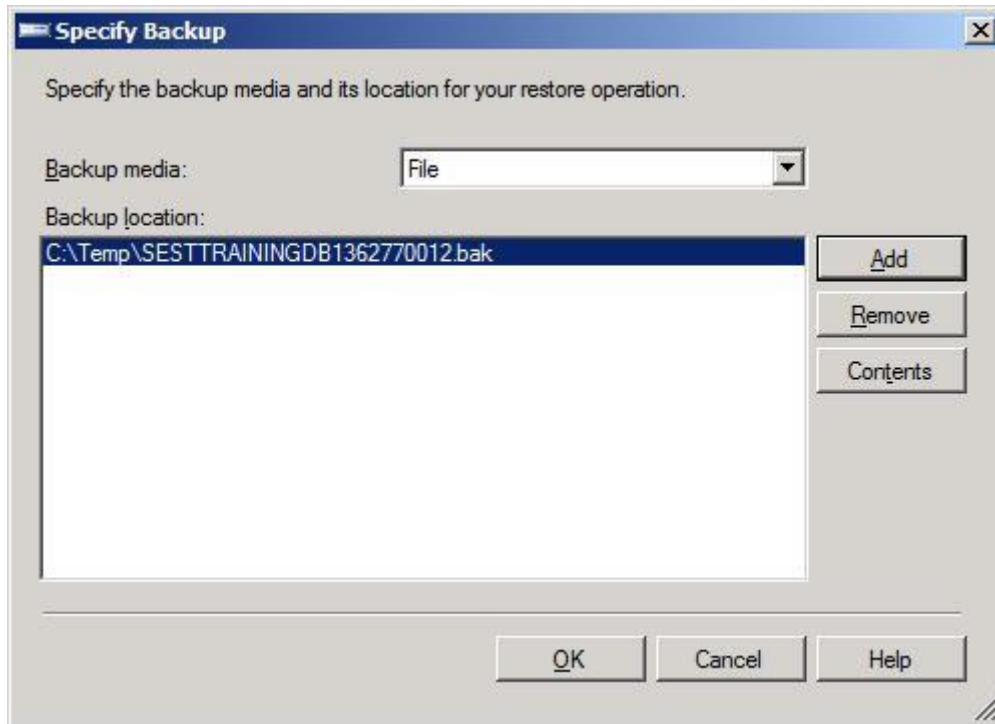
3. Click **Add** in the Specify Backup window. Browse to the location of your recently restored files. Choose the full backup file which should be the first backup file in the list:

Figure B-7: Select the Backup File



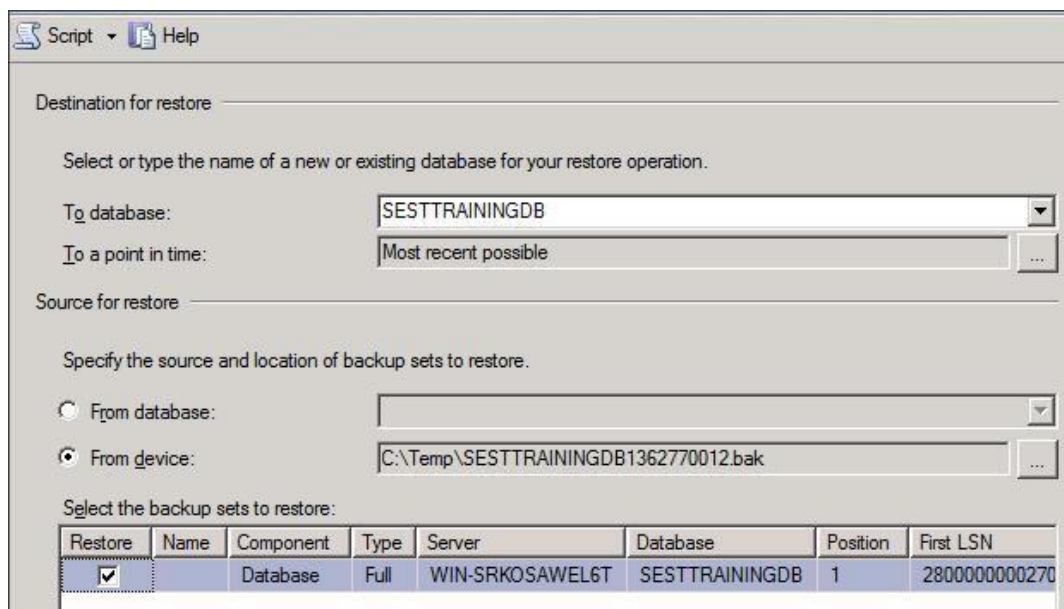
4. Click **OK**; the Specify Backup window is displayed.

Figure B-8: Confirm the Backup File



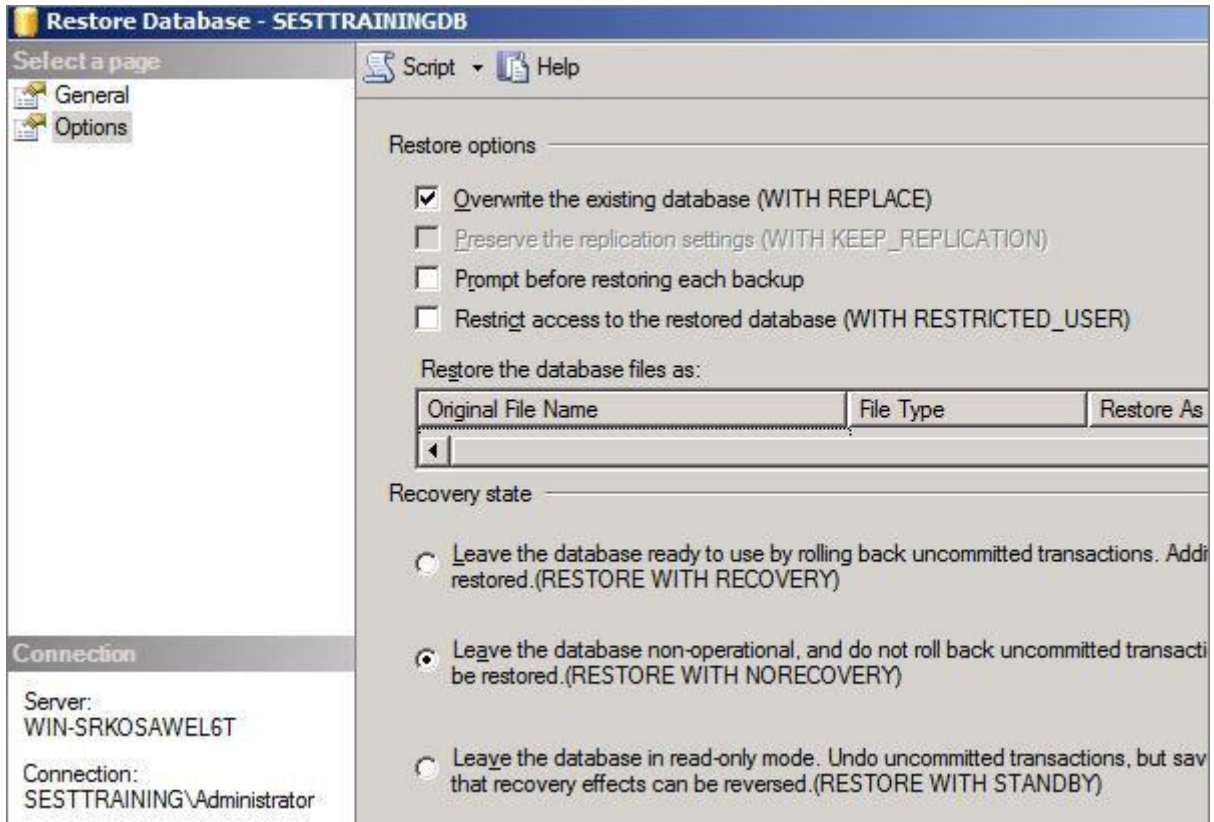
5. Click **OK**.
6. In the screen section 'Destination for restore', select the database to which you want to restore, and then in the 'Select the backup sets to restore' section of the screen, select the backup file you selected above.

Figure B-9: Confirm the Backup File



7. In the left pane, click **Options**, and then select the following:
 - a. In the Restore options' section, select **Overwrite the existing database (WITH REPLACE)** and leave the other options unselected.
 - b. In the Recovery state' section, select Leave the database non-operational, and do not roll back uncommitted transactions. Additional transaction logs can be restored. (RESTORE WITH NORECOVERY):

Figure B-10: Select the Backup File



8. Click **OK** to perform the restore.
9. Complete these steps for each incremental backup file, including the .tm file, until you reach the incremental file containing the point-in-time file to which you want to restore.
10. A "Restoring" message is displayed; you can now proceed with the next section 'Restoring to a Point-in-Time'.

B.2.1 Restore to a Point-in-Time

Use the following steps to restore the last incremental file containing the point-in-time:

1. In Microsoft SQL Server Management Studio, right-click **Databases**, and click **Restore Database**.
2. In the Source for restore' section, select **From Device** and then click the browse button.
3. Click **Add** in the Specify Backup window. Browse to the location of your recently restored flat files, select the **incremental backup file containing the point-in-time to restore to**, and click **OK**.
4. Click **OK** in the Specify Backup window. In the Select the backup sets to restore' section, check the backup file you added in the previous step.
5. In the 'Destination for restore section', select the **database** to which to restore:

Figure B-11: Restore to point of time – Step 1

Destination for restore

Select or type the name of a new or existing database for your restore operation.

To database: SESTTRAININGDB

To a point in time: 3/8/2013 1:54:07 PM

Source for restore

Specify the source and location of backup sets to restore.

From database:

From device: C:\Temp\SESTTRAININGDB1362770028.bak

Select the backup sets to restore:

Restore	Name	Component	Type	Server	Database	Position	First l
<input checked="" type="checkbox"/>			Transaction Log	WIN-SRKOSAWEL6T	SESTTRAININGDB	1	3000

- In the 'Destination for restore' section, click the browse button adjacent to the field 'To a point in time'; the 'Point in time restore' window is displayed.
- Select a specific date and time and choose the **date and time** to which to restore:

Figure B-12: Restore to point of time – Step 2

Point in time restore stops the restoration of the transaction log entries after a specified point in time. You can specify the point in time or the most recent state possible.

Restore to

The most recent state possible

A specific date and time

Date: 3/ 8/2013

Time: 1:54:07 PM

OK Cancel Help

- Click **OK**. In the left pane, click **Options** and make the following selections: In the 'Restore options' section, select **Overwrite the existing database** and leave the other options unselected.
- In the 'Recovery state' section, select **Leave the database ready to use by rolling back uncommitted transactions**. Additional transaction logs can be restored. (RESTORE WITH RECOVERY):

Figure B-13: Restore to point of time – Step 3

Restore Database - SESTRAININGDB

Select a page

- General
- Options

Script Help

Restore options

- Overwrite the existing database (WITH REPLACE)
- Preserve the replication settings (WITH KEEP_REPLICATION)
- Prompt before restoring each backup
- Restrict access to the restored database (WITH RESTRICTED_USER)

Restore the database files as:

Original File Name	File Type	Restore As

Recovery state

- Leave the database ready to use by rolling back uncommitted transactions. Additional transaction logs are restored. (RESTORE WITH RECOVERY)
- Leave the database non-operational, and do not roll back uncommitted transactions. Additional transactions are restored. (RESTORE WITH NORECOVERY)
- Leave the database in read-only mode. Undo uncommitted transactions, but save the undo actions in a way that recovery effects can be reversed. (RESTORE WITH STANDBY)

Connection

Server:
WIN-SRKOSAWEL6T

Connection:
SESTRAINING\Administrator

10. Click **OK** to perform the restore. the restored database is displayed with only those changes up to the specified point-in-time.

C AudioCodes SfB2Teams Migration Tool

This chapter describes the SfB2Teams application which is used to migrate users from On-premises Skype for Business Front End to Microsoft Teams on Azure Cloud. The application can also revert Teams users back to Skype for Business. Access to Microsoft Teams on Azure is managed using the Microsoft Graph API.

This solution includes the following:

- Prerequisite App registration configuration
- SfB2Teams Application
- The solution consumes Migration Service User license (per users).
- A special version of the SfB2Teams application for Professional Services that does not require a User's License.
- Auto Call Routing To Teams through ARM

C.1 Installing the Prerequisites

The following describes the steps for installing the SfB2Teams application migration tool.

Do the following:

- The application requires Windows OS server (WIN 2012R2 and above).
- Install the following prerequisite components:
 - Skype for Business Administrative tools including the latest CU (see Section C.1.1)The above prerequisites are available on the installation ISO (UMP-MT-8.0.100.280.iso and above) in the Prerequisites folder and are numbered 1-10 for the processing order.
- Install the following prerequisites for the Azure Active Directory portal (Customer Portal):
 - .NET framework 4.8 Runtime
 - App Registration

C.1.1 Install SkypeOnline PowerShell

Install Skype Online PowerShell by running "6 - SkypeOnlinePowerShell.Exe".

C.1.2 Install .NET framework 4.8 Runtime

Download and Install .NET framework 4.8 Runtime (<https://dotnet.microsoft.com/download/dotnet-framework/thank-you/net48-web-installer>).

C.2 Create and Register the Azure App

Create App Registration in Azure AD and note **application (client) ID** and **Directory (tenant) ID** for the later install steps. This procedure should be performed with tenant administrator user permissions.

To register and Azure AD App Registration:

1. Sign-in to Azure portal and create a new App registration (**Azure Active Directory** → **App registrations** → **New registration**).
2. Add a name for the new application and under Supported account types, select "Accounts in this organizational directory only – single tenant".

3. Select **Register** and note the Application ID for the following steps.

Figure C-1: App Register

Dashboard > TEST_TEST_Audiocodes_Test > Register an application

Name
The user-facing display name for this application (this can be changed later).
Skype2TeamsMigrator

Supported account types
Who can use this application or access this API?
 Accounts in this organizational directory only (TEST_TEST_Audiocodes_Test 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 | e.g. https://example.com/auth

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

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

Register

Figure C-2: Advanced Settings

Dashboard > Weber-Stephen Products LLC > Skype2TeamsMigrator

Skype2TeamsMigrator | Authentication

Search (Ctrl+) Save Discard Got feedback?

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

- Troubleshooting
- New support request

Got a second to give us some feedback? →

Who can use this application or access this API?
 Accounts in this organizational directory only (Weber-Stephen Products LLC only - Single tenant)
 Accounts in any organizational directory (Any Azure AD directory - Multitenant)
[Help me decide...](#)

Due to temporary differences in supported functionality, we don't recommend enabling personal Microsoft accounts for an existing registration. If you need to enable personal accounts, you can do so using the manifest editor. [Learn more about these restrictions.](#)

Advanced settings

Allow public client flows

Enable the following mobile and desktop flows:

- App collects plaintext password (Resource Owner Password Credential Flow) [Learn more](#)
- No keyboard (Device Code Flow) [Learn more](#)
- SSO for domain-joined Windows (Windows Integrated Auth Flow) [Learn more](#)

Yes No

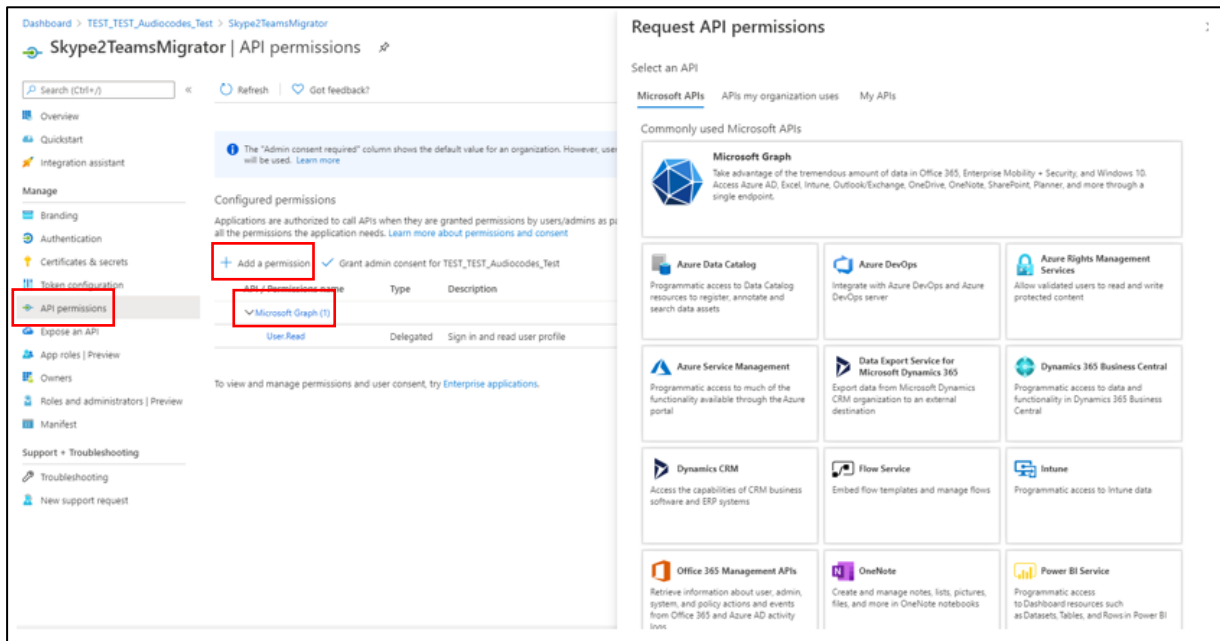
C.3 Set Microsoft Graph API Permissions

This section describes how to add Microsoft Graph Delegation & Appliance API permissions. This procedure should be performed with tenant administrator user permissions.

To set Microsoft Graph API:

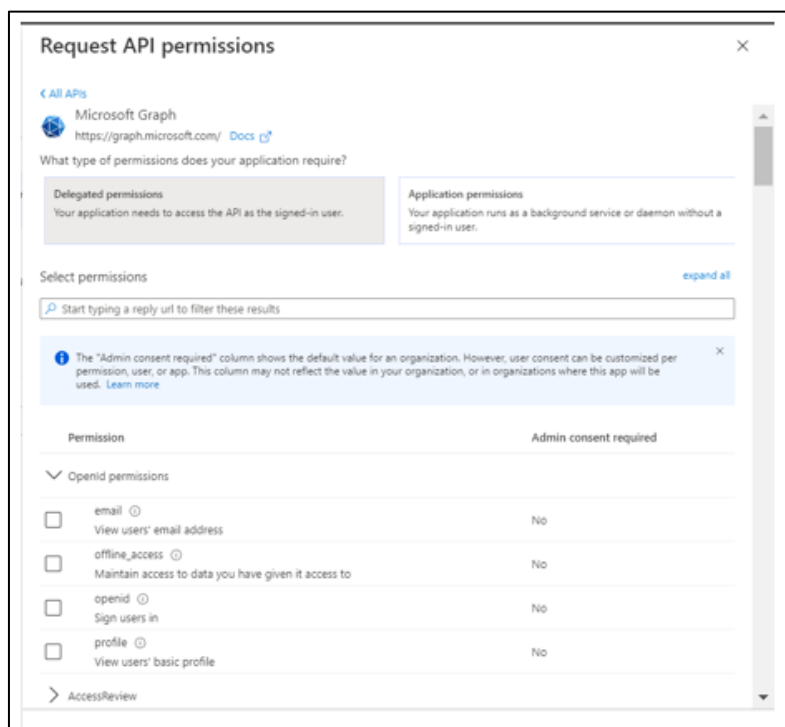
1. In the Navigation pane, select API Permissions.
2. Click **Add a permission** and then select the **Microsoft Graph** tab.

Figure C-3: Microsoft Graph



3. Select Delegated Permission.

Figure C-4: Select Delegate Permission



4. Select the following **Delegation Permissions**.

Figure C-5: Delegation Permissions

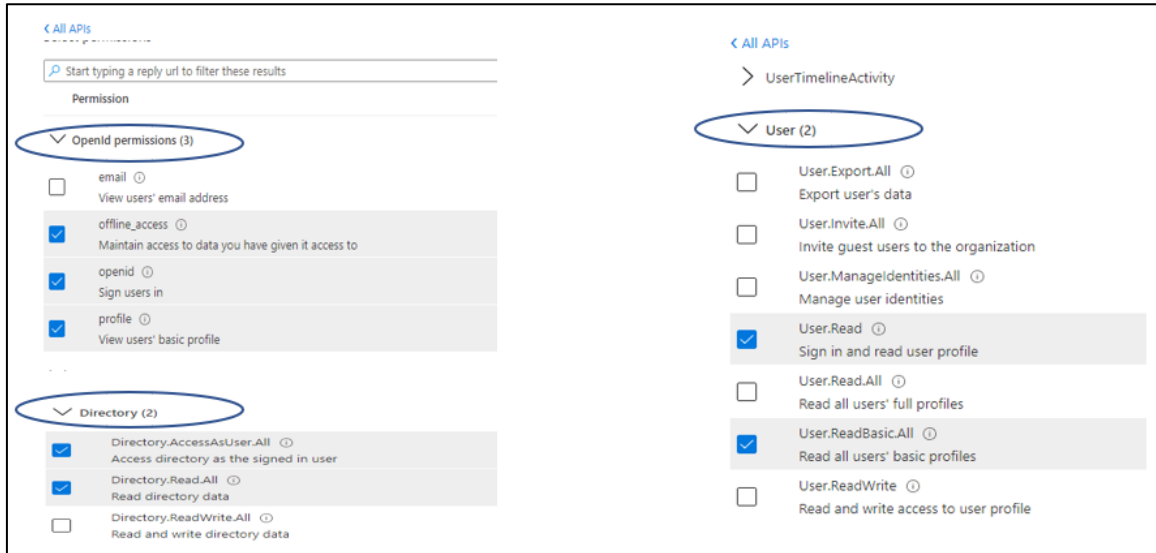
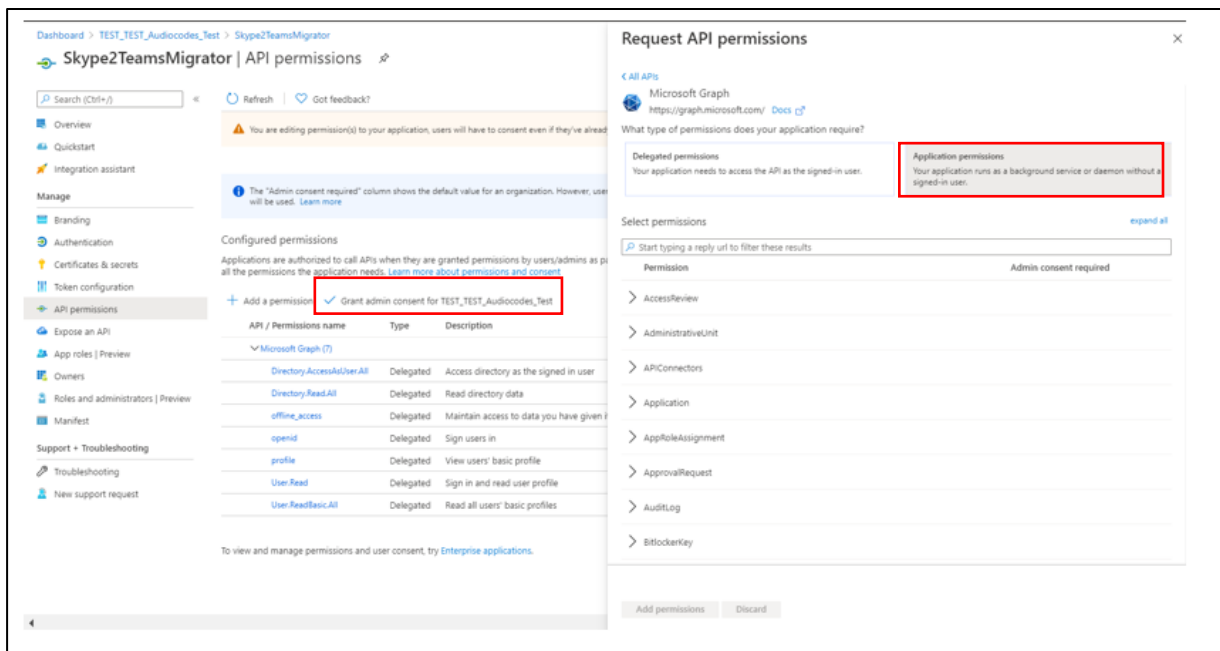


Figure C-6: Select Application Permission



5. Select the “Grant admin consent for...” and select **yes**.

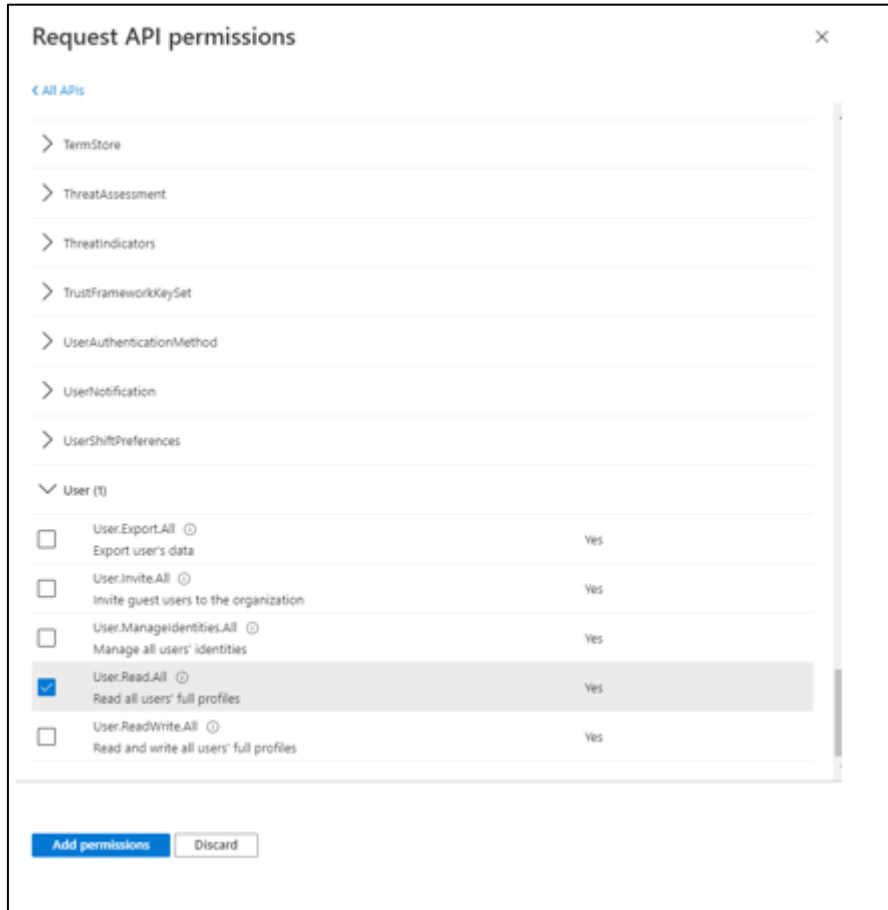


If the App hasn't been granted admin consent, users are prompted to grant consent the first time they use the App.

6. Select Application permissions.

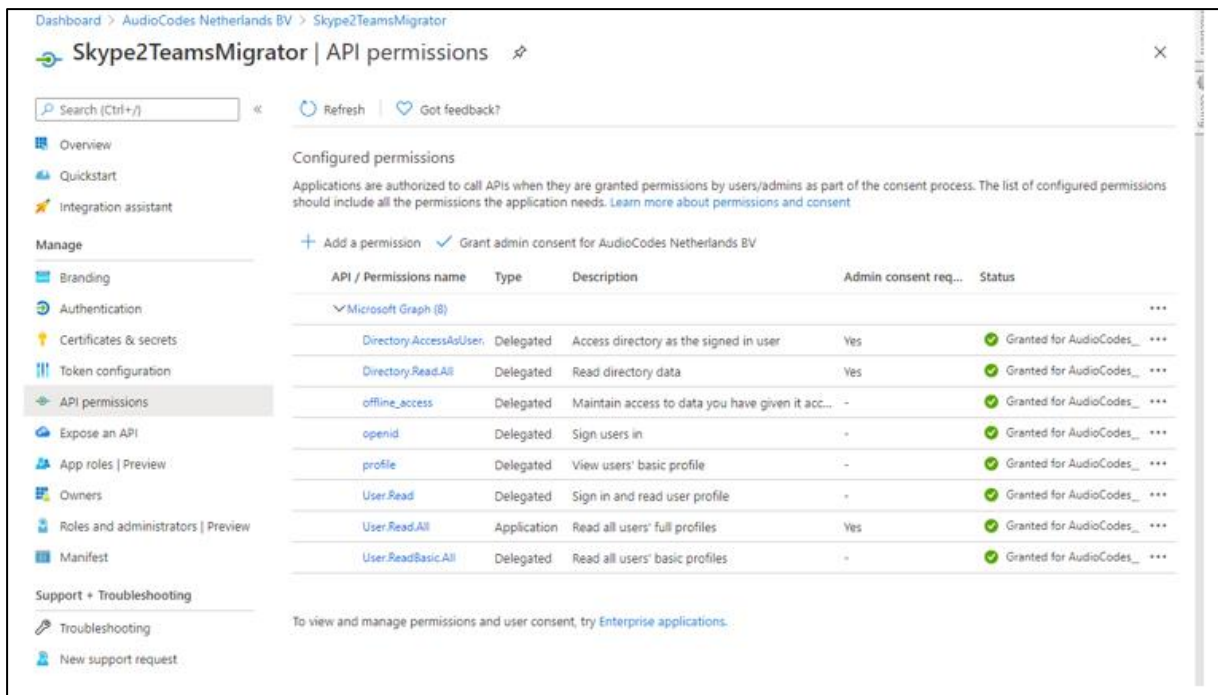
7. Select the following Application permissions.

Figure C-7: Add a Permission



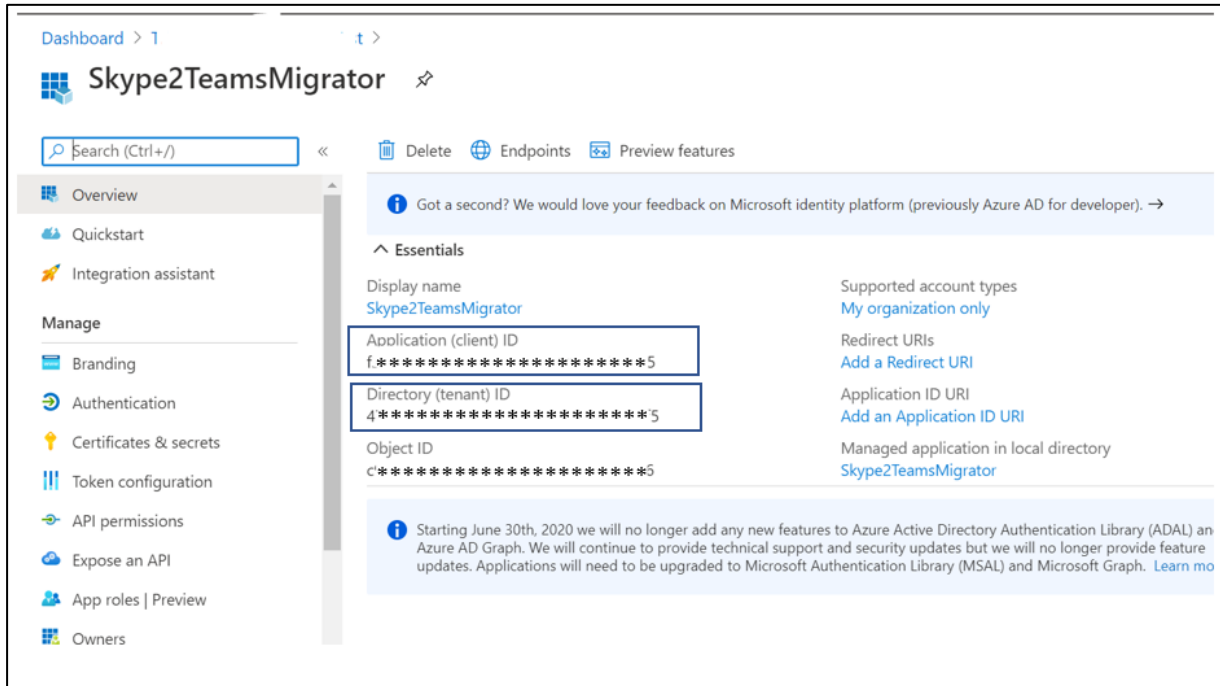
8. Review all permissions.

Figure C-8: API permissions – Summary



9. Copy **application (client) ID** and **Directory (tenant) ID** to notepad as they are required in the procedure in Section C.4.

Figure C-9: App Registration



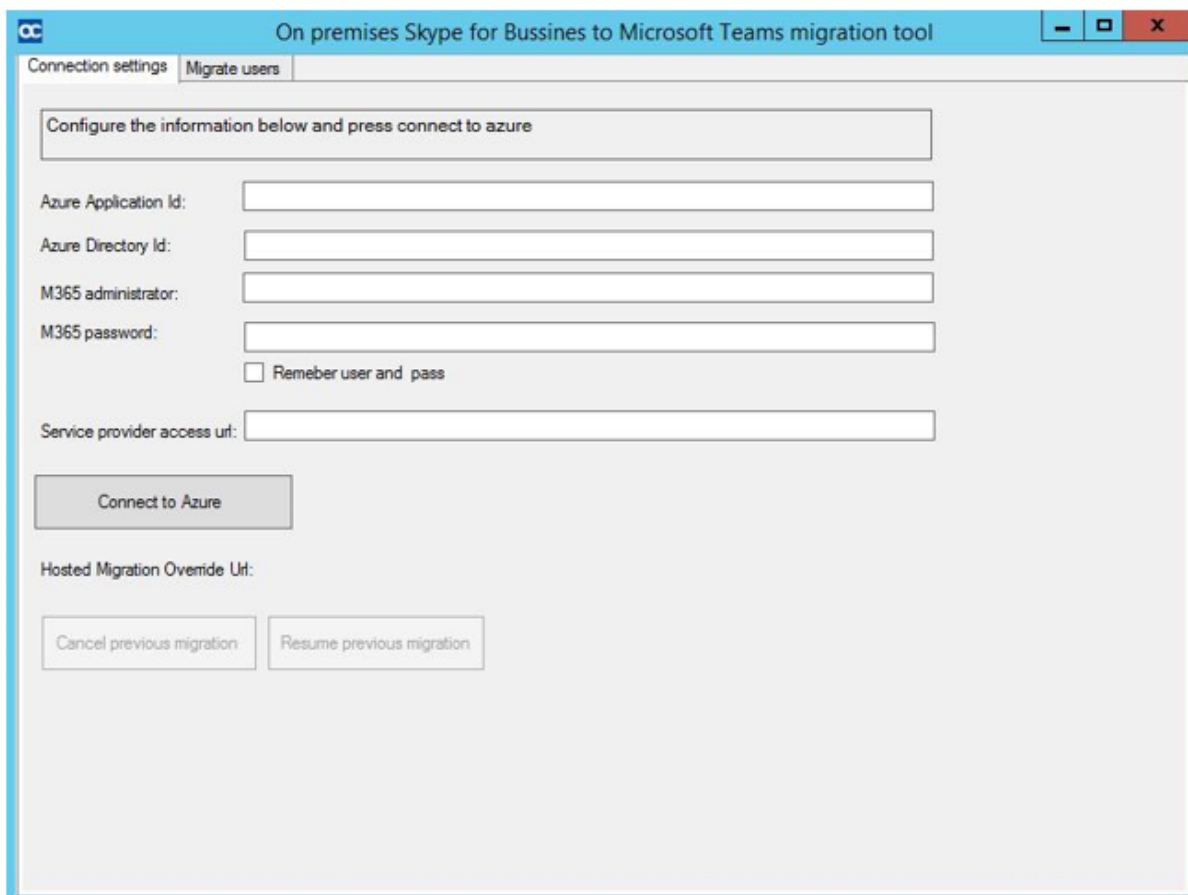
C.4 Running the SfB2Teams Application

This section describes how to setup and run the SfB 2 Teams application. Download Files and Unblock.

Do the following:

1. From the directory C:\SfB2Teams select the file SysAdmin.Skype2MsTeamsMigrator.exe.

Figure C-10: App Registration



On premises Skype for Business to Microsoft Teams migration tool

Connection settings | Migrate users

Configure the information below and press connect to azure

Azure Application Id:

Azure Directory Id:

M365 administrator:

M365 password:

Remember user and pass

Service provider access url:

Connect to Azure

Hosted Migration Override Url:

2. Connection Setting - Set the parameters as follows:
 - **Azure Application ID:** Application ID from the App Registration
 - **Azure Directory ID:** Directory ID from the App Registration
 - **M365 administrator:** UC Admin with SfB Admin and Teams Service Admin privilege.
 - **M365 password:** UC Admin Password.
 - **Service Provider access url:** UMP Customer SysAdmin URL
3. Click Connect to Azure.

Figure C-11: Connection Setting

On premises Skype for Business to Microsoft Teams migration tool

Connection settings | Migrate users

Configure the information below and press connect to azure

Azure Application Id: Application ID from the App Registration

Azure Directory Id: Directory ID from the App Registration

M365 administrator: UC Admin with Sfb Admin and Teams Service Admin privilege

M365 password: UC Admin Password

Remember user and pass

Service provider access url: Customer SysAdmin URL

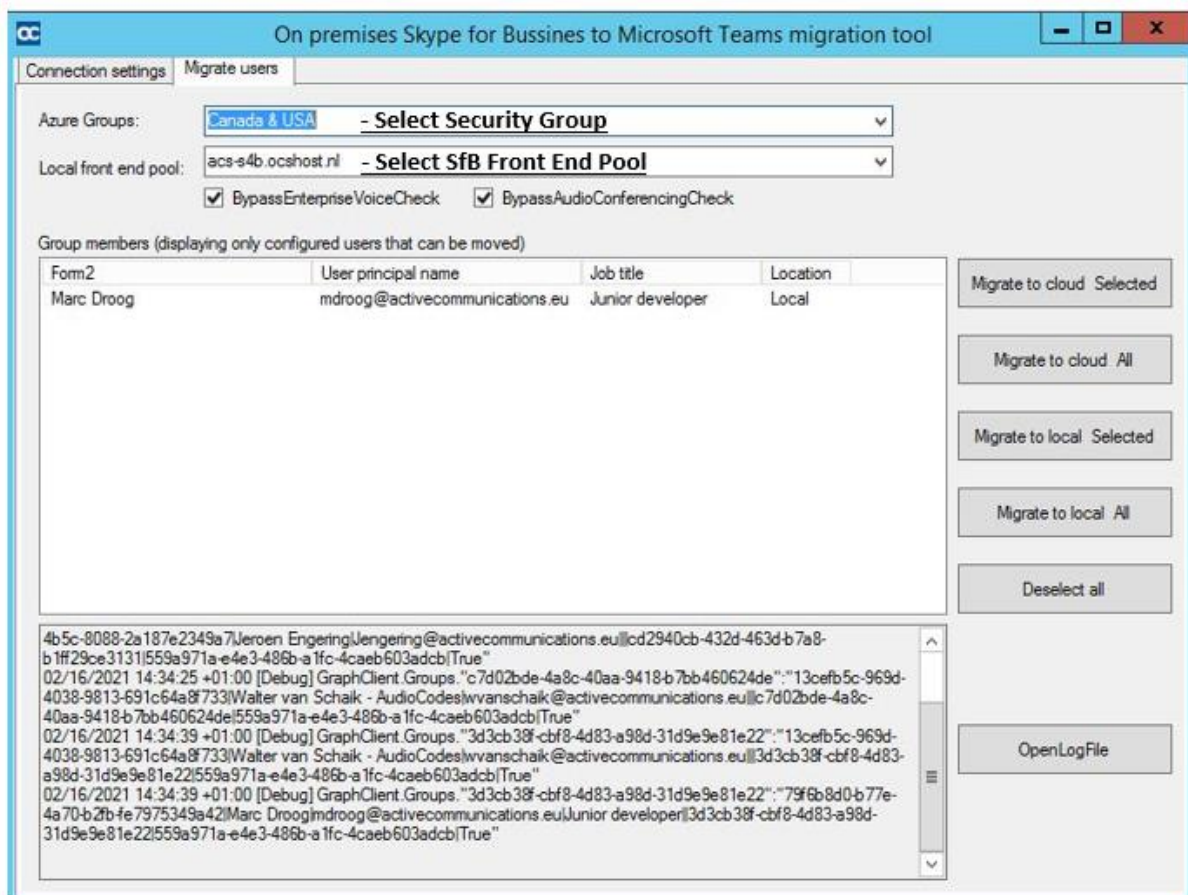
Connect to Azure

Hosted Migration Override Url:

Cancel previous migration | Resume previous migration

4. Migrate Users:
 - Azure Group: Select Security Group.
 - Local front end pool: Select SfB Front End Pool.
5. Select the users from the "Group members"
6. Select one of the following actions:
 - **Migrate to Cloud Selected:** Migrate selected Users to Teams
 - **Migrate to Cloud All:** Migrate all users to Teams
 - **Migrate to Local Selected:** Revert Selected Users to SfB
 - **Migrate to Local All:** Revert All Users to SfB
 - **Deselect All:** Deselect all Users

Figure C-12: Migrate Users

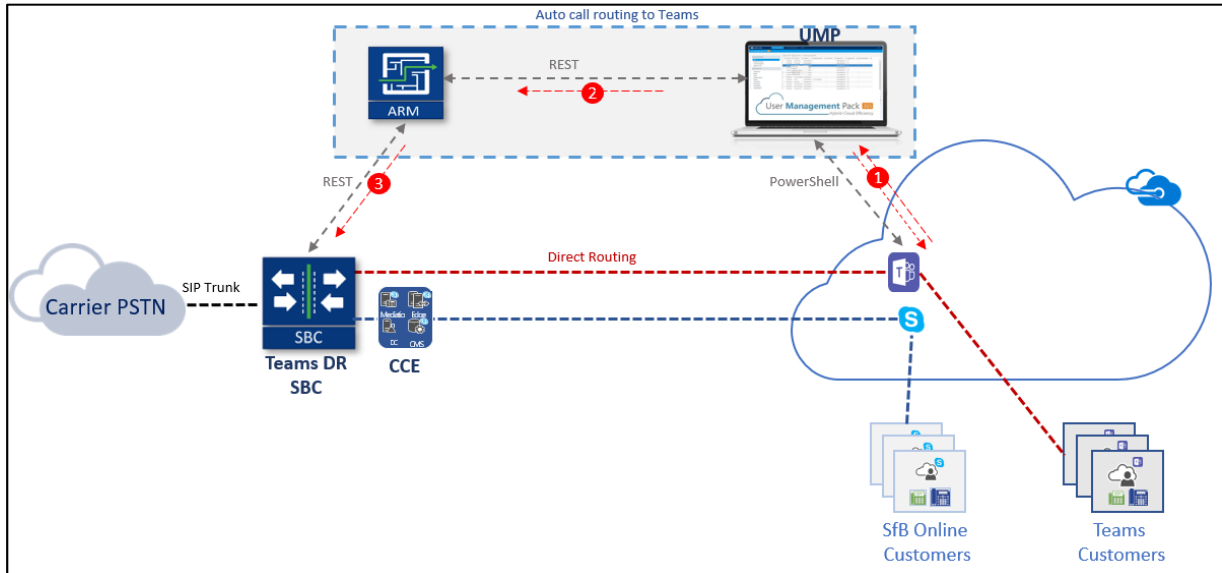


C.5 Auto Call Routing To Teams

UMP optionally supports together with ARM Auto Call Routing to Teams which automates user migration to Teams entirely and eases the migration process, by alleviating the need to configure the SBC. This feature includes the following stages:

1. UMP builds a list of all the Teams users
2. UMP updates the ARM database
3. ARM updates the SBC routing table " to configure the properties and adds a user to the list as shown in the figure below:

Figure C-13: Auto Call Routing to Microsoft Teams



For more information, contact AudioCodes Professional Services.

D Renewing Expired Tokens

When you are not able to login to Azure using Microsoft 365 token authentication then it is most likely that your token has expired. The procedure below describes how to renew an expired token.

Do the following:

1. In the Tenants screen, select the **SysAdmin** link under the tenant for whose token you wish to renew.

Figure D-1: Select Tenant

Customer Name	State	SysAdmin Info	Licensing (licensed users)		Queued commands status
ancaFromOvoc	Deployed	version: 8.0.220.26 replication: 2021.08.23.14.50.01 SysAdmin	M365 - Pro (162)	Edit Delete Undo Deploy Add SBC Site Queue Replication	Queued commands: 0 Executing commands: 1 Replication in progress: no
Automation_Essential_BYOC_Customer	Deployed	SysAdmin	M365 - Essential (0)	Edit Delete Undo Deploy	Queued commands: unknown Executing commands: unknown Replication in progress: unknown
bcb	Deployed	SysAdmin	M365 - Essential (0)	Edit Delete Undo Deploy	Queued commands: unknown Executing commands: unknown Replication in progress: unknown
BradTrunk	Deployed	version: 8.0.220.26 replication: 2021.08.23.14.49.56 SysAdmin	M365 - EssentialPlus (10)	Edit Delete Undo Deploy Add SBC Site Queue Replication	Queued commands: 0 Executing commands: 1 Replication in progress: no
Essential_Customer	Deployed	SysAdmin	M365 - Essential (0)	Edit Delete Undo Deploy	Queued commands: unknown Executing commands: unknown Replication in progress: unknown
Pro_IPPBX_Token_Cust	Deployed	version: 8.0.220.26 replication: 2021.08.23.14.41.58 SysAdmin	M365 - Pro (367)	Edit Delete Undo Deploy Add SBC Site Queue Replication	Queued commands: 5 Executing commands: 0 Replication in progress: no

The UMP interface opens.

Figure D-2: UMP Interface

User Type	Full Name	SIP Address	Line Uri	Template	Department	Online Voice	Online PSTN	Site Location	Usage Locati	EnterpriseVoi...
TeamsOnly	Pure Online 33	sippureonli...			Technical	NL-Almere	eu-lab-sbca...		NL	No
PureOnline	Ump-Activation-User	sipump-acti...							BE	No
PureOnline	Ump-Activation-User	sipump-acti...							BE	No

2. In the Navigation pane, select **O365 Configuration**.
3. In the Office 365 Settings screen, click **Switch to username/password**.
4. Click **Switch to auth token**.

E SQL Server Configuration

This section describes SQL Server configuration actions.

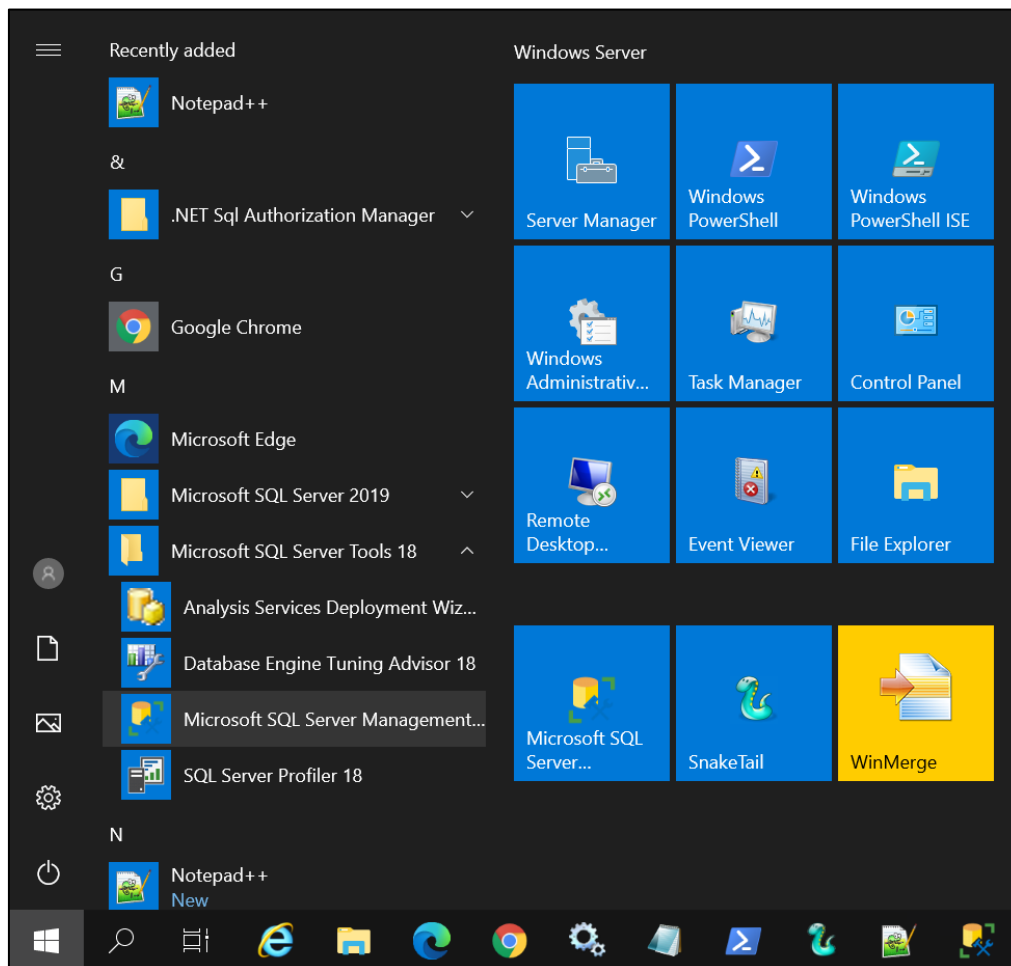
E.1 Setup Microsoft SQL Server for SBC

This section describes how to setup the Microsoft SQL Server for SBC.

To set up the SBC:

1. Run Microsoft SQL Server Management Studio.

Figure E-1: Select SQL Server Management Studio Tool



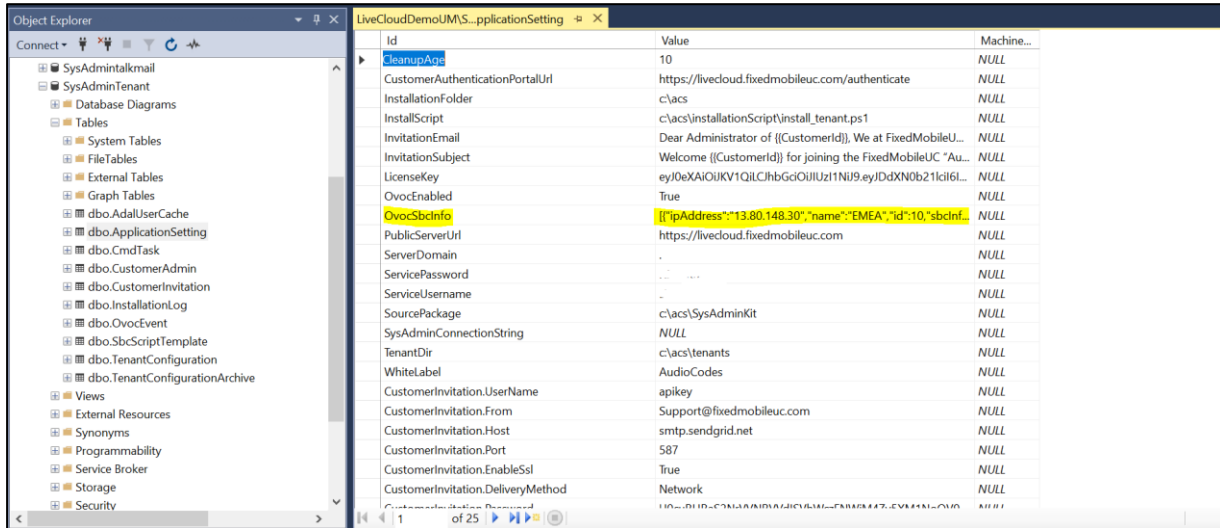
2. Run Microsoft SQL server Management Studio.
3. Expand tables and select SysAdminTenant and dbo.ApplicationSetting, and then select Edit Top 200 Rows.
4. Add or edit the row with ID OvocSbcInfo to include the SBC parameters:
 - ipAddress: "xxx.xxx.xxx.xxx"
 - name: "The SBC Name", this will be the select region name you will select in step 3 - Voice Route Setting. Recommended name City/Region (e.g., "New Jersey, USA")
 - "id":# (SBC ID Number from, e.g., "1")
 - "sbcInfo"
 - ◆ gatewayUser: SBC User Name (default = "Admin")

- ◆ gatewayPassword: SBC User Password (Default = "Admin")

5. Typical String:

```
[{"ipAddress":"x.x.x.x","name":"NewJersey,USA","id":3,"sbcInfo":{"gatewayUser":"Admin","gatewayPassword":"Admin"}}, {"ipAddress":"x.x.x.x","name":"London,UK","id":4,"sbcInfo":{"gatewayUser":"Admin","gatewayPassword":"Admin"}}]
```

Figure E-2: Select SQL Server Management Studio Tool



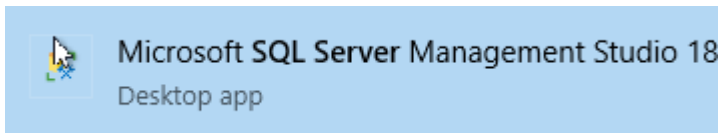
E.2 SQL Server Database Updates



Important: After running wyupdate for build versions prior than build 8.0.100.282, manually run the following SQL scripts from the c:\acs\SQLScript\upgrade folder using SQL Server Management Studio:

- 10.Add-columns.sql
- 20.RefreshSpf.sql

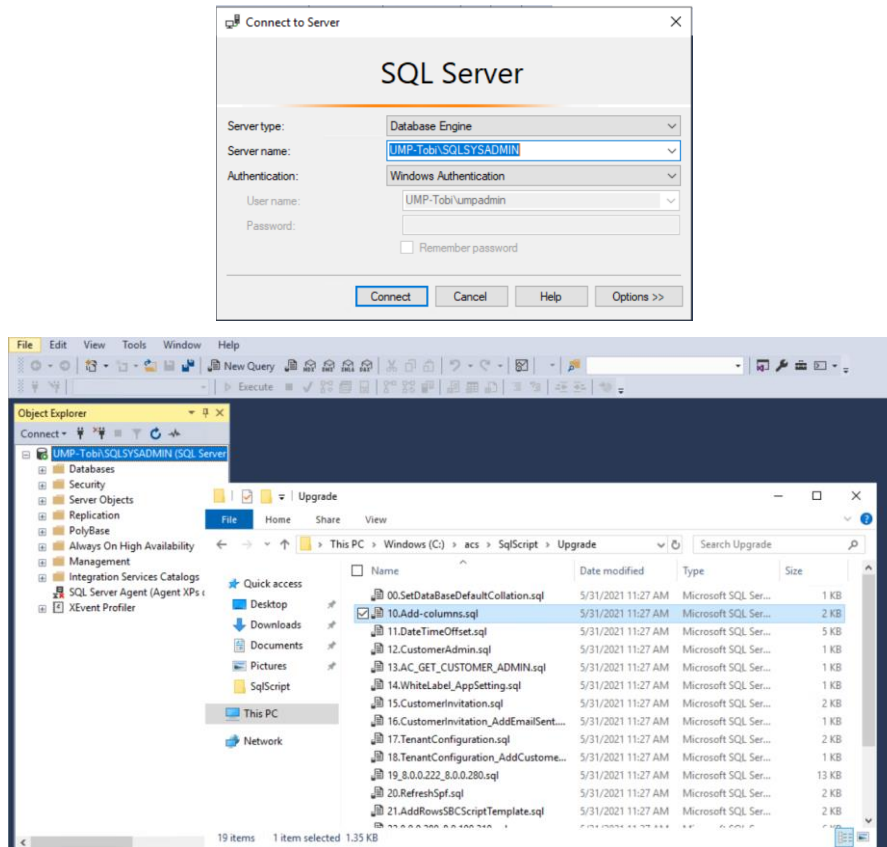
Optional Update SQL scripts (see note above):



Connect to the database

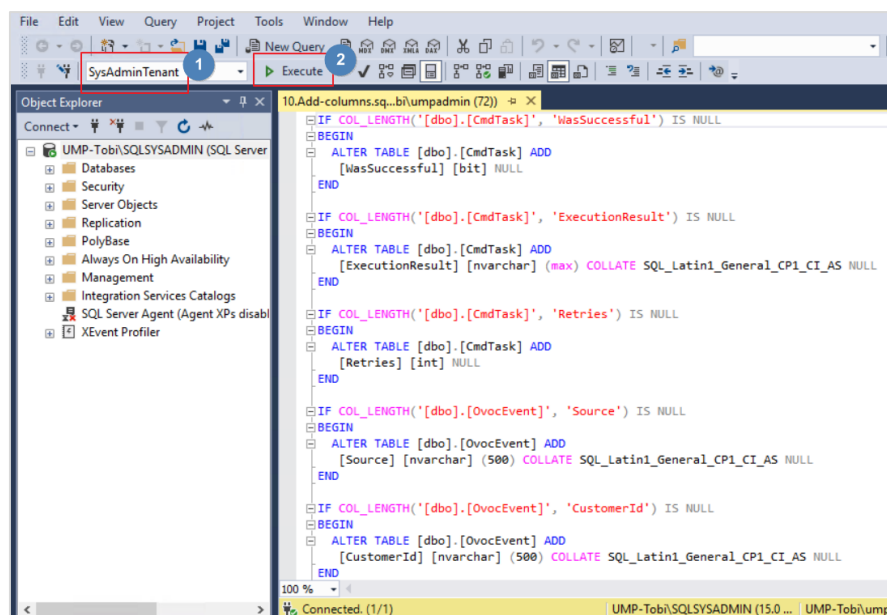
Parameter	Description
Server type	Database Engine
Server name	[servername]\SQLSYSADMIN
Authentication	Windows Authentication

Figure E-3: SQL Server



1. From the Windows Explorer pick “10.Add-columns.sql” and drag and release it into the grey area in the SQL Manager Studio.

Figure E-4: SQL Updates



2. Make sure SysAdminTenant database is selected then press Execute.
3. Repeat the above steps for “20.RefreshSpf.sql”
4. In addition, when UMP-SP is deployed with OVOC, set the ‘OvocEnabled’ parameter to true in the dbo.ApplicationSetting in the SysAdminTenant database.

E.3 Updates for Backend SQL Server

This section describes the changes required to run when customer databases are deployed on an external SQL backend server.



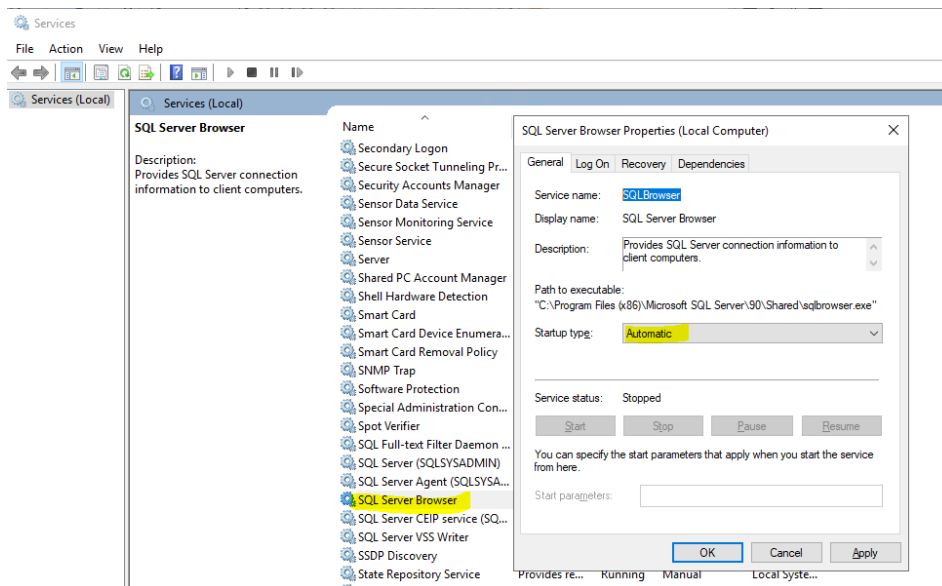
Important:

- Backend SQL server username and password must be equal to the service account used for the installation of the UMP server.
- Create the following directory for database backup for Wyupdates:
c:/acs/dbbackup/

Do the following:

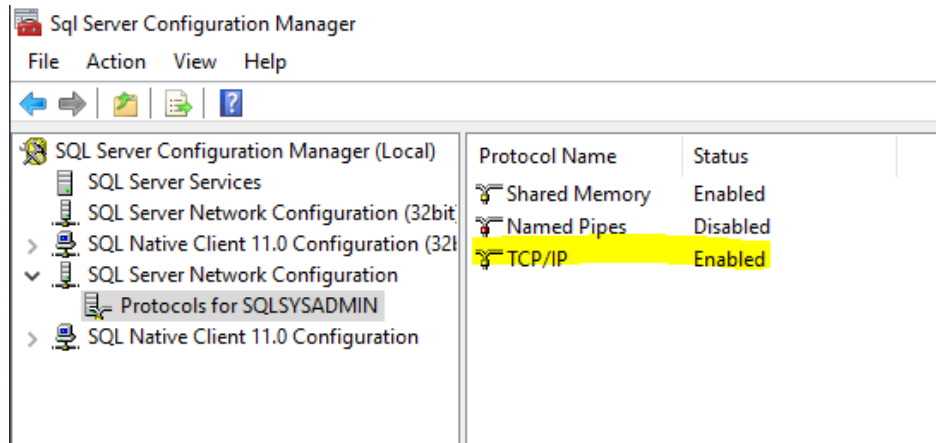
1. Enable Firewall rules to allow connection from remote to the DB (TCP 1433, 4022, 135, 1434, UDP 1434).
2. Enable the SQLBrowser service:

Figure E-5: SQL Browser Service



3. Enable SQL TCP/IP connection.
4. Open the Sql Server Configuration Manager (under Protocols for SQLSYSADMIN) and set TCP/IP to "Enabled".

Figure E-6: SQL Server Configuration Manager



E.4 Configure SQL Server for Enhanced Capacity

The procedure described in this section should be performed if an external SQL server is used in the customer deployment for enhanced capacity requirements (TBD) .



After installing the UMP-LCT, by default , the local SQL server is used when creating new customers.

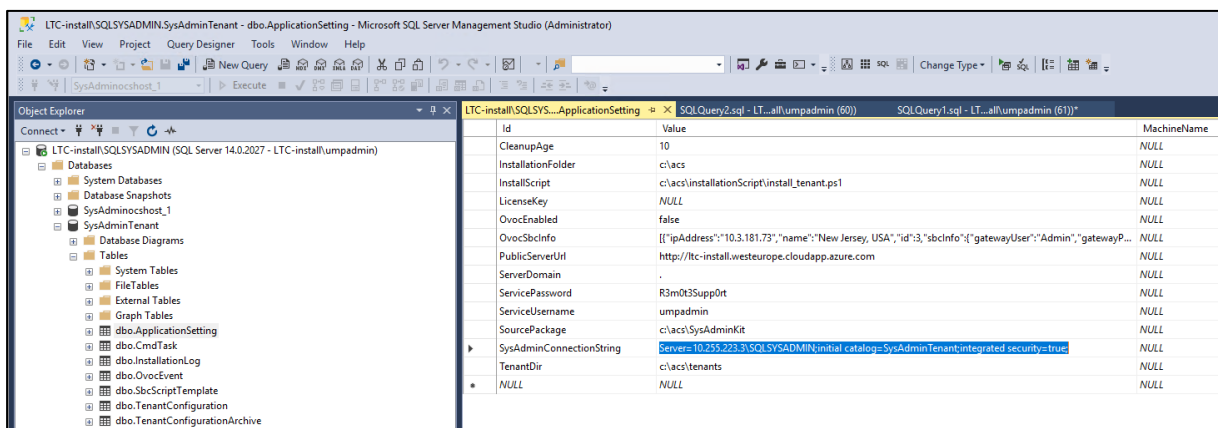
To configure an external SQL server:

1. After installation of the local SQL server, use SQL Server Management Studio to connect to the .\SQLSYSADMIN database engine on the 1st server (where the installation commenced, see) and navigate to the [dbo].[ApplicationSetting] table in the SysAdminTenant database.
2. Modify the SysAdminConnectionString attribute (by right-clicking and selecting “Edit Top 200 Rows”) and set the value to the following:

```
Server=10.255.223.3\SQLSYSADMIN;initial
catalog=SysAdminTenant;integrated security=true;
```

Where 10.255.223.3 is example IP address for the SQL backend server used for the installation of the customer / tenant databases.

Figure E-7: Object Explorer



In this release, there is no automatic configuration of this attribute. Once the attribute is populated with a value, this server is used for the installation of the backend tenant database. Once the SQL backend server reaches its maximum capacity, the value should be

manually changed to point to the next designated external SQL server in the list for future tenant installations.



Windows integrated security is used to communicate to the remote SQL server, so the service account used needs to be either a domain account, or both machines must use the same username and password.

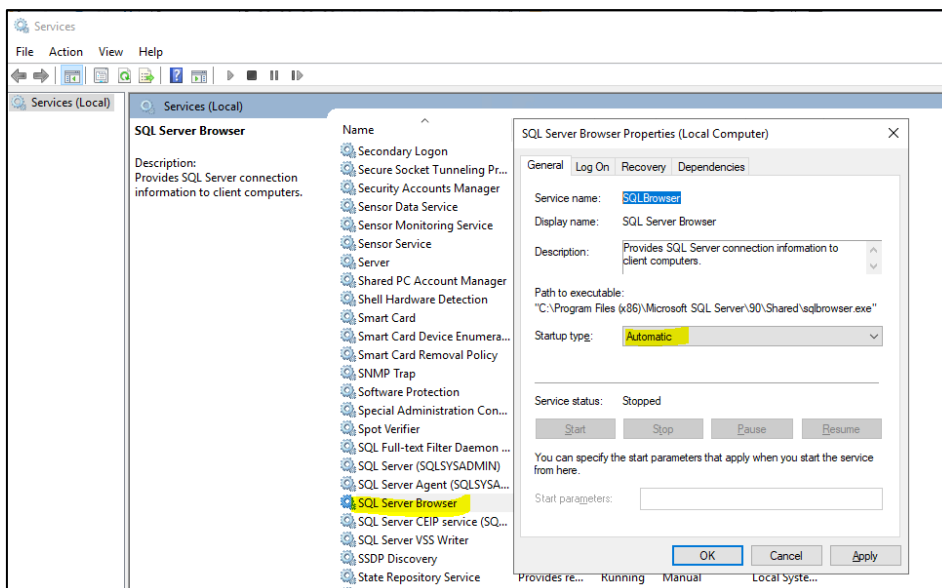
E.5 Run Changes on the External SQL Server

This section describes the changes to run on the external SQL server.

To run changes on external SQL server:

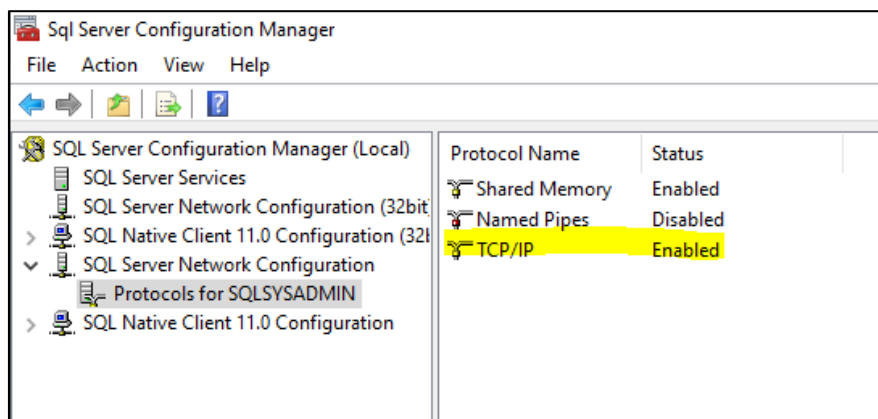
1. Enable Firewall rules to allow connection from remote to the DB (TCP 1433, 4022, 135, 1434, UDP 1434).
2. Enable the SQLBrowser service:

Figure E-8: SQL Browser Service



3. Enable SQL TCP/IP connection.
4. Open the Sql Server Configuration Manager (under Protocols for SQLSYSADMIN) and set TCP/IP to **Enabled**.

Figure E-9: SQL Server Configuration Manager



International Headquarters

1 Hayarden Street,
Airport City
Lod 7019900, Israel
Tel: +972-3-976-4000
Fax: +972-3-976-4040

AudioCodes Inc.

200 Cottontail Lane
Suite A101E
Somerset, NJ 08873
Tel: +1-732-469-0880
Fax: +1-732-469-2298

Contact us: <https://www.audiocodes.com/corporate/offices-worldwide>

Website: <https://www.audiocodes.com>

©2022 AudioCodes Ltd. All rights reserved. AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant, MediaPack, What's Inside Matters, OSN, SmartTAP, User Management Pack, VMAS, VoIPerfect, VoIPerfectHD, Your Gateway To VoIP, 3GX, VocaNom, AudioCodes One Voice, AudioCodes Meeting Insights, AudioCodes Room Experience and CloudBond are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

Document #:LTRT-26359

